"A Cyber Security Dialog"

Keynote Presentation
2018 Annual Conference

Louis J. Giannotti
Deputy for Information Technology/CIO
United States Naval

September 2018

CYBER SECURITY DIALOG

September 2018

Table of Contents

Report

Enclosures (URLs provided for on- line access to reports)

CYBER SECURITY DIALOG

September 2018

1. Genesis, Requirement and Resources.

A. Genesis. Most people who operate small businesses or have home offices of any size, remain concerned about the effectiveness and the integrity of their cyber security solution. They have become increasingly aware of malicious criminal cyber activity, nationally and internationally; by rouge hackers, independent activists as well as nation states. Identifying a simple solution for the average computer user can be a daunting task. Cyber thieves are bold and getting more creative. They are of all ages from young uneducated novices to hardened well educated criminals.

B. Requirement. This document was developed to define and explain the cyber threat issue today, and to offer suggestions for provisioning the appropriate level of cyber security to either a small business or a typical home office.

C. Resources. Enclosures from reputable sources provide the context for this "dialog". They are current (2016 and beyond) and offer an excellent overview of the cyber crime problem. In particular enclosures (1) through (5) illustrate and discuss cyber crime activity and the related costs both nationally and internationally; while enclosures (6) through (10) define different types of malicious software (malware), including the most dangerous financial malware while suggesting the best cyber security practices for home and businesses. URLs are provided for on-line access to reports for enclosures (1) through (5).

2. Facts about Cyber Crime. While the crimes are familiar – fraud, extortion, espionage, theft, etc.; the tools are different. Instead of guns, lock picks, masks, and getaway cars; cyber criminals are unseen, use computers and malicious software tools, travel in the "ether" around the world on Internet highways without physically leaving their computer, and attack individuals, corporations, organizations, and countries at any time with little fear of identification or retaliation. This is crime in the 21st Century. It is costly and destructive. The enclosures are from reputable sources and discuss this subject matter thoroughly. The following are some facts to consider:

A. The FBI is the federal agency for investigating cyber attacks in the United States. It operates an Internet Crime Complaint Center (IC3). In 2017 the FBI IC3 received 305,580 complaints valued at a $1.4 billion of financial loss. The average data breach costs the large enterprise $1.3 million while the cost to a small to medium size company was $177K. The total cybercrime loss worldwide is expected to be in excess of $6 trillion by 2021.

B. Individual victims are targeted by age and location. As an example 50,000 victims over 60 years old lost $335M to cybercrime. Within the United States – California, Texas, and Florida have the most individual cybercrime victims.

C. Cyber Crime also targets specific industries, such as healthcare. The average industry cyber crime cost was $11.7M. This varied significantly by industry. For example cyber crime cost to the Financial Services industry was $18M, while the cyber crime cost to Hospitality industry was $5M.

D. Corporate IT security budgets are now considered an investment and have increased by 23% in 2017. This is no surprise since the annual increase in security breaches is approximately 25%. Recovery takes time and contributes to a significant loss of productivity and therefore a loss in revenue. As an example it takes 50 days to recover from an insider attack while a simple ransomware attack take 23 days to recover.

3. Prevalence of World Wide Cyber Crime Activity. Cyber crime activity is growing at an increasing rate every year with no end in sight. There are many reasons why cyber crime is the problem that it is today. Anyone, at almost any school age, has access to free hacking tools. Most importantly victims of cyber crime can be targeted from anywhere in the world using social media and attacked from anywhere in the world using the Internet.

A. Cyber Crime Rapidly Rising. Cyber crime activity throughout the world has been rising at an unpresented rate, with incidents increasing at approximately 25% per year accompanied by a 30% increase in losses and recovery costs. This includes crimes or theft against individuals, industries, corporations, governments, and many other organizational types. Cyber security methods and tools have been ineffective, consequently, cyber crime has been very successful and very “profitable”.

B. Top Cyber Crime Countries. There are approximately 200 countries in the world today. Of those, 5% account for 60% of the worldwide cyber crime. While no two sources agree on which country is #1 and which country is #10, the sources generally agree that the same countries are always on the lists and they are all the major originators of cyber attacks that are incredibly costly and extremely disruptive. These countries generate, literally, millions of cyber attacks annually. As an example the following is a typical list twenty ranked countries that cause or export the most cyber crime.

1. United States of America	23%	11. India	03%
2. China	09%	12. Russia	02%
3. Germany	06%	13. Canada	02%
4. Britain	05%	14. South Korea	02%
5. Brazil	04%	15. Taiwan	02%
6. Spain	04%	16. Japan	02%
7. Italy	03%	17. Mexico	02%
8. France	03%	18. Argentina	01%
9. Turkey	03%	19. Australia	01%
10. Poland	03%	20. Israel	01%

C. Cyber Crimes against Individuals. In addition to using a variety of malware to cause chaos and disruption within large corporations; cyber crimes, mostly fraud (deception intended to result in personal or financial gain) and extortion (obtaining money through threats) are routinely committed against individuals at alarming rates. The following are the types (defined in

enclosure (3)) of cyber crime committed against individuals in the U.S. most frequently reported to the FBI in 2017:

Non-payment / non delivery	84,079 unique reports by individuals to the FBI
Personal data breach	30,904
Phishing	25,344
Overpayment	23,135
No lead value	20,241
Identity Theft	17,636
Advance Fee	16,368
Employment	16,194
BEC/BAC	15,784
Confidence fraud/romance	15,372

D. Cyber Crimes against Industry. While the five most cyber attacked industries, as reported by Forbes, includes Healthcare, Manufacturing, Financial Services, Government, and Transportation; data breaches are the most troublesome, costly, and most difficult to resolve. Data breaches are increasing significantly each year. Data breaches are cyber crimes committed against organizations that store large amounts of data records. The data below illustrates data breaches from 2014 through mid-2018 against industries.

Industry	2014	2015	2016	2017	2018 (< ½ year's data)
Business	258	312	495	870	309
Medical / Healthcare	333	277	376	374	181
Banking/Credit/ Financial	41	71	51	134	84
Military	92	63	72	74	49
Education	57	58	98	127	45

A single data breach can compromise millions of personal data records. The following are examples of larger data breaches (and when reported) as of March 2018. The cumulative numbers of records stolen related to each incident are in "millions".

Yahoo	Oct 2017	30,000
River City Media	Feb 2017	1,370
Aadhaar	Jan 2018	1,000
Yahoo	Aug 2016	500
MySpace	May 2016	427
Friend Finder Network	Oct 2016	412
US Voter Database	Dec 2015	191
Adobe	Sep 2013	152
eBay	May 2014	145
Eqifax	Sep 2017	143
Heartland	Jan 2009	130
LinkedIn	May 2016	117

4. Understanding the Threat. Think of cyber crime as a disease. It should be taken seriously by everyone. It is a disease that affects our entire society and if ignored can cause chaos and disrupt the life of any individual, organization, or corporation. As with any disease, understand it and treat it. As an example, while everyone includes use of the Internet and social media as part of their everyday lives, both the Internet and social media are not your "friends". They facilitate cyber crime. Ignoring cyber threats will only allow cyber crime activity get worse in the future. In the future it will be fueled by the Internet of Things (IoT), 5th Generation Long Term Evolution (5G LTE) communications and social media where cyber criminals can "surgically" select their next victims. I suggest spending a few moments to watch the following TED Talks:

> TED Talk on Smart Appliances
> 9 minutes - "smart" appliances can talk to you, who else are they talking to?
>
> https://fieldguide.gizmodo.com/your-smart-home-is-spying-on-you-here-s-how-to-spy-bac-1822939698
> How they collected the smart devices transmissions
>
> Big Data sharing
> 21 minutes AI + Data Sharing …Progress??? Only you can decide what's best for you. But, "the world" is pushing ahead!!!

It is a fact that the IoT and 5th Generation Long Term Evolution (5G LTE Advanced) can, and will, generate and share significant data on individuals without their permission. The videos above illustrate data that can be collected unknowingly and widely distributed

A. The Internet as a Threat. The Internet is the single largest communication tool used to conduct business worldwide. Because of this, it is the principal venue for cyber-crime, and therefore, if not treated properly, it can present a significant risk. Consequently, securing and controlling access to and from the Internet are essential first steps when implementing a cyber security solution to mitigate cyber crime risk. Controlling access to the Internet will:

1) Increase cyber security for protection of business assets
2) Optimize available bandwidth which is a costly resource
3) Enhance employee and customer productivity
4) Protect business reputation
5) Reduce legal threats

B. General Types of Internet Related Threats. The three most common threats to a corporate environment, to and from the Internet, include Intrusion, Access to Objectionable Content, and Illegal Activities.

1) Intrusion (outsider threat). There are two types of intrusion. One is mischievous intrusion and the other is malicious intrusion. While both are disruptive and can cause harm, malicious intrusion can be costly and result in irreparable damage.

2) Access to Objectionable Content (insider threat). This includes pornographic material, gambling sites, sites advocating violence, and politically sensitive or subversive site. Persistent access to these types of sites will cause significant damage to personnel and corporate reputations. The outcomes from accessing these sites may also identify your corporation as a potential target for malicious activity.

3) Illegal Activities (outsider threat). Illegal activities include pirating, hacking, and theft of valuable corporate property including sensitive data and financial resources.

C. Assessing the Threat.

1) Method and Process. A broad based cyber search can be conducted by anyone (e.g. potential hacker) to learn about any small business including the business' community of interest (COI) within which the business operates. This might include the corporate mission, any potential controversy that the business activity might generate, information relative to the business's senior leadership; and data suggesting business or personal worth or value.

Lowest common denominator technology can be used such as a Comcast home Internet Service Provider (ISP) and a widely used Internet search engines such as Internet Explorer or Google. The ease or difficulty for a novice hacker or a seasoned cyber thief to research any business or any individual would help determine how susceptible or vulnerable the business or the individual may be. In particular the following was explored: 1) publically available on-line information; 2) valid concerns; 3) prevalence of worldwide cyber crime activity; 4) cyber crime statistics; and 5) a typical community of interest.

2) Publically Available On-Line Information. Today small businesses (and individuals) are targets because of significant business activity and financial data, publicly available from Internet web sites. Web-sites provide names, addresses, salaries, corporate worth, associations, political affiliation, and purpose. No credentials are necessary to gain access to most small businesses or individuals. Information and "opinions" will illustrate appealing targets.

3) Principal Concerns. Principal concerns are fraud, theft, denial of service, and espionage. For intrusion protection against these concerns, identifying the expected cyber crime method or malware used, such as those listed below, is necessary:

a) Fraud
b) Theft
c) Denial of service attack
d) Espionage – all types
e) Social Engineering, Phishing
f) Key-logger
g) Spam, virus
h) Spyware, Worm, Rootkit, Backdoor

Understanding how other corporations were penetrated will also provide insight into cyber security requirements. Enclosures (1) through (4) provide a "snap shot" of cyber crime and illustrate that cyber attacks from organized crime, foreign nation-states, corporate insiders,

individual novice hackers, and political activists continue to increase at an alarming rate, are destructive, and are costly.

4) Cyber Criminals. Experts and novices are equally dangerous. They use technology to install malicious software, known as malware, on targeted computer systems. The expert cyber criminals have the knowledge and experience to hack using sophisticated tools; phishing techniques, and other methods of social engineering; to acquire strictly controlled information and data required to access computer systems on the corporate network or within the entire Community of Interest (COI). This could allow cyber crime activity such as control of the network, exfiltration of sensitive classified corporate information, access to corporate or personal financial data, and general data theft.

The novice is equally effective and can easily acquire the tools to cause the same disruption and damage. While phishing and social engineering do not require sophisticated technology; they do require creativity and excellent persuasive communication skills. Hacking tools can be downloaded for free from various web-sites. As one example (of many), the web site http://www.gohacking.com offers download executable code, and easily understood explanations on such subject matter as

a) How to hack a Facebook
b) How to become a hacker
c) How to spy on a cell phone
d) How to hack an email password
e) How to spy on WhatsApp messages
f) DNS Hijacking
g) Hacking FAQa
h) 10 Security Internet Security Tips

For an illustration of simplicity and ease of hacking, see the "key logger" section of enclosure (6). This is a Key logger USB device, either wired or wireless, that can be purchased inexpensively and used by any novice to capture access data, logins, and passwords from any network. It doesn't get much simpler than this.

5) Malware Defined. Hackers use different types of malware. You should understand what malware is, how it can infect a computer "system" or "network", and the damage it can cause. As a minimum reviewing the following web sites is suggested:

a) http://www.malwaretruth.com/the-list-of-malware-types/

b) http://www.howtogeek.com/174985/not-all-viruses-are-viruses-10-malware-terms-explained

c) https://heimdalsecurity.com/blog/top-financial-malware/

Each category of malware is like a carpenter's tool and performs a particular function. Enclosure (6) defines the common malware categories listed below:

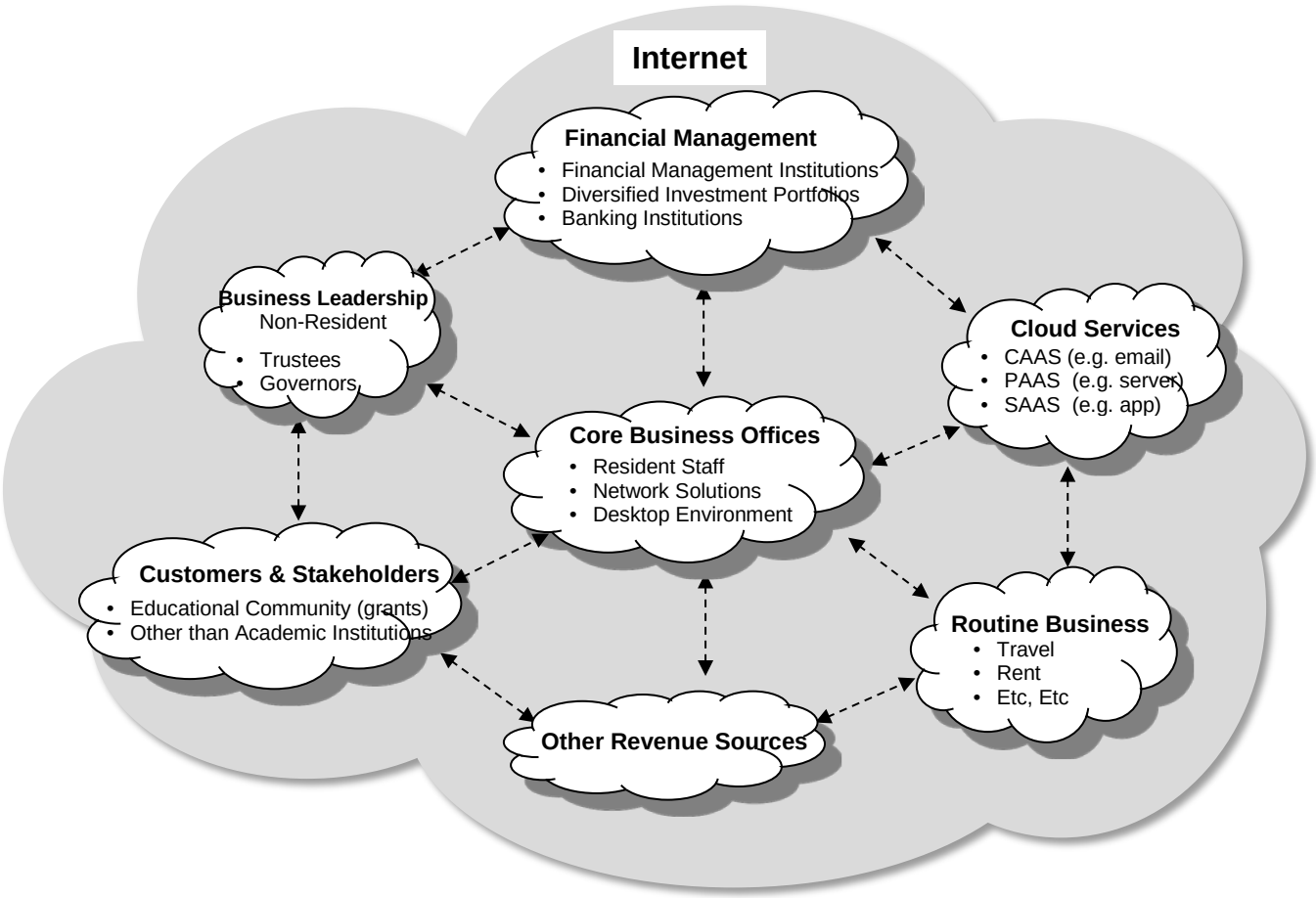
a) Adware
b) Spyware
c) Virus
d) Worm
e) Trojan Horse
f) Rootkit
g) Backdoor
h) Key logger
i) Rogue Security Software
j) Ransomware
k) Browser Hijacker

Financial malware is especially dangerous. It is used to fraudulently access financial and bank accounts. It is worth special attention. The most dangerous financial malware includes:

a) Zeus
b) Zeus Gameover
c) SpyEye
d) IceIX
e) Citadel
f) Carberp
g) Bugat
h) Shylock
i) Torpig
j) CryptoLocker

Most are Trojan Malware. You should understand how this malware can get onto your computer systems, and the damage it can do. Enclosure (6) explains this most dangerous financial malware listed above.

D. Community of Interest (COI). A COI consists of people or businesses who engage each other to pursue or support a particular activity or business, as illustrated below:



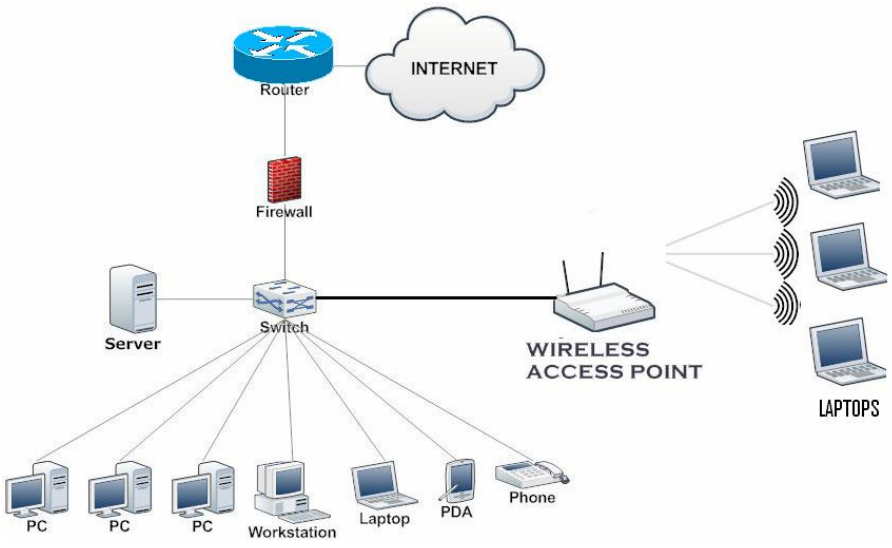
Operating within this environment can be simple, effective, and secure when the entire COI is secure. Left with inadequate security, the entire community is a rich target for fraud, theft, and other malicious cyber activity. Any community illustrated can infect the core business offices. It is necessary that you understand what cyber security technology and operational behavior protects you use when communicating and conducting business among your partners and within your community. Cyber crime activity can begin from anywhere on the Internet, especially within your COI.

5. Short Term – Immediate Action - Securing the Business Office Environment

A. Local Area Network. Begin with your office's local area network. Typically a simple office network as illustrated below will support staff computers, one or more printers, servers, switches or hubs, routers, modems, and firewalls providing connectivity within the office as well as onto the Internet. Consider the following:

1) Carefully select the ISP (consider security provided, performance, and cost)
2) Consider using the ISP email solution
3) Decide on wired or wireless network – or a combination of both
4) If using wireless - install wireless controller
5) Install registration appliance

The switch, firewall, and router can control access to and from the Internet. They can deny access to undesirable or objectionable web sites by name or by category. They can limit access to sensitive data stored on a local server or at another location within the COI. They can also block spam and control access to the core business office's local area network from the Internet. Finally, adding a security appliance can provide additional protection. Security appliances provide intrusion detection (IDS) and/or intrusion protection (IPS). Enterprise sized examples of control appliances and protection appliances include Websense (web filtering) and Tipping Point (intrusion protection).



LAN designs are like personalities – they are endless. A typical office LAN is as illustrated above. For simplicity, other peripherals and security appliances are intentionally missing from this diagram.

B. Office Computer Systems. Next consider the networked staff computers and other peripheral devices connected to the local area network. Include general office software, business specific applications, and stored data. The following actions are suggested for desktop computer systems:

1)	Administrative Rights	Remove admin rights on all desktop computers
2)	Operating System (OS)	Install latest supportable OS with the latest update
3)	Desktop Clients	Identify standard allowable clients
4)	Browser	Install multiple browsers (i.e. IE and Chrome)
5)	Login and Passwords	Implement complexity and periodicity requirements
6)	Office Software	Install updated office suite w/encryption capability
7)	Anti-Virus System	Install anti-virus system: McAfee/Malware Bytes
8)	Data Storage	Encrypt on-board hard drive - data-at-rest
9)	Backup	Encrypt external hard drive (SS if possible)
10)	Business Documents	Encrypt business documents
11)	USB Thumb Drives	Test all thumb drives prior to <u>any</u> use
12)	Autorun	Disable autorun – prevents .exe files from running

C. Electronic Mail (email). Email is the glue that connects users on the Internet. It is the primary means of communicating and consequently email is a principal vehicle for delivering malware to office networks. The following is suggested for email:

1) Implement a SPAM filter for incoming email
2) Do not open an email from an unknown source
3) Do not open an email with .exe or .pdf attachment
4) Implement encryption requirements for sensitive business specific outgoing email
5) Implement digital signature requirements for non-repudiation

D. Staff Operational Behavior. Operational behavior includes the habits and methods of using information technology to conduct business. This eventually would extend to COI organizations, institutions, people, and businesses. Acceptable operational behavior begins with a simple, effective, easily understood training program. Examples of staff training topics would include the following:

1) Managing email
2) Logins and Passwords Requirements
3) Protecting Personal Identifiable Information (PII)
4) Universal Serial Bus (USB) Device Issues
5) Data in Motion (DIM) Requirements
6) Data-at-Rest (DAR) Storage Requirements
7) Personal Electronic Devices (PED)

8) Encryption Methods and Requirements
9) Social Engineering and Phishing (types and methods)
10) Malware (identification and treatment)
11) Hacking Methods
12) Home Computing and Mobile Smart Device Computing

E. Business Policy. Eventually, establishing minimum corporate policy is a good idea. This can be a part of the staff training. Simple common sense requirements such as a prohibition against surfing Internet web sites while at work and a prohibition against conducting personal business while at work. Both of these can prevent hackers from infecting your LAN with malware. A corporate policy for receiving information or data from a business partner may also be warranted.

6. Long Term Approach.

A. Phased Process. Below is a long term process for provisioning information technology to a corporate staff. This starts from "scratch" with a clean sheet of paper. This is a good idea since your cyber security solution can be an integral, effective and efficient part of the solution, rather than an after-thought. Enclosures (7) and (8) discuss best cyber security practices for business and how to reduce cyber crime.

1) IT Service Provider
   a) Conduct basic analytics to determine best approach to the IT staffing issue
      – Determine who will do the planning and who will do the work
   b) Consider the following alternatives:
      – Organic staff –responsible for provisioning IT/ security solution
      – Outsourced service provider –responsible for provisioning IT/security solution
      – Single Director of Services/CIO - Plan and lead/manage a contracted service

2) Discovery Phase – Assessment
   a) Define the core location of conducting your business or corporate offices.
   b) Conduct a site survey/inventory of the information technology currently in use in the locations defined above. An example of what you might find includes
      – Local area network (LAN)
      – Internet access provider (ISP)
      – ISP equipment
      – Security Appliances
      – LAN associated peripheral hardware such as switches, hubs, routers, modems, and WAPS
      – Desktop computers or notebooks (include configuration and LCM data)
      – Multi-functional printer/fax devices (networked or standalone)
      – Servers and storage devices
      – Projectors and/or big screens
      – Operating systems and application software for all systems
      – Smart devices

- Security technology currently in use: firewalls, anti-virus sys, appliances, etc
- Staff training periodically conducted.
- Corporate computing policy or standards

3) Stabilization Phase – Stabilize and secure current (corporate and COI) environment
   a) Define the most probable threat based on literature review
   b) Apply the 'right' level of security to existing IT suite
   c) Develop and implement cybersecurity policy
   d) Determine COI methods to communicate and collaborate with corporate offices
   e) Identify security COI security use and practices

4) Planning Phase
   a) Develop a complete IT and cybersecurity plan on a clean sheet of paper
   b) Define the basic IT functional computing requirements
   c) Select the desired business technology hardware/software products
   d) Define the cyber security functional requirements based on the threat level.
   e) Select the cyber security products, procedures, or policy
   f) Conduct a thorough threat assessment
   g) Define the minimum security requirements for COI to conduct business with you.

5) Migration Phase
   a) Execute the Plan from the 'Planning Phase'
   b) Use as much of the current on-board technology investment as possible
   c) Execute staff training
   d) Implement security based policy requirements
   e) Develop a 'complete' life-cycle-maintenance (LCM) plan

6) Documentation
   a) Develop a technology strategic plan
   b) Develop a technology business plan
   c) Develop a life-cycle-management plan

7) Culture of Understanding. Through leadership, instill a culture of security understanding and constant vigilance among the business office staff. Require annual staff security training developed by your IT service provider. Develop a staff security and policy manual. This manual should be required reading.

B. Proactive Defensive Posture. Every long term information technology plan should implement a proactive defensive security posture to mitigate both known and unknown computing vulnerabilities. Some examples of a strong defensive security posture include: practicing continuous migration of technology; using appliance technology; using embedded operating systems; and securing every level of the Open System Interconnect (OSI) model; embedded operating systems and the OSI model are discussed further.

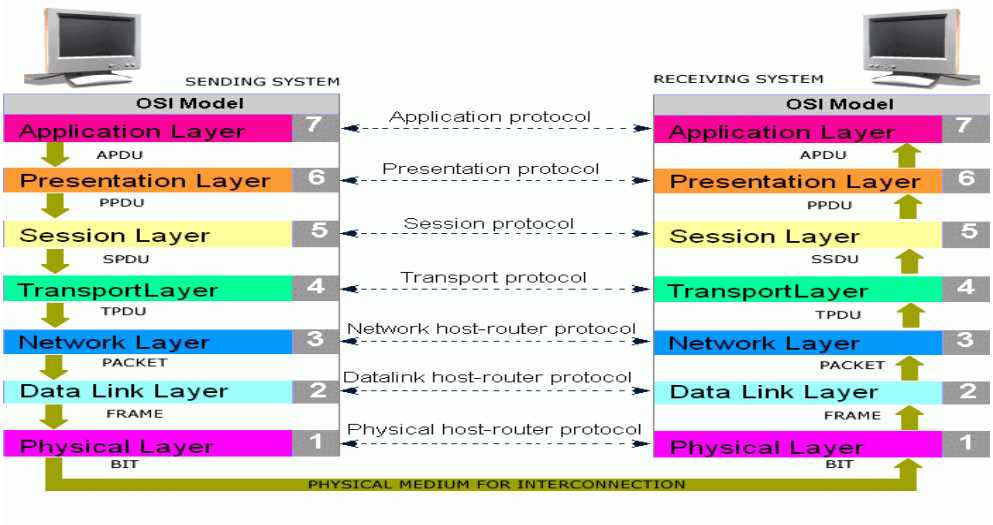
1) Embedded Operating Systems. When selecting computers, consider the computer's operating system. This includes desktop staff computers as well as special purpose servers. Computer systems with general use operating systems are more susceptible to hacking. An excellent example of a general use operating system is Microsoft Windows operating systems (i.e. Windows XP, Windows 7, Windows 8, and Windows 10). Computers with embedded operating systems are less susceptible to hacking. While totally embedded operating systems may not be a feasible office solution, good alternatives include operating systems such as MAC OS, UNIX, and LINUX. They are more difficult to hack. Consider the following illustration

Operating System Spectrum

Easy to hack		More difficult to hack		Impossible to hack
General Use Op System Multiple Functionalities Very Programmable - Many Instruction Sets Simple, Easy to Access, Intuitive				Single Function Embedded OS No Instruction Sets Requires User Manual
MS Win NT MS Win 2000 MS Win XP MS Win Vista MS Win 7	MAC OS	UNIX Unix Variants IRIX LINUX	MiraPoint Tipping Point Bradford WebSense Security Gateway	Cruise Control Micro Wave GPS

Provide user interface through choice of software clients, protocols, and/or overlays

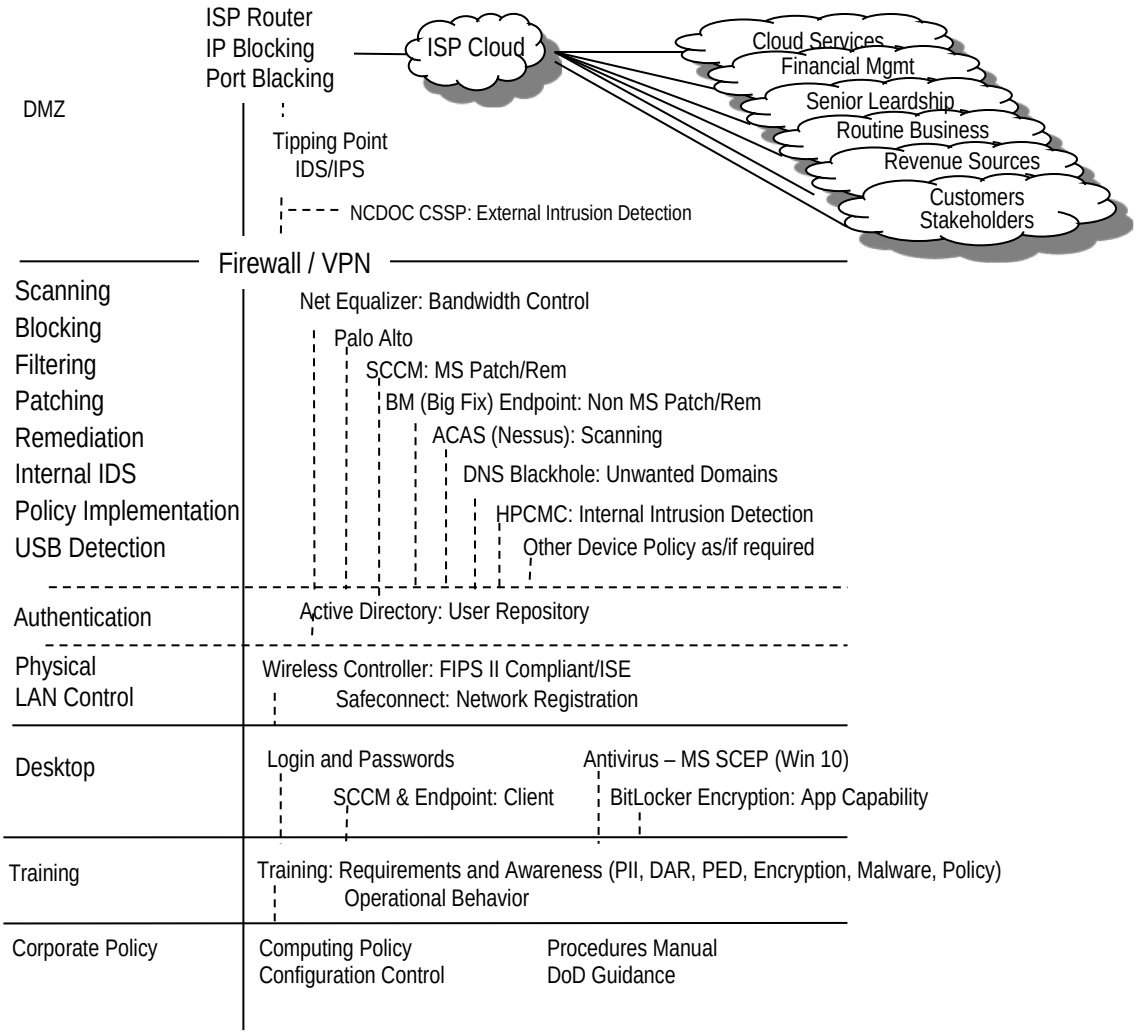
2) OSI Model. The OSI model represents seven layers of technology through which data travels when one user communicates or sends data from his/her desktop to another user's desktop. This includes malware or virus data. If a 'system' is infected, malware can 'hide', within these layers to control networks, access computer systems, and execute exfiltration of sensitive corporate information including PII and financial access data, corrupt business documents, and



participate in a variety of other destructive nefarious activity. Use appliances or systems to secure and protect every layer of the OSI model.

3) The Complete Cyber Security Infrastructure. The infrastructure illustrated below addresses is a complete security system that will secure every level of the OSI model and provide an excellent defensive security posture to your office environment, regardless of the desktop operating system selected. This commonly referred to as a "security stack".

Cyber Security Infrastructure



4) Policies and Plans. This can be considered the frosting-on-the-cake. It is principally documentation and consists of policies and plans for ensuring the maximum level of cyber-security is available to your corporate offices. From a risk management perspective, this may not be considered feasible to develop and implement. However, it is suggested that your corporate or business senior leadership dedicate time to a discussion of the following:

a) Acceptable Use Policy and Common User Agreement
b) Computer Naming Policy
c) Configuration Control Board (Management Plan and Charter)
d) Continuity of Operations Plan
e) Disaster Recovery Plan
f) Incident Response Plan
g) Information Assurance Strategy
h) Mobile Device Policy
i) Password Guidance for Operating Systems and Networks
j) Removable hard drives and mobile systems
k) Risk Analysis Process for Procurement of IA services or Applications
l) Vulnerability Management Plan
m) Desktop and Servers Configuration and Upgrade Guidance
n) Digital Signature Policy
o) Cyber Security Work Force Plan
p) Approved Mobile Devices – Smart Devices – Protection and Registration
q) Home Computing – use of VPN for access to corporate offices

7. The Home Office.

Configuring a home office for security is as important as configuring a corporate or business office. It is anticipated that home offices will be major targets for cyber crime for the future. It has been my observation that providing adequate security to home offices is usually minimized or completely ignored. Many times home computers are not configured for security; anti-virus software, operating systems, and applications are not updated or patched. Wireless routers are usually installed without strengthening the manufacturer provided passwords. Finally, at home, operational behavior is at best poor. Transacting with credit unions or banks, accessing business or corporate offices, or socially communicating with email or other social media from an unprotected home office presents an undesirable risk.

The following is suggested:

A. Operating System. Use a up-to-date operating system that is continues to be supported by the manufacturer. As an example, for a personal computer with a Microsoft operating system, use Windows 10. If you have a choice between a 32 bit or 64 bit system, chose the 64 bit system.

B. Security Suite. Install adequate security applications. There is a wide range of choices. A simple google search will provide lists of available products for different computing venues. Antivirus software (and beyond) examples include:
:

1) BitDefender
2) McAfee
3) Kaspersky

4) BullGuard
5) Norton
6) Trend
7) Vipre
8) Ad-Ware
9) Pareto
10) eseT
11) Panda
12) Avira
13) eScan
14) Zone Alarm
15) eData

Obviously, the list is long and selecting the right product can be difficult. Therefore, for PC users I suggest Malwarebytes and Microsoft's Computer Essentials as a minimum. They are excellent and if kept up-to-date will provide excellent security.

C. Administrator and User Accounts. For you home PC establish an administrator account with a strong password and a user account. When conducting routine business, surfing the web, communicating on email, etc. use the "User Account". When installing devices (e.g. printers) or changing system configuration use the Administrator account. Do not use the Administrator account for routine business.

D. Web Browser. Select a web browser with sand-boxing capabilities, that is difficult to infect or hi-jack such as Chrome. I understand that some applications require the use of Internet Explorer, therefore install it and use only when necessary.

E. PDF Reader. Use a PDF reader that also has sandboxing capabilities to prevent malware intrusion. While Adobe is my choice, there are others. Since PDF documents are the source of malware, keeping your PDF reader up-to-date- is critical.

F. Application Software. Keep application software up-to-date. Hackers exploit vulnerabilities discovered in software applications to infect computers with malware. If using MS Office products, updating is quick, easy, and automatic.

G. Encryption. Full disk encryption is the best method of protection. There are various products to do this. BitLocker is available for MS operating systems such as Windows 7 or beyond. As a minimum encrypt software products that are created from word processors, or spread sheets, etc. This capability is provided by the application.

H. Passwords. As a minimum use different passwords for social computing (e.g. email), business or financial computing (e.g. bank accounts), and professional computing (e.g. work place accounts). The passwords should be complex and changed often. Don't get lazy!

I. Home Network Security. Securing a home network is an important as securing your computer and adopting good operational behavior when using your technology. Areas of concern for home networks include:

1) Using WiFi Protected Access (WPA2)
2) Disabling iPv6 Tunneling
3) Implement a Firewall capability
4) Consider using an alternate DNS capability – consider openDNS

Enclosure (8), *Best Practices for Keeping Your Home Network Safe* and enclosure (9), *Small Office/Home Office Security,* for more recommendations.

8. Conclusion. A healthy respect for the threat, the ease with which a novice hacker can steal, and a broad high level understanding of a typical information technology office environment is worth the investment in time. It will provide you with knowledge and information to make excellent decisions that will mitigate the cyber security risk at an acceptable cost with good ROI. In the long run it will pay for itself.

Enclosure (1)

Heritage Foundation Issue Brief

Cyber Attacks on U.S. Companies

Heritage Foundation
Issue Brief

Cyber Attacks on U.S. Companies in 2016

https://www.heritage.org/defense/report/cyber-attacks-us-companies-2016

Riley Walters
Riley Walters is policy analyst, Asia Economy and Technology in The Heritage Foundation's Asian Studies Center.

This *Issue Brief* is a continuation of a series of papers on cyber-attacks against U.S. companies since 2014[1] and 2015.[2] While the means of cyber-attacks vary, the pattern of targets has been relatively consistent. Large databases, as well as point-of-sale systems, continue to be targeted for financial gain. Hackers with possible ties to nation-states continue to target infrastructure as well as systems for political insight.
Because reporting companies may not realize their systems have been compromised until long after the attack began, the list below is organized by date of when attacks or breaches were publicly announced, rather than when they might have occurred.

December 2015

- **Bowman Dam (infrastructure).** Iranian hackers reportedly gained control of this New York dam's sluice system in 2013, although the controls were manually disconnected at the time of the cyber breach.[3] In March 2016, the Department of Justice (DOJ) indicted one of the hackers employed at an Iran-based computer company with possible ties to the Islamic Revolutionary Guard Corps.[4]

- **Hyatt Hotels Corporation (hotel).** The hotel chain owner announced that it had identified malware on payment processing systems used at a number of locations.[5] Weeks of investigation revealed that malware had affected the systems at 250 locations between August and December 2015.[6] The malware collected payment information specific to credit card information.[7]

- **MacKeeper (technology).** Security researcher Chris Vickery discovered in Shodan (a specialized search engine and online database) the usernames, passwords, and other information for 13 million users of MacKeeper, a performance optimizing software for Apple computers.[8]

- **A Whole Lot of Nothing LLC (spam e-mail company).** The DOJ arrested three men linked to a hacking and scamming scheme that originated as early as 2011. The group targeted the personal information of almost 60 million people—often contained in targeted corporate databases—to be used in spam campaigns. Their operations ultimately generated $2 million in illegal profits.[9]

- **Voter records.** Vickery found the information of 191 million registered U.S. voters in a public-facing database.[10] While there were only 142 million register voters in 2014,

information in the database goes as far back as 2000—meaning it could still contain the information of deceased registered voters. There also may be instances of duplication from combining multiple databases. As of yet, no one has come forward as the owner of the database.

- **Alliance Health (online health portal).** The online portal that facilitates support and information communities across health providers may have exposed personal health information of its 1.5 million users. The exposure likely came from a misconfiguration with its MongoDB database installation.[11] Forty thousand individuals were eventually informed their information had been exposed for 30 months.[12]

January 2016

- **Voter records.** Vickery discovered another public-facing database, storing upwards of 56 million voters' information.[13]

- **The Wendy's Company (restaurant).** Wendy's first reported it would be investigating a possible breach that compromised customer payment information at its franchise stores. By June, investigators determined that at least 1,025 Wendy's locations had been affected, beginning as early as fall 2015.[14]

February 2016

- **U.S. Department of Homeland Security, Federal Bureau of Investigation (government).** A hacker with the Twitter handle @DotGovs released online the names and contact information of 29,000 Department of Homeland Security and FBI employees.[15]

March 2016

- **Verizon Enterprise Solutions (network management).** One-and-a-half million Verizon Enterprise customers' contact information was possibly compromised by a security vulnerability. A prominent hacker offered access to the online database for $100,000.[16]

May 2016

- **LinkedIn (online social networking).** Updating the impact of a 2012 breach that saw the exposure of 6.5 million users' passwords, the company confirmed that the true number is now likely closer to 167 million users, 117 million of whom had both their e-mails and passwords exposed.[17]

- **Myspace (online social media).** The same hacker who advertised the compromised LinkedIn database online claim to have a database of Myspace users' credentials—427 million passwords and 360 million e-mail addresses.[18]

- **Noodle & Company (restaurant chain).** The food chain first began investigating its networks after unusual activity was noticed by its credit card processor. Malware led to customers' credit and debit card information being compromised at a number of its locations between January and June.[19]

June 2016

- **Democratic National Committee (political organization).** The political organization's networks were illegally accessed by two separate cyber groups with possible affiliation to the Russian government's Russia Main Intelligence Directorate (GRU) and Federal Security Service (FSB).[20]

- **Voter information.** Chris Vickery found another online database holding 154 million U.S. voters' information and discovered that an IP address based out of Serbia had been interacting with the database as early as April 2016.[21]

- **CiCi's Pizza (restaurant chain).** News of this point-of-sale breach affecting customers' payment information first broke on KrebsOnSecurity. CiCi's Pizza eventually acknowledged the breach and that the compromise to its systems began as early as March 2016.[22] CiCi's Pizza has 135 locations.

July 2016

- **Citibank (banking).** Ninety percent of Citibank's networks across North America were taken offline after an employee in charge of the bank's IT systems, following a poor performance review, sent malicious code to 10 core Citibank Global Control Center routers, shutting down nine of them. He has since been sentenced to 21 months in federal prison and fined $77,200.[23]

August 2016

- **Dropbox (online).** The number of account credentials exposed in a 2012 breach was increased to 68 million users.[24] Hackers were reportedly able to access accounts utilizing a Dropbox employee's password and credentials, possibly taken from the 2012 LinkedIn breach.[25]Yevgeniy Nikulin was indicted on October 20, 2016, for his involvement with both the Dropbox and LinkedIn breaches.[26]

- **Banner Health (health care).** Almost four million patients, physicians, and customers were affected. The breach was first noticed on July 7, 2016, affecting payment card information. A subsequent breach led to the unauthorized access of patients' personal identifiable information, such as birthdates, claims information, and possibly social security numbers.[27]

- **Oracle MICROS (payment).** Operator of 330,000 cash registers globally, this point-of-sale service was reportedly infected by malware.[28] The exploit has a possible connection to the Carbanak gang, an Eastern European hacker group linked to stealing $1 billion from up to 100 banks worldwide,[29] and may also have ties to a Russian security firm.[30]

September 2016

- **Yahoo Inc. (online).** The online company reported that more than 500 million of its users' names, e-mail addresses, birthdates, phone numbers, and passwords were compromised in a 2014—possibly state-sponsored—breach. Yahoo began investigating

the breach after 280 million users' information was being offered for sale on the dark web.[31]

- **SS&C Technology (technology).** Tillage Commodities Fund, one of SS&C's clients, was scammed for $5.9 million by reported Chinese hackers. The hackers sent SS&C staff scam e-mails ordering wire transfers of Tillage's money.[32]

October 2016

- **Dyn (online).** The domain name service server was taken offline a number of times, attributed to widespread denial of service attacks. Internet-facing devices were used in this attack after being formed into a botnet through malware. The outage affected how users could access popular sites such as Twitter, Netflix, and *The New York Times*.[33]

- **U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC) (government).** In November 2015, a former employee at the OCC downloaded swaths of information onto two portable storage devices before his retirement, leading to the unauthorized removal of more than 10,000 unclassified records.[34]

November 2016

- **Friend Finder Networks (online).** The company behind adult online websites such as Adultfriendfinder.com reported that the accounts of 412 million users were exposed online.[35]The online servers were reportedly breached by hackers in October.[36] No credit card information was exposed, but usernames, e-mails, passwords, and date-of-last-visit became available.

Conclusion

This list of successful and notable cyber incidents hardly scratches the surface of the number of smaller attacks or breaches that occur on a daily basis. With this in mind, Congress and the Administration should continue to encourage the sharing of threat information. Either through formal methods with the government and information-sharing centers or through informal communication, threat information sharing can help mitigate the spread of malicious software. The U.S. should continue to improve and encourage the use of existing avenues of information sharing such as those created by the Cybersecurity Act of 2015.[37]

Serious discussions need to take place on how to empower the private sector to engage in more active defense of its networks. The U.S. should create a defined system of active cyber defense that enables private companies to do more to defend their networks. This system should not allow unrestricted "hack back," but should permit firms to use more assertive cyber tools that improve investigatory and attribution capabilities. Despite the potential threats that malicious actors may pose to U.S. online databases and network systems, the Internet and electronic devices continue to drive the economies of the world. The U.S. needs to take cybersecurity seriously while at the same time allowing innovation to continue to thrive.

Appendix: Additional Resources on Cybersecurity and Cyber Incidents

Steven Bucci, Paul Rosenzweig, and David Inserra, "A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2785, April 1,

2013, http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace.

David Inserra and Paul Rosenzweig, "Continuing Federal Cyber Breaches Warn Against Cybersecurity Regulation," Heritage Foundation *Issue Brief* No. 4288, October 27, 2014, http://www.heritage.org/research/reports/2014/10/continuing-federal-cyber-breaches-warn-against-cybersecurity-regulation.

Riley Walters, "Continued Federal Cyber Breaches in 2015," Heritage Foundation *Issue Brief* No. 4488, November 19, 2015, http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015.

Riley Walters, "Cyber Attacks on U.S. Companies in 2014," Heritage Foundation *Issue Brief* No. 4289, October 27, 2014, http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014.

Riley Walters, "Cyber Attacks on U.S. Companies Since November 2014," Heritage Foundation *Issue Brief* No. 4487, November 18, 2015, http://www.heritage.org/research/reports/2015/11/cyber-attacks-on-us-companies-since-november-2014.

Enclosure (2)

Price Waterhouse Coopers

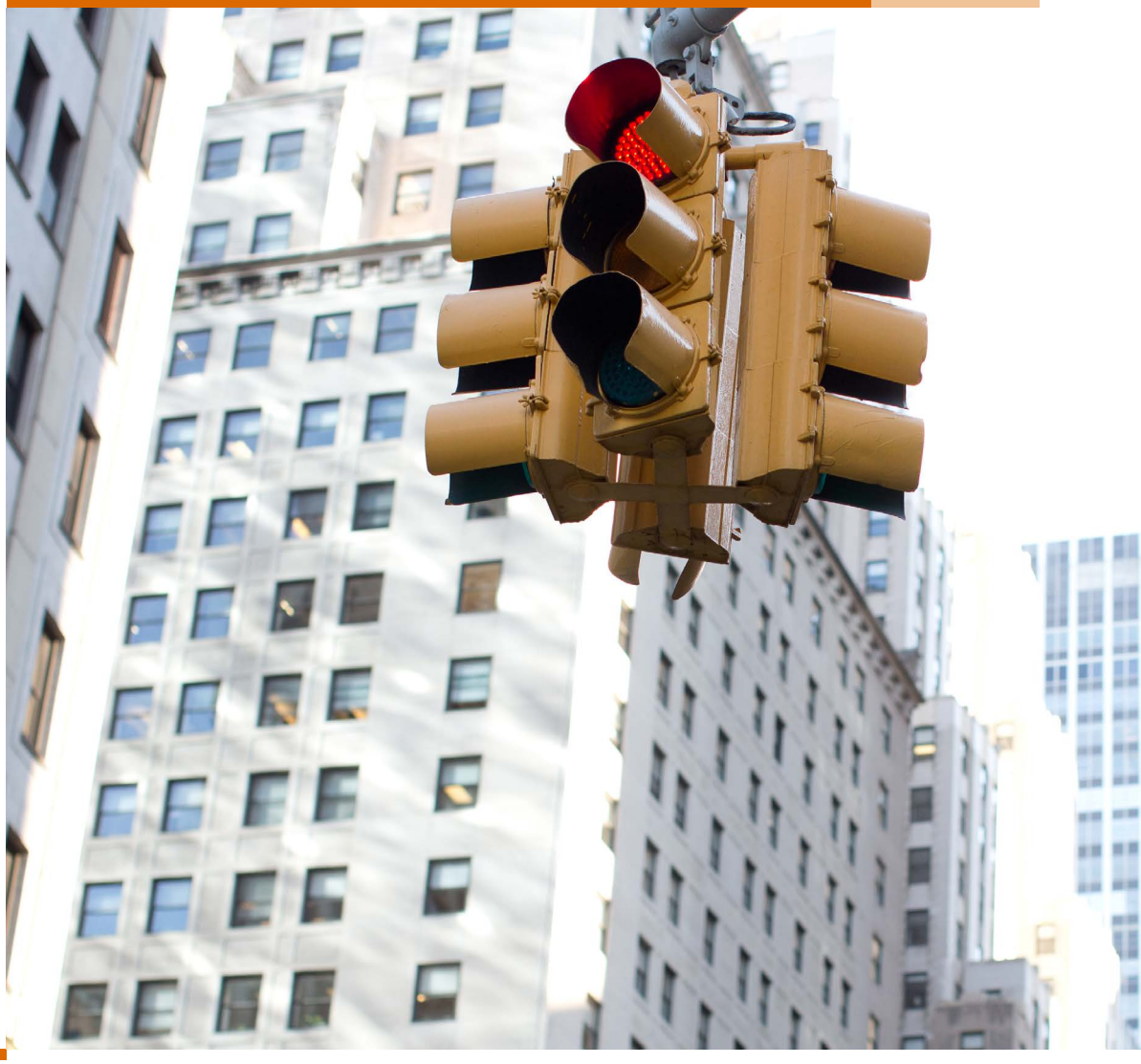
U.S. State of Cybercrime

www.pwc.com/cybersecurity

US cybersecurity: Progress stalled

Key findings from the 2015 US State of Cybercrime Survey

July 2015



pwc

About the 2015 US State of Cybercrime Survey

The 2015 US State of Cybercrime Survey was co-sponsored by PwC, *CSO,* the CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and the United States Secret Service.

Cybersecurity leaders from these organizations worked together to evaluate survey responses from more than 500 executives of US businesses, law enforcement services, and government agencies. We evaluated trends in the frequency and impact of cybercrime incidents, cybersecurity threats, information security spending, and the risks of third-party business partners in private and public organizations. We also assessed how businesses are adapting to evolving expectations of the information security function and the Board of Directors.

In addition to analysis of the survey results, this report also draws on previous PwC research that includes PwC's 18th Annual Global CEO Survey, The Global State of Information Security® Survey 2015, and the 2015 Digital IQ Survey. We leveraged these surveys to provide a more thorough and balanced look into the current state of cybersecurity and cyberthreats.

It's been a watershed year for cybercrime

Cybercrime continues to make headlines—and cause headaches among business executives.

76%

said they are more concerned about cyberthreats this year.

Cybersecurity incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors. It's clear that adversaries continue to advance their threats, techniques, and targets. They are investing in technologies, sharing intelligence, and training their crews to attack with purpose and competence.

It's no wonder, then, that we found rising concern among the 500 US executives, security experts, and others from the public and private sectors who participated in the 2015 US State of Cybercrime Survey. In fact, 76% of respondents said they are more concerned about cybersecurity threats this year than in the previous 12 months, up from 59% the year before. We have noticed a similar increase in apprehension in other research. In PwC's 18th Annual Global CEO Survey 2015, for example, 87% of US chief executives said they were worried that cyberthreats could impact growth prospects, up from 69% the year before.[1]

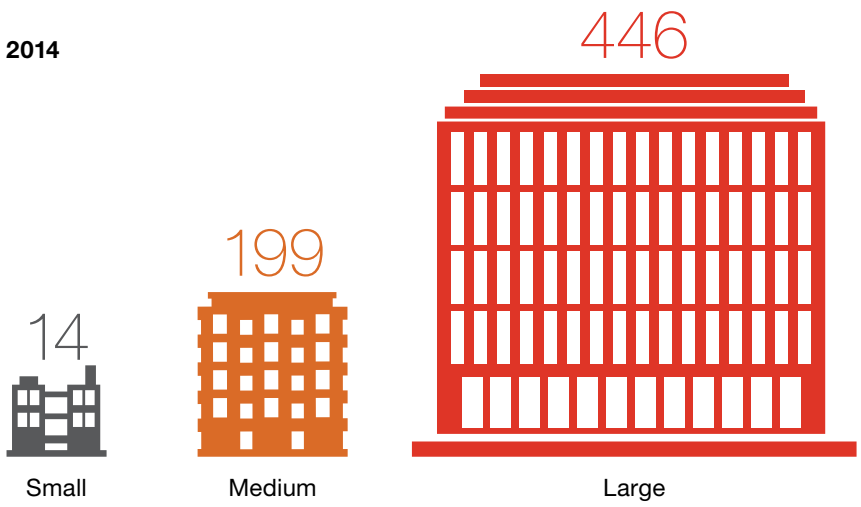
Heightened awareness and concern are well-warranted: A record 79% of survey respondents said they detected a security incident in the past 12 months. Many incidents go undetected, however, so the real tally is probably much higher.

We found a significant correlation between company size and the ability to detect cybersecurity incidents. As a general rule, larger organizations tend to identify more incidents year over year. In fact, respondents from large businesses detected 31 times more incidents than small companies. It's a pattern we have observed in previous research. In The Global State of Information Security® Survey 2015, large organizations detected 28% more incidents in 2014 compared with the year before, while small companies detected 5% fewer incidents during the same time period.[2]

These findings make sense, given that bigger organizations tend to have mature security technologies, processes, and resources that enable them to detect more incidents.

Not surprisingly, the most-frequently cited types of compromise are typically crimes committed by external threat actors, those who are not employees or third-party partners with trusted access to networks and data. Particularly worrisome are phishing campaigns, which are comparatively easy to initiate and can rapidly spread across an organization, targeting top executives as well as employees and managers. Almost one-third (31%) of respondents said they had been hit by a phishing attack in 2014, making it one of the most frequent types of incidents.

Detected incidents by company size*



** Size by number of employees Small: Fewer than 1,000; Medium: 1,000 to 9,999; Large: 10,000 or more*

1 PwC, 18th Annual Global CEO Survey, January 2015

2 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

The lines separating the intents of nation-states, hacktivists, and organized crime are beginning to blur.

Cyberattacks are becoming more destructive

Globally, a record 1 billion data records were compromised in 2014, according to a report by security firm Gemalto.[3] Many of those security incidents were very widely reported: The year 2014 saw the term "data breach" become part of the broader public vernacular, with *The New York Times* devoting more than 700 articles related to data breaches, versus fewer than 125 the previous year.[4]

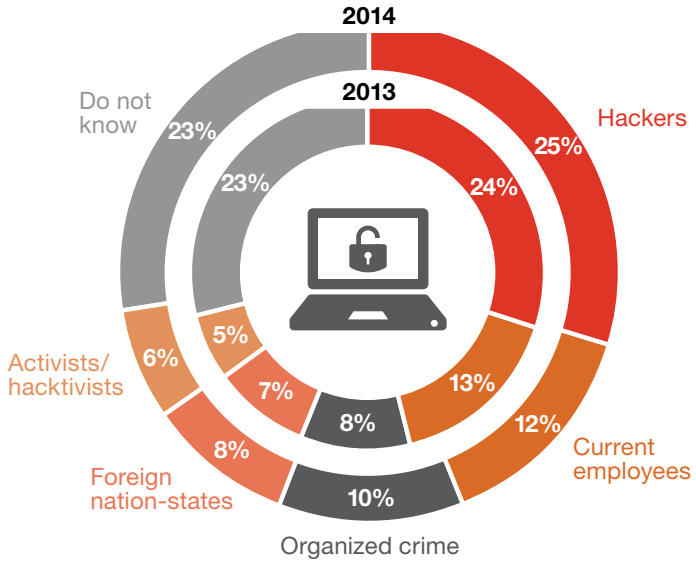
It's not just the number of incidents—detected or not—that's on the rise. Attacks are also becoming increasingly public and prominent.

In the past, public knowledge of cybercrime was typically limited to only those incidents requiring disclosure. That, as it turns out, was merely the tip of the iceberg. The huge mass of risks (and attacks) once lurking below the surface are now splashed across websites, social media, and newspapers on a daily basis. In part, that's because behavior of threat actors has become increasingly egregious, and their attacks can be progressively more destructive.

The high-profile assault on a global entertainment company late last year demonstrated that threat actors' motives and means are varied, and that lines separating the intents of nation-states, hacktivists, organized crime, and individuals with malicious intent are beginning to blur. The perpetrator of the hack, thought to be a nation-state acting on political motivations, released personal data and damaging employee communications, as well as sensitive corporate documents and payroll information. The attack also disrupted the company's email and telephone systems, and introduced a new level of malice that included a threat of physical violence to individuals.

As motives and means continue to evolve, so do the methods of attack. Distributed denial of service (DDoS) attacks are becoming increasingly potent and are one of the most frequent types of cybersecurity incidents, cited by 18% of survey respondents this year. DDoS assaults most often result in damage to reputation, but they also can put businesses at risk by disrupting e-commerce and other business processes.

Greatest cyberthreats to organizations



3 Gemalto, Gemalto Releases Findings of 2014 Breach Level Index, February 12, 2015

4 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

The retail and consumer products industry, after two years of high-profile attacks, significantly increased information security spending.

Ransomware, a comparatively new type of cybercrime, is becoming more sophisticated and commonplace. The FBI recently warned that this type of attack, in which adversaries take control of a company's data until it pays a ransom, is on the rise.[5] In 2014, 13% of Cybercrime Survey respondents said they had been a victim of ransomware. We expect that reports of ransomware will continue to mount.

Some categories of cybercrime have been around for decades, but rarely spark the interest of the media. Take wire fraud. While not widely reported, this type of cybercrime is becoming more prominent and costly. The FBI and the Internet Crime Complaint Center recently said that global wire fraud cost businesses $215 million during a 14-month period, with US companies representing 84% of those financial losses.[6] Our survey shows that 21% of law enforcement respondents cited wire fraud as among the top five areas that consume their caseload time. It's a crime that frequently begins with phishing campaigns that often target top executives.

Large companies and retailers boost security spending

On a more positive note, the recent rash of security incidents may be convincing companies to step up their investments in cybersecurity.

While this survey did not measure the average security budgets of respondents, in The Global State of Information Security® Survey 2015 we found that US information security budgets have grown at almost double the rate of IT budgets over the last two years.[7]

The Cybercrime Survey indicated that industries that have been impacted by high-profile cyberattacks were more likely to significantly boost information security investments. In fact, 38% of retail and consumer companies, which have been frequent targets of attack in the past two years, increased their security spending by 20% or more over the year before—higher by far than any other industry. By contrast, only 17% of banking and finance and 15% of healthcare respondents reported 20% increases in security budgets.

The appropriate level of cybersecurity investment will vary by industries and their threat environments, of course. A spending increase of 20% or more may be unnecessary for banking and finance organizations, which typically spend more on security than businesses in other sectors. Healthcare organizations, by comparison, tend to spend less on cybersecurity yet are being hit with new types of attacks across expanded vectors. The PwC Health Research Institute predicts that recent data breaches will prompt health companies to take extra steps to protect sensitive personal information and increase investments in information security.[8] While the Cybercrime Survey did not ask respondents about information security budgets for 2015, The Global State of Information Security® Survey found that 51% of healthcare payers and providers plan to boost security spending in 2015.[9]

The Cybercrime Survey determined that large businesses were more likely to substantially increase information security spending. In fact, 20% of companies with more than 10,000 employees said they raised security investments by 20% or more in 2014, while 12% of small companies did so.

This explains, in part, why large companies typically have more mature security practices: They have consistently invested more over the years.

No matter the size, as companies boost their security budgets, executives will likely place a greater emphasis on the return on investment in cybersecurity. After all, they will want to make sure that the increased spending results in measurable improvements in the company's security posture.

5 Federal Bureau of Investigation, Ransomware on the Rise, January 20, 2015

6 eWeek, Spam Campaign Business E-mail Compromise Pilfers $215 Million, January 23, 2015

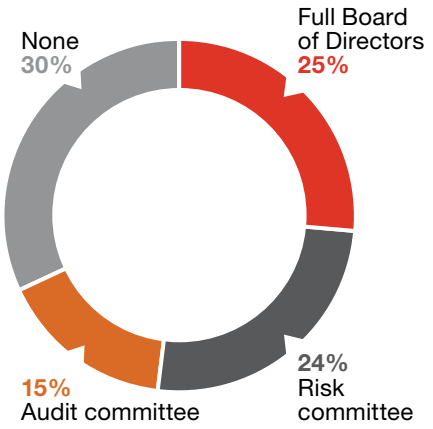
7 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

8 PwC Health Research Institute, Medical Cost Trend: Behind the Numbers 2016, June 2015

9 PwC, *CSO, CIO* magazine, The Global State of Information Security® Survey 2015, September 2014

Almost half of Boards still view cybersecurity as an IT matter, rather than an enterprise-wide risk issue.

Board engagement in cyber-risks



Boards are concerned, but not always engaged

Another result of the barrage of breaches over the past year is that many Boards of Directors now take a very active interest in cybersecurity. They want to know about current and evolving risks, as well as the organization's security preparedness and response plans. The question is how often security leaders provide cyber-risk briefings to their Boards.

Our research shows that one in four (26%) respondents said their Chief Information Security Officer (CISO) or Chief Security Officer (CSO) makes a security presentation to the Board only once a year, while 30% of respondents said their senior security executive makes quarterly security presentations. But 28% of respondents said their security leaders make no presentations at all.

As with other cybersecurity best practices, CISOs and CSOs from large companies are more likely to make quarterly Board presentations and small organizations are least likely to do so. In fact, one-third (33%) of respondents from small companies said their security leaders never advise the Board on security risks, compared with 18% of large companies.

While there is no universal approach to Board participation in oversight of cyber-risks, as a general guideline the National Association of Corporate Directors (NACD) recommends that risk oversight be a function of the full Board. The critical link between strategy and risks points to the need for the full Board—and not just one committee—to have responsibility for cybersecurity risk, according to the NACD.[10] So it was a bit worrisome to find that 30% of respondents said no Board committees or members are engaged in cyber-risks. At the other end of the spectrum, only 25% of respondents said their full Board is involved in cyber-risks.

It seems curious that just 15% of respondents said the audit committee is engaged in cyber-risks. In the past several years, we have seen many companies add a raft of internal insight issues—including cybersecurity—to the audit committee's agenda. One explanation for the comparatively weak engagement of the audit committee may be that companies are shifting cybersecurity oversight responsibilities to the entire Board or special risk committees.

10 National Association of Corporate Directors, Cyber-Risk Oversight: Directors Handbook Series, 2014

Security executives should not wait for the Board to ask questions about cyber-risks and cybersecurity preparedness.

These statistics are alarming when viewed through a post-breach lens. The lack of substantive consideration of operational cyber-risks by the Board may lead regulators and plaintiff's counsel to conclude the operational risk lacked preventive and detective controls that management is responsible for implementing and the Board is responsible for monitoring.

It's also essential that Boards treat cybersecurity as an overarching corporate risk issue rather than simply an IT risk. Many have yet to adopt this approach, however. Almost half (49%) of Boards view cybersecurity as an IT risk, while 42% see cybersecurity through the lens of corporate governance.

Organizations that treat cybersecurity as a matter of enterprise-wide risk should be able to demonstrate to external stakeholders that they understand and appropriately manage cybersecurity activities and related obligations, as well as the intent to be a good corporate citizen. This level of engagement and awareness often requires a carefully designed oversight program based on corporate governance methodologies and corporate standards that have succeeded in the past. An oversight program can help companies streamline Board reporting, integrate multi-department activities required to mitigate operational cyber-risks, and demonstrate that reasonable security protocols and procedures are in place.

In an effort to better understand enterprise risk, some forward-looking organizations are moving toward a formalized quantitative estimate of cyber-risks and exposures, an approach typically referred to as cybersecurity value at risk. This quantitative estimate is developed within a conceptual framework consistent with traditional financial services value at risk methods. It can help CEOs, CROs, and Boards better understand what digital assets are at risk, how to project potential losses, and how to abate risks using alternative security models, investments, and cybersecurity insurance.

One thing is clear: Security executives should not wait for the Board to ask questions about cyber-risks and cybersecurity preparedness. CISOs and CSOs should proactively update the Board on cybersecurity risks on a semiannual basis—at the very least.

7 reasons why cybersecurity is a Board oversight issue

Cyberthreats are among the most significant business risks facing organizations today—and Boards are now held accountable. As a result, directors must view cybersecurity as an enterprise-wide risk issue that should be addressed from strategic, cross-functional, and economic perspectives. Following are seven reasons why Boards should be asking serious questions about cyberthreats and their organization's cybersecurity capabilities:

1. The impact of cybersecurity is systemic. Incidents can impact an organization's global operations even when a risk point is thousands of miles away.
2. The financial impact can be significant and can include costly class-action lawsuits, which may reflect on Boards' fiduciary responsibility to preserve corporate financial value.
3. As regulations evolve, compliance is becoming more challenging and increasingly costly. The European Union's Data Protection Directive, for instance, includes a proposal for fines of up to 5% of a company's global revenue.[11] This also lays the foundation for civil litigation.
4. The Internet of Things has brought new threats, including compromise of industrial controls and smart building systems that can cause extreme risks and tremendous physical damage.
5. Cybersecurity insurance should be considered as a regulatory hedge against cyber-risks. A risk committee should ask questions regarding coverage for directors' and officers' liability, commercial general liability, prior acts, and property and casualty insurance.
6. Adversaries such as nation-states and organized crime are working together to attack organizations for objectives like economic sabotage, theft of trade secrets, money laundering, terrorism, and military and intelligence operations.
7. Cyberattacks can result in substantial financial losses and damage brand reputation by disrupting an organization's strategic objectives, such as a planned merger or acquisition, the launch of a new product, or a business deal with a potential customer.

11 European Commission, Stronger data protection rules for Europe, June 15, 2015

New ISAOs will be more flexible, enabling businesses to share information across industries as well as by issues, geographies, and specific threats.

Information sharing is front and center

To say that information sharing is having a moment would be an understatement. And President Barack Obama's February 2015 executive order calling for the creation of new Information Sharing and Analysis Organizations (ISAOs) is clearly fueling the discussion.

Sharing reliable, actionable, and timely intelligence advances situational awareness of threats, defense agility, informed decision-making, and rapid notification to affected customers and businesses as well as regulatory bodies. It's also a relatively inexpensive way to gain a fuller picture of threats facing an organization.

Despite the benefits, we found an underwhelming level of participation in industry-specific Information Sharing and Analysis Centers (ISACs): Only 25% of respondents said they were involved in ISACs in 2014, virtually the same as the year before. Industries most likely to participate are electric power, water, banking and finance, and government agencies.

Many industry observers anticipate that the president's executive order will boost participation in information-sharing initiatives. Unlike today's industry-specific ISACs, membership in ISAOs will be more flexible, enabling businesses and public-sector agencies to share information specific to individual industries as well as intelligence related to geographies, issues, events, or threats.

ISAOs may also enable organizations to share information across industries. For example, significant challenges often do not differ by sector (such as financial services or pharmaceuticals) but rather by an entity's size or constituency. A big Wall Street bank might have more in common with a large pharmaceutical company than it does with a regional bank. Indeed, middle-market participants often have different challenges than larger businesses.

ISAOs might resolve these issues, but many foundational objectives must first be addressed. A successful information-sharing model will require a clear mission and focus, should be operated by rules determined (and strictly enforced) by its members, must clearly demonstrate value to its membership, and generate and sustain trust.

A key roadblock to information sharing is a lack of a unified framework, platform, and data standards. Threat intelligence and response tactics should be distributed in real time—which will be impossible to achieve without an integrated and automated infrastructure. To this end, the Department of Homeland Security and others are working to promote specific, standardized message and communication formats such as TAXII, STIX, and CybOX. Clear data on their adoption rates is not yet available, however, nor do we know if they represent the best possible formats.

One thing we do know is that speed is of the essence. Based on attacks observed by cyberthreat firm RiskAnalytics during 2014, 75% of attacks spread from victim 0 to victim 1 within one day (24 hours). Over 40% hit the second organization in less than an hour.[12]

Finally, a successful information-sharing model will need to provide clear guidelines on the privacy of consumer data, as well as a resolution to the thorny public-private conflict on the use of encryption by technology companies. US lawmakers are currently considering information-sharing legislation that, if enacted, may eliminate some of these roadblocks.

12 Verizon, 2015 Data Breach Investigations Report, April 15, 2015

A lopsided investment in technology

Although cybersecurity budgets are on the rise, for better or worse, surging anxiety about cybercrime has led to a greater reliance on technology solutions to fend off digital adversaries and manage risks.

Consider that 75% of US chief executives responding to PwC's 18th Annual Global CEO Survey ranked cybersecurity solutions as "very important" to the company's business strategy.[13] We found a similar enthusiasm for technology in PwC's 2015 Digital IQ Survey: 69% of respondents said they are investing in cybersecurity technologies, more than any other spending category.[14]

So it was not surprising to find that respondents to the US Cybercrime Survey are similarly bullish on technology. Almost half (47%) said adding new technologies is a spending priority, higher than all other initiatives. Notably, only 15% cited redesigning processes as a priority and 33% prioritized adding new skills and capabilities.

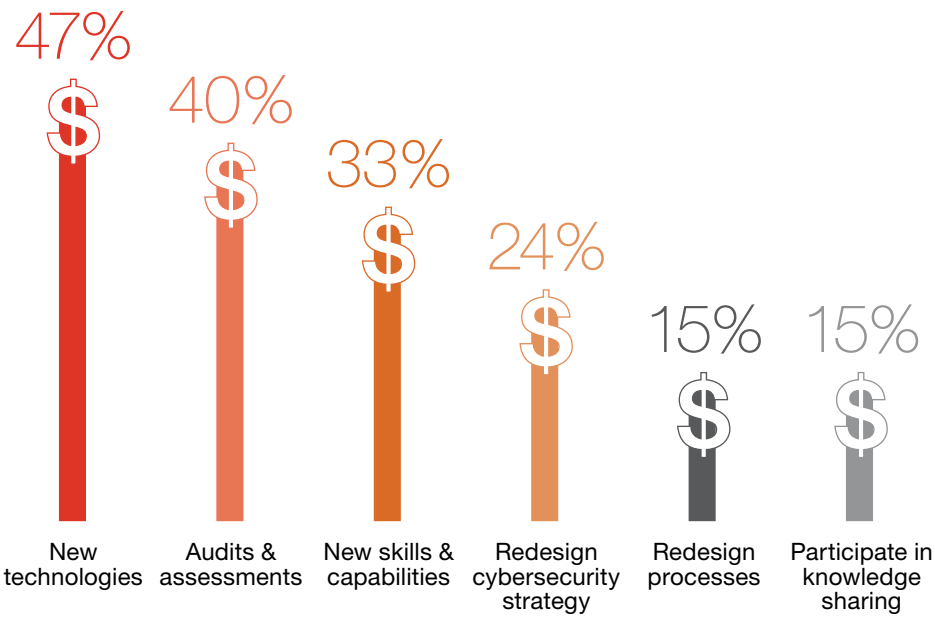
When we asked whether organizations have the expertise to address cyber-risks associated with implementation of new technologies, only 26% said they have capable personnel on staff. Most rely on a combination of internal and external expertise to address cyber-risks of new solutions.

Companies that implement new technologies without updating processes and providing employee training will very likely not realize the full value of their spending. To be truly effective, a cybersecurity program must carefully balance technology capabilities with redesigned processes and staff training skills.

Employee training and awareness continues to be a critical—and often neglected—component of cybersecurity. Only half (50%) of survey respondents said they conduct periodic security awareness and training programs, and the same number offer security training for new employees.

In addition to a thorough employee security awareness program, it will also be critical to have regularly tested and updated incident-response and crisis-management playbooks in place. These plans should include frequent tabletop exercises for security and business stakeholders, as well as ongoing training for employees and executive leaders. In today's cybercrime environment, the issue is not whether a business will be compromised, but rather how successful an attack will be; organizations that are well-prepared will have a better ability to limit the impact. Preparedness will also enable security executives to convey confidence and control to the C-suite and Board.

Cyber-risk spending priorities



13 PwC, 18th Annual Global CEO Survey, January 2015

14 PwC, Three surprising digital bets for 2015, January 2015

Regulators in the financial services industry are leading the charge in focusing on due diligence of third-party suppliers.

Third-party risks are not adequately addressed

The need for due diligence of the security capabilities of third parties has gained prominence in the past year, in part because of high-profile breaches that began with attacks on the systems of business partners.

That's not to say the need to assess the cybersecurity of third parties is new, however. What's different is that regulators are becoming increasingly serious about third-party risk management and expect that organizations will be able to prove due diligence, as well as ongoing supervision and governance.

Regulators in the financial services industry are leading the charge. The Federal Financial Institutions Examination Council (FFIEC) has developed a Cybersecurity Assessment Tool to help institutions identify risks and determine their cybersecurity maturity. Management can use the tool to assess the institution's inherent risk profile based on technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats.[15]

The New York State Department of Financial Services is focusing on security assessments of third-party providers. In October 2014, the department polled 40 regulated banking organizations for information about due diligence, policies and procedures, safeguards for sensitive data, and protections against loss incurred as a result of third-party information security failures.[16]

This increased regulatory scrutiny is likely to spread to other industries, so it was encouraging to see some advances in the number of respondents who assess risks associated with supply chains and business ecosystems. This year, 62% said they evaluate the security risks of third-party partners and 57% said they do so for contractors, while only 42% of respondents consider supplier risks.

Assessment of business ecosystem risks

15 Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, June 2015

16 New York State Department of Financial Services, Update on Cyber Security in the Banking Sector: Third Party Service Providers, April 2015

Almost one in five (19%) of C-suite executives said they are not concerned about cybersecurity risks associated with third-party and supply chain partners.

But it's worrisome that almost one in five (19%) CEOs, CFOs, and COOs said they are not at all worried about any kind of supply-chain risk. It may be that many of these executives presume that the IT department is responsible for third-party threats. If so, we've got some potentially troubling news for them: 19% of CIOs themselves were unconcerned about supply-chain risks.

It's clear, then, that due diligence of business partners is far from adequate. If you need further proof, consider that only 16% of respondents said they evaluate third parties' cybersecurity more than once a year—and 23% do not evaluate third parties at all. Similarly, most companies do not have a process for assessing the cybersecurity capabilities of third-party partners before they do business with them, nor do they conduct incident-response planning with external partners.

It is essential that the right to assess a partner's security capabilities is stipulated in contracts. Organizations that do not legally plan for due diligence when executing contracts or preparing for a potential M&A transaction may not be allowed to later perform adequate assessments. Also consider that an increasing proportion of security spending occurs outside of the IT function on services like cloud computing. Contracts executed outside of IT may not allow for due diligence and, in fact, they may not require critical information security and privacy safeguards.

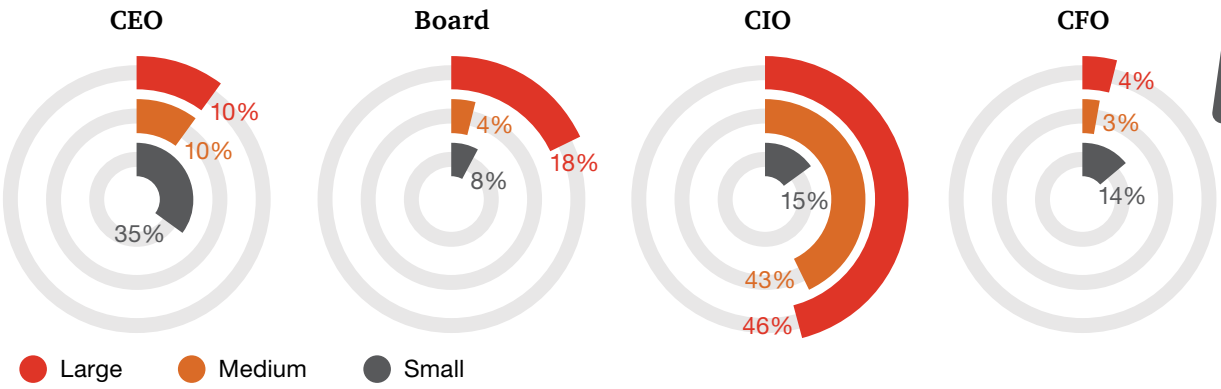
As noted, it will be equally essential that businesses implement and regularly test a response plan for third-party breaches. In the pressure of the moment, incident-response plans may fall apart if they are not well-tested and continually updated.

The strategic role of the CISO

The role and responsibilities of the Chief Information Security Officer continue to evolve as cybercrime becomes a more prominent enterprise-wide risk. This has amplified the debate about how to integrate the security function into the organizational structure and to whom the top security executive should report.

Our survey found that most CISOs and Chief Security Officers report to the CIO, followed by the CEO, CFO, COO, and the Board, in that order. While the organizational structure varies by industry and company size, most sectors follow these patterns, with the CIO being the most likely reporting structure in almost all sectors.

Where the CISO/CSO reports by company size*



** Size by number of employees Small: Fewer than 1,000; Medium: 1,000 to 9,999; Large: 10,000 or more*

In this year's Cybercrime Survey, we found that the top security executive is most likely to report to the CEO in small organizations, while in medium-size companies the CISO or CSO reports to the CIO. Among large companies, the security leader typically reports to the CIO or the Board.

The fact that security leaders most often report to the CIO suggests that organizing the security function under IT is the most effective structure. In reality, this broad generalization does not hold true because the right organizational structure depends on a variety of individual factors, and the role of the CIO differs across companies and industries. In financial services, for example, bank regulators have demanded greater accountability from CISOs and have taken steps to ensure that security leaders do not directly report to the CIO. We have also seen that the role of the CISO is evolving to include both risk as well as security technologies, and that the reporting line is sometimes split between risk officers and general counsel, in addition to dotted-line reports to IT. We expect the role of the CISO to continue to evolve as cybersecurity risks continue to escalate.

No matter the formal organizational structure, the CISO's responsibilities and competencies have irrevocably deepened in the past several years. The role is more senior—and visible—than ever before. The CISO is held accountable for risks, and is expected to deliver a minimum information security posture across the organization.

Today's CISO should be a general manager who has the same level of experience as C-suite officers. He or she should have expertise not only in security but also risk management, corporate governance, and communications. The security leader should have access to key executives to provide insight into business risks and should be able to competently articulate risk-based security issues to the C-suite, Board, and oversight groups like audit, legal, and compliance. Put simply, the information security leader should have the ability to effect change on par with other senior executives.

It's time to take a stance

It's clear that the threats, techniques, and targets of adversaries continue to dynamically—and successfully—evolve. Cybercriminals are investing in technologies, sharing intelligence, and attacking with purpose and persistence.

Businesses must keep up with the capabilities of their adversaries. It's essential to note, however, that keeping pace is not simply a matter of increased cybersecurity spending. Rather, staying abreast of threats may require that organizations redirect limited resources to initiatives that deliver the greatest return. These can include enhanced threat analytics capabilities, prioritizing security of the most critical assets, performing simulations to improve response capabilities across the organization, and stepping up security awareness efforts. Organizations also should be prepared to proactively share information on cybersecurity threats and response tactics. A sustained effort, from the Board down to individual employees, will be needed for many years to come.

We've said it before and we'll say it again: The time for change is now. Organizations must summon the vision, determination, skills, and resources to build a risk-based cybersecurity program that can quickly detect, respond to, and limit fast-moving threats. Those that do not risk becoming tomorrow's front-page news.

Contacts

To have a deeper conversation about cybersecurity, please contact:

David Burg
Principal
david.b.burg@us.pwc.com

Michael Compton
Principal
michael.d.compton@us.pwc.com

Peter Harries
Principal
peter.harries@us.pwc.com

John D. Hunt
Principal
john.d.hunt@us.pwc.com

Mark Lobel
Principal
mark.a.lobel@us.pwc.com

Gary Loveland
Principal
gary.loveland@us.pwc.com

Joseph Nocera
Principal
joseph.nocera@us.pwc.com

Shawn Panson
Partner
shawn.panson@us.pwc.com

Grant Waterfall
Partner
grant.waterfall@us.pwc.com

Contributing authors

Charles Beard
Principal
charles.e.beard@us.pwc.com

Kevin Mickelberg
Director
kevin.j.mickelberg@us.pwc.com

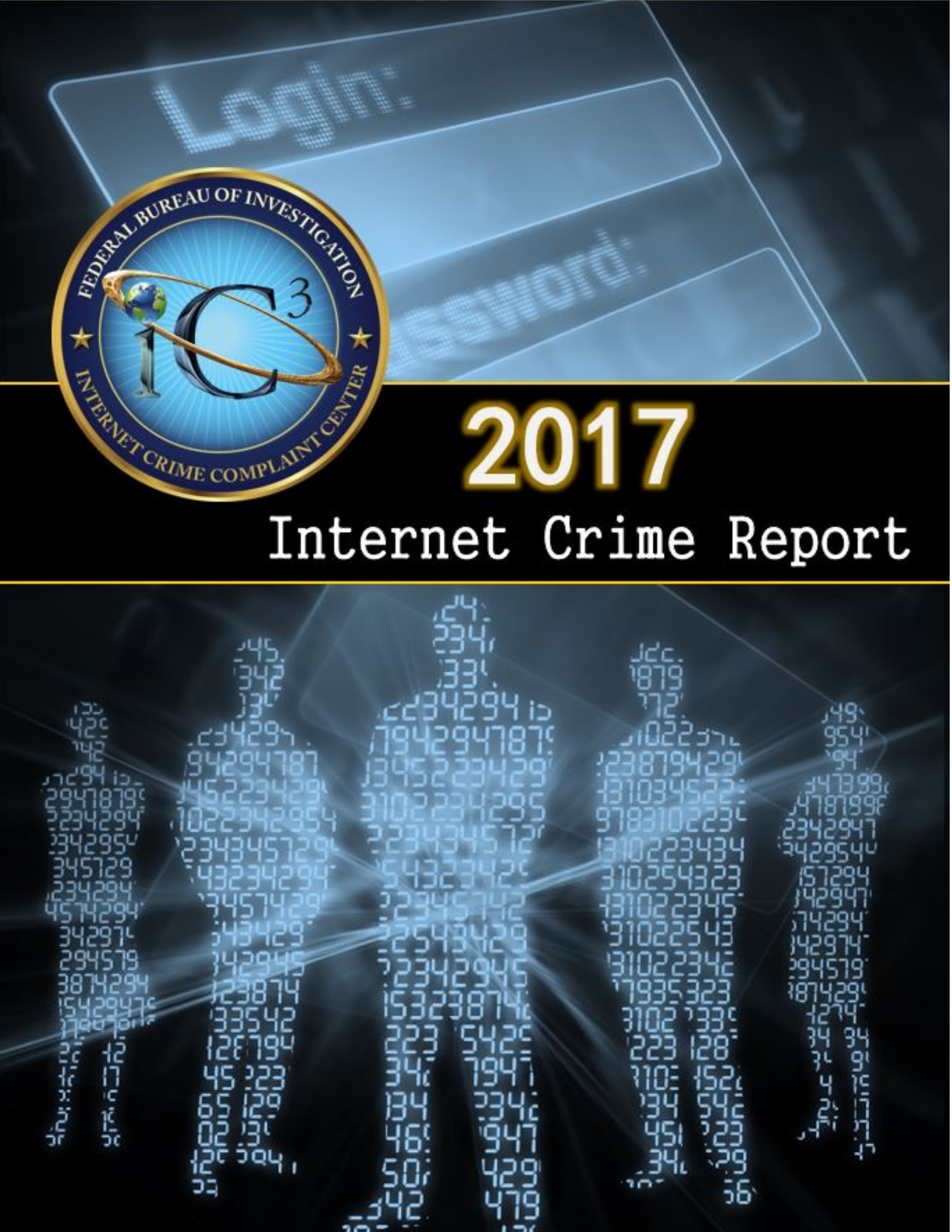
Emily Stapf
Principal
emily.stapf@us.pwc.com

Don Ulsch
Managing Director
don.ulsch@us.pwc.com

www.pwc.com/cybersecurity

Enclosure (3)

Federal Bureau of Investigation
Internet Crimes Report



2017 Internet Crime Report

2017 Internet Crime Report

Table of Contents

Introduction

Dear Reader,

2017 was a milestone year for the FBI's Internet Crime Complaint Center (IC3). On October 12, 2017, at 4:10pm, the IC3 received its 4 millionth consumer internet crime complaint.

As the lead federal agency for investigating cyber-attacks by criminals, overseas adversaries, and terrorists, the FBI's IC3 provides the public with a trustworthy and convenient reporting mechanism to submit information concerning suspected Internet-facilitated criminal activity. The IC3 also strengthens the FBI's partnerships with our law enforcement and private industry partners. As cyber criminals become more sophisticated in their efforts to target victims, we must continue to transform and develop in order to address the persistent and evolving cyber threats we face.

The 2017 Internet Crime Report emphasizes the IC3's efforts in monitoring trending scams such as Business Email Compromise (BEC), Ransomware, Tech Support Fraud, and Extortion. The report also highlights the Elder Justice Initiative promoting justice for the nation's seniors. In 2017, IC3 received a total of 301,580 complaints with reported losses exceeding $1.4 Billion.

This past year, the most prevalent crime types reported by victims were Non-Payment/Non-Delivery, Personal Data Breach, and Phishing. The top three crime types with the highest reported loss were BEC, Confidence/Romance fraud, and Non-Payment/Non-Delivery.

This year's report features success stories from two different successful cases initiated from IC3 complaints. Additionally, the Operation Wellspring (OWS) Initiative continues to build the cyber investigative capability by utilizing Cyber Task Force officers, thus strengthening state and local law enforcement collaboration.

We hope this report provides additional information of value as we work together to protect our nation against cyber threats.

Scott S. Smith

Assistant Director

Cyber Division

Federal Bureau of Investigation

About the Internet Crime Complaint Center

The mission of the FBI is to protect the American people and uphold the Constitution of the United States.

The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners. Information is analyzed and disseminated for investigative and intelligence purposes, for law enforcement, and for public awareness.

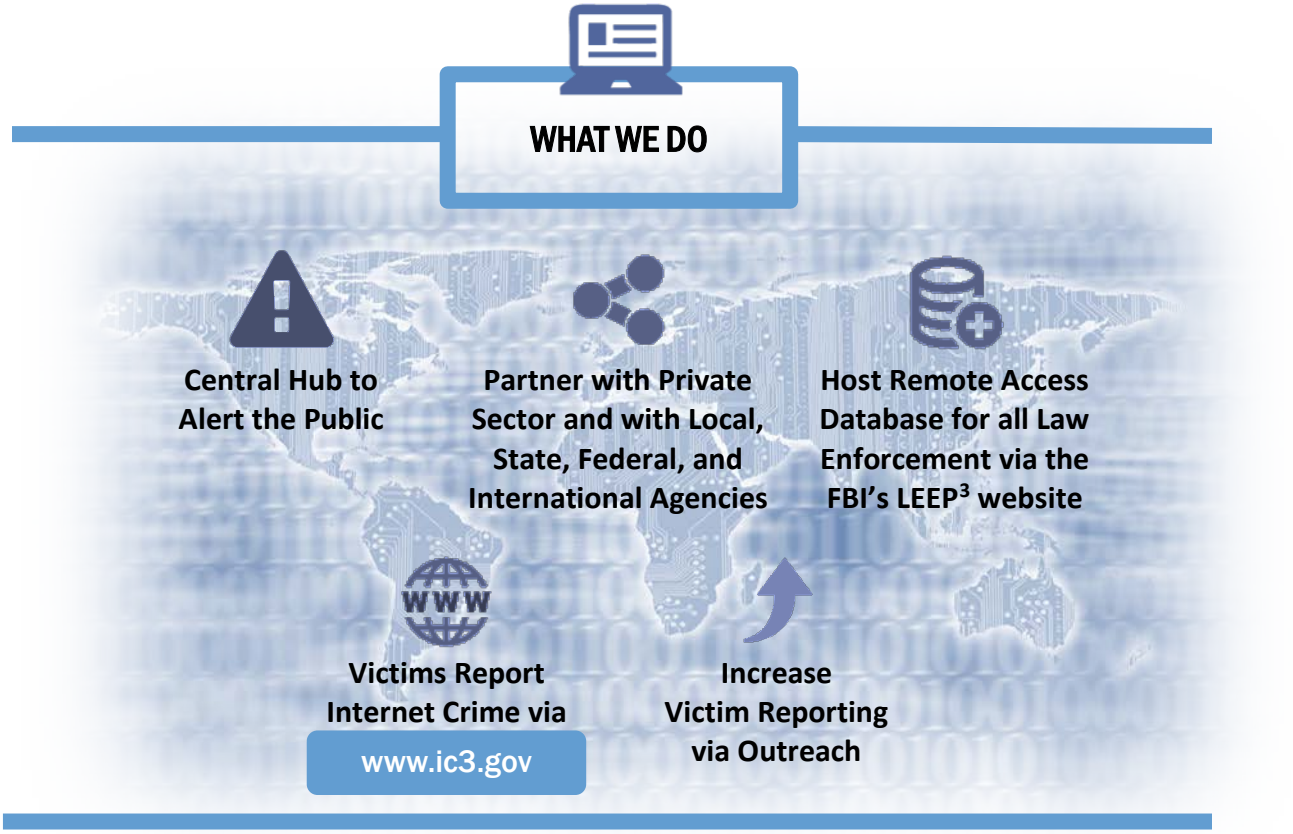
In an effort to promote public awareness, the IC3 produces this annual report to aggregate and highlight the data provided by the general public. The quality of the data is directly attributable to the information ingested via the public interface www.ic3.gov. The IC3 attempts to standardize the data by categorizing each complaint based on the information provided. The IC3 staff analyzes the data to identify trends in Internet-facilitated crimes and what those trends may represent in the coming year.

IC3 History

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. There have been 4,063,933 complaints reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of more than 284,000 complaints per year. The complaints address a wide array of Internet scams affecting victims across the globe.[1]

[1] Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2013 to 2017. Over that time period, IC3 received a total of 1,420,555 complaints, and a total reported loss of $5.52 billion.

The IC3 Role in Combating Cyber Crime[2]



Collection

Victims are encouraged and often directed by law enforcement to file a complaint online at www.ic3.gov. Complainants are asked to document accurate and complete information related to the Internet crime, as well as any other relevant information necessary to support the complaint. In addition to reporting the crime via www.ic3.gov, complainants should take steps to mitigate further loss. Victims can take actions such as contacting banks, credit card companies, and/or credit bureaus to block accounts, freeze accounts, dispute charges, or attempt recovery of lost funds. Victims should be diligent in reviewing credit reports to dispute any unauthorized transactions and should also consider credit monitoring services.

---

[2] Accessibility description - image depicts what IC3 does to include providing a central hub to alert the public: partner with private sector and with local, state, federal, and international agencies; host a remote access database for all law enforcement via the FBI's LEEP website; victim reporting at www.ic3.gov; and increase victim reporting via outreach.

[3] Federal Bureau of Investigation. Law Enforcement Enterprise Portal (LEEP)

Analysis

The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends.

Public Awareness

Public service announcements (PSAs), scam alerts, and other publications outlining specific scams are posted to the www.ic3.gov website. As more people become aware of Internet crimes and the methods utilized to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.

IC3 Core Functions[4]

Referrals

The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement conducts an investigation and determines a crime has been committed, legal action may be brought against the perpetrator.

[4] Accessibility description: image contains the IC3 logo against a digital background. Core functions are listed in individual blocks- Collection, Analysis, Public Awareness, and Referrals as components of an ongoing process.

Supporting Law Enforcement

IC3 Database Remote Access

All sworn law enforcement can remotely access and search the IC3 database through the FBI's Law Enforcement Enterprise Portal (LEEP).

LEEP is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources all in one centralized location. These resources can be used to strengthen case development for investigators and enhance information sharing between agencies. This web-based access additionally provides users the ability to identify and aggregate victims and losses within a jurisdiction.

The IC3 expanded the remote search capabilities of the IC3 database by allowing users to gather IC3 complaint statistics. Users now have the ability to run city, state, county, and country reports and sort by crime type, age, and transactional information. The user can also run overall crime type reports and sort by city, state, and country. The report results can be returned as a portable document format (PDF) or exported to Excel. This search capability allows users to better understand the scope of cyber crime in their area of jurisdiction and enhance cases.

Successes

International Investment Scam: FBI Houston

Beginning in 2015, the IC3 provided multiple complaints to FBI Houston regarding an elaborate investment scheme. The scheme involved the impersonation of Branch Banking & Trust (BB&T) and JPMorgan Chase (Chase) executives, the fabrication of U.S. government documents, the creation of fraudulent investment agreements in the name of BB&T and Chase, and the purchase of luxury vehicles to launder the proceeds of the scheme. It was perpetrated by individuals primarily living in West Africa, who impersonated U.S. bank officials and financial consultants, and made fraudulent offers of investment funding to victims all over the world via the Internet and phone. Victims were deceived into believing they would receive millions of dollars of investment funding as part of joint ventures with U.S. banks, usually BB&T or Chase. The perpetrators utilized false domain names to make it appear their emails were affiliated with BB&T or Chase. To convince victims the opportunities were authentic, the perpetrators recruited U.S. citizens to pose as bank "representatives" at in-person meetings with the victims. If the victims lived outside the U.S., the perpetrators orchestrated bogus visits to the local U.S. embassy or consulate and fabricated U.S. government documents to convince the victims the U.S. government was sponsoring the investment agreements. The victims were then induced to pay tens of thousands, and often hundreds of thousands, of dollars to U.S.-based bank accounts on the belief that such payments were necessary to effectuate their investment agreements.

Once the funds hit the U.S.-based accounts, money movers controlling the accounts used various means to liquidate the proceeds and move the funds to West Africa, including outgoing wire transfers to exporters, cash withdrawals, and the purchase of luxury vehicles which were shipped to West Africa.

The scheme allegedly resulted in losses of more than $7 million from victims in more than 20 countries. To date, a house in Richmond, vehicles and approximately $200,000 in cash, all directly traceable to victims' payments, have been seized[5].

Harassment/Extortion: FBI Los Angeles

Since October 2017, FBI Los Angeles has been investigating a reported intrusion of a company's network that also involved harassment and extortion by an unknown subject. This individual continuously harassed the company with emails and phone calls that greatly impacted the victim company's business. The harassment continued until the company agreed to make payments for the attacks to stop.

The case was initiated by an IC3 complaint sent to FBI Los Angeles. During the course of the investigation, IC3 linked another complaint to the victim company and provided that information to FBI Los Angeles as well. The information contained within the linked IC3 complaint was instrumental in providing probable cause for a search warrant and then used in the interview of a subject, which ultimately led to a full confession.

[5] International Investment Scam Details

Operation Wellspring (OWS) Initiative

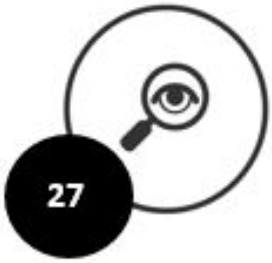
Operation Wellspring builds the cyber investigative capability and capacity of the state and local law enforcement community. Through close collaboration with FBI field offices, IC3 helps state and local law enforcement partners identify and respond to malicious cyber activity.

Key Components

- Serves as a national platform to receive, develop, and refer Internet-facilitated fraud complaints.
- Coordinates with FBI Cyber and Criminal components.
- Trains state and local law enforcement officers on cyber crime investigations.
- Addresses Internet-facilitated criminal cases not meeting most federal investigative thresholds by utilizing Cyber Task Force (CTF) state and local officers.

CTFs

The OWS Initiative was launched in August 2013 with the Salt Lake City CTF, in partnership with the Utah Department of Public Safety. Since then, OWS has expanded to 13 field offices: Albany, Buffalo, Kansas City, Knoxville, Las Vegas, New York City, New Orleans, Oklahoma City, Omaha–Des Moines, Phoenix, Richmond, Salt Lake City, and San Diego.



Total OWS Opened Investigations

The IC3 receives, on average, 800 complaints per day, and OWS offers CTFs a consistent resource to identify Internet fraud subjects and victims located throughout the world. As a result of OWS, 27 investigations were opened in 2017. Accomplishments included arrests, disruptions, convictions, indictments, and asset forfeitures. In addition, financial restitutions were obtained and criminals were sentenced.

Victim Complaints

The IC3 provided 289 referrals to 13 CTFs based on 1,867 victim complaints. The total victim loss associated with these complaints was approximately $15.7 million.

OWS Statistics[6]

[6]Accessibility description: images containing the number of Field Offices (13) involved with the OWS initiative, the number of opened investigations (27), and the number of victims (1,867).

OWS Success Stories

SAN DIEGO

Multiple victims reported on www.IC3.gov that they had been defrauded by the same subject over the internet. The victims shipped high end clothing and jewelry to the subject without receiving the agreed compensation. The subject broke off all communication after receiving the products. The Deputy District Attorney from the San Diego County District Attorney's Computer and Technology Crime High-Tech Response Team (CATCH) agreed to handle the case at the state level. The investigation included the execution of a physical search warrant and arrest at the suspect's home by members of the FBI San Diego CTF and members of the San Diego District Attorney's CATCH team. As a result of the search and arrest, investigators recovered stolen property and obtained a recorded interview in which the suspect admitted to the theft. The San Diego Regional Computer Forensics Laboratory (RCFL) was also used to analyze devices seized during the search warrant providing additional evidence for the case. The cooperative effort between IC3, the San Diego District Attorney's CATCH team, the San Diego RCFL and FBI San Diego CTF resulted in a theft conviction and the return of stolen property.

SAN DIEGO

This case involved the employee theft of approximately $25,000 worth of merchandise from a San Diego-based electronics internet retailer and the coordinated sale of the stolen items on a co-conspirator's auction website. A component of this case included an internet return fraud scheme in which the subjects purchased items from an online seller and later returned less valuable products for a refund. Working with the OWS Task Force, the Deputy District Attorney from the San Diego County District Attorney's CATCH agreed to handle the case at the state level. Analysis of search warrant returns showed the sale of the stolen items and the division of the proceeds between the two subjects. Both subjects admitted to the crimes during recorded interviews and were later arrested. Both subjects pled guilty to felony charges and were required to pay restitution to the victim.

KNOXVILLE

In the spring of 2016, Brandon Douglas Shanahan began impersonating a former, well-known University of Tennessee football player to extort and threaten multiple female victims. Utilizing a username posing as the player, Shanahan would threaten bodily harm and demand inappropriate photographs. Multiple victims were identified with similar reports of harassment during the investigation and through IC3 complaints. In June 2016, Shanahan was arrested and activities disrupted. Shanahan knowingly transmitted in interstate and foreign commerce with intent to extort money and other things of value. In December 2016, Shanahan entered a guilty plea on the count of interstate communications with the intent to extort. Shanahan broke his bond agreement, was re-arrested, and pled guilty to an additional count. Shanahan was sentenced to 30 months in a Federal Bureau of Prisons (BOP) Facility, followed by a one-year probation.

KNOXVILLE

Multiple victims reported to the IC3 that they had not received vehicles purchased and paid for via the internet. The IC3 aggregated the complaints, conducted independent research, and provided the information to the FBI Knoxville CTF. The resulting investigation determined Irvin Cachu-Melo and Luis Javier Martinez-Melo were operating as "money mules" in an on-going wire fraud scam involving the fraudulent sales of automobiles. Cachu-Melo and Martinez-Melo used stolen identities acquired by Martinez-Melo, to conduct wire transfers of the funds.

In 2017, The investigation determined Cachu-Melo was arrested and pled guilty to Conspiracy to Commit Money Laundering. Cachu-Melo was sentenced to 25 months in a BOP Facility along with three years of supervised release. Martinez-Melo was also arrested and pled guilty to Conspiracy to Commit Bank Fraud, Aggravated Identity Theft, and Conspiracy to Commit Wire Fraud. Martinez-Melo was sentenced to serve 57 months in a BOP Facility and is subject to 5 years of supervised release.

Hot Topics for 2017

Business Email Compromise

BEC is a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform wire transfer payments. The Email Account Compromise (EAC) variation of BEC targets individuals who regularly perform wire transfer payments. It should be noted while most BEC and EAC victims reported using wire transfers as their regular method of transferring business funds, some victims reported using checks. The fraudsters used the method most commonly associated with their victims' normal business practices. Both scams typically involve one or more fraudsters, who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Because the techniques used in the BEC and EAC scams have become increasingly similar, the IC3 began tracking these scams as a single crime type in 2017.

Fraudulent transfers conducted as a result of BEC and EAC have been routed through accounts in many countries with a large majority traveling through Asia.

BEC and EAC are constantly evolving as scammers become more sophisticated. In 2013, victims indicated the email accounts of Chief Executive Officers or Chief Financial Officers were hacked or spoofed, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. In 2014, victims reported personal email accounts were being compromised, and fraudulent requests for payment were sent to vendors identified out of their personal contact lists. In 2015, victims reported being contacted by subjects posing as lawyers or law firms instructing them to make secret or time sensitive wire transfers.

BECs may not always be associated with a request for transfer of funds. In 2016, the scam evolved to include the compromise of legitimate business email accounts and fraudulent requests for Personally Identifiable Information or Wage and Tax Statements commonly known as W-2 forms for employees. In 2017, the real estate sector was heavily targeted with many victims reporting losses during real estate transactions.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams. The victims of these scams are usually U.S.-based and may be recruited to illegally transfer money on behalf of others.

In 2017, the IC3 received 15,690 BEC/EAC complaints with adjusted losses of over $675 million.

Ransomware

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing.

In one scenario, spear phishing emails are sent to end users resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, typically in virtual currency such as Bitcoin. The actor will purportedly provide an avenue to the victim to regain access to their data once the ransom is paid.

Recent iterations target specific organizations and their employees, making awareness and training a critical preventative measure.

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance.

In 2017, the IC3 received 1,783 complaints identified as ransomware with adjusted losses of over $2.3 million.

Tech Support Fraud

Tech Support Fraud is a widespread scam in which criminals claim to provide customer, security, or technical support in an effort to defraud unwitting individuals and gain access to the individuals' devices. There are many variations of this scam, and criminals are constantly changing their tactics to continue the fraud. For example, in addition to telephone calls, pop-up and locked screens, search engine advertising, and URL hijacking/typosquatting, criminals now use phishing emails with malicious links or fraudulent account charges to lure their victims. Criminals also pose as a variety of different security, customer, or technical support representatives and offer to resolve any number of issues, including compromised email, bank accounts, computer viruses, or offer to assist with software license renewal. Some recent complaints involve criminals posing as technical support representatives for income tax assistance, GPS, printer, or cable companies, or support for virtual currency exchanges. In some variations, criminals pose as government agents, who offer to recover losses related to tech support fraud schemes or request financial assistance with "apprehending" criminals.

The "fake refund" variation of tech support fraud is increasing in reports and losses. In this scheme, the criminal contacts the victim offering a refund for tech support services previously rendered. The criminal pretends to refund too much money to the victim's account and requests the victim return the difference. The "refund and return" process can occur multiple times, resulting in the victim potentially losing thousands of dollars.

During this scheme, if the criminal can connect to the victim's devices, the criminal will download the victim's personal files containing financial accounts, passwords, and personal data, like health records, social security numbers, and tax information. The information is used to request bank transfers or open new accounts to accept and process unauthorized payments. Criminals will also send phishing emails to the victim's personal contacts from the victim's computer.

Additional information, explanations, and suggestions for protection regarding tech support fraud is available in a recently published Tech Support Fraud Public Service Announcement[7] on the IC3 website.

In 2017, the IC3 received 10,949 complaints related to tech support fraud. The claimed losses amounted to nearly $15 million, which represented a 90% increase in losses from 2016. While a majority of tech support fraud involves victims in the U.S., IC3 has received complaints from victims in 85 different countries.

[7] Federal Bureau of Investigation. Internet Crime Complaint Center. Tech Support Fraud Public Service Announcement

Elder Justice Initiative

On February 22, 2018, in response to a coordinated sweep of elder fraud cases, Attorney General Jeff Sessions stated "The Justice Department and its partners are taking unprecedented, coordinated action to protect elderly Americans from financial threats, both foreign and domestic … When criminals steal the hard-earned life savings of older Americans, we will respond with all the tools at the Department's disposal – criminal prosecutions to punish offenders, civil injunctions to shut the schemes down, and asset forfeiture to take back ill-gotten gains … I have directed Department prosecutors to coordinate with both domestic law enforcement partners and foreign counterparts to stop these criminals from exploiting our seniors."[8] The mission of the Elder Justice Initiative is to support and coordinate the Department's enforcement and programmatic efforts to combat elder abuse, neglect and financial fraud and scams that target our nation's seniors. We engage in this work by focusing on the following mission areas:

Building local, state, and federal capacity to fight elder abuse: Providing targeted training and resources to elder justice professionals including: prosecutors, law enforcement, judges, victim specialists, first responders, civil legal aid employees and multi-disciplinary teams to enhance their ability to respond to elder abuse efficiently and effectively.

Promoting justice for older Americans: Investigating and prosecuting financial scams targeting older adults. Promoting greater local, state, and federal coordination to resolve cases where long-term care entities provide grossly substandard care to their residents or patients.

Supporting research to improve elder abuse policy and practice: Promoting foundational research into elder abuse and financial exploitation in order to transform the practice of professionals in ways that positively impact the lives of older adults.

Helping older victims and their families: Connecting older adults and their families or caregivers with appropriate investigative agencies, as well as empowering them with information about abuse and recovering from its effects.

Further information is available at the DOJ Elder Justice Initiative website.[9] The US Senate Special Committee on Aging provides additional information in their publication, "Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors".[10]

In 2017, the IC3 received 49,523 complaints from victims over the age of 60 with adjusted losses in excess of $342 million.

[8]U.S. Department of Justice. Protecting Elderly Americans From Financial Threats
[9]Elder Justice Initiative. DOJ Elder Justice Initiative Website
[10] U.S. Senate Special Committee on Aging. Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors

Extortion

Extortion occurs when a criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is used in various schemes reported to the IC3, including Denial of Service attacks, hitman schemes,[11] sextortion,[12] government impersonation schemes, loan schemes,[13] and high-profile data breaches.[14] Virtual currency is commonly demanded as the payment mechanism because it provides the criminal an additional layer of anonymity when perpetrating these schemes.

In 2017, the IC3 received 14,938 extortion-related complaints with adjusted losses of over $15 million.

[11] A *hitman scheme* involves an email extortion in which a perpetrator sends a disturbing email threatening to kill a victim and/or their family. The email instructs the recipient to pay a fee to remain safe and avoid having the hit carried out.

[12] *Sextortion* occurs when a perpetrator threatens to distribute an individual's private and sensitive material unless the individual provides the perpetrator images of a sexual nature, sexual favors, or money.

[13] A *loan scheme* involves perpetrators contacting victims claiming to be debt collectors from a legitimate company and instructing victims to pay fees in order to avoid legal consequences.

[14] A *high profile data breach* is when sensitive, protected or confidential data belonging to a well-known or established organization is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

2017 Overall Statistics [15]

Important Stats

 # Of Complaints Reported Since Inception ('00)
4,063,933

Approximately 284,000
Average Complaints Received Each Year

$1.42 Billion
Victim Losses in 2017

Over 800
Average Complaints Received Per Day

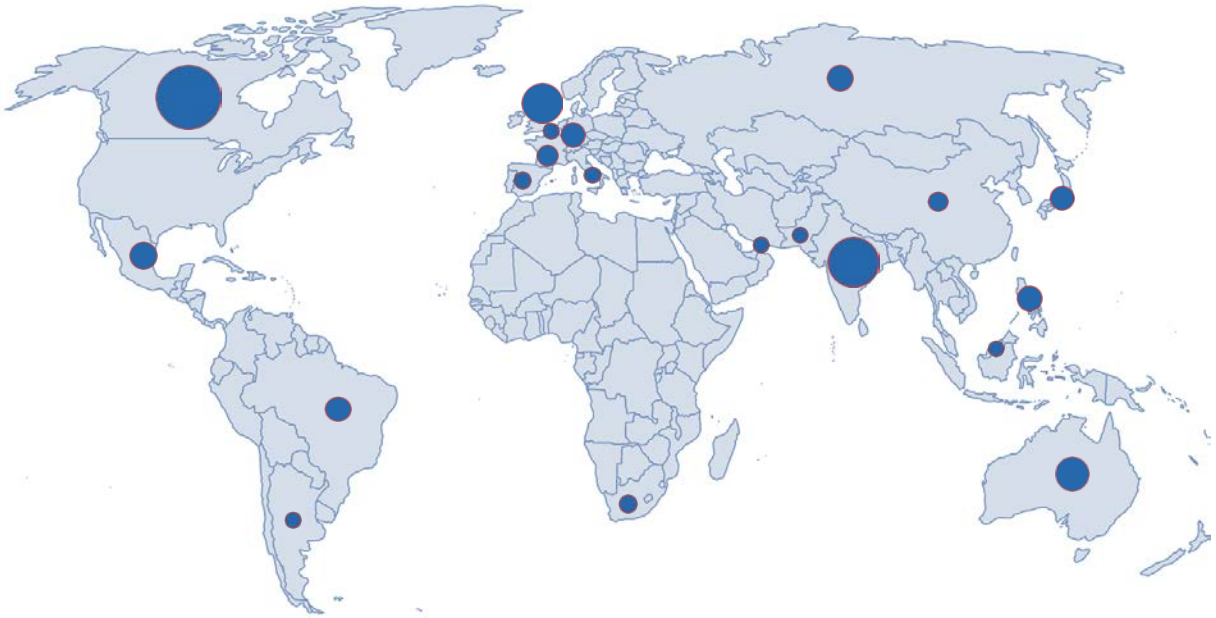
2017 Victims by Age Group

Victims		
Age Range[16]	Total Count	Total Loss
Under 20	9,053	$8,271,311
20 - 29	41,132	$67,981,630
30 - 39	45,458	$156,287,698
40 - 49	44,878	$244,561,364
50 - 59	43,764	$275,621,946
Over 60	49,523	$342,531,972

[15] Accessibility description: image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints for the years 2013 to 2017. The total number of complaints received since the year 2000 is 4,063,933. IC3 receives approximately 284,000 complaints each year, or more than 800 per day.
[16] Not all complaints include an associated age range—those without this information are excluded from this table.

Top 20 Foreign Countries by Victim

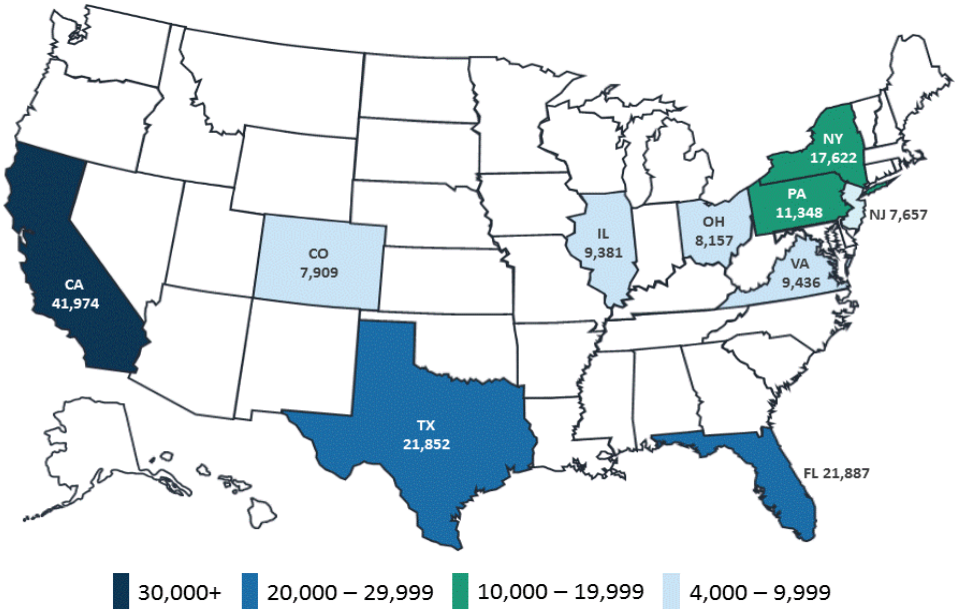
Excluding the United States[17]



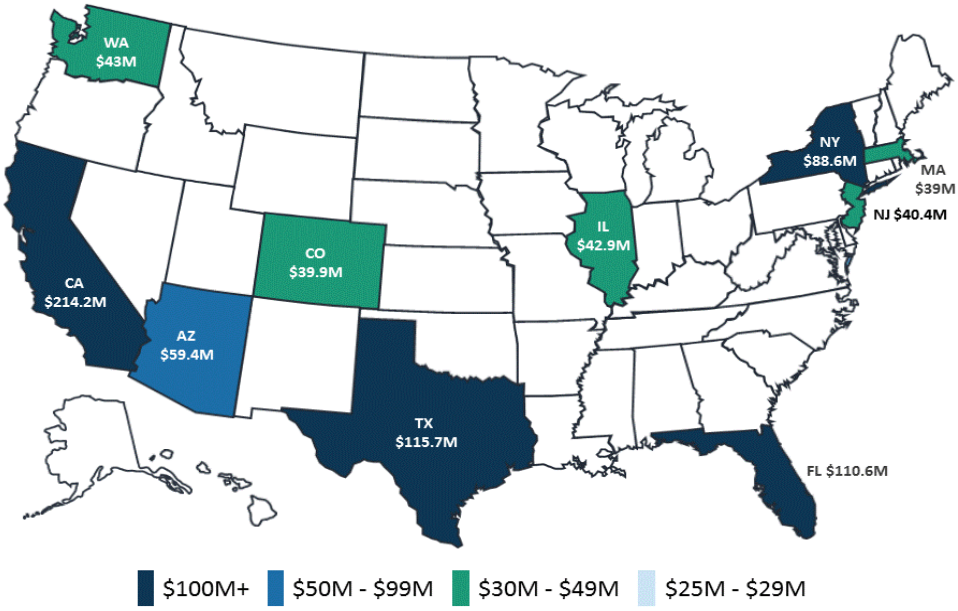
1. Canada	3,164	6. Russian Federation	594	11. France	368	16. Netherlands	266
2. India	2,819	7. Brazil	558	12. China	366	17. Malaysia	265
3. United Kingdom	1,383	8. Germany	466	13. South Africa	349	18. United Arab Emirates	259
4. Australia	989	9. Philippines	453	14. Italy	291	19. Spain	248
5. Mexico	632	10. Japan	413	15. Pakistan	276	20. Argentina	238

[17] Accessibility description: image includes a world map with circles corresponding in size to the total number of reports received from specific countries. The top twenty countries are indicated. Specific statistics for each country ranked in descending order of victim figures can be found in the text table immediately below the image.

Top 10 States by Number of Victims [18]



Top 10 States by Victim Loss [19]



[18] Accessibility description: image depicts the United States, with the top ten states (based on reported victims) highlighted. These include California (41,974), Florida (21,887), Texas (21,852), New York (17,622), Pennsylvania (11,348), Virginia (9,436), Illinois (9,381), Ohio (8,157), Colorado (7,909), and New Jersey (7,657).

[19] Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California ($214.2M), Texas (115.7M) Florida ($110.6M), New York ($88.6M), Arizona ($59.4M), Washington ($43M), Illinois ($42.9M), New Jersey ($40.4M), Colorado ($39.9M), and Massachusetts ($39M).

2017 Crime Types

By Victim Count			
Crime Type	**Victims**	**Crime Type**	**Victims**
Non-Payment/Non-Delivery	84,079	Misrepresentation	5,437
Personal Data Breach	30,904	Corporate Data Breach	3,785
Phishing/Vishing/Smishing/Pharming	25,344	Investment	3,089
Overpayment	23,135	Malware/Scareware/Virus	3,089
No Lead Value	20,241	Lottery/Sweepstakes	3,012
Identity Theft	17,636	IPR/Copyright and Counterfeit	2,644
Advanced Fee	16,368	Ransomware	1,783
Harassment/Threats of Violence	16,194	Crimes Against Children	1,300
Employment	15,784	Denial of Service/TDoS	1,201
BEC/EAC	15,690	Civil Matter	1,057
Confidence Fraud/Romance	15,372	Re-shipping	1,025
Credit Card Fraud	15,220	Charity	436
Extortion	14,938	Health Care Related	406
Other	14,023	Gambling	203
Tech Support	10,949	Terrorism	177
Real Estate/Rental	9,645	Hacktivist	158
Government Impersonation	9,149		

Descriptors*		
Social Media	19,986	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	4,139	

2017 Crime Types *Continued*

By Victim Loss			
Crime Type	**Loss**	**Crime Type**	**Loss**
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/ Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/ Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

		Descriptors*
Social Media	$56,478,483	*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected.
Virtual Currency	$58,391,810	

2017 Overall State Statistics

Count by Victim per State*					
Rank	State	Victims	Rank	State	Victims
1	California	41,974	30	Connecticut	2,662
2	Florida	21,887	31	Utah	2,260
3	Texas	21,852	32	Hawaii	1,923
4	New York	17,622	33	Mississippi	1,799
5	Pennsylvania	11,348	34	Kansas	1,767
6	Virginia	9,436	35	Arkansas	1,753
7	Illinois	9,381	36	Iowa	1,533
8	Ohio	8,157	37	Alaska	1,418
9	Colorado	7,909	38	New Mexico	1,415
10	New Jersey	7,657	39	Idaho	1,186
11	Washington	7,505	40	District of Columbia	1,143
12	North Carolina	7,316	41	Nebraska	1,140
13	Georgia	7,007	42	New Hampshire	1,106
14	Maryland	6,789	43	West Virginia	1,085
15	Arizona	6,417	44	Delaware	759
16	Michigan	6,400	45	Maine	740
17	Wisconsin	5,245	46	Montana	737
18	Massachusetts	5,221	47	Rhode Island	704
19	Tennessee	4,779	48	Puerto Rico	605
20	Nevada	4,675	49	Vermont	451
21	Missouri	4,187	50	Wyoming	434
22	Indiana	4,067	51	South Dakota	404
23	Alabama	3,865	52	North Dakota	355
24	South Carolina	3,687	53	Guam	66
25	Minnesota	3,619	54	U.S. Minor Outlying Islands	51
26	Oregon	3,455	55	U.S. Virgin Islands	48
27	Louisiana	3,319	56	American Samoa	17
28	Oklahoma	2,809	57	Northern Marina Islands	13
29	Kentucky	2,740			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Loss by Victim per State*					
Rank	**State**	**Loss**	**Rank**	**State**	**Loss**
1	California	$214,217,307	**30**	Alabama	$9,949,873
2	Texas	$115,680,902	**31**	Idaho	$7,657,726
3	Florida	$110,620,330	**32**	Kentucky	$7,220,342
4	New York	$88,633,788	**33**	Mississippi	$6,786,910
5	Arizona	$59,366,635	**34**	Kansas	$5,045,755
6	Washington	$42,991,213	**35**	Arkansas	$4,823,489
7	Illinois	$42,894,106	**36**	New Mexico	$4,716,033
8	New Jersey	$40,441,739	**37**	Nebraska	$4,286,773
9	Colorado	$39,935,041	**38**	Iowa	$4,013,395
10	Massachusetts	$38,962,867	**39**	New Hampshire	$3,725,739
11	Georgia	$38,353,746	**40**	Rhode Island	$3,390,078
12	Pennsylvania	$36,319,408	**41**	Hawaii	$3,368,323
13	Virginia	$35,438,537	**42**	District of Columbia	$2,707,684
14	Ohio	$30,672,149	**43**	Montana	$2,553,804
15	Maryland	$30,045,488	**44**	South Dakota	$2,472,062
16	Michigan	$25,362,646	**45**	West Virginia	$2,435,608
17	North Carolina	$22,203,108	**46**	Delaware	$2,376,718
18	Nevada	$19,578,132	**47**	Wyoming	$2,331,692
19	Missouri	$19,475,647	**48**	North Dakota	$2,006,821
20	Minnesota	$19,126,165	**49**	Alaska	$1,709,126
21	Wisconsin	$15,787,242	**50**	Puerto Rico	$1,590,979
22	Tennessee	$13,561,295	**51**	Maine	$1,310,506
23	Indiana	$13,228,744	**52**	Vermont	$1,291,941
24	South Carolina	$13,048,133	**53**	Guam	$819,163
25	Connecticut	$12,465,243	**54**	U.S. Virgin Islands	$625,169
26	Oklahoma	$11,671,198	**55**	U.S. Minor Outlying Islands	$61,445
27	Oregon	$11,165,342	**56**	Northern Mariana Islands	$21,320
28	Louisiana	$10,696,284	**57**	American Samoa	$2,200
29	Utah	$10,302,892			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Count by Subject per State*					
Rank	State	Subjects	Rank	State	Subjects
1	California	14,786	30	District of Columbia	873
2	Texas	8,785	31	Delaware	821
3	Florida	8,709	32	Utah	785
4	New York	7,162	33	Wisconsin	716
5	Virginia	3,795	34	Kentucky	701
6	Illinois	3,627	35	Connecticut	677
7	Georgia	3,228	36	Mississippi	677
8	Maryland	3,161	37	Montana	673
9	New Jersey	2,876	38	Iowa	621
10	Washington	2,514	39	Arkansas	510
11	Ohio	2,384	40	West Virginia	372
12	Pennsylvania	2,361	41	North Dakota	318
13	Nebraska	2,153	42	New Mexico	304
14	Nevada	2,082	43	Idaho	280
15	Arizona	1,874	44	Maine	264
16	Michigan	1,868	45	Alaska	252
17	North Carolina	1,817	46	Hawaii	234
18	Louisiana	1,717	47	Rhode Island	212
19	Tennessee	1,473	48	New Hampshire	186
20	Colorado	1,400	49	Wyoming	154
21	Massachusetts	1,392	50	South Dakota	139
22	Missouri	1,355	51	Puerto Rico	115
23	South Carolina	1,193	52	Vermont	77
24	Oregon	1,192	53	U.S. Minor Outlying Islands	18
25	Indiana	1,148	54	U.S. Virgin Islands	15
26	Oklahoma	1,101	55	Guam	9
27	Minnesota	1,030	56	American Samoa	5
28	Alabama	1,022	57	Northern Mariana Islands	5
29	Kansas	953			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

2017 Overall State Statistics *Continued*

Subject Earnings per Destination State*					
Rank	State	Loss	Rank	State	Loss
1	California	$83,676,865	30	Kansas	$3,185,500
2	Texas	$70,647,821	31	District of Columbia	$2,931,263
3	Florida	$47,274,025	32	Utah	$2,634,496
4	New York	$39,107,593	33	Arkansas	$2,631,804
5	Georgia	$22,691,044	34	Iowa	$2,367,889
6	Illinois	$17,081,877	35	Wisconsin	$2,254,829
7	Ohio	$16,646,002	36	Mississippi	$2,253,167
8	New Jersey	$11,424,449	37	New Hampshire	$1,989,281
9	Maryland	$11,309,325	38	Kentucky	$1,957,108
10	Nevada	$11,077,774	39	Montana	$1,924,196
11	Washington	$9,654,732	40	Delaware	$1,616,234
12	Pennsylvania	$9,516,714	41	New Mexico	$1,464,315
13	Virginia	$9,457,095	42	Maine	$1,298,749
14	Michigan	$8,437,965	43	Idaho	$1,237,269
15	North Carolina	$8,357,577	44	Rhode Island	$1,119,321
16	Colorado	$8,052,578	45	Hawaii	$947,310
17	Arizona	$6,792,467	46	North Dakota	$865,639
18	Oklahoma	$6,636,529	47	West Virginia	$770,919
19	Massachusetts	$6,588,675	48	South Dakota	$756,336
20	Oregon	$5,866,936	49	Wyoming	$711,958
21	Nebraska	$5,150,696	50	Vermont	$536,348
22	Connecticut	$4,674,297	51	Alaska	$446,294
23	Louisiana	$4,585,139	52	Puerto Rico	$340,309
24	Indiana	$4,539,775	53	North Mariana Islands	$181,180
25	Minnesota	$4,314,856	54	U.S. Minor Outlying Islands	$131,727
26	South Carolina	$3,985,279	55	American Samoa	$8,370
27	Tennessee	$3,764,353	56	U.S. Virgin Islands	$5,854
28	Missouri	$3,522,518	57	Guam	$4,977
29	Alabama	$3,429,023			

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information.

Appendix A: Crime Type Definitions

419/Overpayment: "419" refers to the section in Nigerian law regarding con artistry and fraud and is associated with requests for help facilitating the transfer of money. The sender of the "419" letter or email offers the recipient a commission or share in the profits of a transfer of money, but will first request the recipient send money to pay for some of the costs associated with the transfer. The recipient may be sent a payment and instructed to keep a portion of the payment, but send the rest on to another individual or business.

Advanced Fee: In advance fee schemes, the perpetrator informs a victim that the victim has qualified for a large financial loan or has won a large financial award, but must first pay the perpetrator taxes or fees in order to access the loan or award. The victim pays the advance fee, but never receives the promised money.

Auction: A fraudulent transaction or exchange that occurs in the context of an online auction site.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Charity: Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.

Civil Matter: Civil lawsuits are any disputes formally submitted to a court that is not criminal.

Confidence/Romance Fraud: A perpetrator deceives a victim into believing the perpetrator and the victim have a trust relationship, whether family, friendly or romantic. As a result of that belief, the victim is persuaded to send money, personal and financial information, or items of value to the perpetrator or to launder money on behalf of the perpetrator. Some variations of this scheme are romance/dating scams or the grandparent's scam.

Corporate Data Breach: A leak or spill of business data that is released from a secure location to an untrusted environment. It may also refer to a data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Credit Card: Credit card fraud is a wide-ranging term for fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Criminal Forums: A medium where criminals exchange ideas and protocols relating to intrusion.

Denial of Service: An interruption of an authorized user's access to any system or network, typically caused with malicious intent.

Employment: An individual believes they are legitimately employed, and loses money or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

Government Impersonation: A government official is impersonated in an attempt to collect money.

Hacktivist: A computer hacker whose activity is aimed at promoting a social or political cause.

Harassment/Threats of Violence: Harassment occurs when a perpetrator uses false accusations or statements of fact to intimidate a victim. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

Health Care Related: A scheme attempting to defraud private or government health care programs, usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or may involve medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums or social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The theft and illegal use of others' ideas, inventions, and creative expressions, to include everything from trade secrets and proprietary products to parts to movies, music, and software.

Identity Theft/Account Takeover: Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud. Account Takeover is when a perpetrator obtains account information to perpetrate fraud on existing accounts.

Investment: Deceptive practice that induces investors to make purchases on the basis of false information. These scams usually offer the victims large returns with minimal risk. Variations of this scam include retirement schemes, Ponzi schemes and pyramid schemes.

Lottery/Sweepstakes: An individual is contacted about winning a lottery or sweepstakes they never entered and are asked to pay a tax or fee in order to receive their winnings.

Malware/Scareware: Software intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds.

Misrepresentation: Merchandise or services were purchased or contracted by individuals online for which the purchasers provided payment. The goods or services received were of a measurably lesser quality or quantity than was described by the seller.

No Lead Value: Incomplete complaints which do not allow a crime type to be determined.

Non-Payment/Non-Delivery: In non-payment situations, goods and services are shipped, but payment is never rendered. In non-delivery situations, payment is sent, but goods and services are never received.

Other: Other types of fraud not listed.

Personal Data Breach: A leak or spill of personal data that is released from a secure location to an untrusted environment. It may also refer to a security incident in which an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual.

Phishing/Vishing/Smishing/Pharming: Unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

Ransomware: A type of malicious software designed to block access to a computer system until money is paid.

Re-shipping: Individuals receive packages purchased through fraudulent means and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Fraud involving real estate, rental or timeshare property.

Social Media: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

Tech Support: Attempts to gain access to a victim's electronic device by falsely claiming to offer tech support, usually for a well-known company. Scammer asks for remote access to the victim's device to clean-up viruses or malware or to facilitate a refund for prior support services.

Terrorism: Violent acts intended to create fear that is perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants.

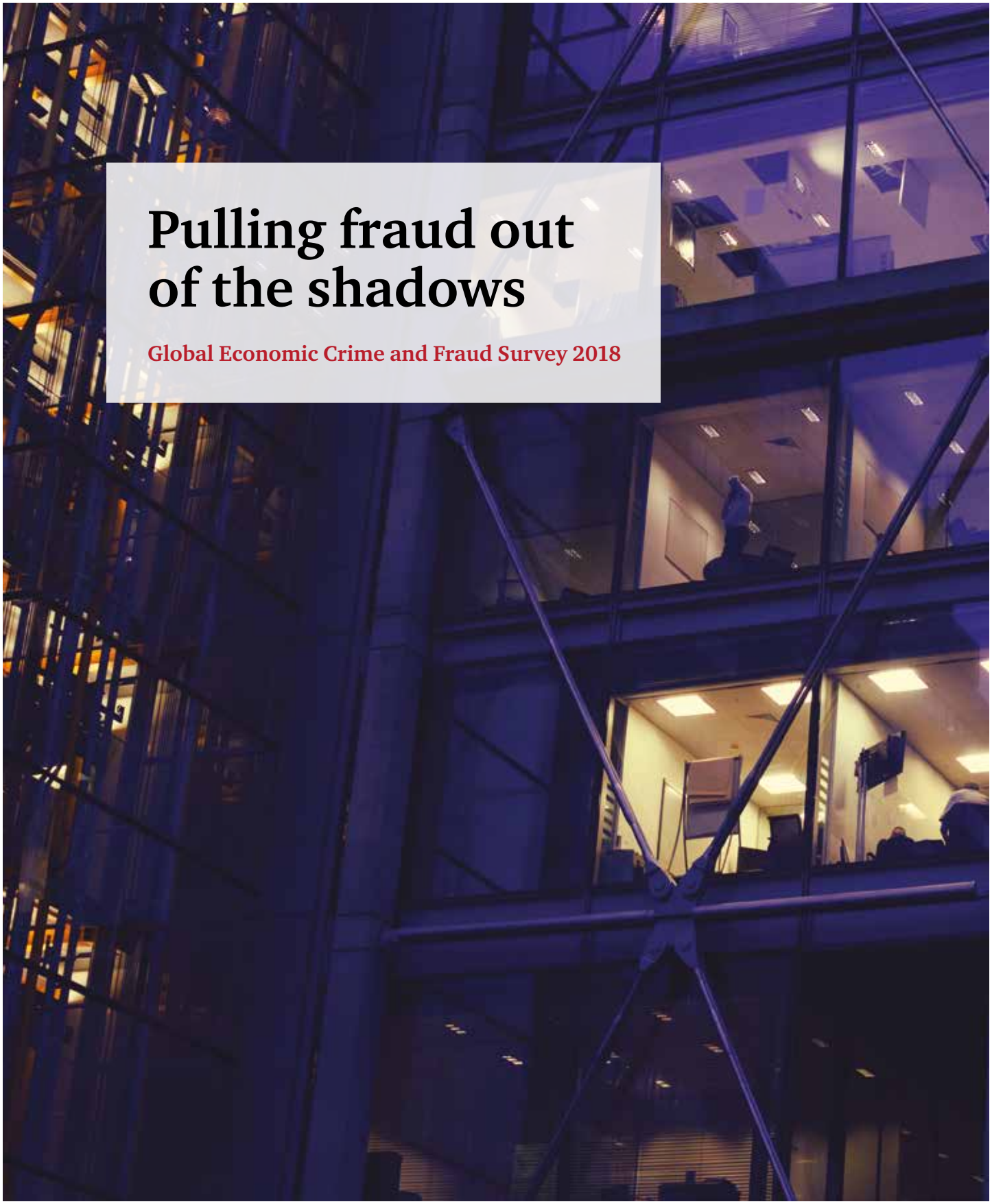
Virus: Code capable of copying itself and having a detrimental effect, such as corrupting the system or destroying data.

Virtual Currency: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.

Enclosure (4)

Price Waterhouse Coopers

Global Economic Crime and Fraud Report



Pulling fraud out of the shadows

Global Economic Crime and Fraud Survey 2018

pwc

www.pwc.com/fraudsurvey

Executive Summary

Didier Lavion
Principal, Global Economic Crime and Fraud Survey Leader, PwC US

In PwC's 2018 Global Economic Crime and Fraud Survey, only 49% of global organisations said they'd been a victim of fraud and economic crime. However, we know this number should be much higher. So, what about the other 51%?

The reality is, too few companies are fully aware of the fraud risks they face. That's why this year's Global Economic Crime and Fraud Survey, gathering valuable data from more than 7,200 respondents across 123 different territories, aims to pull fraud out from the shadows – and shed much-needed light on some of the most important strategic challenges confronting every organisation.

The biggest competitor you didn't know you had

Today, fighting fraud has moved front and centre to become a core business issue. Long gone are the days when it was viewed as an isolated incident of bad behaviour, a costly nuisance, or a mere compliance issue. That's because the scale and impact of fraud has grown so significantly in today's digitally enabled world. Indeed, it can almost be seen as a big business in its own right – one that is tech-enabled, innovative, opportunistic and pervasive. Think of it as the biggest competitor you didn't know you had.

It's not hard to see how we got here. On the one hand, technology has advanced in leaps and bounds, helping fraudsters become more strategic in their goals and more sophisticated in their methods. On the other hand, regulatory regimes in much of the world have become far more robust, with enforcement intensifying, often in cross-border cooperation. Moreover, in the face of well-publicised corruption and other corporate scandals, public expectations around the world are converging around common standards of transparency and accountability.

More and more companies, organisations and nation states are now recognising that corruption and fraud are holding them back from competing on the global stage – and have simply become too costly to ignore.

A perfect storm of risks

In this era of unparalleled public scrutiny, today's organisations face a perfect storm of fraud-related risks – internal, external, regulatory and reputational. The time is therefore right for them to adopt a new, more holistic view of fraud. One that recognises the true shape of the threat: not merely a cost of doing business, but a shadow industry which can impact every territory, every sector and every function. Since it hides in the shadows, a lack of fraud-awareness within an organisation is highly dangerous.

So, the important question is not: is your organisation the victim of fraud? Rather it's: are you aware of how fraud is touching your organisation? Are you fighting it blindfolded, or with eyes wide open?

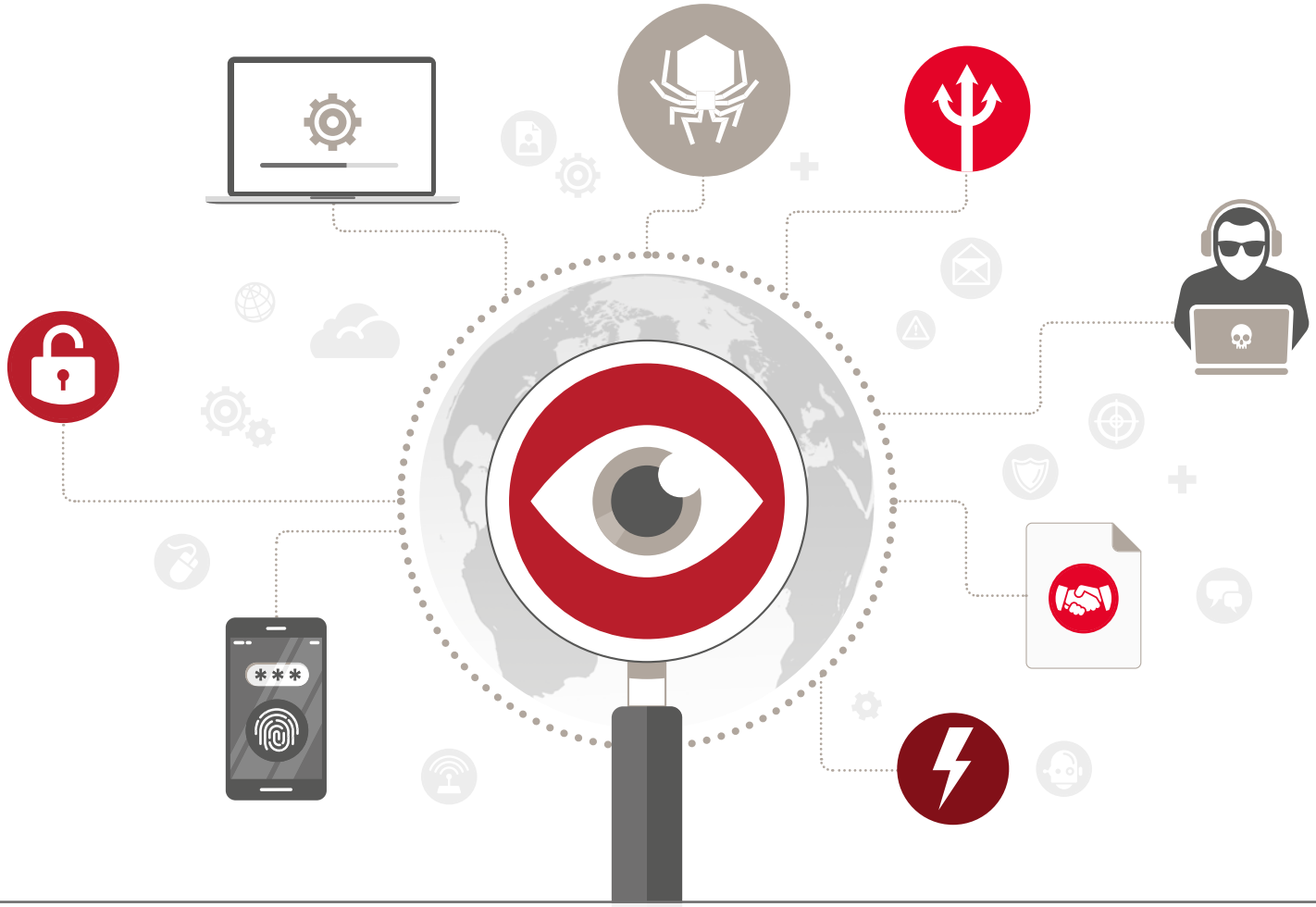
The fraud you don't see is as important as the fraud you do

PwC's 2018 Global Economic Crime and Fraud Survey shows that, while there is growing awareness of the perils of economic crime, too few companies are fully aware of the individual risks they face. This report sets out to plug that awareness gap. In it, we explore not only the visible fraud that companies say they are facing, but also the blind spots that stop them seeing the big picture – and what they can and should do about them.

So, what does our survey tell us about the steps your organisation can take today to fight fraud more effectively?

Four steps to fight fraud

Recognise fraud when you see it

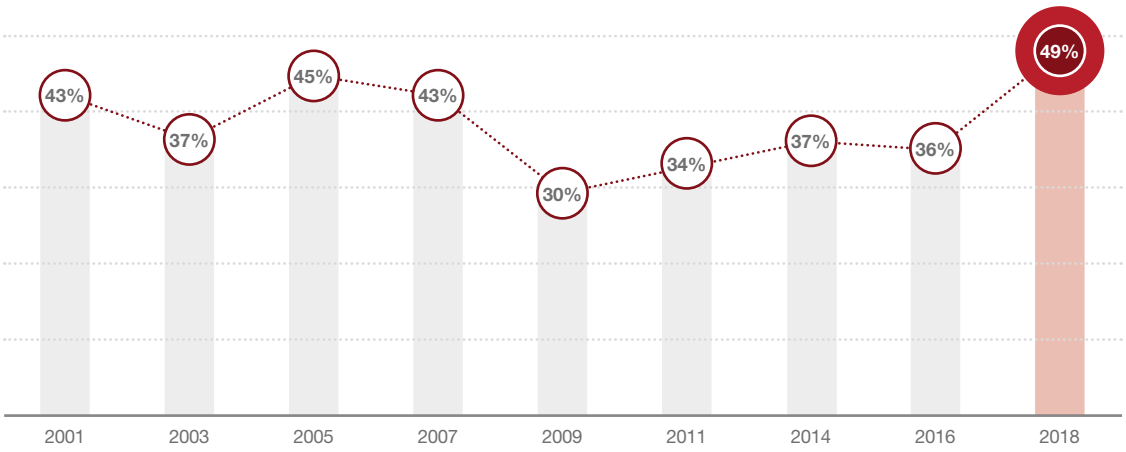


Is fraud really on the rise – or just our awareness of it?

This year, 49% of respondents to our Global Economic Crime and Fraud Survey said their companies had been victims of fraud or economic crime, up from 36% in 2016. This rise can be explained by a combination of growing global awareness of fraud, a larger number of survey responses, and greater clarity about what 'fraud' actually means. But every organisation – no matter how vigilant – is vulnerable to blind spots. And because those blind spots usually only become apparent with hindsight, throwing light onto them as early as possible can vastly enhance fraud-fighting efforts.

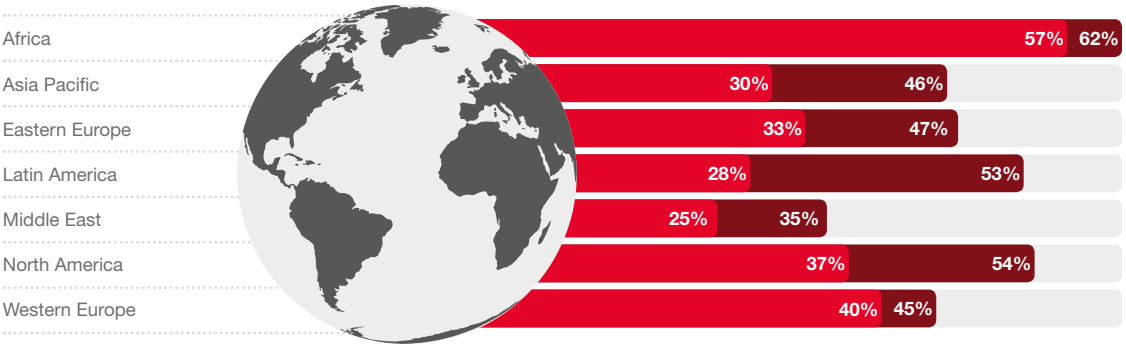
Companies today face a perfect storm of fraud risk – internal, external, regulatory and reputational

Exhibit 1: The reported rate of economic crime is on the rise



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 2: The reported rate of economic crime has increased across all territories



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Just as the reported rate of economic crime has increased since 2016, so has the amount that companies are spending to fight it:

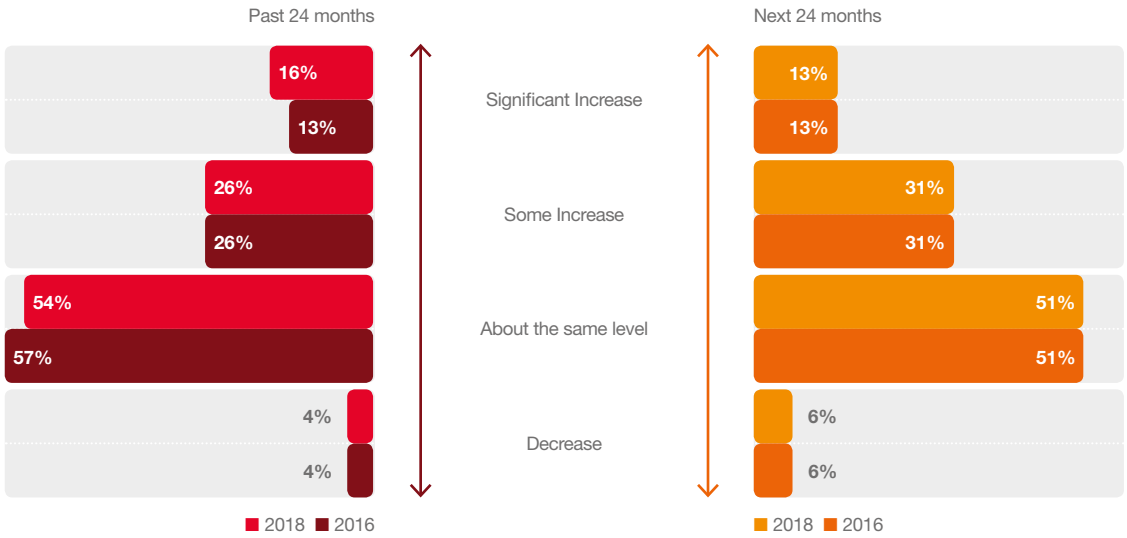
- 42% of respondents said their companies had increased spending on combatting fraud and economic crime over the past two years (up from 39% in 2016).
- 44% of respondents said they plan to boost spending over the next two years.

Where is this money being spent? Organisations are using ever-more powerful technology and data analytics tools to fight fraud. And, in addition to these technology-based controls, many are also expanding whistle-blower programmes and taking steps to keep leadership in the loop.

But do these measures represent a genuine shift to more proactive approaches to fraud and corruption? Or are they just a rear-guard action, driven principally by enhanced anti-bribery/anti-corruption legislation and increasingly globalised forms of enforcement? In other words, are we still missing something vital in the fight against fraud?

Our survey results strongly suggest we are.

Exhibit 3: Organisations continue to increase spending on combatting fraud



Q. How has/is your organisation adjusting the amount of funds used to combat fraud and/or economic crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

59%

of CEOs agree or strongly agree that organisations are currently experiencing increased pressure to hold individual leaders accountable for any organisational misconduct

Source: PwC's 21st CEO Survey

71%

of CEOs measure trust between their workforce and their organisation's senior leadership

Source: PwC's 21st CEO Survey

Fraud risk assessments are the first step in preventing fraud before it takes root

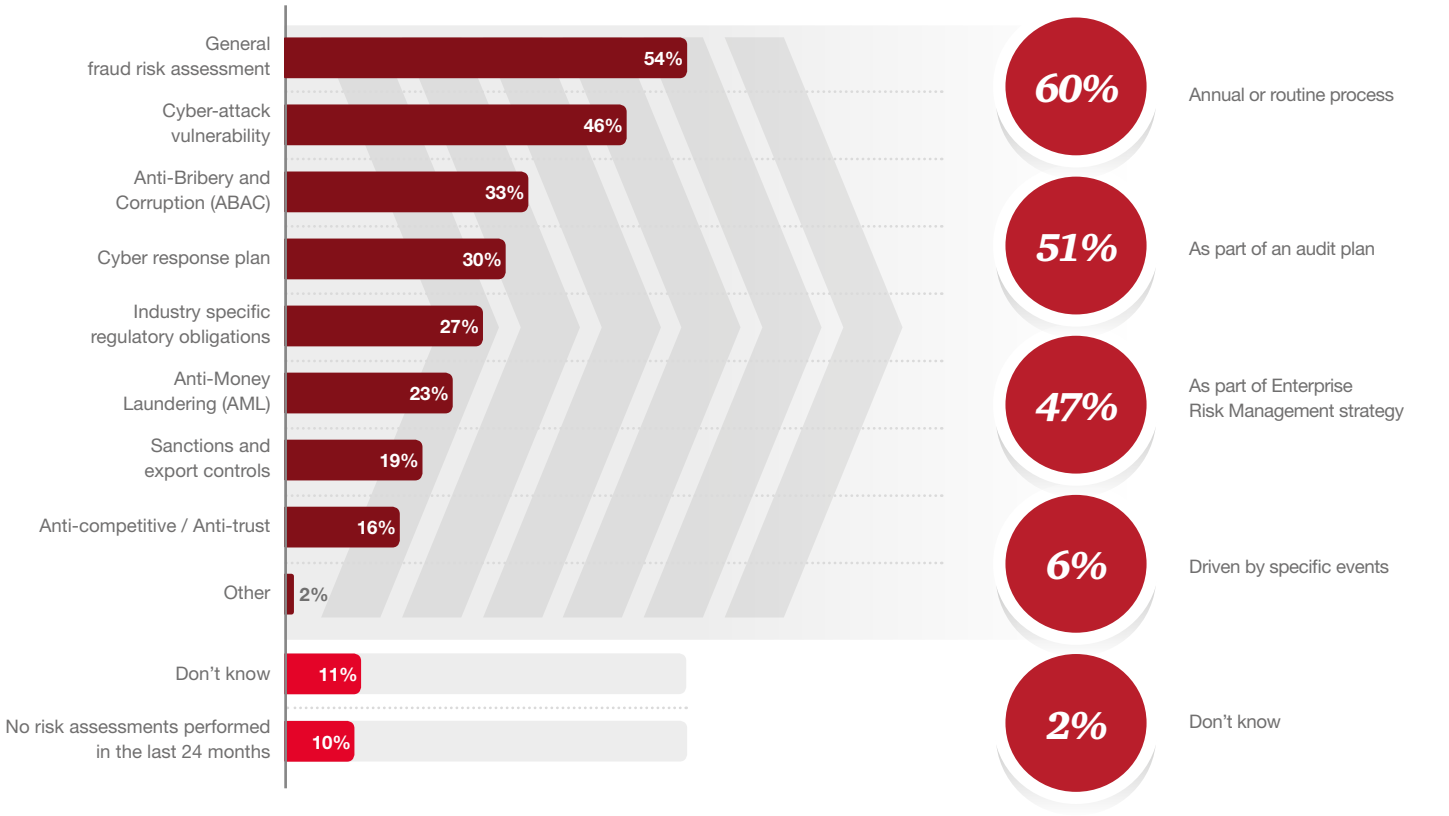
Despite the increase in spending, many organisations are still addressing fraud prevention by using a reactive, defensive approach:

- **Only 54% of global organisations said they have conducted a general fraud or economic crime risk assessment in the past 2 years.**
- Less than half said they had conducted a cybercrime risk assessment.
- Fewer than a third said their company performed risk assessments in the critical areas of anti-bribery and corruption, anti-money laundering, or sanctions and export controls.
- **One in ten respondents had not performed any risk assessments at all in the past 2 years.**

However, the rules of the game are changing profoundly and irreversibly. Public tolerance for corporate and/or personal misbehaviour is vanishing. Not only is sensitivity to corporate misconduct at an all-time high, some corporations and leaders are also now being held to account for past behaviour, conducted when the 'unspoken rules' of doing business might have been thought to be different. PwC's 21st CEO Survey underscores this theme: in it, chief executives cite trust and leadership accountability as two of the most significant threats to business growth.

This points to a heightened risk when fraud or economic crime spills into public view – and a greater need for organisations to take a lead in preventing fraud before it can take root. Fraud risk assessments can help organisations do so by identifying the specific frauds they need to look for. Moreover, these assessments are increasingly looked on favourably by regulators in enforcement actions.

Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years



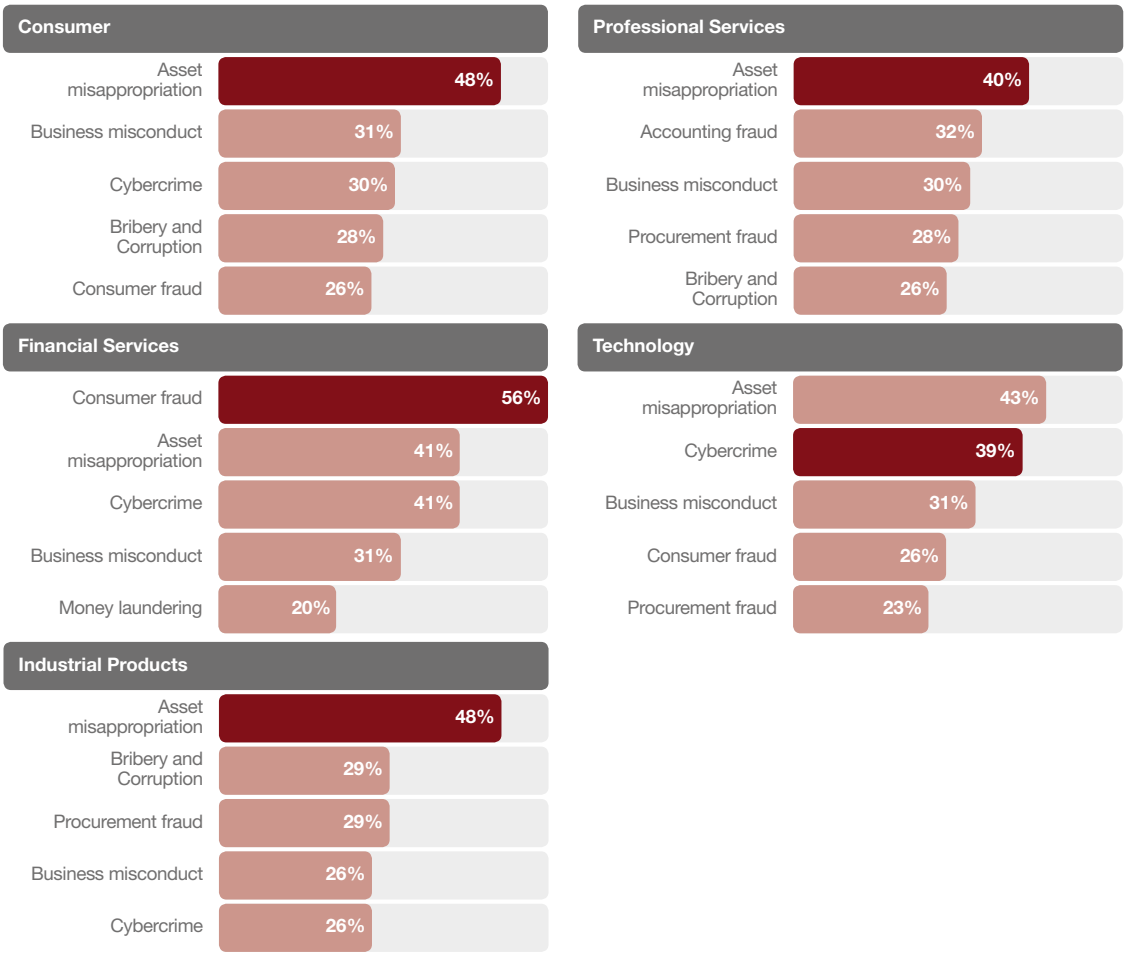
Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Q. What prompted your organisation to perform a risk assessment?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 5: Asset misappropriation, consumer fraud and cybercrime were the most frequently reported frauds across industries



Q. What type of fraud and/or economic crime has your organisation experienced in your country within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Conduct risk: the 'hidden risk' behind many internal frauds

Two types of fraud – consumer fraud and business misconduct – have grown in prominence to such an extent that this year's survey is measuring them as separate threats for the first time. Of the respondents who indicated their companies had experienced fraud in the last two years, 29% said they had suffered from consumer fraud and 28% said they had suffered from business misconduct (making these, respectively, the 3rd and 4th most frequently reported frauds this year, behind asset misappropriation at 45% and cybercrime at 31%). It should be noted that the significant decrease in reported incidents of asset misappropriation (down from 64% in 2016) is at least partly explained by the inclusion of these new frauds in the survey.

These methodological changes reflect the growing recognition of a broad category of internal fraud risk: "conduct risk". This is the risk that employee actions will imperil the delivery of fair customer outcomes or market integrity. And, unlike operational breakdowns or external threats (which can often be checked by internal controls), conduct risk requires a more holistic response – and a shift in attitude.

At present, many companies treat compliance, ethics and enterprise risk management as separate functions – sometimes they even exist in separate siloes within an organisation. But, like all organisational silos, this means these functions rarely add up to a strategic whole. The parts of an organisation that investigate fraud, the parts that manage the risk of fraud, and the parts that report fraud to the board or regulators become disjointed.

When that happens, operational gaps can emerge and fraud can too easily be brushed under the carpet or seen as someone else's problem – to the detriment of the overall effectiveness of fraud prevention, financial performance and regulatory outcomes.

A more innovative approach is to reframe these functions as components of conduct risk. It enables a company to better measure and manage compliance, ethics and risk management horizontally and embed them in its strategic decision-making process. It also means fraud and ethical breaches can be approached more dispassionately, with less emotion, as a fact of life that every organisation has to deal with. Moreover, adopting this more systemic – and realistic – stance towards conduct risk can enable cost efficiencies between ethics, fraud and anti-corruption compliance programmes. It is an important step in breaking down the silos between key anti-fraud functions – and pulling fraud out of the shadows.

Looking for fraud in the right places

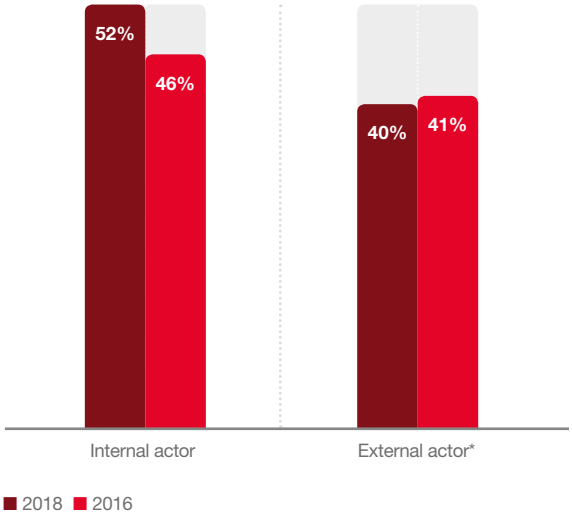
Our survey revealed a significant increase in the share of economic crime committed by internal actors (from 46% in 2016 to 52% in 2018) and a dramatic increase in the proportion of those crimes attributed to senior management (from 16% in 2016 to 24% in 2018). Indeed, internal actors were a third more likely than external actors to be the perpetrators of the most disruptive frauds.

However, one of a company's biggest fraud blind spots – and biggest threats – is often not to do with its employees, but rather the people it does business with. These are the third parties with whom companies have regular and profitable relationships: agents, vendors, shared service providers and customers. In other words, the people and organisations with whom a certain degree of mutual trust is expected, but who may actually be stealing from the company.

24%

of reported internal frauds were committed by senior management

Exhibit 6: Internal actors are the main perpetrators of fraud

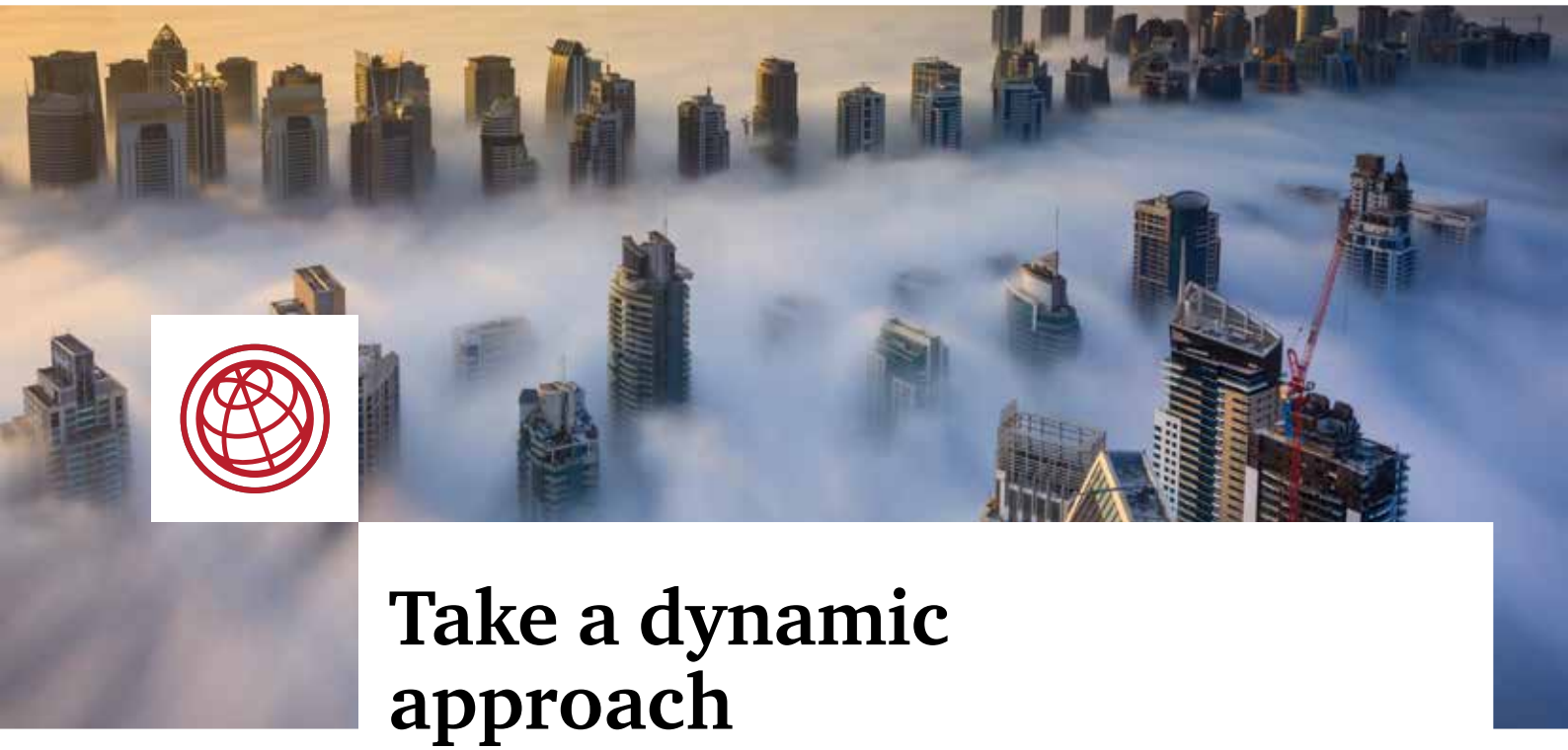


***68%**

of external actors committing the fraud are 'frenemies' of the organisation – agents, vendors, shared service providers and customers

Q. Who was the main perpetrator of the most disruptive fraud?

Source: PwC's 2018 Global Economic Crime and Fraud Survey



Take a dynamic approach

Chief executives are accountable

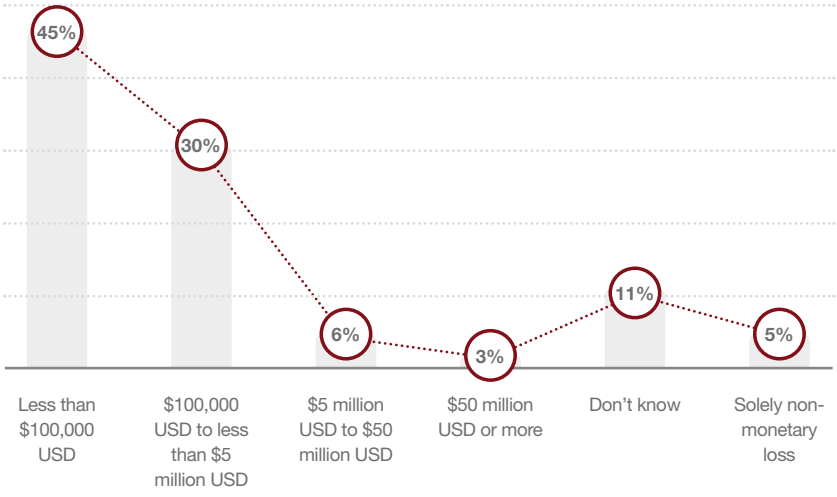
Our survey underscores that the direct monetary cost of fraud and its aftermath can be substantial. But when secondary costs (such as investigations and other interventions) are included, the true picture of overall cost can be much higher.

46%

of respondents said their organisation spent the same or more on investigations and other interventions than was directly lost to fraud itself

When the financial costs of fraud hit the bottom line of a business, it is only natural for the board and shareholders to require explanations from senior management. In today's world, however, a leader's responsibility doesn't stop there. In fact, that's just the beginning.

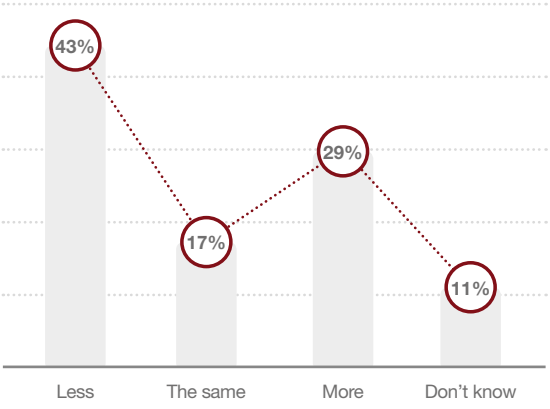
Exhibit 7: Direct monetary losses due to fraud can be substantial



Q. In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 8: The amount spent on investigations and other interventions as a result of fraud is significant



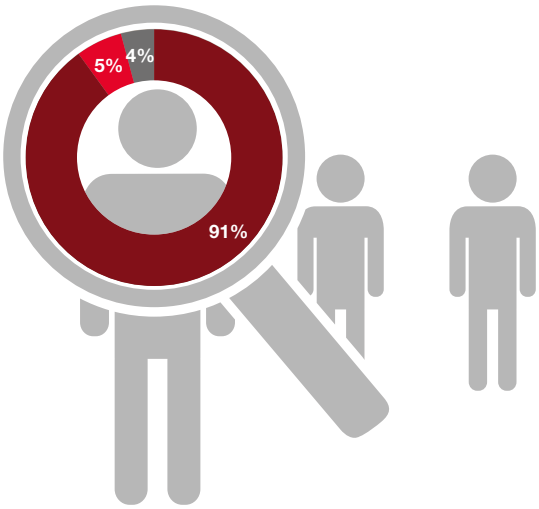
Q. As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

A chief executive is increasingly seen as the personal embodiment of an organisation – with their finger on the pulse of every facet of its culture and operations at all times. So, when ethical or compliance breakdowns happen, these individuals are often held personally responsible – both by the public and, increasingly, by regulators. Whether merited or not, one thing is clear: the C-suite can no longer claim ignorance as an excuse.

Our survey shows that in nine in every ten cases, the most serious incidents of fraud have been brought to the attention of senior management. In addition, 17% of respondents indicated that the CEO has primary responsibility for their organisation's ethics and compliance programme. This puts a sharp spotlight on how the front office is managing the crisis – and the extent to which they are (or are not) adjusting their risk profiles accordingly.

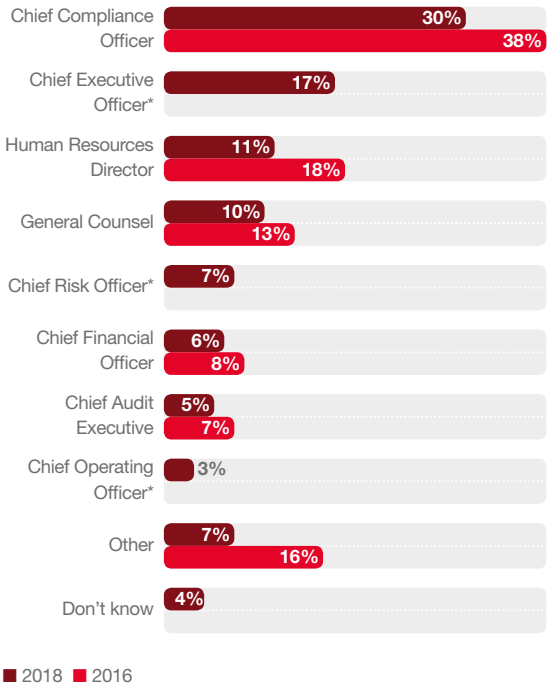
Exhibit 9: Organisations are reporting serious frauds to senior management



Q. Was the most disruptive incident you indicated brought to the attention of your board level executives or to senior leaders charged with governance?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 10: Primary accountability for ethics and compliance programmes resides with the C-suite



* New option in 2018.

Q. Who has primary responsibility for the business ethics and compliance programme in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Whereas traditionally fraud prevention and detection would have been the domain of the organisation's second line of defence – risk management, legal, compliance, etc. – today's enterprises are increasingly embedding their newly reinforced fraud prevention measures into the fabric of their first line of defence.

This is likely to be just the beginning of a significant shift, where first-line fraud prevention and detection capabilities continue to mature and strengthen. As they do so, they will enable the second line of defence to shift to a more traditional second-line approach: governance and oversight and setting risk tolerance, frameworks and policies.

In a world where the boundaries between industries, technologies and regulatory bodies continue to blur – and where fraudsters are looking for soft spots to attack beyond their traditional, highly protected financial services targets – this is an important development.

Bad news travels fast: reputational risk now outstrips regulatory risk

A pronounced shift in the way the world looks at fraud and corruption has taken place over the past few years. And our survey data reflects this now deep-seated demand for accountability, from both the public and from regulators, across the private and public sectors.

This is not a phenomenon limited to developed markets, either. Across vastly different cultures, in every region of the world, there are signs of convergence around standards of transparency and expectations of conduct. Nation states in which the rule of law and levels of transparency have traditionally been weak have seen public outrage in the streets, politicians and business leaders jailed, and in some cases even governments toppled.

For an organisation on the receiving end, perhaps with only fragmented information about what has happened, this represents a serious reputational risk. It can find itself punished from all quarters for its perceived inability to respond appropriately – well before the board has a plan for what to do.

Your reputation is subject to no jurisdiction, law or due process

Exhibit 11: Fraud detection moves up to the first line of defence

1

Executive management

The CEO and executives are responsible for management of risk and are held accountable by the Board.

2

Risk functions

The CRO and the risk function are not responsible for managing risk; that is management's job.

3

Internal audit

The Internal Auditor is responsible for independent assurance and is accountable to the Audit and Risk Committee.

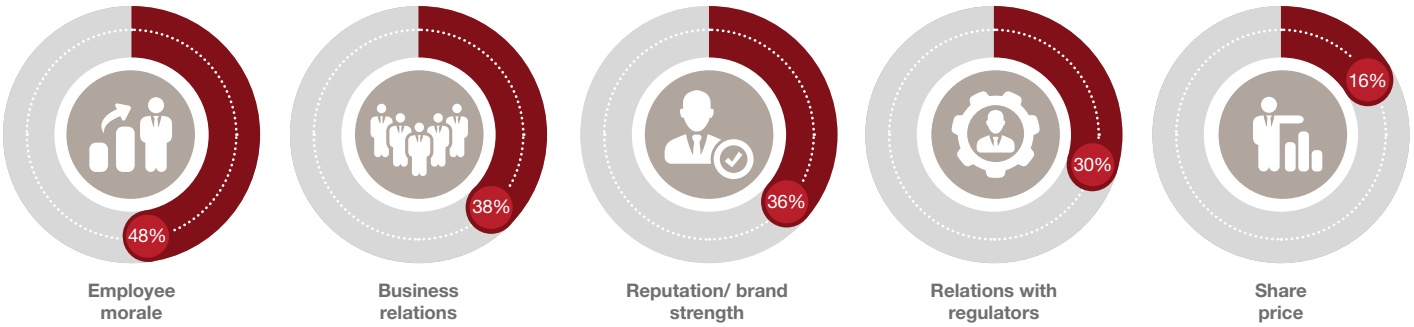
That's because, in this era of radical transparency, companies often don't get to decide when an issue becomes a crisis. Rather, that's down to the jury of public opinion. Moreover, society's rules can change much faster than regulators' – and there is little public tolerance for those who break them. Regulators, by definition, operate within a limited jurisdiction and in accordance with well-defined rules. A company's brand reputation, on the other hand, is subject to no fixed jurisdiction, law or due process.

The executives we surveyed consistently ranked reputational harm at or near the top of negative impacts from various forms of economic crime, with public perception (reputation/brand strength, business relations and share price) taking the hardest hit – a level of impact that has increased since 2016.

Regulatory compliance remains as critical as ever – if not more so. Across the board, regulations and reporting requirements, touching both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise globally, and cross-border regulatory cooperation is becoming increasingly routine.

In our survey, 54% of respondents involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) indicated they had experienced an Anti-Money Laundering (AML) regulatory enforcement or inspection in the last two years (up by 4 percentage points from 2016). And an identical proportion (54%) expect recent changes in the geopolitical regulatory environment to have a greater impact on their organisations over the next two years.

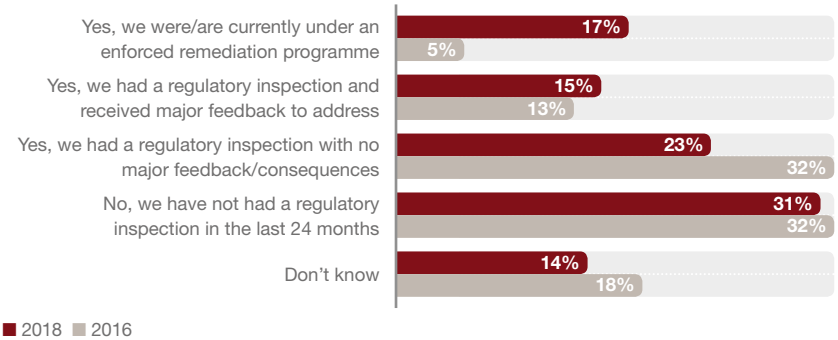
Exhibit 12: Fraud and economic crime impact all elements of the business



Q. What was the level of impact of the most disruptive fraud/economic crime experienced on the following aspects of your business operations?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 13: The number of regulatory enforcements and inspections continues to rise



*Organisations involved in money movement and/or any of these lines of business are: Financial Institution, Mutual Funds, Money Service Business, Broker Dealer, Insurance Company, Dealers in Precious Metals, Stones or Jewels.

Q. Has your organisation experienced any regulatory enforcement/inspection in relation to AML in the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

54%

said they expect changes in the regulatory environment to have an increased impact on their organisation in the next 2 years

Is there a correlation between economic development and fraud?*

Our survey reveals some interesting nuances about global approaches to fraud, which could offer valuable pointers for nation states as they continue on the path of economic development.

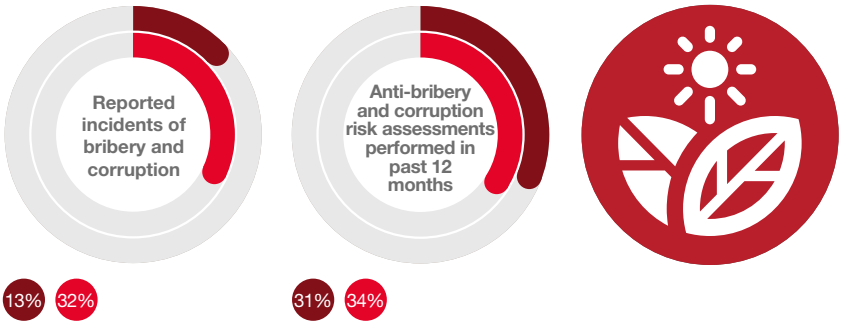
In developing territories, 58% of companies involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) told us they had experienced anti-money laundering (AML) regulatory enforcement or inspection in the last two years. The equivalent figure in developed territories was just 48%.

In developing territories, 15% of companies told us they expect to significantly increase funding for anti-fraud investments in the next 24 months. The equivalent figure in developed territories was just 9%.

In developing territories, respondents told us that economic crime is more often committed by internal actors (59%). The equivalent figure in developed territories was just 39%.

* Our grouping of developed and developing territories was based on the United Nations Conference on Trade and Development classifications. For the purposes of this survey, transitioning territories were treated as developing territories.

Exhibit 14: Developing territories continue to be challenged by corruption risk



Source: PwC's 2018 Global Economic Crime and Fraud Survey

Organisations in developing territories are almost three times as likely to experience corruption as those in developed territories. However, only one third perform risk assessments on anti-bribery and corruption measures, nearly equal to those performed by those in developed territories.

83%

of CEOs report experiencing no negative impact on revenue growth after a well-managed crisis

Source: PwC's CEO Pulse on Crisis

"Instead of tone at the top, organisations should be focused on action at the top"

Tania Fabiani, Partner, PwC US

Learn to leverage the small shocks… and emerge stronger

In any organisation, the occasional breakdown or mishap is unavoidable. And our data suggests that there is plenty of upside to learning how to leverage the small shocks. In fact, they can be a blessing in disguise – an opportunity to test systems and make improvements.

The maturation of a process – for companies as well as countries – happens in part by weathering storms. When a crisis or unplanned event is well managed, 83% of CEOs report experiencing no negative impact on revenue growth. Beyond revenue, how the C-Suite deals with what can become a crisis has a high likelihood of becoming the measure by which it will be judged.

It is natural for a relatively inexperienced company to have a knee-jerk response to a crisis that blindsides it. However, the more a company learns to react to micro-disruptions effectively, the better prepared it is for responding to mega-crises. It acquires a form of 'muscle memory' enabling it to be more proactive in its approach, leveraging mature ethics and compliance programmes and a battle-tested front office.

Harness the protective power of technology

Finding the technology sweet spot

When it comes to fraud, technology is a double-edged sword. It is both a potential threat and a potential protector. Thus, as companies come to view fraud as first and foremost a business problem which could seriously hamper growth, many have made a strategic shift in their approach to technology. These companies are making a business case for robust new investments in areas such as detection, authentication and the reduction of customer friction.

29%

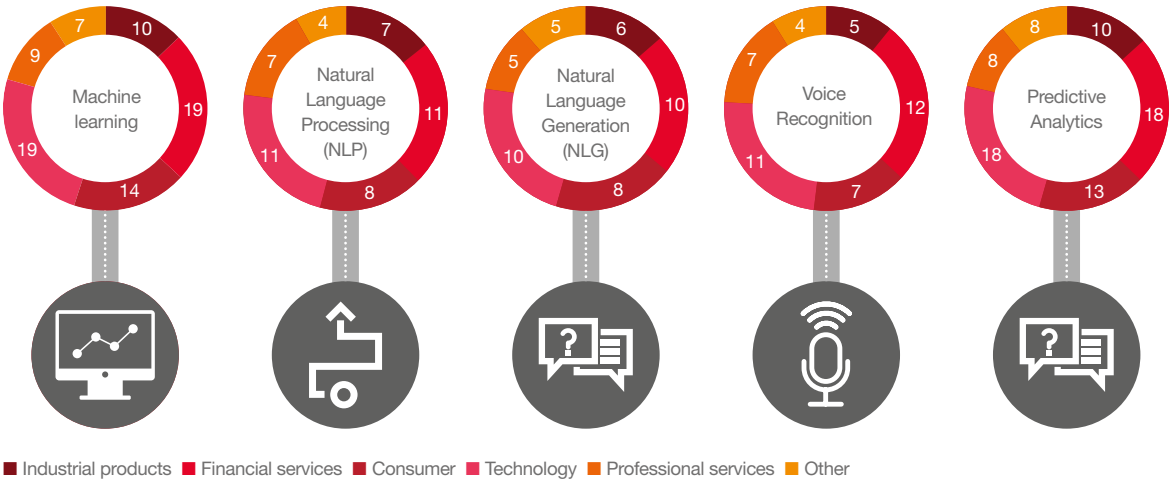
of companies said they spent at least twice as much on investigating and preventing fraud as was lost through the most disruptive economic crimes

42%

of companies said they have increased funds used to combat fraud and/or economic crime

Today, organisations have access to a wealth of innovative and sophisticated technologies with which to defend themselves against fraud, aimed at monitoring, analysing, learning and predicting human behaviour. These include machine learning, predictive analytics and other artificial intelligence techniques. And our survey shows companies are using these technologies, to varying degrees, depending on the industry sector. Technology is expensive to buy and to adopt across a large organisation – prohibitively so, for some. And the decision about what to purchase, and when, is a delicate one. Some invest in emerging or disruptive technologies that they don't use optimally, for instance. Others adopt technology too late and find themselves behind the curve.

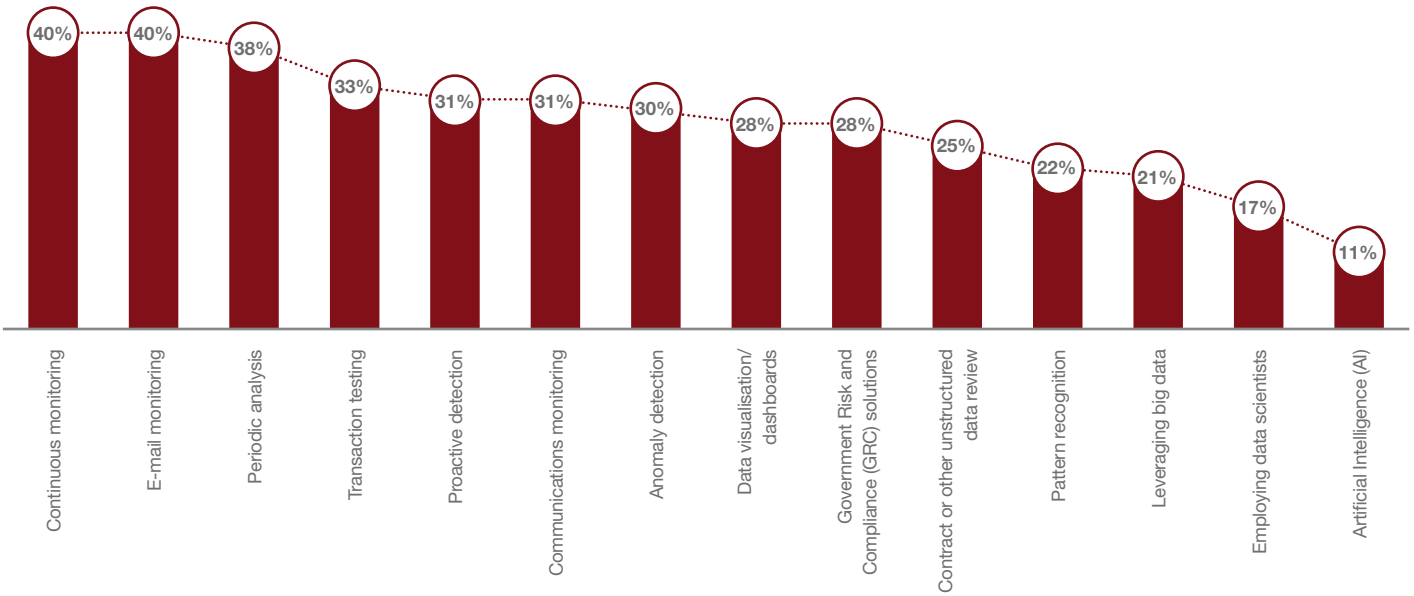
Exhibit 15: The Financial Services and Technology industries are finding the most value in Artificial Intelligence (AI) and Advanced Analytics



Q. To what degree is your organisation using and finding value from Artificial Intelligence or Advanced Analytics to combat/monitor for fraud and other economic crimes? (% of respondents who said their organisation uses and derives value)

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 16: Organisations are beginning to derive value from alternative and disruptive technologies in combatting fraud



Q. To what degree is your organisation using and finding value from the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/or economic crime? (% of respondents who said their organisation uses and derives value)

Source: PwC's 2018 Global Economic Crime and Fraud Survey

The use of innovative technologies to combat fraud is now a worldwide phenomenon. Indeed, our survey shows that companies in developing territories are actually investing in advanced technologies at a faster rate than those in developed territories. We found 27% of companies in developing territories said they currently use or plan to implement artificial intelligence to combat fraud, while just 22% of companies in developed territories said the same. For those developing territories, this approach could represent an effective means of catching up in an area in which other nations have already sunk considerable infrastructure costs.

In the end, the ubiquity of technology creates a double challenge for all organisations: how to find the sweet spot between a technology's effectiveness and its cost while remaining ahead of the fraudsters.

What is customer friction?

As a customer, it can be reassuring – at first – to know a company is continuously monitoring fraud in the services it provides. But if that monitoring leads to frequent or repetitive alerts, that reassurance can quickly turn to irritation.

This is known as customer friction. And it is a growing challenge for organisations as they seek to strike the right balance between acting appropriately to fraud red flags and being overzealous in alerting their customers.

That is not an easy balance to strike – and the margin for error is small. Be too passive and the organisation risks missing a fraudulent transaction, with all the financial and reputational fallout that follows. But be too proactive, and they risk alienating, or even losing, their customer base.

When it comes to new technology adoption, the developing world is now accelerating ahead of the developed world.'

Philip Upton, Partner, PwC US

34%

of respondents said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positives

Customers aren't just one consideration of your business – they are your business

Customers are the lifeblood of any business. But, as business models continue to evolve through the digital revolution, many of those customers are being exposed to payment fraud for the first time. How an organisation handles that fraud will profoundly affect its outcomes. Here are some of the characteristics and challenges of today's digital fraud:

New digital products are creating new attack surfaces

To bring products to market, companies once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider attack surface – and much more room for fraud to break through.

Industry lines are blurring

Non-financial services companies are venturing into payment systems. These relative newcomers sometimes lack the anti-fraud and anti-money laundering experience and know-how of traditional financial services companies, making them, and their third-party ecosystems, susceptible to both fraud and regulatory risk.

The technical sophistication of external fraudsters continues to grow

Digital fraud attacks are becoming more and more sophisticated, thorough and devastating. Single ransomware attacks can cripple organisations and fraudsters manage to move billions of dollars between bank accounts every day.

You can change your credit card number, but you can't change your date of birth

The knowledge-based authentication tools long used to control fraud are outdated and new techniques – such as digital device ID and voice biometrics – are now necessary to protect customers' assets. But most companies are yet to adopt them. This is important because a major data theft is nothing like the loss of a replaceable asset like cash. Rather, what is lost is an individual's unique, deeply personal, permanent identity markers (such as date of birth or social security number). Because this is the very data that knowledge-based authentication tools use to verify identity and prevent fraud, its theft opens the door for fraudsters to take over a person's identity.

Cybercrime: a disconnect between ends and means

Cybercrime has long passed beyond infancy and adolescence. Today's cybercriminals are as savvy and professional as the businesses they attack. This maturity calls for a new perspective on the multifaceted nature of cyber threats and accompanying frauds.

Often, the first sign an organisation gets that something systemic is amiss is the detection of a cyber-enabled attack, such as phishing, malware or a traditional brute force attack. The increasing frequency, sophistication and lethality of these attacks are spurring companies to look for ways to pre-empt them. This approach has the added benefit of enabling a deeper focus on fraud prevention.

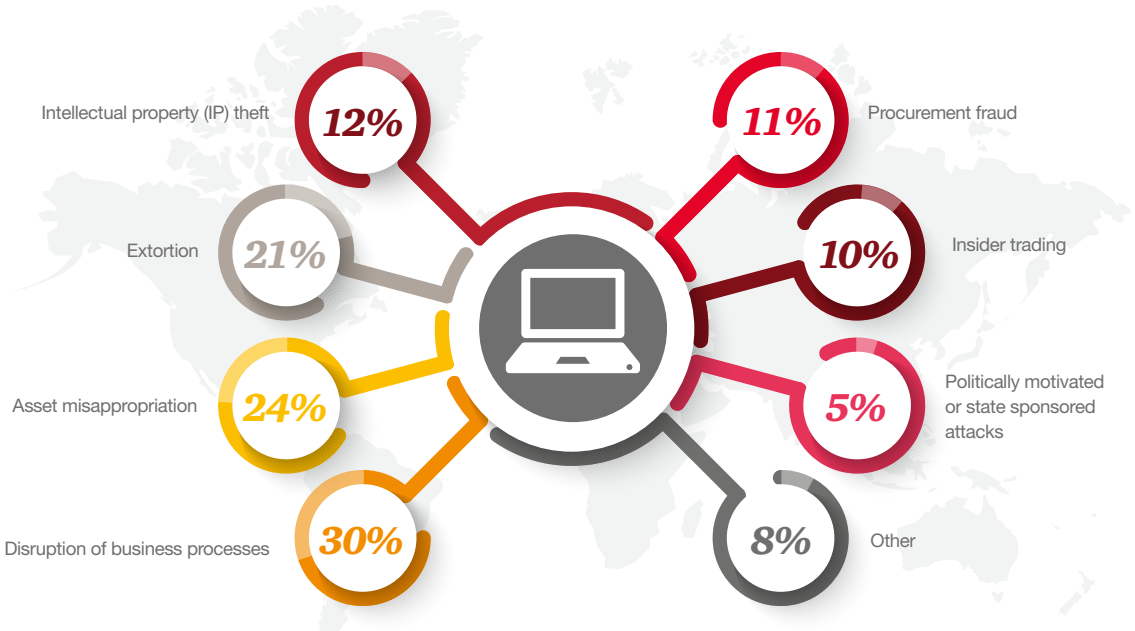
Although it can be difficult for companies to accurately measure the financial impact of cyber-attacks, 14% of survey respondents who said cybercrime was the most disruptive fraud told us they lost over $US1 million as a result, with 1% indicating they lost over $US100 million.

Cybercrime was more than twice as likely than any other fraud to be identified as the most disruptive and serious economic crime expected to impact organisations in the next two years (26% of respondents said they expected a cyber-attack in the next two years and that it would be the most disruptive; 12% said they expected bribery and corruption to be most disruptive; while 11% said the same about asset misappropriation). In fact, cyber-attacks have become so pervasive that measuring their occurrences and impacts is becoming less strategically useful than focusing on the mechanism that the fraudsters used in each case.

41%

of executives surveyed said they spent at least twice as much on investigations and related interventions as was lost to cybercrime

Exhibit 17: Types of fraud that organisations were a victim of through a cyber-attack



Q. Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

While all digital fraud is fraud, not all fraud is digital. It can therefore be helpful to distinguish two forms of cybercrime:

(1) As digital theft (the stolen goods, not the smashed door). This type of attack could include stealing cash, personal information, and intellectual property, and could involve extortion, ransomware, or a host of other crimes.

(2) As digital fraud. This type of attack is in many ways the more long-lasting and disruptive, because the fraudster penetrates an open door (typically, but not always, a customer- or employee-facing access point) and uses the company's own business processes to attack it. To combat this type of fraud, the organisation must use digital methods – both as a vaccine and as a remedy.

Exhibit 18: Cyber-attack techniques used against organisations

36% Malware

33% Phishing

13% Network scanning

10% Yes, but unsure of technique

8% Brute force attack

7% Man in the middle

3% Other technique

Q. In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were digitally extorted.

Beyond compensating customers… where'd the money go?

While keeping customers happy is the first order of business, there are deeper dimensions to fraud prevention. These involve the fraud underworld, and the regulation and enforcement regimes whose mission is to control it.

In the case of identity theft, for instance, a bank or merchant will cover the loss to the customer and absolve them of further responsibility if, say, a fraudster opens a credit card in her name and runs up a significant balance. Until now, the system of remedying such external frauds has worked in this way, and all parties – banks, merchants, consumers and regulators – have accepted it as part of the cost of doing business together.

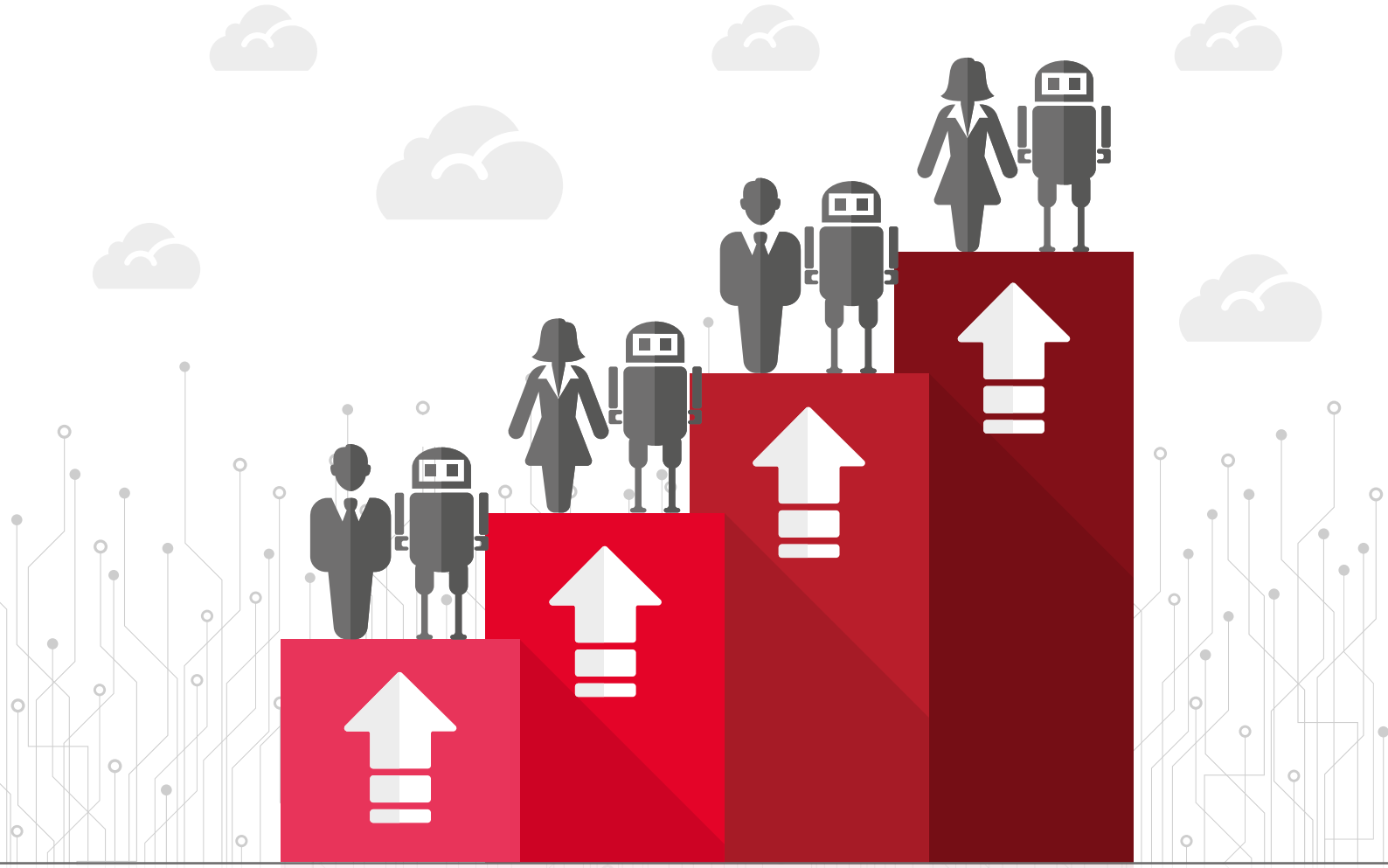
While these fraudulent activities can be detected by the transaction monitoring systems built in response to the United States' Bank Secrecy Act (BSA) and similar rules in other countries, it is likely that both banks and money services businesses (MSBs) are missing the manner in which these transactions manifest themselves in the system. This has been shown in recent regulatory enforcement around lack of detection by businesses in the context of human trafficking, for example.

Non-financial companies may not have the same regulatory obligations as their financial counterparts, but they could still find themselves falling foul of the law. Regulators and law enforcement are now looking beyond the primary impact of a crime – for example, trafficking in counterfeit goods – to examine which illicit activities the stolen assets went to finance. As part of their remit, they are scrutinising non-financial services companies' compliance and anti-fraud measures for signs that they may be, consciously or not, aiding and abetting criminal activities.

The business case

The business case for investment in anti-fraud technology goes beyond protecting the organisation from reputational, regulatory and/or financial damage. It also includes reducing the cost of fraud prevention through efficiencies and enabling an organisation to safely build and sell new products and services on a digital platform. Furthermore, it enables a business to fine-tune a fraud programme to reduce customer friction – allowing customers to interact more freely with its platform and its product.

Invest in people, not just machines



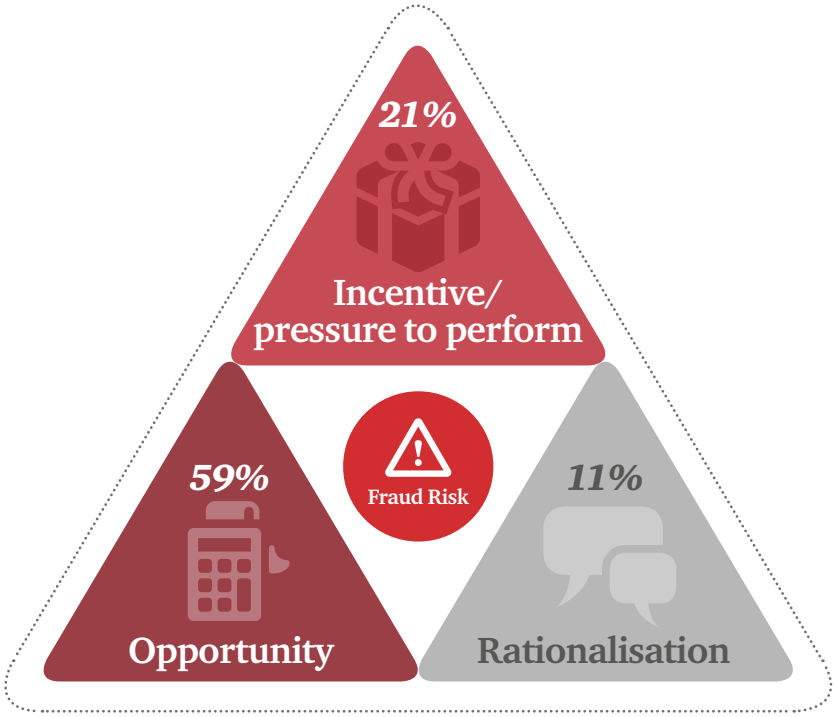
A small investment in people can pay huge dividends

Confronted with the seeming intractability of dealing with fraud, many organisations decide to pour ever more resources into technology. Yet these investments invariably reach a point of diminishing returns, particularly in combatting internal fraud. So, while technology is clearly a vital tool in the fight against fraud, it can only ever be part of the solution.

This is because fraud is the result of a complex mix of conditions and human motivations. The most critical factor in a decision to commit fraud is ultimately human behaviour – and this offers the best opportunity for combatting it. There is a powerful method for understanding and preventing the three principal drivers of internal fraud – the fraud triangle.

The fraud triangle starts with an incentive (generally a pressure to perform from within the organisation) followed by an opportunity, and finally a process of internal rationalisation. Since all three of these drivers must be present for an act of fraud to occur, each of them should be addressed individually.

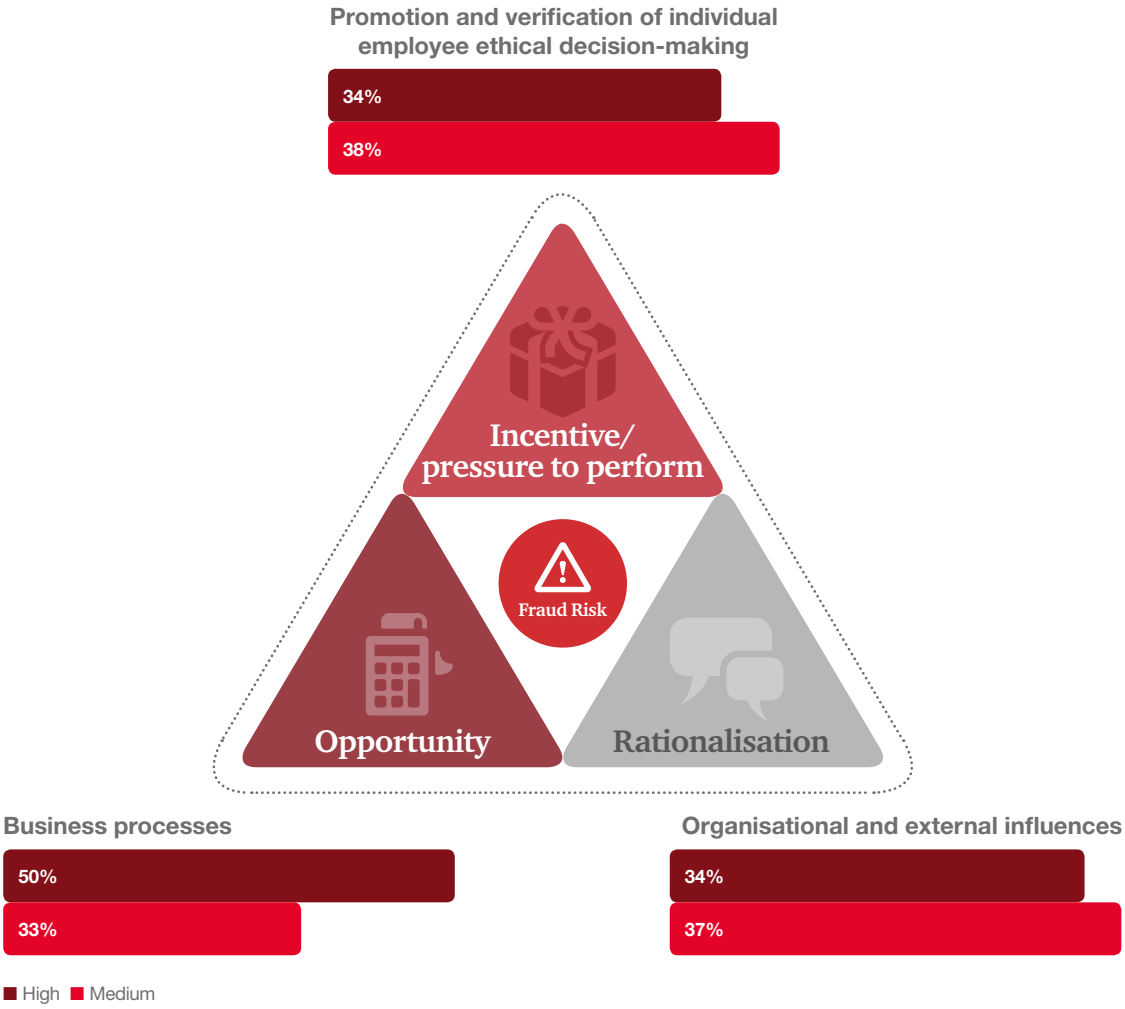
Exhibit 19: The fraud triangle: what makes an employee commit fraud?



Q. To what extent did each of the following factors contribute to the incident of fraud and/or economic crime committed by internal actors? (% of respondents who ranked the factor as the leading contributing factor to internal fraud)

Source: Global Economic Crime and Fraud Survey 2018.

Exhibit 20: The level of organisational effort required to combat internal fraud



Q. What level of effort does your organisation apply to the following categories in order to combat fraud and/or economic crime internally?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing the opportunity: controls

Most organisations' anti-fraud efforts in recent years have been focused on reducing the opportunities for fraudulent acts: 50% of survey respondents said they expend a high degree of effort in building up business processes, such as internal controls, that target opportunities to commit fraud. And, while 59% of respondents ranked opportunity as the leading contributor to the most disruptive frauds committed by internal actors, this was 10 percentage points lower than the equivalent figure in 2016 (69%). This is evidence that technology has a key role to play – and, more to the point, that companies are generally employing it effectively.

Unfortunately, companies are putting significantly less effort into measures to counteract incentives and rationalisation, with only 34% indicating they spent a high level of effort targeting these factors. Our survey highlights the result of these choices: 21% of respondents ranked incentives/ pressure as the leading contributing factor of the most disruptive fraud committed by internal actors, twice the amount reported in 2016 (11% identified rationalisation as the leading motivating factor – the same proportion as in 2016).

This under-emphasis on cultural/ethical measures points to a potential blind spot, and indeed may be one reason why internal fraud is so resilient. Because fraud is the result of the intersection of human choices with system failures, it is important to be wary of the false sense of security that internal controls, even well-designed ones, can bring.

Indeed, there is a fundamental flaw with the belief that internal technology-driven controls alone can catch fraud: it assumes that management will always behave ethically. In fact, experience shows that virtually every significant internal fraud is a result of management circumventing or overriding those controls. Our survey backs this up: it reveals that the share of reported serious internal fraud committed by senior management has risen dramatically – by 50% – over the past two years (from 16% of respondents in 2016 to 24% in 2018). To overcome this structural problem, organisations need to create controls that actually account for management override or collusion in targeted areas.

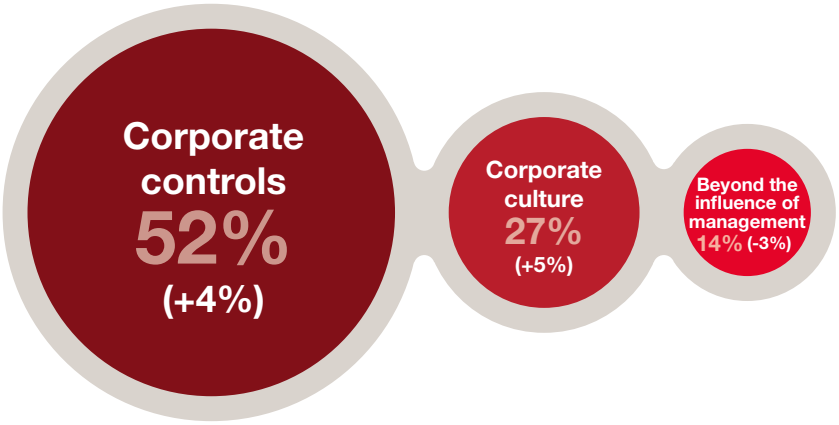
Preventing the incentive: openness

Corporate-sized frauds are generally connected to corporate pressures – and the pressure to commit fraud can arise at any level of the organisation. Our survey shows that 28% of organisations that experienced fraud in the last two years suffered business conduct/misconduct fraud (incentive abuse), and 16% of global organisations with offices in other territories experienced business conduct/misconduct fraud in those other territories. Meanwhile, 24% of respondents indicated that senior management was responsible for the most disruptive crime experienced.

It is important not to over-emphasise financial incentives when considering what drives a person to commit fraud. Fear and embarrassment about having made a mistake may be equally important. Thus, the incentives coming from the top of the organisation must be examined: to what extent do they align with regulations and with 'doing the right thing'?

In addition, short-term bespoke controls can serve as useful checks on whether aggressive sales programmes are leading to fraudulent behaviour. A well-publicised open-door or hotline policy can also provide a valuable early-warning system of potential problems in an organisation.

Exhibit 21: Just over half of the most disruptive frauds were detected by corporate controls



Includes		Includes		Includes	
Internal audit (routine)	14%	Tip off (internal)	13%	By accident	8%
Fraud risk	13%	Tip off (external)	7%	By law enforcement	4%
Suspicious activity monitoring	13%	Whistleblowing hotline	7%	Investigative media	2%
Corporate security	5%				
Data analytics	4%				
Rotation of personnel	1%				

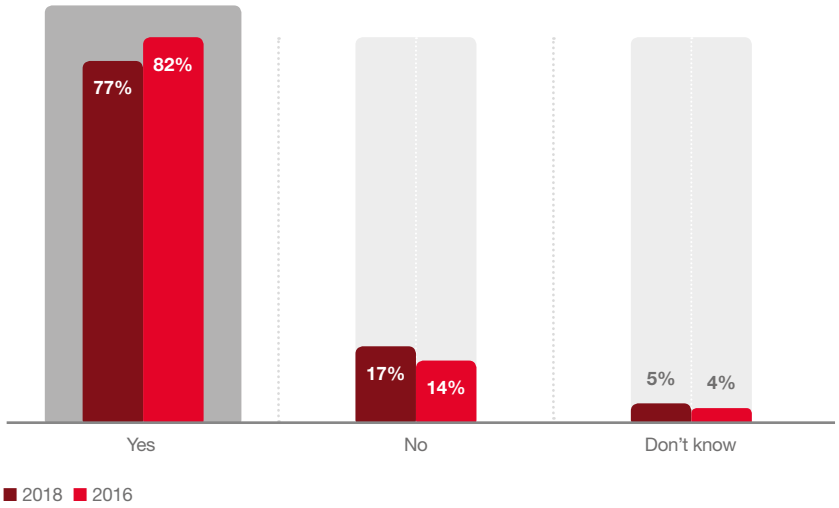
Q. How was the most disruptive fraud and/or economic crime initially detected?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Fraud can occur with the best of intentions

Fraud needn't necessarily be a malicious or selfish act. From a legal point of view, there are actually two kinds of fraud – fraud committed for personal gain (such as embezzlement, or false reporting intended to boost compensation) and fraud committed for "corporate motives" (such as the survival of the company, or the protection of the workforce). The latter could occur with the best of intentions set on increasing the company's success. For example, what might start as a sales strategy designed to increase market share and profitability (to the benefit of employees) might ultimately morph into fraudulent sales tactics. Either way, the result is the same: the executive suite will be held responsible.

Exhibit 22: Fewer companies report having ethics and compliance programmes



Q. Do you have a formal business ethics and compliance programme in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing rationalisation: culture

While incentives and opportunities can be influenced and managed, preventing the rationalisation of a fraudulent act is more of a challenge. This is a process that occurs entirely within the human mind and is thus far harder to influence.

One of the peculiarities of internal fraud is that those who commit it often see it as a victimless crime and cannot visualise any person who will be directly harmed by their actions. This helps explain why nearly three-quarters of survey respondents told us that an internal actor was the main perpetrator of the following most disruptive economic crimes, including human resources fraud (81%), asset misappropriation (75%), insider trading (75%), accounting fraud (74%) and procurement fraud (73%).

The first step in preventing rationalisation is to focus on the environment that governs employee behaviour – the organisational culture. Surveys, focus groups and in-depth interviews should therefore be used to assess the strengths and weaknesses of that culture. Consistent training is also key. If people clearly understand what constitutes an unacceptable action – and why – rationalising fraudulent activity will be harder.

However, our survey found a decreasing number of organisations investing in the kind of training that can make a material difference to fraud prevention. The percentage of respondents who indicated they have a formal business ethics and compliance programme has dropped from 82% to 77% since our 2016 survey. And only 58% of companies with such a programme indicated that programme has specific policies targeting general fraud.

The task of detecting and preventing economic crime or fraud is undoubtedly a complex one. It means finding the right blend of technological and people-focused measures, guided by a clear understanding of the motivations behind fraudulent acts and the circumstances in which they occur. Organisations need not resign themselves to the belief that technology is the only solution, or that a certain amount of fraud is simply part of the cost of doing business. Rather, by establishing a culture of honesty and openness from the top down, they can imbue their organisations with a spirit of open accountability – and pull fraud out of the shadows.

Conclusion

Be prepared. Face the fraud. Emerge stronger.

Our survey shows that many companies are under-prepared to face fraud, for both internal and external reasons. This is why shining a light on an organisation's fraud blind spots, and sharing a clear understanding of what constitutes fraud – and what needs to be done to prevent it – is so important.

Doing so can also unlock significant opportunities. It can help make positive structural improvements across the organisation – which can make the business stronger and more strategic in both good times and bad. That includes removing siloes in functions like compliance, ethics, risk management and legal – and enabling a culture that is more positive, cohesive and resilient.

It's true that the value proposition of an up-to-date fraud programme can be hard to quantify, making it sometimes difficult to secure the investments needed. But the opportunity cost – financial, legal, regulatory and reputational – of failing to establish a culture of compliance and transparency can be far greater.

Not only has the threat of economic crime intensified in recent years, the rules and expectations of all stakeholders – from regulators and the public to social media and employees – have also changed, irrevocably. Today, transparency and adherence to the rule of law are more critical than they have ever been.

And that's a good thing, because in the court of public opinion, where reputations can be won and lost overnight, a business will be held accountable tomorrow for what happens today. Therefore, how it responds when a fraudulent event or compliance issue arises will be as important for the company as the event itself.

Understanding this principle gives a business the opportunity to get ahead of fast-moving events, and to demonstrate to both internal and external stakeholders that it is on top of the issues. Not only are there considerable reputational benefits to 'owning' transparency, in an atmosphere of zero-tolerance, doing so can actually enhance the job security of senior management – while attracting the next generation of leaders to the organisation.

An unplanned event can quickly spiral into a crisis if not well managed. But with the right mechanisms in place – a culture of cohesion and openness and a sophisticated control environment – a company will be well positioned to absorb the shocks, build 'muscle memory', and emerge stronger. The imperatives are clear: place transparency at the heart of corporate purpose, use it to unite strategy, governance, risk management and compliance, and find yourself better positioned to transform a potentially serious business problem into an opportunity to come out ahead.

Contacts

Want to know more about what you can do in the fight against fraud? Contact one of our subject matter experts

Survey Leadership

Didier Lavion
Principal
PwC US
+1 (646) 818 7263
didier.lavion@pwc.com

Forensic Services Leaders

Kristin Rivera
Global Forensics Leader
PwC US
+1 (415) 498 6566
kristin.d.rivera@pwc.com

Dinesh Anand
Partner
PwC India
+91 (124) 330 6005
dinesh.anand@pwc.com

Dyan Decker
Partner
PwC US
+1 (646) 313 3636
dyan.a.decker@pwc.com

John Donker
Partner
PwC Hong Kong
+852 2289 2411
john.donker@hk.pwc.com

Ian Elliott
Partner
PwC UK
+44 (0) 771 191 2415
ian.elliott@pwc.com

Trevor Hills
Partner
PwC South Africa
+27 (11) 797 5526
trevor.hills@pwc.com

Leonardo Lopes
Partner
PwC Brazil
+55 (11) 3674 2562
leonardo.lopes@pwc.com

Richard Major
Partner
PwC Singapore
+65 6236 3058
richard.j.major@sg.pwc.com

Domenic Marino
Partner
PwC Canada
+1 (416) 941 8265
domenic.marino@pwc.com

Claudia Nestler
Partner
PwC Germany
+49 (69) 9585 5552
claudia.nestler@pwc.com

Sirshar Qureshi
Partner
PwC Czech Republic
+420 251 151 235
sirshar.qureshi@pwc.com

Nick Robinson
Partner
PwC United Arab Emirates
+971 4304 3974
nick.e.robinson@pwc.com

Malcolm Shackell
Partner
PwC Australia
+61 (2) 8266 2993
malcolm.shackell@pwc.com

About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 territories. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1,000 employees.

www.pwc.com/fraudsurvey

Enclosure (5)

Accenture

Cost of Cybercrime Report

2017

COST OF CYBER CRIME STUDY

INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE

Ponemon INSTITUTE

Independently conducted by Ponemon Institute LLC
and jointly developed by Accenture

EXECUTIVE SUMMARY

Average annualized cost of cybersecurity (USD)

$11.7M

Percentage increase in cost of cybersecurity in a year

22.7%

Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4%

PRIORITIZING BREAKTHROUGH INVESTMENTS

Over the last two years, the accelerating cost of cyber crime means that it is now 23 percent more than last year and is costing organizations, on average, US$11.7 million. Whether managing incidents themselves or spending to recover from the disruption to the business and customers, organizations are investing on an unprecedented scale—but current spending priorities show that much of this is misdirected toward security capabilities that fail to deliver the greatest efficiency and effectiveness.

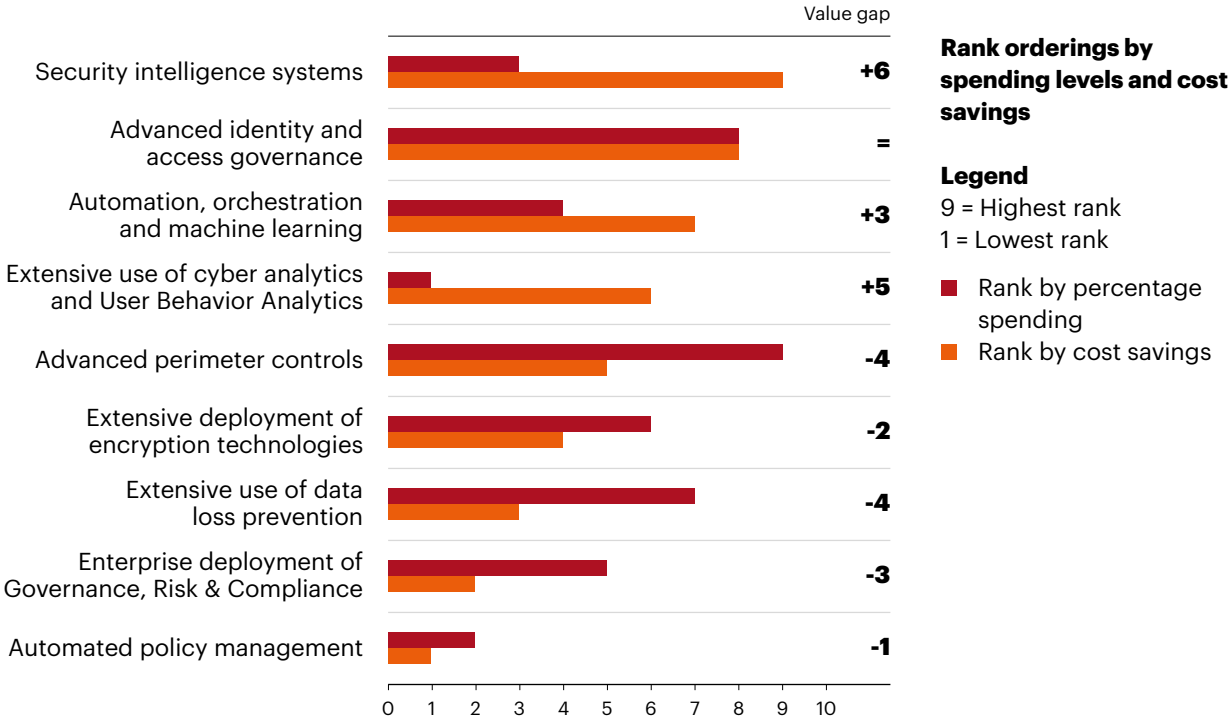
A better understanding of the cost of cyber crime could help executives bridge the gap between their own defenses and the escalating creativity—and numbers—of threat actors. Alongside the increased cost of cyber crime—which runs into an average of more than US$17 million for organizations in industries like Financial Services and Utilities and Energy—attackers are getting smarter. Criminals are evolving new business models, such as ransomware-as-a-service, which mean that attackers are finding it easier to scale cyber crime globally.

EXECUTIVE SUMMARY

With cyber attacks on the rise, successful breaches per company each year has risen more than 27 percent, from an average of 102 to 130. Ransomware attacks alone have doubled in frequency, from 13 percent to 27 percent, with incidents like WannaCry and Petya affecting thousands of targets and disrupting public services and large corporations across the world. One of the most significant data breaches in recent years has been the successful theft of 143 million customer records from Equifax—a consumer credit reporting agency—a cyber crime with devastating consequences due to the type of personally identifiable information stolen and knock-on effect on the credit markets. Information theft of this type remains the most expensive consequence of a cyber crime. Among the organizations we studied, information loss represents the largest cost component with a rise from 35 percent in 2015 to 43 percent in 2017. It is this threat landscape that demands organizations re-examine their investment priorities to keep pace with these more sophisticated and highly motivated attacks.

To better understand the effectiveness of investment decisions, we analyzed nine security technologies across two dimensions: the percentage spending level between them and their value in terms of cost-savings to the business. The findings illustrate that many organizations may be spending too much on the wrong technologies. Five of the nine security technologies had a negative value gap where the percentage spending level is higher than the relative value to the business. Of the remaining four technologies, three had a significant positive value gap and one was in balance. So, while maintaining the status quo on advanced identity and access governance, the opportunity exists to evaluate potential over-spend in areas which have a negative value gap and rebalance these funds by investing in the breakthrough innovations which deliver positive value.

THE POSITIVE OR NEGATIVE VALUE GAPS ASSOCIATED WITH SECURITY INVESTMENTS



Following on from the first *Cost of Cyber Crime*[1] report launched in the United States eight years ago, this study, undertaken by the Ponemon Institute and jointly developed by Accenture, evaluated the responses of 2,182 interviews from 254 companies in seven countries—Australia, France, Germany, Italy, Japan, United Kingdom and the United States. We aimed to quantify the economic impact of cyber attacks and observe cost trends over time to offer some practical guidance on how organizations can stay ahead of growing cyber threats.

1: The study examines the total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

EXECUTIVE SUMMARY

HIGHLIGHTS FROM THE FINDINGS INCLUDE:

Organizations need to better balance investments in security technologies.

Security intelligence systems (67 percent) and advanced identity and access governance (63 percent) are the top two most widely deployed enabling security technologies across the enterprise. They also deliver the highest positive value gap with organizational cost savings of US$2.8 million and US$2.4 million respectively. As the threat landscape constantly evolves, these investments should be monitored closely so that spend is at an appropriate level and maintains effective outcomes. Aside from systems and governance, other investments show a lack of balance. Of the nine security technologies evaluated, the highest percentage spend was on advanced perimeter controls. Yet, the cost savings associated with technologies in this area were only fifth in the overall ranking with a negative value gap of minus 4. Clearly, an opportunity exists here to assess spending levels and potentially reallocate investments to higher-value security technologies.

Compliance technology is important but don't bet the business on it.

Spending on governance, risk and compliance (GRC) technologies is not a fast-track to increased security. Enterprise-wide deployment of GRC technology and automated policy management showed the lowest effectiveness in reducing cyber crime costs (9 percent and 7 percent respectively) out of nine enabling security technologies. So, while compliance technology is important, organizations must spend to a level that is appropriate to achieve the required capability and effectiveness, enabling them to free up funds for breakthrough innovations.

Organizations need to grasp the innovation opportunity.

Innovations are generating the highest returns on investment, yet investment in them is low. For example, two enabling security technology areas identified as "Extensive use of cyber analytics and User Behavior Analytics (UBA)" and "Automation, orchestration and machine learning" were the lowest ranked technologies for enterprise-wide deployment (32 percent and 28 percent respectively) and yet they provide the third and fourth highest cost savings for security technologies. By balancing investments from less rewarding technologies into these breakthrough innovation areas, organizations could improve the effectiveness of their security programs.

RECOMMENDATIONS

$2.8M cost savings from security intelligence systems and most positive value gap

The foundation of a strong and effective security program is to identify and "harden" the higher-value assets. These are the "crown jewels" of a business—the assets most critical to operations, subject to the most stringent regulatory penalties, and the source of important trade secrets and market differentiation. Hardening these assets makes it as difficult and costly as possible for adversaries to achieve their goals, and limits the damage they can cause if they do obtain access.

EXECUTIVE SUMMARY

By taking the following three steps, organizations can further improve the effectiveness of their cybersecurity efforts to fend off and reduce the impact of cyber crime:

1 > Build cyber-security on a strong foundation

Invest in the "brilliant basics" such as security intelligence and advanced access management and yet recognize the need to innovate to stay ahead of the hackers.

2 > Undertake extreme pressure testing

Organizations should not rely on compliance alone to enhance their security profile but undertake extreme pressure testing to identify vulnerabilities more rigorously than even the most highly motivated attacker.

3 > Invest in breakthrough innovation

Balance spend on new technologies, specifically analytics and artificial intelligence, to enhance program effectiveness and scale value.

Organizations need to recognize that spending alone does not always equate to value. Beyond prevention and remediation, if security fails, companies face unexpected costs from not being able to run their businesses efficiently to compete in the digital economy. Knowing which assets must be protected, and what the consequences will be for the business if protection fails, requires an intelligent security strategy that builds resilience from the inside out and an industry-specific strategy that protects the entire value chain. As this research shows, making wise security investments can help to make a difference.

$2.4 million average cost of malware attack spend and the top cost to companies

50 days average time to resolve a malicious insiders attack

23 days average time to resolve a ransomware attack

KEY FINDINGS

The average total cost by country, organizational size and industry

The financial consequence of a cyber attack is worsening. **P12**

The cost of cyber crime varies by organizational size. **P17**

Financial services has the highest cost of cyber crime. **P20**

The cost of cyber crime by type of attack

Certain attacks are more costly based on organizational size. **P21**

Ransomware attacks have doubled. **P23**

Country costs vary considerably by the type of cyber attack. **P24**

Costs vary significantly among countries. **P25**

The cost of cyber crime is also influenced by the frequency of attacks. **P26**

Malware and Web-based attacks are the two most costly attack types. **P27**

Malicious code attacks are taking longer to resolve and, as a result, are more costly. **P28**

Analysis of the costs to resolve the consequences of the cyber attack

Information theft remains the most expensive consequence of a cyber crime. **P29**

Companies spend the most on detection and recovery. **P30**

How companies allocate resources and achieve cost savings

Budget allocations are slowly shifting from the network to application and data layers. **P32**

Security intelligence systems have the biggest return on investment. **P35**

Maturity and effectiveness of an organization's security posture

Program maturity is weighted toward the middle stages. **P37**

Findings reveal a non-linear relationship between total cost of cyber crime and maturity stage of the cybersecurity program. **P38**

Two countries have a negative security effectiveness score. **P39**

The findings reveal a high SES decreases the total cost of cyber crime. **P40**

More investment is needed in breakthrough technologies. **P41**

The cost of cyber crime varies by country, organizational size, industry, type of cyber attack and maturity and effectiveness of an organization's security posture. In addition to presenting the range of costs according to these variables, we also analyzed the average expenditures and allocation of resources to resolve the cyber attack. Topics covered in this report include:

- Average total cost by country, organizational size and industry
- The cost of cyber crime by type of cyber attack
- Analysis of the costs to resolve the consequences of the cyber attack
- How companies allocate resources and achieve cost savings
- Maturity and effectiveness of an organization's security posture

The average total cost by country, organizational size and industry

KEY FINDING 1

The financial consequence of a cyber attack is worsening.

Figure 1 presents the global average cost of cyber crime over the last five years. After a steady increase for the first three years, the significant increase we uncovered last year has continued with an increase of 27.4 percent in the last year alone.

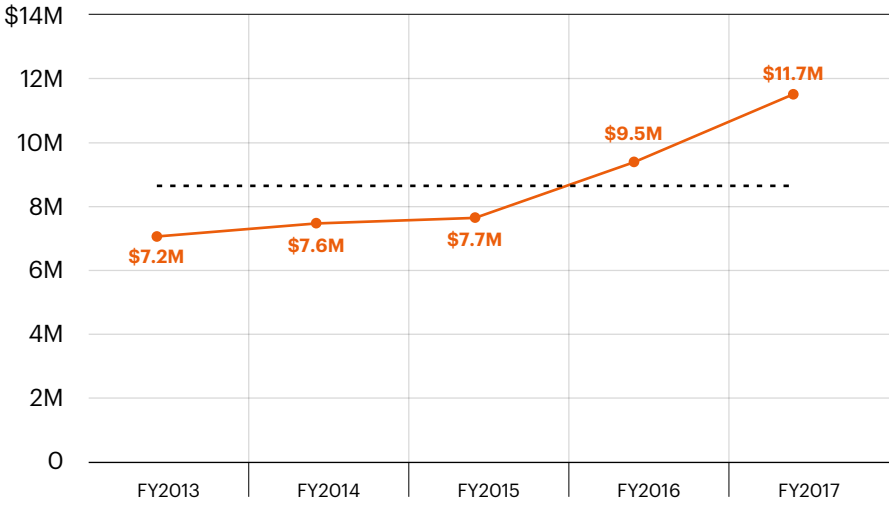


FIGURE 1
The global average cost of cyber crime over five years
US dollars

Legend
Consolidated view
n = 254 separate companies

Total average cost
Five-year average

Percentage change in average cost over five years is 62 percent

Figure 2 presents the estimated average cost of cyber crime for seven countries, involving 254 separate companies, for the past three years. Companies in the United States report the highest total average cost at US$21 million and Australia reports the lowest total average cost at US$5.41 million.

To determine the average cost of cyber crime, the 254 organizations in the study were asked to report what they spent to deal with cyber crimes experienced over four consecutive weeks. Once costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost.[2]

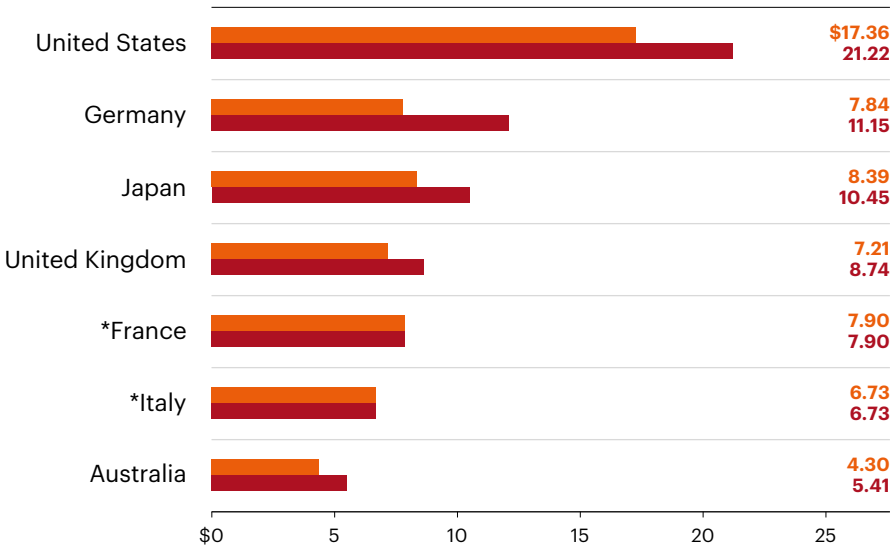


FIGURE 2
Total cost of cyber crime in seven countries
*Historical data does not exist for newly added country samples

Legend
US$ millions
n = 254

FY2016 (US$ millions)
FY 2017 (US$ millions)

2: Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

KEY FINDINGS

Figure 3 summarizes the percentage increase in cyber crime costs between 2016 and 2017 as measured by the US dollar. As shown, Germany experienced the most significant increase in total cyber crime cost and the United Kingdom had the lowest change.

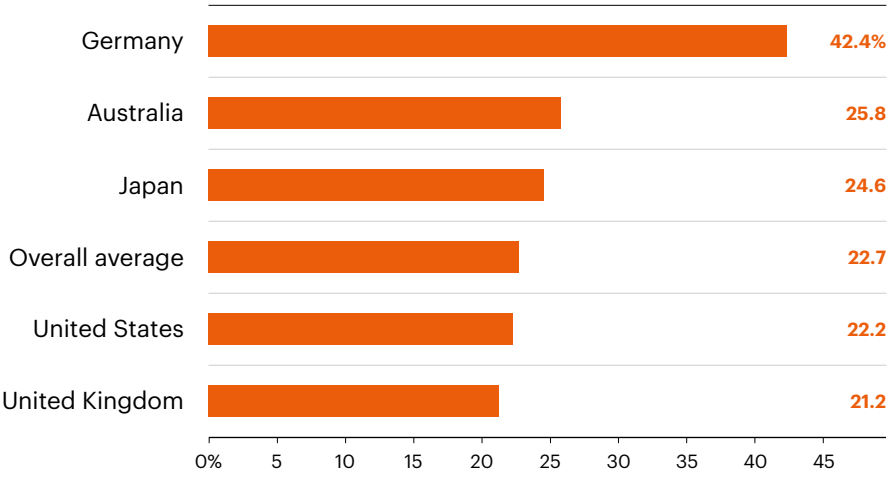


FIGURE 3
One-year percentage increase in cyber crime by country sample
Percentage increase could not be calculated for France and Italy as they were included for the first time in this report

Legend
Mean = 20.4%
n = 254 companies

Figure 4 reports the distribution of annualized total cost for 254 companies. As can be seen, 90 companies in our sample incurred total costs above the mean value of US$11.7 million, indicating a skewed distribution. The highest cost estimate of US$77.1 million was determined not to be an outlier based on additional analysis. A total of 163 organizations experienced an annualized total cost of cyber crime below the mean value.

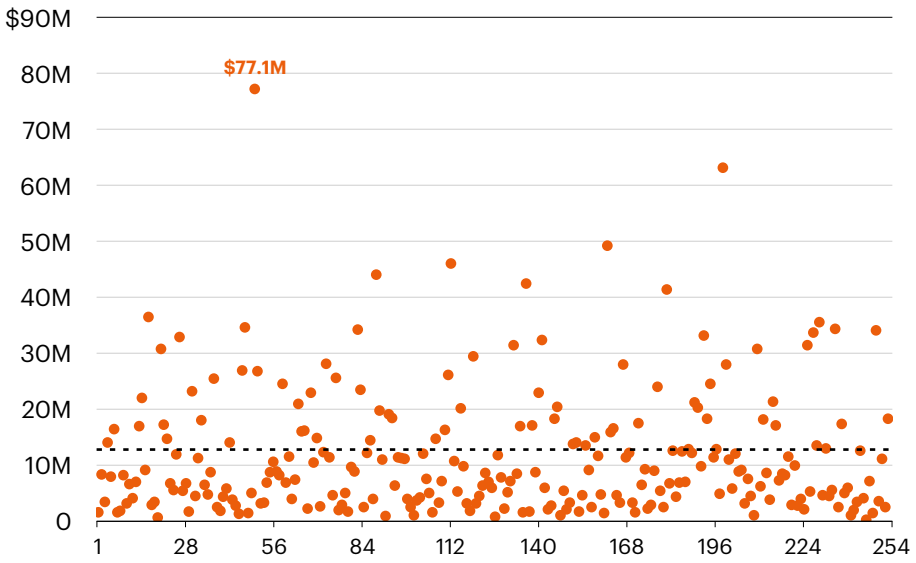


FIGURE 4
Scattergram of total cost of cyber crime for 254 participating companies
Cost expressed in US$

Legend
2017 Average total cost
2017 Annualized total cost

KEY FINDINGS

As part of our analysis we calculated a precision interval for the average cost of US$11.7 million. The purpose of this interval is to demonstrate that our cost estimates should be thought of as a range of possible outcomes, rather than a single point or number.

The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 5. Specifically, at a 90 percent level of confidence we expect the range of cost to be between US$11 million to US$12.3 million.

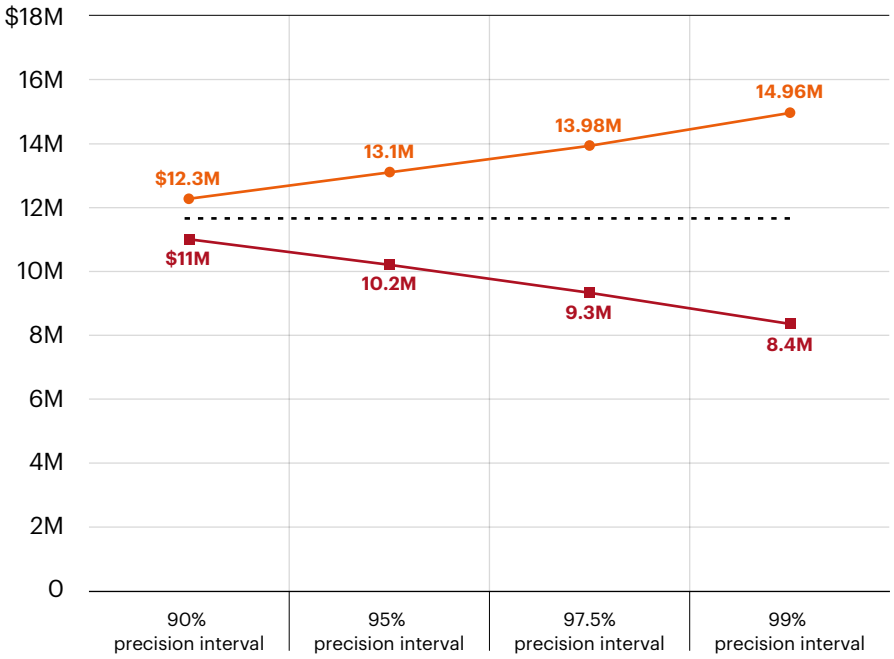


FIGURE 5
Precision interval for the mean value of annualized total cost
Cost expressed in US$

Legend
- Minimum
- Mean
- Maximum

KEY FINDING 2

The cost of cyber crime varies by organizational size.

As shown in Figure 6, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost. This positive correlation is indicated by the upward sloping regression line. The number of seats ranges from a low of 1,050 to a high of 259,000.

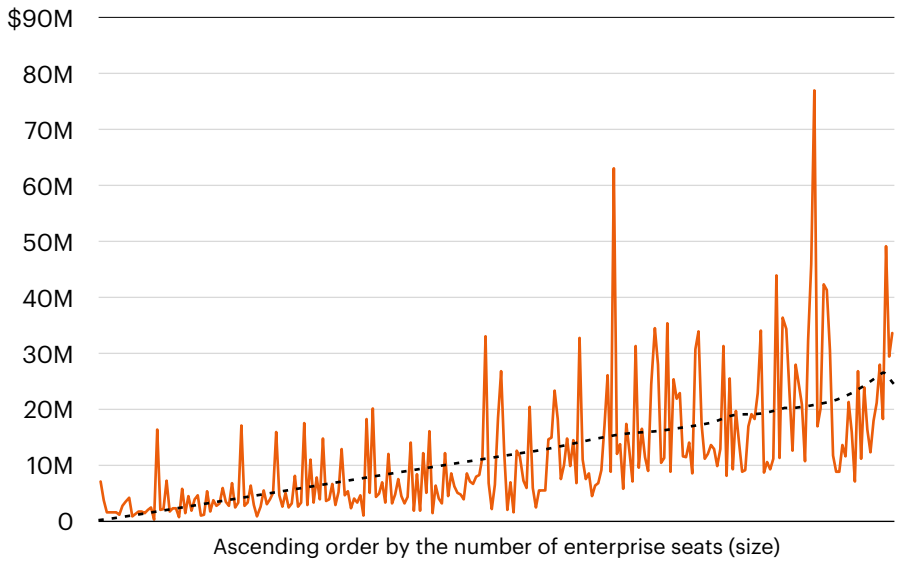


FIGURE 6
Annualized cost in ascending order by the number of enterprise seats
Cost expressed in US$

Legend
— 2017 Annualized total cost
--- Regression

KEY FINDINGS

Organizations are placed into one of four quartiles based on their total number of enterprise seats[3] (which we use as a size surrogate). We do this to create a more precise understanding of the relationship between organizational size and the cost of cyber crime. Table 1 shows the quartile average cost of cyber crime for five years. Approximately 64 companies are in each quartile.

TABLE 1
The quartile average cost of cyber crime over five years

TABLE 1 Quartile analysis	**FY 2017**	**FY 2016**	**FY 2015**	**FY 2014**	**FY 2013**
Cost expressed in US$	(n=254)	(n=237)	(n=252)	(n=257)	(n=234)
Quartile 1 (smallest)	$3,556,300	$3,477,633	$3,279,376	$2,967,723	$2,965,464
Quartile 2	$5,685,633	$5,567,110	$5,246,519	$5,107,532	$4,453,688
Quartile 3	$10,125,414	$9,854,250	$8,987,450	$8,321,024	$6,659,478
Quartile 4 (largest)	$16,852,250	$14,589,120	$13,372,861	$13,805,529	$14,707,980

3: Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Table 2 reports the average cost per enterprise seat (also known as the per capita cost) compiled for four quartiles ranging from the smallest (Quartile 1) to the largest (Quartile 4). Consistent with prior years, the 2017 average per capita cost for organizations with the fewest seats is approximately four times higher than the average per capita cost for organizations with the most seats (US$1,726 versus US$436).

TABLE 2
The average cost per enterprise seat

TABLE 2 Quartile analysis	**2017 cost/seat**	**2016 cost/seat**	**2015 cost/seat**	**2014 cost/seat**	**2013 cost/seat**
Cost expressed in US$	(n=254)	(n=237)	(n=252)	(n=257)	(n=234)
Quartile 1 (smallest)	$1,726	$1,688	$1,555	$1,601	$1,388
Quartile 2	$975	$952	$878	$962	$710
Quartile 3	$655	$698	$709	$726	$532
Quartile 4 (largest)	$436	$401	$368	$437	$431

KEY FINDING 3

Financial services has the highest cost of cyber crime.

The average annualized cost of cyber crime varies by industry segment. In this year's study we compare cost averages for 15 different industry sectors. As shown in Figure 7, the cost of cyber crime for companies in financial services and utilities and energy have the highest annualized cost. In contrast, companies in life science, education and hospitality incurred a much lower cost on average.[4]

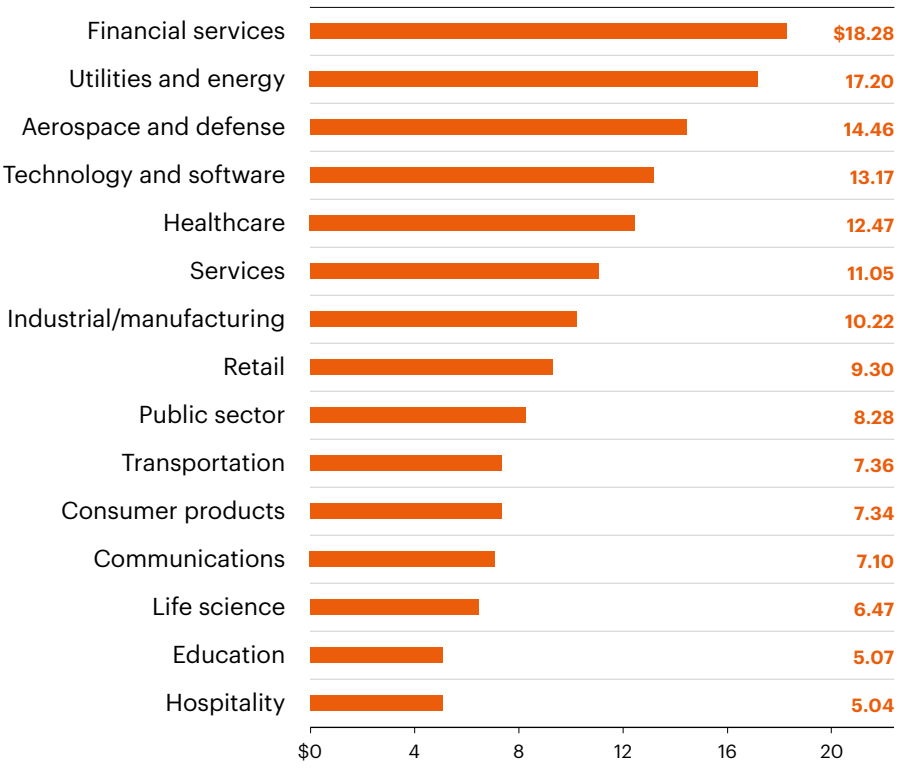


FIGURE 7
Average annualized cost by industry sector
US$ millions

Legend
Consolidated view
n = 254 companies

Total annualized cost ($1 million omitted)

4: This analysis is for illustration purposes only. The sample sizes in several sectors are too small to make definitive conclusions about industry differences.

The cost of cyber crime by type of attack

KEY FINDING 4

Certain attacks are more costly based on organizational size.

The study focuses on nine different attack vectors as the source of the cyber crime. In Figure 8, we compare smaller and larger-sized organizations based on the sample median of 8,560 seats.

Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to malware, Web-based attacks, phishing and social engineering attacks and stolen devices. In contrast, larger organizations (above the median) experience a higher proportion of costs relating to denial of services, malicious insiders and malicious code.

In the context of this research, malicious insiders include employees, temporary employees, contractors and, possibly other business partners. We also distinguish viruses from malware. Viruses reside on the endpoint and as yet have not infiltrated the network but malware has infiltrated the network. Malicious code attacks the application layer and includes SQL attack.

KEY FINDINGS

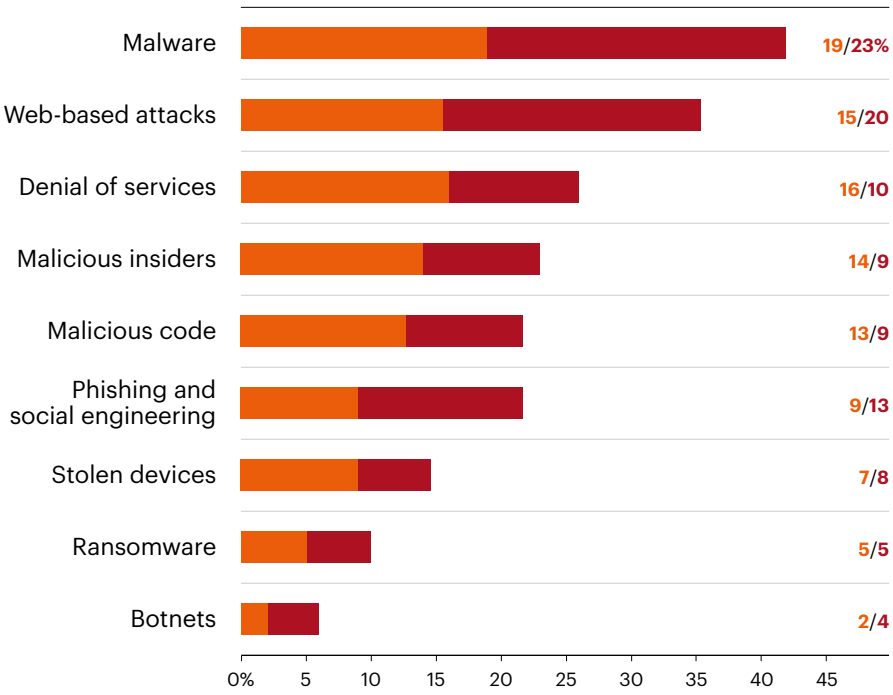


FIGURE 8
Organizational size affects the cost of nine attack types
Size measured according to the number of enterprise seats within the participating organizations

Legend
Consolidated view
n = 254 companies

- Above median number of enterprise seats
- Below median number of enterprise seats

This year, the benchmark sample of 254 organizations experienced a total of 635 discernible cyber attacks. Table 3 shows the number of successful attacks for the past six years, which has steadily increased.

TABLE 3
Frequency of discernible cyber attacks over six years

Year of study	Sample size	Total number of attacks	Successful attacks per company each week
FY 2017	254	635	2.5
FY 2016	237	465	2.0
FY 2015	252	477	1.9
FY 2014	257	429	1.7
FY 2013	234	343	1.4
FY 2012	199	262	1.3

KEY FINDING 5

Ransomware attacks have doubled.

Figure 9 summarizes in percentages the types of attack methods experienced by participating companies. As shown, ransomware attacks increased significantly from 13 percent to 27 percent since last year.

Virtually all organizations had attacks relating to viruses, worms and/or trojans and malware over the four-week benchmark period. Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack. Sixty-nine percent of companies experienced phishing and social engineering and 67 percent of companies had Web-based attacks.

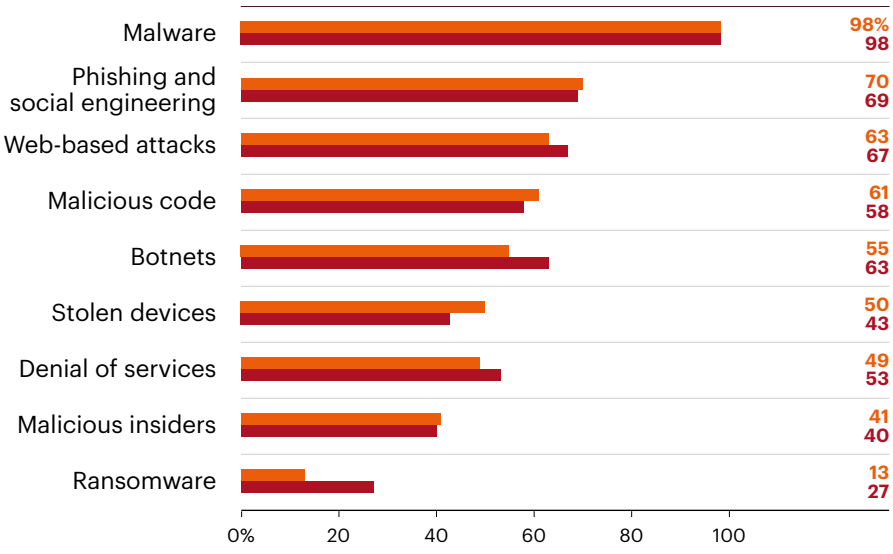


FIGURE 9
Types of cyber attacks experienced by companies

Legend
Consolidated view
n = 254 companies

FY 2016
FY 2017

KEY FINDING 6

Country costs vary considerably by the type of cyber attack.

Figure 10 compares benchmark results for seven countries, showing the percentage of annualized cost of cyber crime allocated to nine attack types compiled from all benchmarked organizations. Germany and Australia have the most costly malware attacks (both 23 percent), France has the most costly Web-based attacks (20 percent) and Germany and the United Kingdom have the most costly denial of service attacks (both 15 percent).

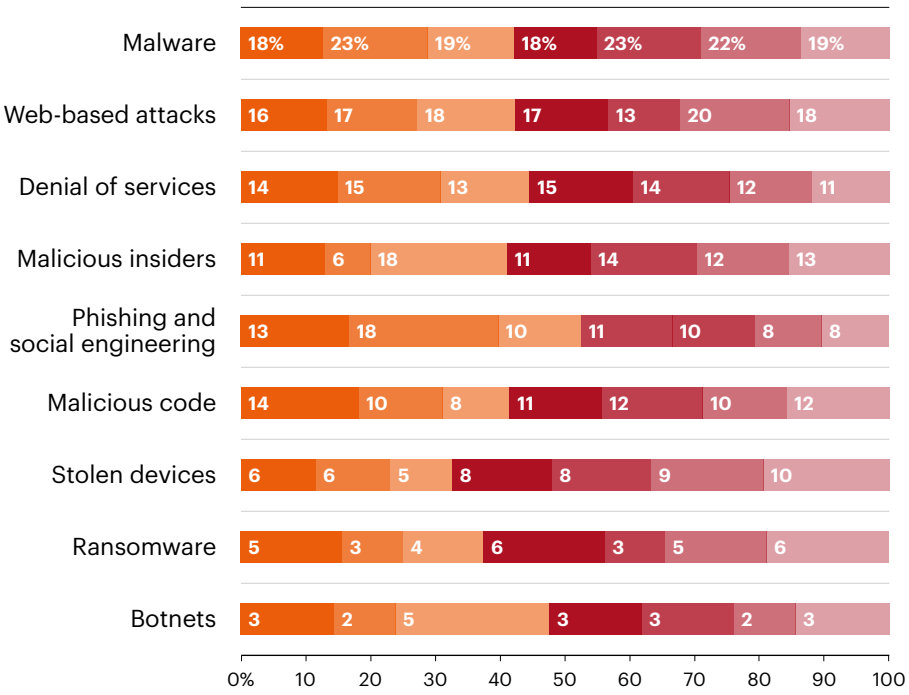


FIGURE 10
Percentage annualized cyber crime cost by attack type and country

Legend
Consolidated view
n = 254 companies

- United States
- Germany
- Japan
- United Kingdom
- Australia
- France
- Italy

KEY FINDING 7

Costs vary significantly among countries.

As shown in Figure 11, United States companies are paying more to resolve all types of cyber attack, especially for malware and Web-based attacks (US$3.82 million and US$3.40 million per attack, respectively). The least expensive attack type for all countries is a botnet.

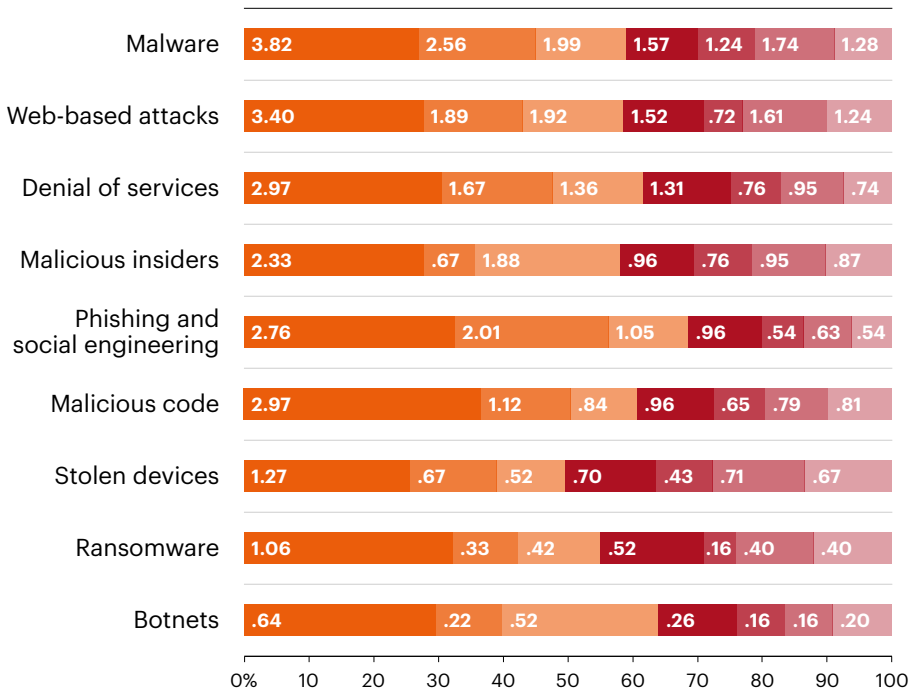


FIGURE 11
Annualized cyber crime cost by attack type and country
US$ millions

Legend
Consolidated view
n = 254 companies

- United States
- Germany
- Japan
- United Kingdom
- Australia
- France
- Italy

KEY FINDING 8

The cost of cyber crime is also influenced by the frequency of attacks.

Figure 12 reveals the most to least expensive cyber attacks when analyzed by the frequency of incidents. The most expensive attacks are malicious insiders, denial of service and malicious code.

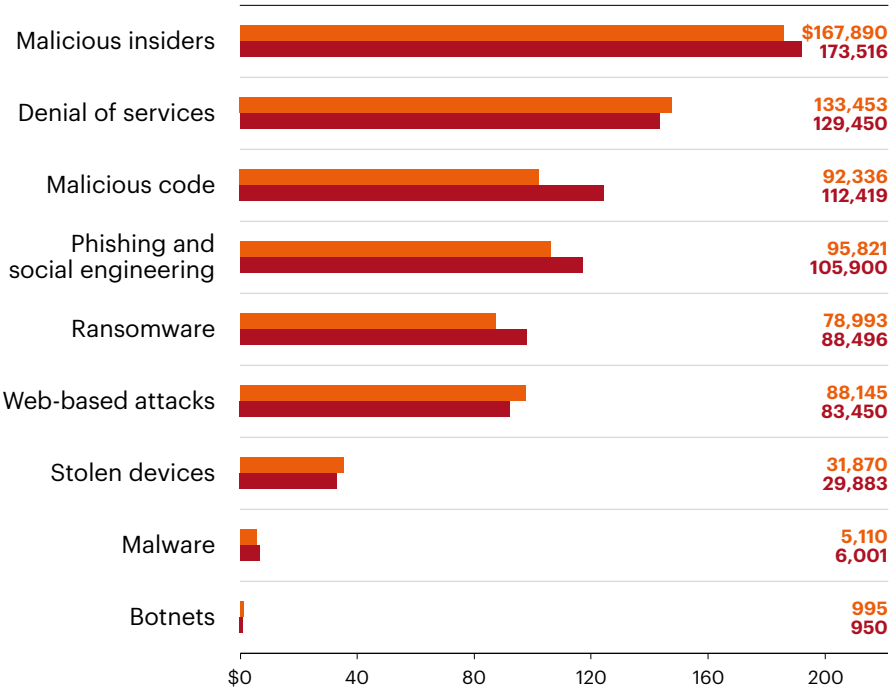


FIGURE 12
Average annualized cyber crime cost weighted by attack frequency

Legend
Consolidated view
n = 254 separate companies

FY 2016
FY 2017

KEY FINDING 9

Malware and Web-based attacks are the two most costly attack types.

As shown in Figure 13, companies spent an average of US$2.4 million and US$2 million on malware and Web-based attacks, respectively. Least costly are stolen devices, ransomware and botnets (US$865,985; US$532,914 and US$350,012, respectively).

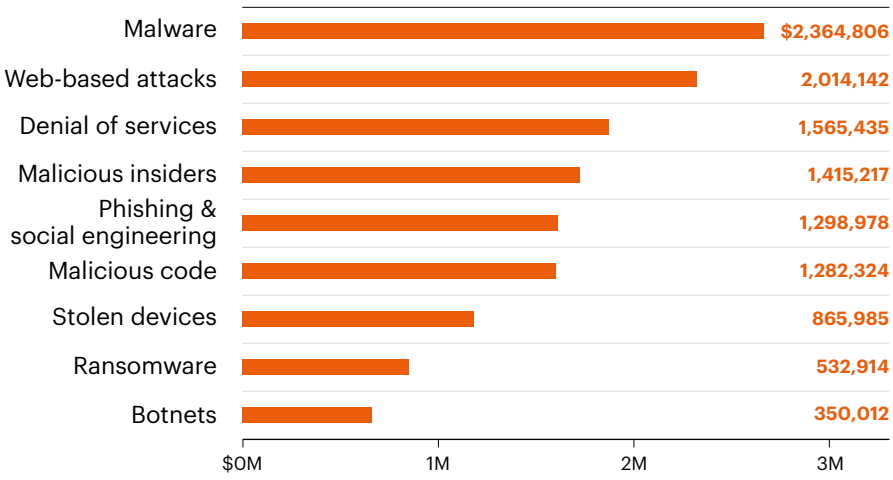


FIGURE 13
Total annualized cyber crime cost for attack types
US$ millions

Legend
Consolidated view
n = 254 separate companies

KEY FINDING 10

Malicious code attacks are taking longer to resolve and, as a result, are more costly.

As shown, the time it takes to resolve the consequences of the attack increases the cost of a cyber crime.

Figure 14 reports the average days to resolve cyber attacks for attack types studied in this report. It is clear from this chart that it takes the most amount of time, on average, to resolve attacks from malicious code, malicious insiders and ransomware (hackers). Malware, viruses and botnets on average are resolved relatively quickly (that is, in a few days). Since 2016, companies are spending more time to deal with malicious code (between 49.6 days and 55.2 days) and less time to deal with Web-based attacks (between 25.3 and 22.4 days).

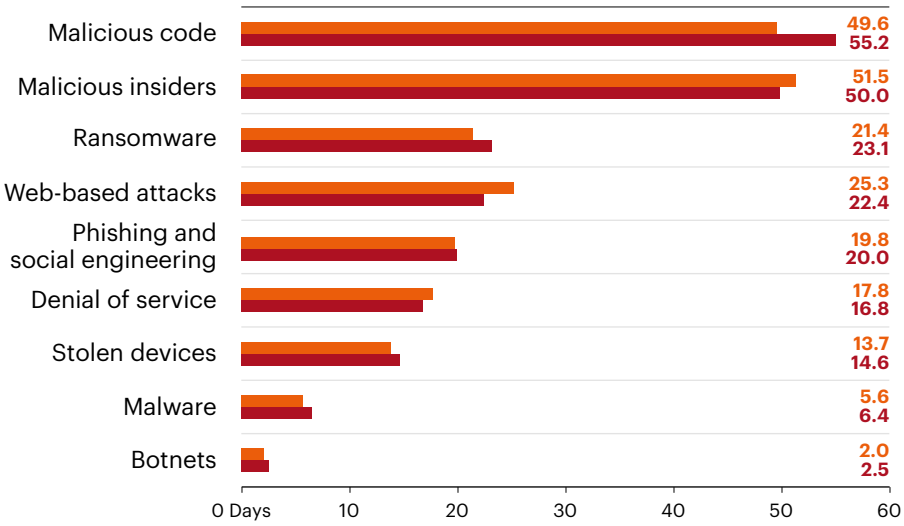


FIGURE 14
Length of time to resolve an attack in days
Estimated average time is measured for each attack type in days

Legend
Consolidated view
n = 254 separate companies

FY 2016
FY 2017

Analysis of the costs to resolve the consequences of the cyber attack

KEY FINDING 11

Information theft remains the most expensive consequence of a cyber crime.

In this research we look at four primary consequences of a cyber attack: business disruptions, the loss of information, loss of revenue and damage to equipment.

As shown in Figure 15, among the organizations represented in this study, information loss represents the largest cost component (43 percent). The cost of business disruption has decreased significantly from 39 percent in 2015 to 33 percent in this year's research. Business disruption costs include diminished employee productivity and business process failures that happen after a cyber attack. Revenue losses and equipment damages follow at 21 percent and 3 percent, respectively.

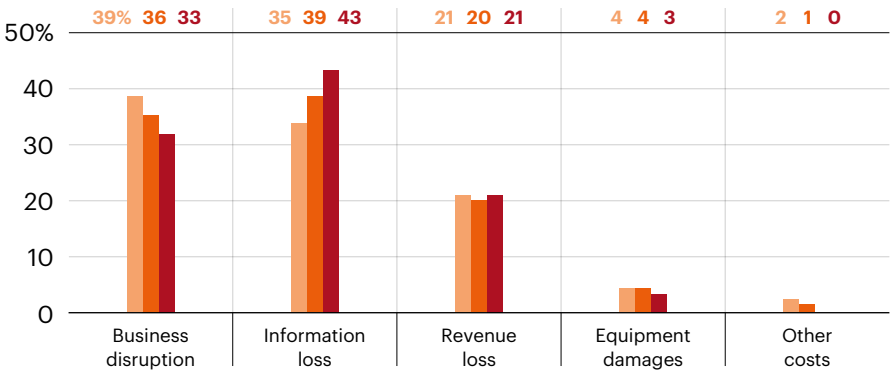


FIGURE 15
Percentage cost by consequence

Legend
Consolidated view
n = 254 separate companies

FY 2015
FY 2016
FY 2017

KEY FINDING 12

Companies spend the most on detection and containment.

Cyber crime detection and containment activities account for 56 percent of total internal activity cost (35 percent plus 21 percent), as shown in Figure 16. This is followed by recovery and investigation cost (at 20 percent and 11 percent, respectively). While detection costs have increased since 2015, recovery costs have decreased. Detection and recovery cost elements highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and deploy enabling security technologies to help facilitate the detection process.

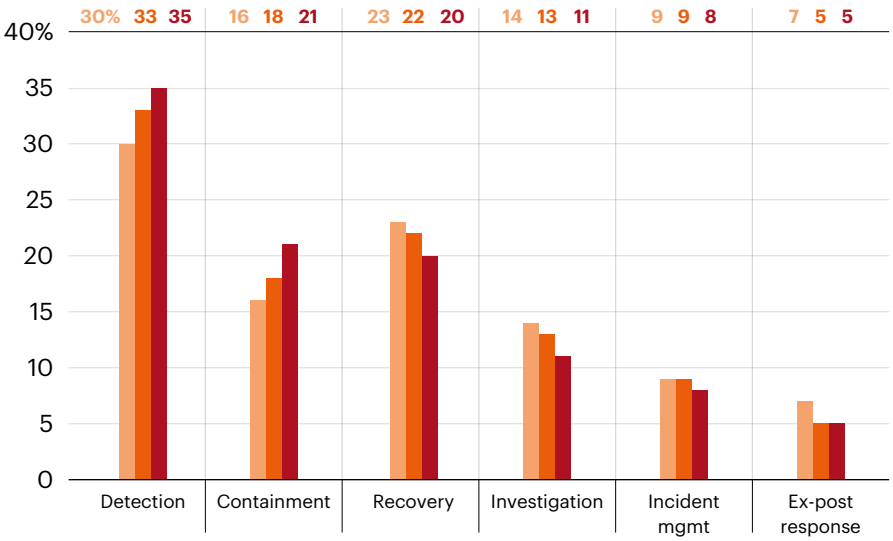


FIGURE 16
Percentage cost by internal activities

Legend
Consolidated view
n = 254 companies

- FY 2015
- FY 2016
- FY 2017

The percentage of annualized costs can be further broken down into five specific expenditure components, which include: productivity loss (31 percent) direct labor (26 percent), cash outlays (20 percent), indirect labor (17 percent) and overhead (6 percent). Costs not included in these components are represented in the "other" category (Figure 17).

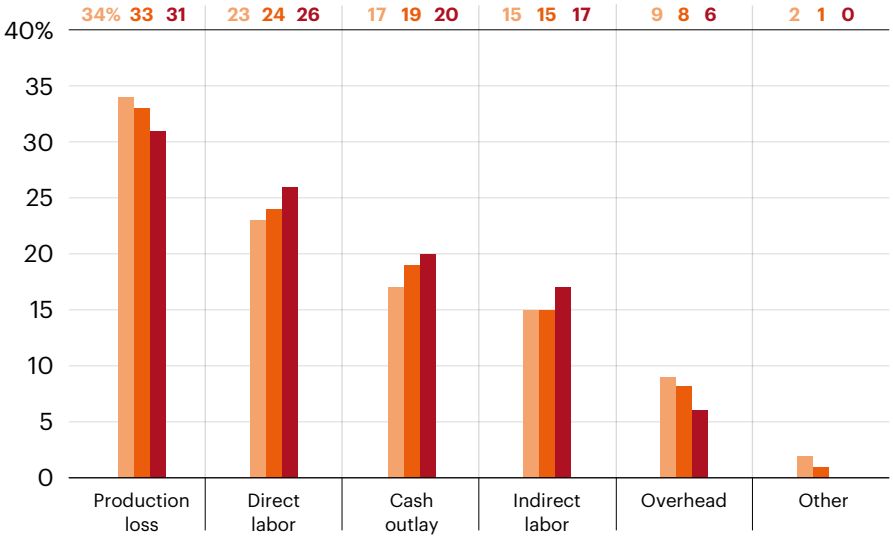


FIGURE 17
Percentage cost by specific components

Legend
Consolidated view
n = 254 companies

FY 2015
FY 2016
FY 2017

How companies allocate resources and achieve cost savings

KEY FINDING 13

Budget allocations are slowly shifting from the network to application and data layers.

Figure 18 summarizes six layers in a typical multi-layered IT security infrastructure for all benchmarked companies. Each bar reflects the percentage dedicated spending according to the presented layer. The network layer receives the highest allocation at 27 percent of total dedicated IT security funding. At only six percent, the host layer receives the lowest funding level.

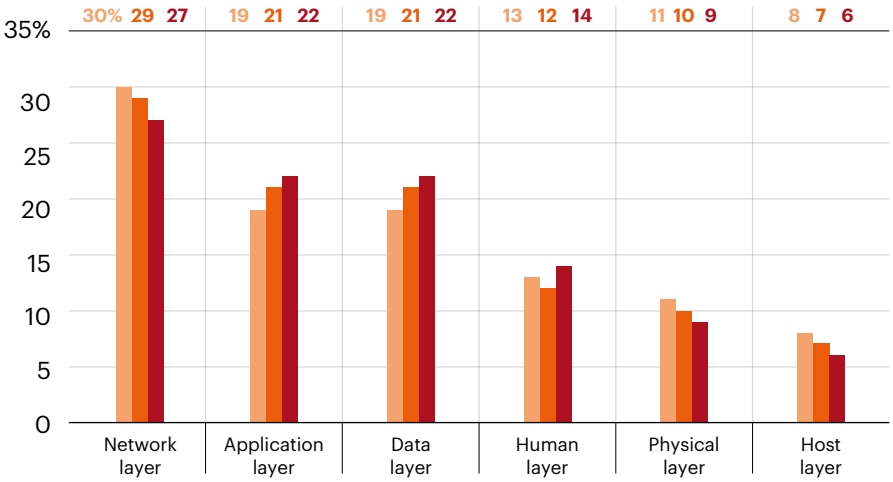


FIGURE 18
Percentage spending levels by six IT security layers

Legend
Consolidated view
n = 254 companies

FY 2015
FY 2016
FY 2017

Figure 19 shows nine enabling security technology categories by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: security intelligence systems (67 percent), access governance tools (63 percent), and advanced perimeter controls (58 percent). Cyber analytics and UBA and automation, orchestration and machine learning are not widely deployed (32 percent and 28 percent, respectively).

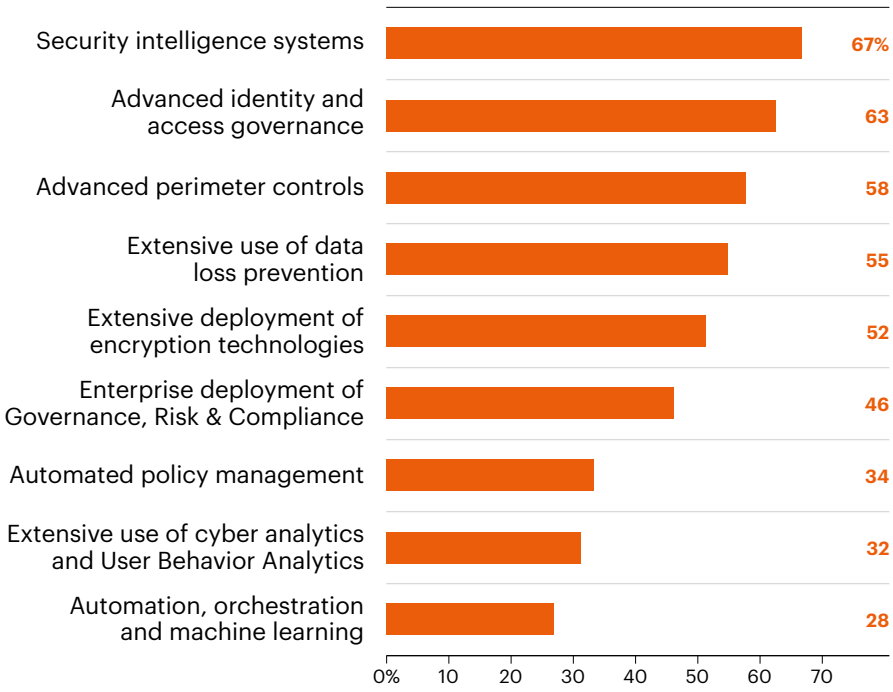


FIGURE 19
Nine enabling security technologies deployed

Legend
Consolidated view
n = 254 companies

Percentage deployment frequency

KEY FINDINGS

Figure 20 shows the money companies can save by deploying each one of nine enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of US$2.8 million.

Similarly, companies deploying advanced identity and access governance tools experience cost savings of US$2.4 million on average. While not widely used, automation, organization and machine learning can provide significant cost savings (an average of US$2.4 million). Please note that these extrapolated cost savings are independent of each other and cannot be added together.

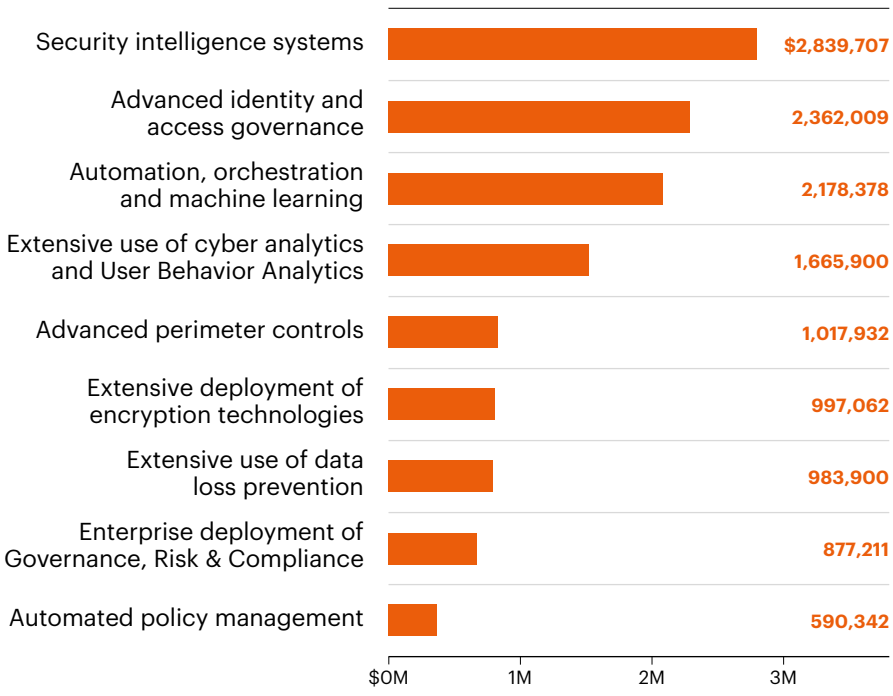


FIGURE 20
Cost savings when deploying enabling technologies

Legend
Consolidated view
n = 254 companies

Annual cost savings (US$)

KEY FINDING 14

Security intelligence systems have the biggest return on investment.

Figure 21 summarizes the estimated return on investment (ROI) realized by companies for each one of the nine categories of enabling security technologies.[5] At 21.5 percent, companies deploying security intelligence systems, on average, experience a substantially higher ROI than all other technology categories in this study.

Also significant are the estimated ROI results for companies that utilize advanced identity and access governance and automation, orchestration and machine learning technologies (19.7 percent and 17.1 percent, respectively). The estimated average ROI for all nine categories of enabling security technologies is 14.1 percent.

5: The return on investment calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years. The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value.

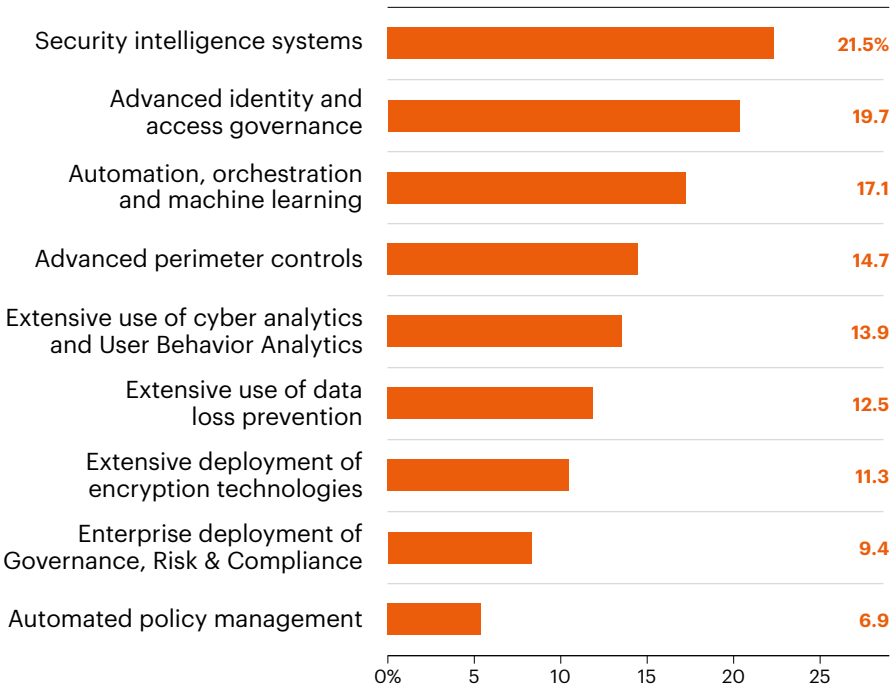


FIGURE 21
Estimated ROI for enabling security technologies

Legend
Consolidated view
n = 254 companies

■ Estimated annual return on investment (ROI)

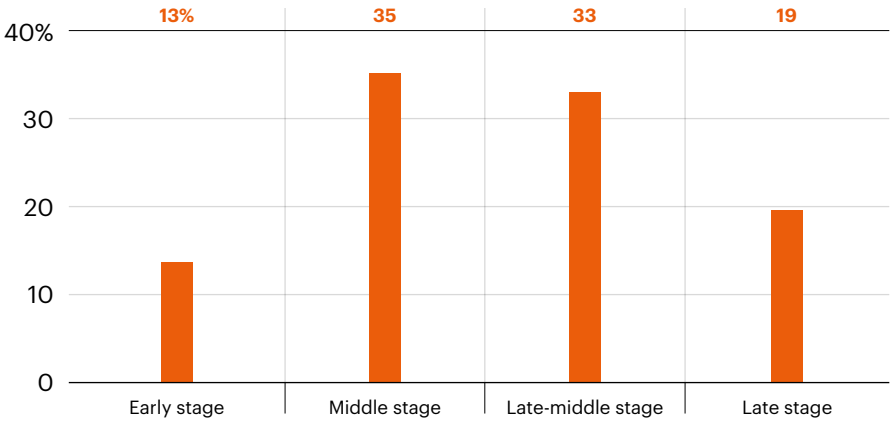


FIGURE 22
Distribution of the sample according to program maturity stage

Legend
n = 254 companies

■ Stages of IT security program maturity

Maturity and effectiveness of an organization's security posture

KEY FINDING 15

Program maturity is weighted toward the middle stages.

Figure 22 reports the distribution of our global sample of 254 companies according one of four maturity stages of the cybersecurity program, defined as follows:

- Early stage—many cybersecurity program activities have not as yet been planned or deployed
- Middle stage—cybersecurity program activities are planned and defined but only partially deployed
- Late-middle stage—many cybersecurity program activities are deployed across the enterprise
- Mature stage—most cybersecurity program activities are deployed across the enterprise

As can be seen, 35 percent of the sample is located in the middle stage. Only 13 percent of the sample is located in the early stage. Another 19 percent is located in the late stage.

KEY FINDING 16

Findings reveal a non-linear relationship between total cost of cyber crime and maturity stage of the cybersecurity program.

As can be seen in Figure 23, organizations in the early stage experience the lowest total cost at US$8.32 million. Middle stage organizations experience the highest total cost at US$13.87 million.

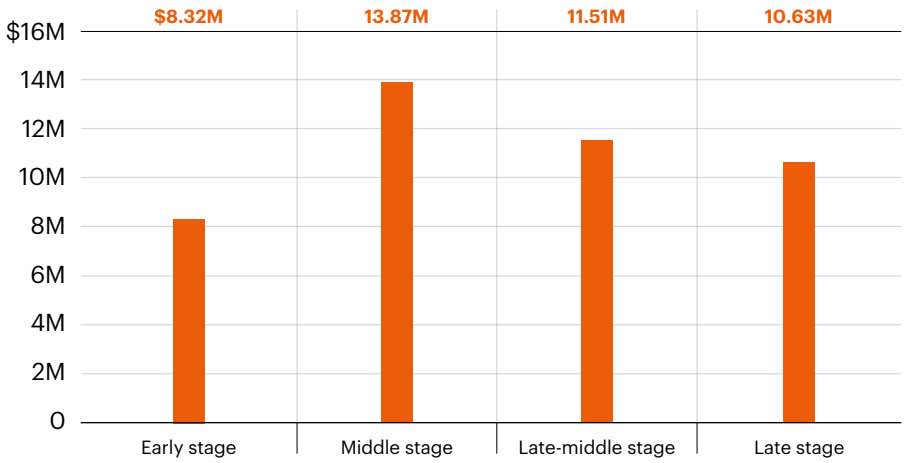


FIGURE 23
Total cost by program maturity stage

Legend
Mean = $11.7
n = 254 separate companies

Total cost (US$ millions)

KEY FINDING 17

Two countries have a negative security effectiveness score.

To better understand how security practises affect the total cost of cyber crime, we split the sample according to each company's security posture, which is measured by the Security Effectiveness Score (SES). Ponemon Institute developed this proprietary benchmarking methodology more than 10 years ago. The SES score is derived from rating numerous security practises, including the deployment of enabling security technologies.

This method has been validated from more than 50 independent studies conducted for more than a decade. The SES provides a range of +2 (most favorable) to -2 (least favorable) with a theoretical mean of zero. Hence, a score greater than zero is viewed as net favorable and a score less than zero is net unfavorable. A high favorable score (such as +1 or above) indicates that the organization's investment in people and technologies is both effective in achieving its security mission and is efficient in utilizing limited resources.

It is our belief that companies with a high SES are more cyber resilient and will have methods that will lessen the cost impact of cyber crimes. The mean SES for all 254 companies in our global sample is +.57. The highest SES was +1.76 and the lowest SES was -1.61. Figure 24 shows the mean SES by country sample. Germany achieved the highest overall SES at +1.03. In contrast, Italy had the lowest SES at -0.15. net favorable and a score less than zero is net unfavorable.

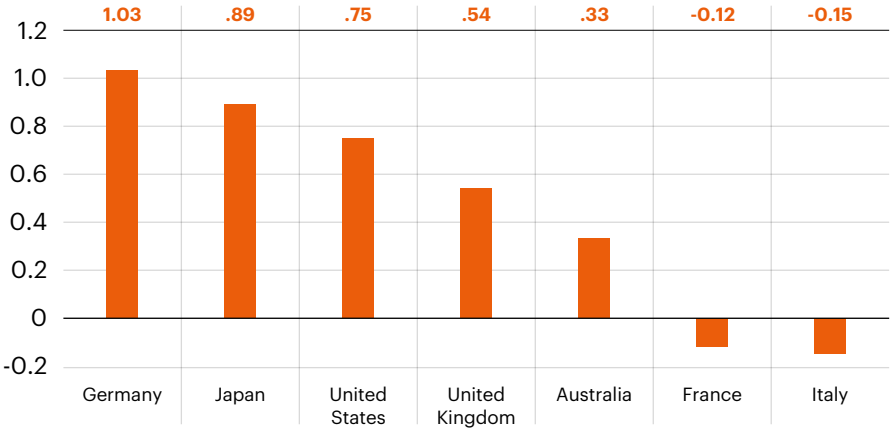


FIGURE 24
Average SES by country samples

Legend
Mean = +57
n = 254 separate companies

Security effectiveness score (SES)

KEY FINDING 18

The findings reveal a high SES decreases the total cost of cyber crime.

Organizations in the highest SES quartile experienced an average total cost of cyber crime at US$9.0 million. In contrast, organizations in the lowest SES quartile experienced an average total cost at US$15.3 million, as shown in Figure 25.

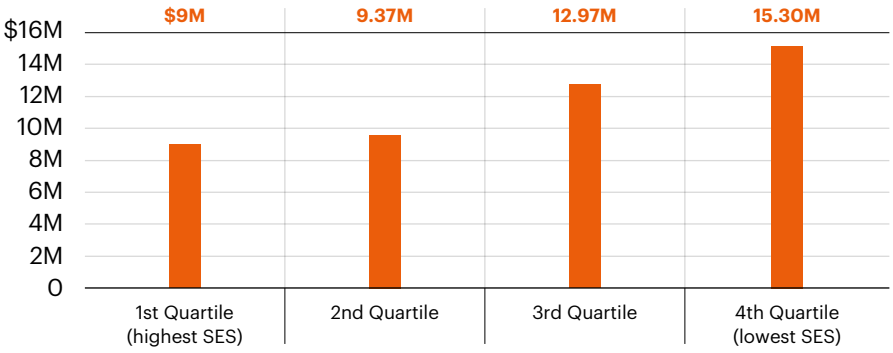


FIGURE 25
Total cost of cyber crime by SES quartile
US$ millions

Legend
Mean = $11.7
n = 254 separate companies

Total annualized cost ($US millions)

KEY FINDING 19

More investment is needed in breakthrough technologies.

Figure 26 presents the results of two independent rankings. The first ranking shows the order of nine (9) enabling security technologies as defined above. As shown, security intelligence systems provide the greatest cost savings, thus earning a rank equal to 9. In contrast, automated policy management provides the lowest savings, with a rank equal to 1.

The second ranking shows the order of enabling security technologies based on the percentage spending level during FY 2017. Here, security intelligence systems has a rank of 3 (third from the bottom). In terms of spending level, advanced perimeter controls has the highest rank of 9, but only a rank of 5 with respect to cost savings. Hence, differences or value gaps between these two rankings suggest possible inefficiencies in the allocation of resources on security solutions.

KEY FINDINGS

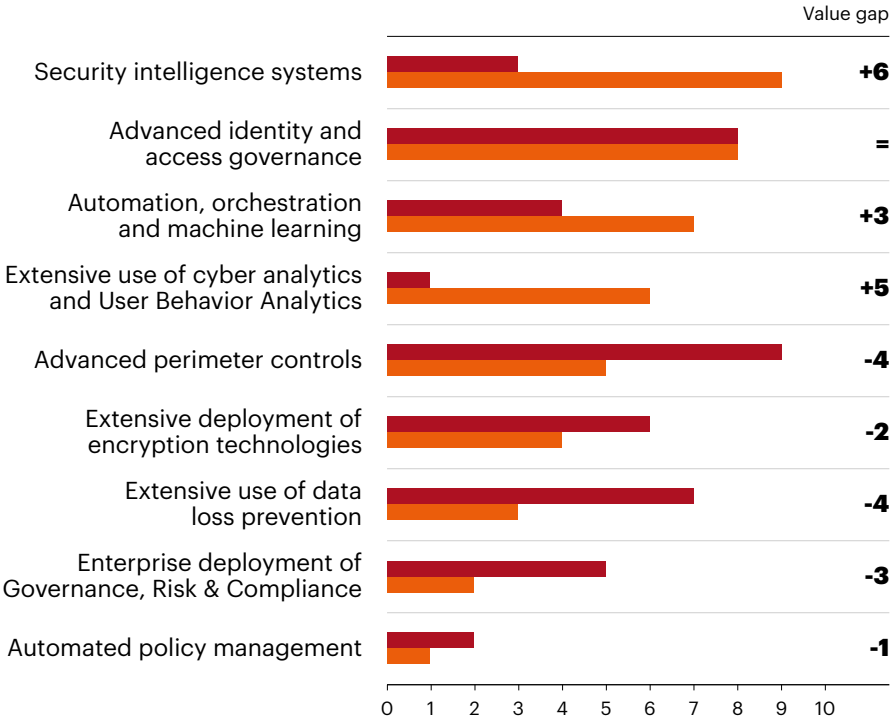


FIGURE 26
Rank orderings by spending levels and cost savings

Legend
9 = Highest rank
1 = Lowest rank

- Rank by percentage spending
- Rank by cost savings

COST OF CYBER CRIME
Frequently Asked Questions

What types of cyber attacks are included in this research?
For purposes of this study, we define cyber attacks as criminal activity conducted through the organization's IT infrastructure via the internal or external networks or the Internet. Cyber attacks also include attacks against industrial controls. A successful cyber attack is one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

How does benchmark research differ from survey research?
The unit of analysis in the *2017 Cost of Cyber Crime Study* is the organization. In survey research, the unit of analysis is the individual. In our experience, a traditional survey approach does not capture the necessary details required to extrapolate cyber crime costs. We conduct field-based research that involves interviewing senior-level personnel about their organizations' actual cyber crime incidents.

How do you collect the data?
In our 2017 study, our researchers collected in-depth qualitative data through 2,182 separate interviews conducted over a 10-month period in 254 companies in seven countries: the United States, the United Kingdom, Germany, France, Italy, Australia and Japan. In each of the 254 participating organizations, we spoke with IT, compliance and information security practitioners who are knowledgeable about the cyber attacks experienced by the company and the costs associated with resolving the cyber crime incidents. For privacy purposes we did not collect organization-specific information.

ABOUT THE RESEARCH

How do you calculate the cost?

To determine the average cost of cyber crime, organizations were asked to report what they spent to deal with cyber crimes over four consecutive weeks. Once the costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost. These are costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to reduce business disruption and the loss of customers. These costs do not include expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Are you tracking the same organizations each year?

For consistency purposes, our benchmark sample consists of only larger-sized organizations (that is, a minimum of approximately 1,000 enterprise seats).[6] Each annual study involves a different sample of companies. In short, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach.

6: Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Framework

The purpose of this research is to provide guidance on what a successful cyber attack can cost an organization. Our 2017 Cost of Cyber Crime Study is unique in addressing the core systems and business process-related activities that drive a range of expenditures associated with a company's response to cyber crime. Cost figures have been converted into United States dollars for comparative purposes.[7]

In this study, we define a successful attack as one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

Figure 27 presents the activity-based costing framework used to calculate the average cost of cyber crime. Our benchmark methods attempt to elicit the actual experiences and consequences of cyber attacks. Based on interviews with a variety of senior-level individuals in each organization we classify the costs according to two different cost streams:

- The costs related to dealing with the cyber crime or what we refer to as the internal cost activity centers.
- The costs related to the consequences of the cyber attack or what we refer to as the external consequences of the cyber attack.

7: *The Wall Street Journal*'s August 16, 2017 currency conversion rates.

ABOUT THE RESEARCH

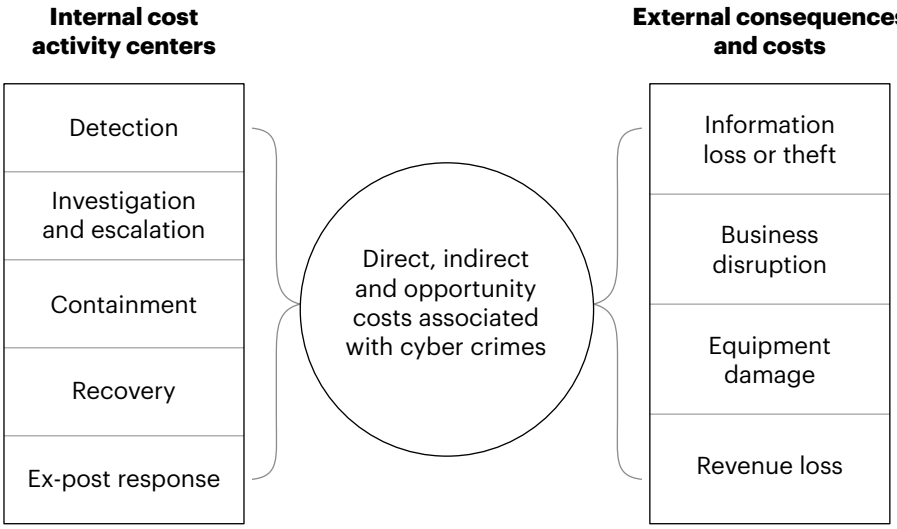


FIGURE 27
Cost framework for cyber crime

We analyzed the internal cost centers sequentially—starting with the detection of the incident and ending with the ex-post or final response to the incident, which involves dealing with lost business opportunities and business disruption. In each of the cost activity centers we asked respondents to estimate the direct costs, indirect costs and opportunity costs. These are defined as follows:

- Direct cost—the direct expense outlay to accomplish a given activity.
- Indirect cost—the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- Opportunity cost—the cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident.

External costs, including the loss of information assets, business disruption, equipment damage and revenue loss, were captured using shadow-costing methods. Total costs were allocated to nine discernible attack vectors: viruses, worms, trojans; malware; botnets;

Web-based attacks; phishing and social engineering; malicious insiders; stolen or damaged devices; malicious code (including SQL injection); and denial of services.[8]

This study addresses the core process-related activities that drive a range of expenditures associated with a company's cyber attack. The five internal cost activity centers in our framework include:[9]

Detection

Activities that enable an organization to reasonably detect and possibly deter cyber attacks or advanced threats. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.

Investigation and escalation

Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents. The escalation activity also includes the steps taken to organize an initial management response.

Containment

Activities that focus on stopping or lessening the severity of cyber attacks or advanced threats. These include shutting down high-risk attack vectors such as insecure applications or endpoints.

8: We acknowledge that these nine attack categories are not mutually independent and they do not represent an exhaustive list. Classification of a given attack was made by the researcher and derived from the facts collected during the benchmarking process.
9: Internal costs are extrapolated using labor (time) as a surrogate for direct and indirect costs. This is also used to allocate an overhead component for fixed costs such as multi-year investments in technologies.

ABOUT THE RESEARCH

Recovery

Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and other IT (data center) assets.

Ex-post response

Activities to help the organization minimize potential future attacks. These include containing costs from business disruption and information loss as well as adding new enabling technologies and control systems.

In addition to the above process-related activities, organizations often experience external consequences or costs associated with the aftermath of successful attacks—which are defined as attacks that infiltrate the organization's network or enterprise systems. Accordingly, our research shows that four general cost activities associated with these external consequences are as follows:

Cost of information loss or theft

Loss or theft of sensitive and confidential information as a result of a cyber attack. Such information includes trade secrets, intellectual properties (including source code), customer information and employee records. This cost category also includes the cost of data breach notification in the event that personal information is wrongfully acquired.

Cost of business disruption

The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements.

Cost of equipment damage

The cost to remediate equipment and other IT assets as a result of cyber attacks to information resources and critical infrastructure.

Lost revenue

The loss of customers (churn) and other stakeholders because of system delays or shutdowns as a result of a cyber attack. To extrapolate this cost, we use a shadow costing method that relies on the "lifetime value" of an average customer as defined for each participating organization.

Benchmarking

The cost of cyber crime benchmark instrument is designed to collect descriptive information from IT, information security and other key individuals about the actual costs incurred either directly or indirectly as a result of cyber attacks actually detected. Our cost method does not require subjects to provide actual accounting results, but instead relies on estimation and extrapolation from interview data over a four-week period.

ABOUT THE RESEARCH

Cost estimation is based on confidential diagnostic interviews with key respondents within each benchmarked organization. Table 4 reports the frequency of individuals by their approximate functional discipline that participated in this year's global study.

TABLE 4
Individuals participating in the 2017 global study by functional discipline

Functional areas of interview participants	FREQUENCY	PERCENTAGE (%)
IT security	385	18
IT operations	401	18
Compliance	198	9
Data center management	185	8
Accounting & finance	116	5
Network operations	118	5
Legal	99	5
IT risk management	110	5
Physical security/facilities mgmt	98	4
Human resources	95	4
Internal or IT audit	80	4
Application development	69	3
Enterprise risk management	70	3
Procurement/vendor management	59	3
Industrial control systems	56	3
Quality assurance	43	2
TOTAL	**2,182**	**100**
Interviews per company on average	8.59	

Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number-line format.

The numerical value obtained from the number line, rather than a point estimate for each presented cost category, preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

Cost estimates were then compiled for each organization based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we administered general interview questions to obtain additional facts, including estimated revenue losses as a result of the cyber crime.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. In our experience, a survey focusing on process yields a higher response rate and better quality of results. We also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

To maintain complete confidentiality, the survey instrument did not capture company-specific information of any kind. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

We carefully limited items to only those cost activities we considered crucial to the measurement of cyber crime cost to keep the benchmark

instrument to a manageable size. Based on discussions with learned experts, the final set of items focused on a finite set of direct or indirect cost activities. After collecting benchmark information, each instrument was examined carefully for consistency and completeness. In this study, a few companies were rejected because of incomplete, inconsistent or blank responses.

Field research was conducted over several months, concluding in August 2017. To maintain consistency for all benchmark companies, information was collected about the organizations' cyber crime experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as other organizations in this study. The extrapolated direct, indirect and opportunity costs of cyber crime were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

Sample

The recruitment of the annual study started with a personalized letter and a follow-up telephone call to 1,701 contacts for possible participation and 254 organizations permitted Ponemon Institute to perform the benchmark analysis.

Chart 1 summarizes the current (FY 2017) sample of participating companies based on 15 primary industry classifications. As can be seen, financial services (16 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second and third largest segments include industrial (12 percent) and services (11 percent).

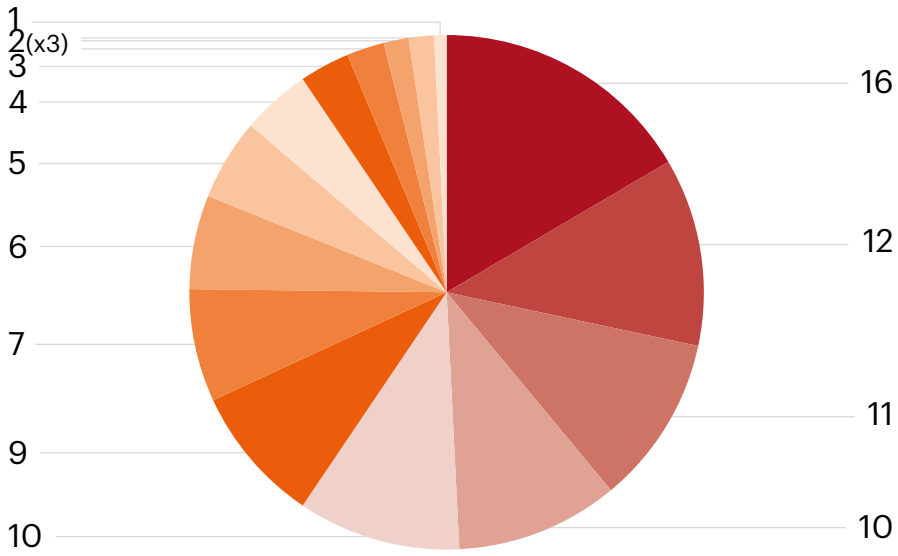


CHART 01
Industry sectors of participating organizations

Legend
Consolidated view
n = 254 separate companies

- Financial services
- Industrial/ manuf'ng.
- Services
- Tech and software
- Retail
- Public sector
- Utilities and energy
- Consumer products
- Healthcare
- Transportation
- Life science
- Hospitality
- Communications
- Education
- Aerospace and defense

Chart 2 shows the percentage frequency of companies based on the number of enterprise seats connected to networks or systems. Our analysis of cyber crime cost only pertains to organizations with a minimum of approximately 1,050 seats. In the 2017 global study, the largest number of enterprise seats exceeded 259,000.

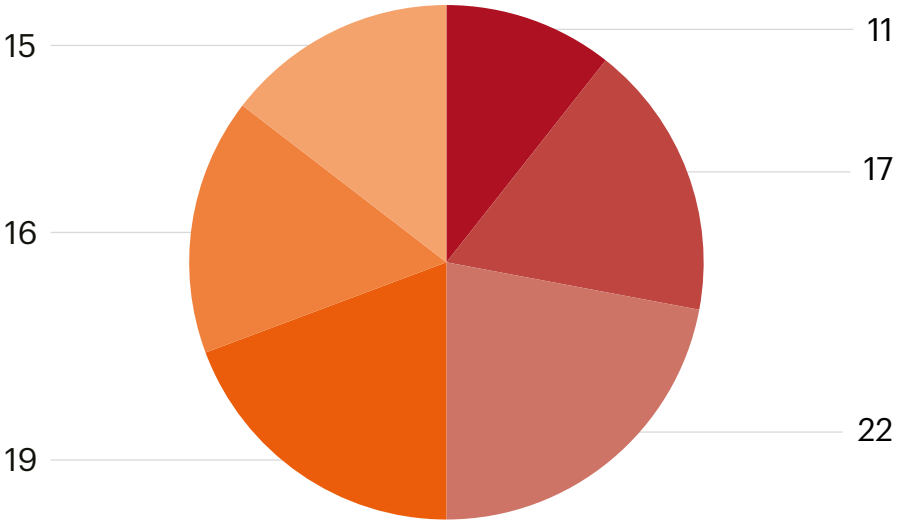


CHART 02
Distribution of participating organizations by enterprise seats (size)

Legend
Consolidated view
n = 254 separate companies

- < 2,000
- 2,000 to 5,000
- 5,001 to 10,000
- 10,001 to 15,000
- 15,001 to 25,000
- > 25,000

Limitations

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

Non-statistical results

The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations of mostly larger-sized entities experiencing one or more cyber attacks during a four-week fielding period. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.

Non-response

The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a targeted group of organizations, all believed to have experienced one or more cyber attacks. A total of 254 companies provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the cyber crime containment and recovery process, as well as the underlying costs involved.

Sampling-frame bias

Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature information security programs.

Company-specific information

The benchmark information is sensitive and confidential. The current instrument does not capture company-identifying information. It also enables individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

Unmeasured factors

To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

Estimated cost results

The quality of survey research is based on the integrity of confidential responses received from companies. Checks and balances were incorporated into the survey process. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.

CONTACT US

Kevin Richards
k.richards@accenture.com

Ryan LaSalle
ryan.m.lasalle@accenture.com

Matt Devost
matt.devost@accenture.com

Floris van den Dool
floris.van.den.dool@accenture.com

Josh Kennedy-White
j.kennedy-white@accenture.com

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49629 USA
1.800.887.3118
research@ponemon.org

Follow us @AccentureSecure

Connect with us

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. **Visit us at www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

ABOUT PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Enclosure (6)

Common Malware

Keylogger Malware

Financial Malware

The Truth About Malware

http://www.malwaretruth.com/the-list-of-malware-types/

May 2018

List of Common Malware Types:

This list of Malware types only scratches the surface in that Malware is being developed by those trying to gain access to your computer for monetary gain. The list of Malware types focuses on the most common and the general categories of infection

1. **Adware:**. The least dangerous and most lucrative Malware. Adware displays ads on your computer.

2. **Spyware**:. Spyware is software that spies on you, tracking your internet activities in order to send advertising (Adware) back to your system.

3. **Virus:** A virus is a contagious program or code that attaches itself to another piece of software, and then reproduces itself when that software is run. Most often this is spread by sharing software or files between computers.

4. **Worm:** A program that replicates itself and destroys data and files on the computer. Worms work to "eat" the system operating files and data files until the drive is empty.

5. **Trojan:** The most dangerous Malware. Trojans are written with the purpose of discovering your financial information, taking over your computer's system resources, and in larger systems creating a "denial-of-service attack " Denial-of-service attack: an attempt to make a machine or network resource unavailable to those attempting to reach it. Example: AOL, Yahoo or your business network becoming unavailable.

6. **Rootkit:** This one is likened to the burglar hiding in the attic, waiting to take from you while you are not home. It is the hardest of all Malware to detect and therefore to remove; many experts recommend completely wiping your hard drive and reinstalling everything from scratch. It is designed to permit the other information gathering Malware ~~in~~ to get the identity information from your computer without you realizing anything is going on.

7. **Backdoors:** Backdoors are much the same as Trojans or worms, except that they open a “backdoor” onto a computer, providing a network connection for hackers or other Malware to enter or for viruses or SPAM to be sent.

8. **Keyloggers:** Records everything you type on your PC in order to glean your log-in names, passwords, and other sensitive information, and send it on to the source of the keylogging program. Many times keyloggers are used by corporations and parents to acquire computer usage information.

9. **Rogue security software:** This one deceives or misleads users. It pretends to be a good program to remove Malware infections, but all the while it is the Malware. Often it will turn off the real Anti-Virus software. The next image shows the typical screen for this Malware program, Antivirus 2010

10. **Ransomware:** If you see this screen that warns you that you have been locked out of your computer until you pay for your cybercrimes. Your system is severely infected with a form of Malware called Ransomware. It is not a real notification from the FBI, but, rather an infection of the system itself. Even if you pay to unlock the system, the system is unlocked, but you are not free of it locking you out again. The request for money, usually in the hundreds of dollars is completely fake.

11. **Browser Hijacker:** When your homepage changes to one that looks like those in the images inserted next, you may have been infected with one form or another of a Browser Hijacker. This dangerous Malware will redirect your normal search activity and give you the results the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not removing the Malware lets the source developers capture your surfing interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in every case they allow other more infectious

Reviews of the Best USB Keyloggers

March 28, 2017

The term “keylogger” will strike fear in a lot of consumers. It’s been hijacked by news organizations trying to create a scary headliner, or antivirus companies looking to push higher volumes of software. While there are certainly instances of hackers using software keyloggers to steal private information, software is usually used because it’s easy to be controlled remotely. In reality, hardware keyloggers are far superior, and commonly used in legitimate situations.

Why would you need a hardware keylogger? Corporations often have them installed to monitor employee activity, and provide a backup of data entered. In other situations, keyloggers can be a form of protection. Having a keylogger installed on a data entry professionals computer is a good way to get a second copy of the file being entered, so any discrepancies can be verified at a later date.

Whether you’ve been given the task of purchasing this hardware for a multinational corporation, or you’re just looking for a way to back up your own personal data, there are a few decisions that need to be made. USB keyloggers aren’t the same simple devices that were available a few years ago. Today, thanks to integrated technology, there are a ton of great features that have never been possible before. Let’s take a look at the three best USB keyloggers on the market. We’ll help you understand the differences between them, and find the model that’s right for you.

Keyllama 8MB USB Forensic Keylogger

As one of the premier names in Keyloggers, Keyllama is often trusted with legal matters where reliability is crucial. They focus on a hardware centric approach, not relying on any questionable software to do the job. This keylogger is capable of storing quite a lot of data, and has an extremely low failure rate.

Design

Above all, the **Keyllama 8MB USB Forensic Keylogger** is designed to be discreet. Looking like littler more than just a tiny USB memory key, it is one of the most minimalist looking keyloggers on the market. When fully installed, it only extends 1.8” from the back of your machine. Just connect it to any available USB port on the machine that you

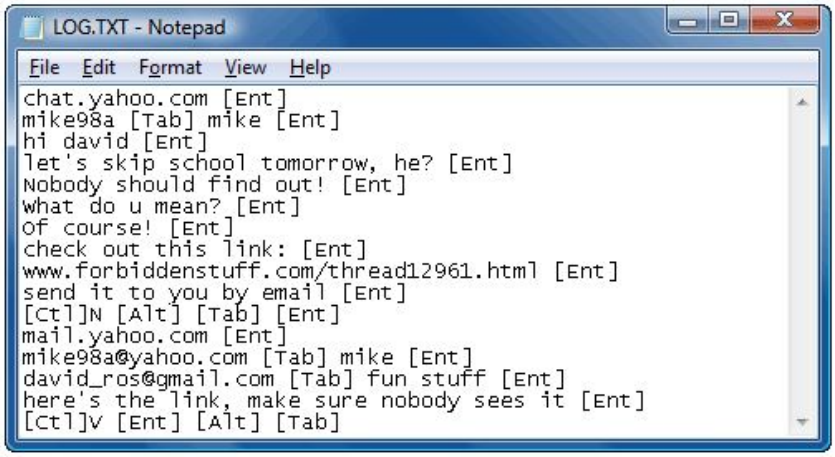
want to log, then plug the USB input device into the back of it. When installed like this, there is very little to catch the eye.

The black plastic enclosure is built to a very high standard, and it feels extremely durable in the hand. Both the male and female USB ports have solid feels to them, inserting with a firm “click.” One of the things we always look for in USB keyloggers is a quality bond between the male USB plug and the board itself. Because there will be a little more pressure on the logger from the cord pulling on the other end, there is risk for damage. Fortunately, we found that this model was built to a very high standard.

Functionality

This USB keylogger operates exclusively using hardware. It simply measures the data being transmitted by the keyboard, records it, then passes the data back through to the computer. From the software side of things, there is absolutely no way for the software to detect this system.

When you first go to set it up, you’ll need to select a password. This password isn’t just to allow you to access the data inside, but also to set up the complex encryption algorithm. In the event that anyone got their hands on this keylogger, they would have no idea what data was inside without the password. It would be scrambled, looking like complete gibberish. This is essential in an environment where you’re working with sensitive data, as you wouldn’t want any private information to get into the wrong hands.



In terms of actually using the keylogger, it's very simple. Just plug it into your computer, enter the password at the prompt, and then it works just like a flash drive. There is 8MB of internal memory. Although this seems like very little, it is actually enough to store up to two years of typing information.

One of the nice features is the fact that it also records the data and time of each line. There is a small internal battery inside, so the time is kept accurate even when the host PC is turned off.

Security

The hardware encryption used in this system, in our eyes, is one of the best systems on the market. With just a single, user settable password, it's incredibly easy to use. But even though it's easy, that doesn't mean it's of low quality. The same encryption schemes are used by law enforcement agencies, making it one of the top choices.

Due to the way this keylogger works, it can also be used as an encrypted flash drive. While you won't be storing too much information in the 8MB of data, it is perfectly suitable for text files and documents.

KeyGrabber USB KeyLogger

Whether you're looking for an affordable model or a top tier solution, KeyGrabber is a brand you'll want to turn to. They've got some of the widest range of offerings, with a keylogger designed to suit almost any situation. The KeyGrabber USB Keylogger is one of the most affordable options on the market, while retaining the high standard we'd like to see.

Design

The design of the **KeyGrabber USB** is a little spunkier than many other models on the market. It's squared off appearance is slightly tapered at each end, with a large USB logo etched onto the face. It looks very intentional, bordering on utilitarian. If someone were to look at it, it seems like it should be there. It's not this mysterious black device connected to the computer, it's some kind of adapter. After all, it's got that USB logo on it!
Personally, if we were to encounter it without knowing what it was for, removing it would be the last thing we'd want to do. It seems as if it's necessary for the keyboard to

function. These changes might seem subtle to you, but it’s surprising how much a few small tweaks can chance our perception of the hardware we use.

Durability is one of the key features of this particular model. The USB port is much more reinforced than we’re used to seeing. You can especially tell on the female port, which has a full size metal guide that runs along the outside of the port. It’s very clear to us that it’s designed to handle the additional weight put on it by the USB cord coming from the keyboard.

Functionality

Like most hardware keyloggers, using this model is simple. Just plug it into the back of the computer, and plug the keyboard into the keylogger. From this point on, every single keystroke will be stored in the keylogger in a time-stamped text file, with one file for each date. This organization format makes it easy to browse through the logs and find the information you’re looking for.

For international users, the KeyGrabber has one unique feature that you’ll be happy to see. It automatically interprets the keystrokes and finds out the locale of the keyboard. If the user is using an international keyboard or a unique key layout, the files will be automatically adjusted to use the correct locale. This can correct issues where the text is garbled due to an incorrectly detected locale.

There is 16MB of internal storage in place, which is enough for use in very high volume applications. Even when users are typing up a storm 8 hours per day, there is still enough storage space for many months, or even years of data.

Security

The KeyGrabber USB uses security through obscurity. There is no encryption or any other privacy features built in. If you have physical access to the keylogger, you can read the data stored inside. That being said, this isn't a particularly common device. To users, it will look as if it's just a dongle for the keyboard. For that matter, the data is only reasonable when the keylogger is plugged in on its own. When there is something inserted into the USB port, it's in logging mode and will not appear on your computer. For this reason, most users will never find out it's true purpose.

KeyGrabber WiFi 2GB Keylogger

We mentioned earlier that KeyGrabber is has one of the most diverse product lines in the industry. If you're looking for the best of the best, look no further than this WiFi model. This is one of the only keyloggers on the market that allows you to access data without having to physically access it.

Design

When you've got something that is supposed to look discreet, it can be hard for manufacturers to differentiate their premium offerings from their affordable options. Despite these challenges, KeyGrabber seems to have pulled it off. While the design of the **KeyGrabber WiFi** is very similar to that of the USB model, the silver casing definitely makes it appealing.
Despite this singular visual change, everything we love about the USB version of this keylogger is back. The high quality components make for something that can last a very long time, so you don't have to worry about durability issues.

Functionality

At its core, this keylogger functions exactly like the USB version. This means that it's easy to set up, and supports a large range of external input devices from all around the globe. However, there is a whole new layer of high tech hardware on top. The 16MB of memory has been replaced with 2GB of flash storage.

At first, this seemed crazy to us. If 16MB can store an entire years' worth of keystrokes, upgrading to 2GB sounds insane, right? But the time you'd fill up the storage, we'll likely have moved on to fully virtual environments with holographic input devices.

In reality, the additional storage is for the firmware. Just like your computer, this teeny tiny piece of hardware is running a compact operating system. It uses a built-in WiFi chipset to connect to a wireless access point, so it can email the daily logs directly to you. This is very easy to get running using the included setup utility, and makes your job much easier.

Security

Although this drive is not encrypted, none of the data is accessible through the USB port. Once you set it up using the included utility, it operates as a ghost. The only device

that can access it is located on a remote server elsewhere, and anyone who stumbles across the key logger won't have any idea what it's purpose is.

Which USB Keylogger is Right for Me?

Not sure which to choose? The first thing you want to think about is the type of environment that you're going to be using it in. Will the end users know that it's being installed? Will they need to access the data? Or would you prefer to keep it secure?

Whether you're a parent monitoring your child or a business owner keeping tabs on how company resources are used, you'll likely want something that nobody can tamper with. In this case, you're best off selecting a wireless model. The **KeyGrabber WiFi Keylogger** is capable of transmitting all of your data remotely, so it can be used without having to interact with the logged computer. This is especially ideal in corporate environments, where you might be managing a large number of computers.
If you're logging data for auditing purposes, it's essential that you prove the data has been unaltered. In this case, the **Keyllama USB Keylogger** is a great choice. The data is fully encrypted, so you can prove that it has been unaltered from it's original form.
Looking to log your own computer for backup purposes? Grab yourself a **KeyGrabber USB Keylogger**. Not only is it one of the cheapest options on the market, but it's perfectly suited for an environment where you need quick access to the data by simply unplugging the keyboard and moving it to another USB port.

Top 10 Most Dangerous Financial Malware

https://heimdalsecurity.com/blog/top-financial-malware/
https://blog.barkly.com/top-banking-trojans-2017

1. Zbot/Zeus

Zeus, also known as **Zbot**, is a notorious **Trojan** which infects Windows users and tries to **retrieve confidential information** from the infected computers. Once it is installed, it also tries to download configuration files and updates from the Internet. The Zeus files are created and customized using a Trojan-building toolkit, which is available online for **cybercriminals**.

Zeus has been created to **steal private data** from the infected systems, such as system information, passwords**, banking credentials** or other financial details and it can be customized to gather banking details in specific countries and by using various methods. Using the retrieved information, **cybercriminals log into banking accounts** and make unauthorized money transfers through a complex network of computers.

Zbot/Zeus is based on the client-server model and requires a **Command and Control serverto** send and receive information across the network. The single Command and Control server is considered to be the weak point in the malware architecture and it is the target of law enforcement agencies when dealing with Zeus.

To counter this weak point, the latest variant of Zeus/Zbot have included a **DGA (domain generation algorithm),** which makes the Command and Control servers resistant to takedown attempts. The DGA generates a list of domain names to which the bots try to connect in case the Command and Control server cannot be reached.

Zeus/Zbot, known by many names including PRG and Infostealer, has already infected as many as 3.6 million systems in the United States. In 2009, security analysts found that the Zeus spread on more than 70,000 accounts of banks and businesses including NASA and the Bank of America.

2. Zeus Gameover (P2P) (Zeus family)

Zeus Gameover is a variant of the Zeus family – the infamous family of financial stealing malware – which relies upon **a peer-to-peer botnet infrastructure**.
The network configuration removes the need for a centralized Command and Control server, including a DGA (Domain Generation Algorithm) which **produces new domains in case the peers cannot be reached**. The generated peers in the botnet can **act as independent Command and Control servers** and are able to download commands or configuration files between them, finally sending the stolen data to the malicious servers.

Zeus Gameover is used by cybercriminals to **collect financial information**, targeting various user data from credentials, **credit card numbers** and passwords to any other private

information which might prove useful in retrieving **a victim's banking information.** GameOver Zeus is estimated to have infected 1 million users around the world.

3. SpyEye (Zeus family)

SpyEye is a data-stealing malware (similar to Zeus) created to steal money from online bank accounts. This malicious software is capable of stealing bank account credentials, social security numbers and financial information that could be used to empty bank accounts.

This banking Trojan contains **a keylogger** that tries to retrieve login credentials for online bank account. The attack toolkit is popular among cybercriminals because it can be customized to attack specific institutions or target certain financial data.

SpyEye is able to start a financial transaction as soon as a targeted user initiates an online operation from his bank account.

4. Ice IX (Zeus family)

Ice IX is a modified variant of Zeus, the infamous banking Trojan, one of the most sophisticated pieces of financial malware out there.

This modified variant is **used by cybercriminals with the same malicious purpose of stealing personal and financial information**, such as credentials or passwords for the e-mail or the online bank accounts.

Like Zeus, Ice IX can control the displayed content in a browser used for online banking websites. The injected web forms are used to extract banking credentials and other private security information.

Ice IX, the modified version of Zeus, improved a few Zeus capabilities. The most important one is a defense mechanism to evade tracker sites, which monitor at present most Command and Control servers controlled by Zeus.

5. Citadel (Zeus family)

Citadel appeared after the source code of the infamous Zeus leaked in 2011. Due to its open source character, the software code has been reviewed and improved by IT criminals for various malware attacks.

For cybercriminals, it is an advanced toolkit which they can use to **trick users into revealing confidential information and steal banking credentials**. The stolen credentials are then used by cybercriminals into accessing online accounts and running fraudulent transactions.

6. Carberp (Zeus family)

Carberp is a Trojan designed to give attackers the ability to **steal private information from online banking platforms** accessed by the infected PCs.

This Trojan's behavior is similar to the other financial malware in the Zeus family and displays stealth abilities from antimalware applications. Carberp is able to steal sensitive data from infected machines and download new data from command-and-control servers.

This Trojan is one of the most widely spread financial stealing malware in Russia. Primarily targeting banking systems and companies which perform a high number of financial transactions, Carberp is not only injecting a code into web pages, but it also tries to exploit several vulnerabilities in the target system so as to escalate to administrative privileges.

Distributed through the typical methods of using malicious e-mail attachments, drive-by downloads or by clicking on a deceptive pop-up window, what is different at this financial malware is the high number of legitimate web resources used to collect information and potentially make fraudulent transactions. It is indicated that cybercriminals have deployed botnets on over 25,000 infected machines.

7. Bugat (Zeus family)

Bugat is another banking Trojan, with similar capabilities to Zeus – the notorious data-stealing Trojan – which is used by IT criminals to steal financial credentials.

Bugat targets an infected user's browsing activity and harvests information during online banking sessions. It can upload files from an infected computer, download and execute a list of running processes or steal FTP credentials.

Bugat communicates with a command and control server from where it receives instructions and updates to the list of financial websites it targets.

The collected information is sent to the cybercriminal's remote server.

Cybercriminals spreads the malware mostly by inserting malicious links in the e-mails they send to the targeted users. When a user clicks a malicious link, he is directed to a dangerous website where the Bugat executable downloads on the system.

8. Shylock (Zeus family)

Shylock is a banking malware, designed to retrieve user's banking credentials for fraudulent purposes.

As soon as it is installed, Shylock communicates with the remote Command and Control servers controlled by the cybercriminals, sending and receiving data to and from the infected PCs. Similar to Zeus Gameover, this malware makes use of a (DGA) Domain generation algorithm which is used to generate a number of domain names that can be used receive commands between the malicious servers and the infected systems.

The Trojan is delivered mostly through drive-by downloads on compromised websites and via malvertising, where malicious code is inserted in adverts that are then placed on legitimate websites.

Another popular method of spreading this financial malware is by inserting malicious JavaScript **into a web page.** This technique produces a pop-up which pushes the user to download a plugin, apparently necessary for the media display on the website.

9. Torpig (Zeus family)

Torpig is a sophisticated type of malware program **designed to harvest sensitive information, such as bank account and credit card information from its victims.**

The Torpig botnet – the network of compromised PCs – which are under the control of cybercriminals are the main means for sending spam e-mails or stealing private information or credentials for the online bank accounts. Torpig also uses a DGA (domain generation algorithm) to generate a list of domains names and locate the Command and Control servers used by hackers.

Users are typically infected through drive-by downloads; a web page on a legitimate website is modified to ask the user for JavaScript code from a web location controlled by the IT criminals. The infected computers run phishing attacks to obtain sensitive data from its victims.

10. CryptoLocker

This malware encrypts your data and displays a message which states that your private information can be decrypted for a sum of money in a limited period of time. Though CryptoLocker can be removed by various security solutions, there isn't any way yet to decrypt the locked files.

CryptoLocker is one of the nastiest pieces of malware ever created. It's not just because it takes money from you or because it can access your private data, but once it manages to encrypt your information, there is no way for you to decrypt those files. This ransomware is so dangerous because the affected users have their private information disclosed (and taken advantage from) and they also lose the files without having any chance of recovering them.

CryptoLocker is a ransomware Trojan which can infect your system in different ways, but usually this happens through the means of an **apparently legitimate e-mail attachment**, from a well-known company or institution. Because it spreads through e-mail attachments, this ransomware is known to target companies and institutions through phishing attacks.

Enclosure (7)

Social Media
Social Networking Sites

60+ Social Networking Sites You Need to Know About in 2018

Updated June 2018

Human nature by default has been programmed to be socially active to a certain extent. Some people are more active, while others are less so!

However, people have always been looking for ways to connect and network with each other. And, in this age of digitization, people have found ways to be socially active on the internet, which is possible with the advent of the numerous social networking platforms and apps.

Now, even relationships begin, grow and end on social media. People no longer need a personal handshake or face-to-face meeting.

Social media sites have also grown in numbers by leaps and bounds. As per the statistics revealed on Statista, approximately 2 billion users used social networking sites and apps in 2015. And, with the increased use of mobile devices, this number is likely to cross the 2.6 billion mark by 2018.

So, in this article, we discuss some of the most popular social media sites that are being explored by the world today. You can find out if your favourite social media platform is a part of this list and even learn about some really good online social platforms that you can start using today.

1 – Facebook

Number of active users per month: 1.59 billion approximately

This is easily the largest social networking site in the world and one of the most widely used. And, Facebook was perhaps the first that surpassed the landmark of 1 billion user accounts.

Apart from the ability to network with friends and relatives, you can also access different Facebook apps to sell online and you can even market or promote your business, brand and products by using paid Facebook ads.

Recently Facebook has lost the trust of millions of its users by allowing 3rd parties to access over 87 million users' personal data. This is a massive breech of trust and has created a feeling of unrest amongst the social media platform's audience. So much so that there is now a #deletefacebook campaign where people are completely removing themselves from Facebook and using other networks instead. If you're concerned about what Facebook is doing with your data, then why not check out my guide on alternatives to Facebook, and see if there's a better place for you to interact with family and friends.

2 – WhatsApp

Number of active users per month: 1 billion approximately

Despite having been acquired by Facebook in 2014, this instant messaging platform exists as an independent entity. It arrived on the scene much later than Facebook, but has been able to capture the imagination of millions of people across the world by giving them the ability to communicate and share instantly with individuals and groups. The WhatsApp call feature is just the icing on the cake!

3- QQ

Number of active users per month: 853 million approximately

Tencent QQ (more popularly known as QQ) is an instant messaging (chat-based) social media platform. It became international (with more than 80 countries using it), after it was launched in China. It can be used to stay in touch with friends through texts, video calls and voice chats. It even has a built-in translator to translate your chats. To find out more, head over to our Chinese Social Media stats page.

4 – WeChat
Number of active users per month: 697 million approximately

This is an all-in-one communications app for messaging and calling (similar to WhatsApp) that enables you to connect with the people of your choice. It was also developed by Tencent in China and can easily work alongside QQ. As per the BI intelligence report, the number of WeChat users are fast catching up with the number of WhatsApp users.

Related article: WeChat keyboard shortcuts

5 – QZone
Number of active users per month: 640 million approximately

Like QQ and WeChat, QZone is yet another social networking service developed by Tencent. It enables you to share photos, watch videos, listen to songs, write blogs, maintain diaries and so on. It also empowers you to choose the accessories and customize the look and feel of your QZone webpages.

6 – Tumblr
Number of active users per month: 555 million approximately

Having been owned by Yahoo since 2013, Tumblr serves as a social media cum micro blogging platform that can be used to find and follow things that you like. You can also use it to post anything, including multimedia, to a short-form blog. Moreover, it gives you the flexibility to customize almost everything.

7 – Instagram

Number of active users per month: 400 million approximately

Instagram was launched as a unique social networking platform that was completely based on sharing photos and videos. This photo sharing social networking app thus enables you to capture the best moments of your life, with your phone's camera or any other camera, and convert them into works of art.

This is possible because Instagram allows you to apply multiple filters to your photos and you can easily post them to other popular social networking sites, such as Facebook and Twitter. It is now part of the Facebook empire. Learn how to grow your Instagram audience.
Read more on Instagram Tools to help you increase social engagement and audience numbers.

8 – Twitter

Number of active users per month: 320 million approximately

This social networking site enables you to post short text messages (called tweets), containing a limited number of characters (up to 140), to convey your message to the world. With the growing craze for online shopping, Twitter also makes it possible to promote your businesses and even shop directly through tweets. Learn how to create the perfect Twitter profile.

9– Google+

Number of active users: 300 million approximately

Owned by the tech giant Alphabet (Google), this interest-based social networking platform enables you to stay in touch with people by sharing messages, photos, videos, useful links to sites and so on. It also extends support for video conferencing through Hangouts and allows businesses to promote their brands and products through Google+ business pages.

10 – Baidu Tieba

Number of active users per month: 300 million approximately

Offered by Baidu of China, a search engine company, Baidu Tieba (known as Postbar internationally) is a social forum network based on the keyword searches in the Baidu search engine. This discussion forum works on the unique concept of allowing you to create a social network group for a specific topic, using the search, or even to join an existing online social group.

11 – Skype
Number of active users per month: 300 million approximately

Skype, owned by Microsoft, is one of the most popular communication-based social networking platforms. It allows you to connect with people through voice calls, video calls (using a webcam) and text messaging. You can even conduct group conference calls. And, the best part is that Skype-to-Skype calls are free and can be used to communicate with anyone, located in any part of the world, over the internet.

12 – Viber
Number of active users per month: 249 million approximately

This multi-lingual social platform, which is available in more than 30 languages, is known for its instant text messaging and voice messaging capabilities. You can also share photos and videos and audio messages, using Viber. It offers you the ability to call non-Viber users through a feature named Viber Out.

13 – Sina Weibo
Number of active users per month: 222 million approximately

This is a highly popular microblogging social platform in China that is known for its hybrid mix of Twitter's and Facebook's features.

14 – LINE
Number of active users per month: 215 million approximately

LINE is a globally available messaging social network that enables you to share photos, videos, text messages and even audio messages or files. In addition, it allows you to make voice and video calls at any time of the day.

15 – Snapchat
Number of active users per month: 200 million approximately

This is an image messaging social platform that enables you to chat with friends by using pictures. It allows you to explore news and even check out live stories that are happening around the world.

16 – YY
Number of active users per month: 122 million approximately

YY is a major video-based social networking platform in China that enables group video chats. In such chats, more than 100,000 members can watch a single person doing an activity. Such an activity can be anything from giving a tutorial video to singing karaoke, which helps the users earn virtual currency that they can later convert into cash.

17 – VKontakte (VK)
Number of active users per month: 100 million approximately

VK is one of the largest social networking platforms in Russia and has quite similar features to Facebook.

18 – Pinterest N
umber of active users per month: 100 million approximately

This is a photo sharing and visual bookmarking social media site or app that enables you to find new ideas for your projects and save them. So, you can do DIY tasks or home improvement projects, plan your travel agenda and so on by using Pinterest.

19- LinkedIn

Number of active users per month: 100 million approximately

LinkedIn is easily one of the most popular professional social networking sites or apps and is available in over 20 languages. It is used across the globe by all types of professionals and serves as an ideal platform to connect with different businesses, locate and hire ideal candidates, and more. It boasts over 400 million members.

20 – Telegram

Number of active users per month: 100 million approximately

This instant messaging network is similar to WhatsApp and is available across platforms in more than eight languages. However, Telegram has always focused more on the privacy and security of the messages you send over the internet by using its platform. So, it empowers you to send messages that are encrypted and self-destructive. This encryption feature has only just been made available for WhatsApp, whereas Telegram has always provided it.

21 – Reddit

Number of active users per month: 100 million approximately

This social media platform enables you to submit content and later vote for the content. The voting determines whether the content moves up or down, which is ultimately organized based on the areas of interest (known as subreddits).

22 – Taringa

Number of active users: 75 million approximately

Taringa is one of the largest social networking platform in Latin America and allows users to share their experiences, content and more.

23 – Foursquare
Number of active users: 40 million approximately

This is a local search- and discovery-based social media platform that enables you to find the ideal places (based on your location) to go to with friends and loved ones. It also gives appropriate search results for the best food outlets, night entertainment places and more in your area. The social networking feature is now available in a separate app named Swarm.

24 – Renren
Number of active users per month: More than 30 million approximately

This is the largest social networking site in China and is literally a platform for everyone. It has been highly popular with the youth due to its similarity to Facebook, as it allows users to easily connect with others, quickly share thoughts and posts, and even update their moods.

25 – Tagged
Number of active users: 25 million approximately

This is a great social media site based on friendship and dating and, in 2011, it acquired another social networking platform called hi5. It enables you to socialise with others through games, browsing profiles, common interests and so on.

26 – Badoo

Number of active users per month: 20 million approximately

This dating-based social networking site operates in more than 200 countries. It shares details about people nearby in your area and even about people whom you may have bumped into in real life.

27 – Myspace
Number of active users: 20 million approximately

This is a music-focused social networking site and provides an interactive and user-submitted network of friends. It also provides blogs, groups, personal profiles, pictures, videos and so on.

28 – StumbleUpon
Number of active users: 25 million approximately

StumbleUpon is an intelligent social networking platform that finds or discovers content and recommends the same to its users. You are thus empowered to discover webpages, images, videos and so on and then rate them as per your interest and taste.

29 – The Dots

the-dots.com is a networking platform that helps everyone involved in the creative process connect, collaborate and commercialise helping build a stronger, more profitable and diverse creative sector. Born out of a genuine passion to make the creative industries more open and meritocratic, founder Pip Jamieson launched the platform in the UK in 2014.

30 – Kiwibox

This is a community-based social networking site, especially for those who live in New York. It offers an online magazine to target teens through fashion tips, advice and chat. It also allows young adults to let everyone know about their skills and interests.

31 – Skyrock

Skyrock is a French social networking site that offers its users a free and personal web space to create and post blogs, add profiles and exchange messages. Apart from French and English, it is also available in five other languages.

32 – Delicious

It is known for being the leading social bookmarking service. Having been launched in 2003, Delicious is ideal for storing, sharing and discovering web bookmarks. It also allows its users to tag them with any keywords.

33 – Snapfish

Snapfish is a web-based photo sharing social networking site that offers unlimited storage to its members for uploading photos. You can thus put away your storage space concerns for your vast collection of images.

34 – ReverbNation

This is the ideal social networking platform for musicians and professionals to connect with others in the music industry. It offers different tools to musicians to manage their careers and offers them the right access to their music industry partners and fans.

35 – Flixster

This is an American social networking site for people who love movies and want to connect with like-minded people by sharing their movie reviews and ratings. Its users are likely to learn about movies and get information about new movies.

36 – Care2

This social media site helps activists connect around the globe with similar individuals, businesses and organisations that are making an impact on society. It also encourages people to lead a healthy and green lifestyle.

37 – CafeMom

This ad-supported social networking website is a community for mothers and mothers-to-be that enables them to get support and advice on various topics, such as pregnancy, fashion, health and food. It also helps them learn from the experiences of other mothers.

38 – Ravelry

Ravelry is a community-based social network that is targeted at people who are interested in fibre arts, such as spinning, knitting, weaving and crocheting. Such people can share their own collections, different ideas and learn from the experiences of other members for better collaboration possibilities.

39 – Nextdoor

This is a private social networking platform for neighbourhoods in the US. The objective is pretty simple: allowing users to get connected with the people in their area.

40 – Wayn

Wayn is a travel- and lifestyle-based social networking platform and offers its users the ability to discover where to go, what to do and how to meet like-minded people to share their experiences.

41 – Cellufun

This social gaming community can easily be accessed on the move from any mobile device. With this mobile gaming-based social network, users can socialise, create avatars, play games and purchase virtual goods.

42 – YouTube

YouTube is the world's largest video-sharing social networking site that enables users to upload and share videos, view them, comment on them and like them. This social network is accessible across the globe and even enables users to create a YouTube channel where they can upload all their personally recorded videos to showcase to their friends and followers.

43 – Vine

This is an entertainment-based, short-form video sharing social media site where members can easily share videos that are six seconds long. It belongs to the Twitter family and allows easy integration with other social networking platforms to share and watch videos.

44 – Classmates

Classmates allows users to find, connect and keep in touch with friends and acquaintances from school and college. It is also possible for users to upload their yearbook from their school years.

45 – MyHeritage

This is an online genealogy social platform which supports more than 42 languages and empowers its users to create family trees, upload and browse through family photos and manage their own family history. It could also be used by people to find their ancestors and get more information about them.

46 – Viadeo

Viadeo is an online business-based social networking site that helps business people, mostly those in Europe, connect with one another. It is available in about different languages.

47 – Xing

This professional social networking site offers features that are similar to LinkedIn's features, with its main users based in Switzerland, Austria and Germany. However, it is unique in the sense that it enables closed group discussions between the members of a certain company or business.

48 – Xanga

This blogging-based social networking platform hosts weblogs, photo blogs and social networking profiles for its users.

49 – LiveJournal

This San Francisco-based social networking site is available in Russia, as Zhivoy Zhurnal or Zhe Zhe. It enables users to maintain a diary, blog or journal, along with privacy controls.

50 – Friendster

Friendster was previously a social networking site to find friends and stay in touch, but is now a social gaming network for game lovers in Asia.

51 – Funny or Die

This comedy video social website is aimed at bringing together the funniest videos from the web. Celebrities follow this social platform a lot and it enables users to share, upload and rate videos.

52 – Gaia Online

Gaia Online is an anime-themed social networking and forums-based website. It gives users access to avatars, virtual world, games and so on.

53 – We Heart It

This photo-sharing social media site, which is available in more than 20 languages, is ideal for users' daily dose of inspiration or motivation. It enables users to view and share highly inspirational images with their friends.

54 – Buzznet

This social media site allows users to share content on the basis of their personal interests in the form of videos, photos and journals. It also seamlessly integrates with Facebook.

55 – DeviantArt

DeviantArt is regarded as the largest online social networking community for art lovers and artists. It enables users to take photos of their artwork and share them with others.

56 – Flickr

This is another highly popular photo-sharing website. It serves as a platform to upload numerous high quality images, especially by photographers or people who love photography. It is also an efficient online photo management and sharing service.

57 – MeetMe

Formerly known as myYearbook, MeetMe is aimed at users who want to find new friends and chat with them. This makes it highly popular among teens and young students.

58 – Meetup

This social networking portal enables you to find groups of like-minded people, who have similar interest to you, near your locality (anywhere in the world). It also facilitates offline group meetings and you can become a part of such groups and their discussions.

59 – Tout

Tout is a social networking cum micro-blogging platform that allows you to view and share videos that are 15 seconds long. The videos that are shared on this platform are known as touts.

60 – Mixi

This is a popular Japanese social networking service that has around 20 million active users. It enables you to connect with your friends and loved ones in a convenient way and even based on your areas of interest.

61 – Douban

This Chinese social networking site has something for registered as well as unregistered users. It enables registered users to record information and create content based on music, films, books and events in the cities of China. Unregistered users of Douban can find reviews and ratings of books, music and movies

Enclosure (8)

Small Home Office Security

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Small Office/Home Office Router Security

Introduction

Home routers have become an integral part of our modern society as our use of the internet has grown to include business from home, schoolwork, social networking, entertainment and personal financial management. Wired and now wireless routers have moved into our homes to facilitate this additional connectivity. The internet service provider (ISP) sells these devices pre-configured and ready to use. Users typically connect immediately to the internet without performing any additional configuration. They may not know how to perform additional configuration because it either seems too difficult, or they may be reluctant to spend the time with advanced configuration settings.

Unfortunately, the default configuration of most home routers offer little security and leave home networks vulnerable to attack. Small businesses and organizations that lack the funding for an information technology (IT) infrastructure and support staff often use these same home routers to connect to the internet. These organizations frequently also set up the routers without implementing security precautions and therefore are exposing their organization to attack.

Security Concerns

The default configurations of most home routers offer little security. Home routers are directly accessible from the internet, are easily discoverable, are usually powered-on at all times, and in many cases are vulnerable due to misconfiguration. These characteristics offer an intruder the perfect attack vector. The wireless features incorporated into many of these devices adds another vulnerable attack vector.

Mitigation

The mitigation steps listed below are designed to increase the security of home routers and reduce the vulnerability of the internal network against attacks from external sources.

- **Change the default login username and password:** Manufacturers set default usernames and passwords for these devices at the factory to provide users access to configure the device. These default usernames and passwords are readily available in different publications and are well known to attackers; therefore, they should be immediately changed during the initial router installation. A strong password that uses a

combination of letters and numbers with 14 characters or more is recommended. Furthermore, change passwords every 30 to 90 days.

- **Change the default SSID:** A service set identifier (SSID) is a unique name that identifies a particular wireless LAN (WLAN). All wireless devices on a WLAN must use the same SSID in order to communicate with each other. Manufacturers set a default SSID at the factory that typically identifies the manufacturer or the actual device. An attacker can use the default name to identify the device and any vulnerability associated with it. Users sometimes set the SSID to a name that identifies their organization, their location, their own name, etc. This makes it easier for the attacker to identify their specific business or home network based upon an SSID easily identified with their name. For example, an SSID that broadcasts a company name is a more attractive target then a router broadcasting "ABC123". When choosing an SSID, follow the best practices policy for password complexity as described below:
    - The minimum length of an SSID should be greater than eight characters long.
    - Use alphanumeric and symbols in the SSID.
    - Change the SSID on a reoccurring basis and discourage the use of previous passwords.
- **Configure WPA2-AES for data confidentiality:** Wireless Equivalent Privacy (WEP) is a security algorithm intended to provide data confidentiality (authentication and encryption) but has serious weaknesses. WEP was superseded by the 802.11 standard implemented as Wi-Fi Protected Access (WPA), which has a newer version, WPA2. WPA and WPA2 provide stronger authentication and encryption using dynamically changing keys. WPA and WPA2 come in personal and enterprise versions. WPA-Personal, also referred to WPA-PSK (Pre-Shared Key), was designed for homes and small offices using pre-shared keys without requiring an authentication server. If using WPA-PSK, set a long pre-shared key and change it periodically. WPA-Enterprise requires a RADIUS authentication server, uses Extensible Authentication Protocol (EAP), and provides added security, but it entails a larger budget and more complicated implementation. WPA2 incorporates AES 128-bit encryption accepted by government agencies. WPA2 with AES represents the most secure option, and all wireless devices must be WPA2 compliant. If WPA2 is not feasible, WPA is an alternative. WEP represents the least secure option. If used, WEP should be configured with the 128-bit key option with the longest pre-shared key the router administrator can manage.
- **Limit WLAN coverage:** LANs are inherently more secure than WLANs because they are protected by the physical structure in which they reside. WLAN coverage frequently extends beyond the perimeters of your home or organization. This allows eavesdropping by intruders outside your network perimeter. Therefore, antenna placement, antenna type, and transmission power levels are important aspects to consider. Limit the broadcast coverage area when securing your WLAN. A centrally located omni-directional antenna is the most common type used. If possible, use a directional antenna to direct WLAN coverage to only the areas needed. Experimenting with transmission levels and signal strength will also limit the coverage to only the areas needed.

- **Turn the network off when not in use:** The ultimate in wireless security measures, shutting down the network, will most certainly prevent outside attackers from breaking in. While it may be impractical to turn the devices off and on frequently, consider this approach during travel or extended periods offline.

- **Disable UPnP:** Universal Plug and Play (UPnP) is a handy feature allowing networked devices to seamlessly discover and establish communication with each other on the network. Though the UPnP feature eases initial network configuration, it is also a security hazard. For example, malware within your network could use UPnP to open a hole in your router firewall to let intruders in. Therefore, disable UPnP when not needed.

- **Upgrade firmware:** Just like software on your computers, the router firmware (the software that operates it) must have current updates and patches. Many of the updates address security vulnerabilities that could affect the network.

- **Use static IP addresses or limit DHCP reserved addresses:** Most home routers are configured as Dynamic Host Configuration Protocol (DHCP) servers. DHCP makes configuration of client devices easy by automatically configuring their network settings (IP address, gateway address, DNS info, etc.). However, this also allows unauthorized users to obtain an IP address on your network. Disabling DHCP and configuring clients manually is the most secure option, but it may be impractical depending on the size of your network and support staff. If using DHCP, limit the number of IP addresses in the DHCP pool. It may limit the number of users, potentially including unauthorized users, that can connect to your network.

- **Disable remote management:** Disable this to keep intruders from establishing a connection with the router and its configuration through the wide area network (WAN) interface.

- **Disable remote upgrade**: This feature, if available, allows the router to listen on the WAN interface for TFTP traffic that could potentially compromise the router firmware. Therefore, it should be disabled.

- **Disable DMZ**: The router's demilitarized zone (DMZ) creates a segregated network exposed to the internet, used for hosts that require internet access (web servers, etc.). Disable this feature if not needed. Users or administrators sometimes enable it for troubleshooting reasons and then forget to deactivate it, exposing any system inadvertently placed there. A firewall is recommended if this feature is used.

- **Disable unnecessary services:** As with any computer system, disable all unnecessary services in order to reduce the router’s exposure.

- **Disable ping response:** The ping response setting is usually disabled by default. With this feature enabled, reconnaissance on the router becomes easier then when it is disabled. It allows your router to respond to ping commands issued from the internet, and it potentially exposes your network to intruders. Although disabling this feature will not

shield you from discovery, it will at least increase the difficulty of discovery. Verify that the service is disabled.

- **Enable router firewall:** Most home routers include an internal firewall feature. Ensure this feature is activated and carefully configured to allow only authorized users and services access to the network. Activate stateful packet inspection (SPI) on your firewall if it is an available function. SPI extends firewall capability by inspecting packets to distinguish legitimate traffic from unsolicited traffic. Another feature offered by many home routers is the creation of whitelists or blacklists to allow or disallow a list of websites, services, ports, etc. Take advantage of this feature if it is available. Note that the firewall built in to the router does not prevent wireless users within range of your wireless network from connecting to it.

- **Logging:** Enable router logging and periodically review the logs for important information regarding intrusions, probes, attacks, etc.

- **Monitor the wireless traffic:** Monitor the wireless traffic to identify any unauthorized use of your network by performing routine log reviews of the devices that have accessed the router. If an unknown device is identified, then a firewall or MAC filtering rule can be applied on the router. For further information regarding how to apply these rules, see the literature provided by the manufacturer or the manufacturer's site.

- **Administrator workstations:** Verify that any administrator workstation used to manage the router is on a trusted segment of the network to mitigate outsiders sniffing the management data and collecting information about your network.

- **Disable bridging and use network address translation (NAT):** Home routers separate the internal network from the internet using network address translation (NAT). NAT provides private IP addresses for all the devices on your network. It is not directly accessible from the internet, nor can discovery of the network's internal addresses be accomplished easily. The IP address of the external interface of the router conceals the devices on your network that are behind it. This adds an additional layer of security.

- Some routers include a feature that allows them to act as a bridge between two networks. This feature can be used to connect segments or devices on the same intranet to the internet using a routers routable IP address. Disable this feature if not required, to further limit the attack surface of the router.

Keep in mind, this is only a list of suggested steps that can potentially help secure your small office or home router. Employing some of these suggested steps may not be feasible in your network or your environment. If further assistance is required, see your router manufacturer's literature or the following documentation:

- Securing WLANs using 802.11i

- Using Wireless Technology Securely

- Home Wireless Security

Enclosure (9)

Best Security Practice Guidelines for Businesses

10 Security Best Practice Guidelines for Businesses

Reference: Ken Hess March 4, 2013

Summary: Businesses need extreme security measures to combat extreme threats. Here are 10 best practices that provide defense against the majority of all security threats.

1. **Encrypt your data:** Stored data, filesystems, and across-the-wire transfers all need to be encrypted. Encryption is essential to protecting sensitive data and to help prevent data loss due to theft or equipment loss.

2. **Use digital certificates to sign all of your sites:** Save your certificates to hardware devices such as routers or load balancers and not on the web server as is traditionally done. Obtain your certificates from one of the trusted authorities.

3. **Implement DLP and auditing:** Use data loss prevention and file auditing to monitor, alert, identify, and block the flow of data into and out of your network.

4. **Implement a removable media policy:** Restrict the use of USB drives, external hard disks, thumb drives, external DVD writers, and any writeable media. These devices facilitate security breaches coming into or leaving your network.

5. **Secure websites against MITM and malware infections:** Use SSL, scan your website daily for malware, set the Secure flag for all session cookies, use SSL certificates with Extended Validation.

6. **Use a spam filter on email servers:** Use a time-tested spam filter such as SpamAssassin to remove unwanted email from entering your users' inboxes and junk folders. Teach your users how to identify junk mail even if it's from a trusted source.

7. **Use a comprehensive endpoint security solution:** Symantec suggests using a multi-layered product (theirs, of course) to prevent malware infections on user devices. Antivirus software alone is not enough. Antivirus, personal firewall, and intrusion detection are all part of the total approach to endpoint protection.

8. **Network-based security hardware and software:** Use firewalls, gateway antivirus, intrusion detection devices, honey pots, and monitoring to screen for DoS attacks, virus signatures, unauthorized intrusion, port scans, and other "over the network" attacks and attempts at security breaches.

9. **Maintain security patches:** Some antivirus programs update on what seems like a daily basis. Be sure that your software and hardware defenses stay up to date with new antimalware signatures and the latest patches. If you turn off automatic updating, set up a regular scan and remediate plan for your systems.

10. **Educate your users:** As I wrote in The second most important BYOD security defense: user awareness , "it might be the most important non-hardware, non-software solution available. An informed user is a user who behaves more responsibly and takes fewer risks with valuable company data, including email".

    Other such "obvious" measures are to use security-screened software, use software that has been regression tested with your operating system, use VPNs, use strong passwords, and so on.

    Businesses can't afford to take chances with security. Doing so is costly. The average is $429,000* loss for large companies due to mobile computing "mishaps". It's best to stay on top of security with a multilayered, multi-tiered approach. Vigilance is key and so is awareness.

Enclosure (10)

Best Practices for Keeping Your Home Office Secure

Best Practices for Keeping Your Home Network Secure

As a user with access to sensitive corporate or government information at work, you are at risk at home. In order to gain access to information typically housed on protected work networks , cyber adversaries may target you while you are operating on your less secure home network.

Don't be a victim. You can help protect yourself, your family, and your organization by following some common sense guidelines and implementing a few simple mitigations on your home network.

Personal Computing Device Recommendations

Personal computing devices include desktop computers, laptops, smartphones, and tablets. Because the bulk of your information is stored and accessed via these devices, you need to take special care in securing them.

1. Migrate to a Modern Operating System and Hardware Platform

The latest version of any operating system (OS) inevitably contains security features not found in previous versions. Many of these security features are enabled by default and help prevent common attack vectors . In addition, using a 64-bit OS on a 64-bit hardware platform substantially increases the effort for an adversary to obtain privileged access on your computer.

2. Install A Comprehensive Security Suite

Install a comprehensive security suite that provides layered defense via anti-virus, anti-phishing, safe browsing, host-based intrusion prevention, and firewall capabilities. In addition, several security suites, such as those from McAfee®[11], Norton®[12], and Symantec®[13], provide access to a cloud-based reputation service for leveraging corporate malware knowledge and history. Be sure to enable the suite's automatic update service to keep signatures up to date.

3. Limit Use of the Administrator Account

In your operating system, the highly-privileged administrator (or root) account has the ability to access any information and change any configuration on your system. Therefore, web or email delivered malware can more effectively compromise your system if executed while you are logged on as an administrator. Create a nonprivileged "user" account for the bulk of your activities including web browsing, e-mail access, and document creation/editing. Only use the privileged administrator account for system reconfigurations and software installations/ updates.

4. Use a Web Browser with Sandboxing Capabilities

Visiting compromised or malicious web servers is a common attack vector. Consider

using one of several currently available web browsers (e.g. Chrome™[4], Safari®[5]) that provide a sandboxing capability. Sandboxing contains malware during execution, thereby insulating the underlying operating system from exploitation.

5. Use a PDF Reader with Sandboxing Capabilities

PDF documents are a popular mechanism for delivering malware. Use one of several commercial or open source PDF readers (e.g. Adobe®[6], Foxit®[7]) that provide sandboxing capabilities and block execution of malicious embedded URLs (website links) within documents.

6. Update Application Software

Attackers often exploit vulnerabilities in unpatched, outdated software applications running on your computing device. Enable the auto-update feature for applications that offer this option, and promptly install P<:1tches or a new version when pop-up notifications indicate an update is available. Since many applications do not have an automated update feature, use one of several third-party products, such as those from Secunia and eEye Digital Security®[8], which can quickly survey installed software and report which applications are end-of-life or need patches or updates.

7. Implement Full Disk Encryption (FOE) on Laptops

To prevent data disclosure in the event that a laptop is lost or stolen, implement FOE. Most modern operating systems offer a built-in FOE capability, for example Microsoft's Bitlocker®[9], Apple's Filevault®[10], or LUKS for Linux. If your OS does not offer FOE , use a third party product.

8. Download Software Only from Trusted Sources

To minimize the risk of inadvertently downloading malware, only download software and mobile device apps from reputable sources. On mobile devices, grant apps only those permissions necessary to function, and disable location services when not needed.

9. Secure Mobile Devices

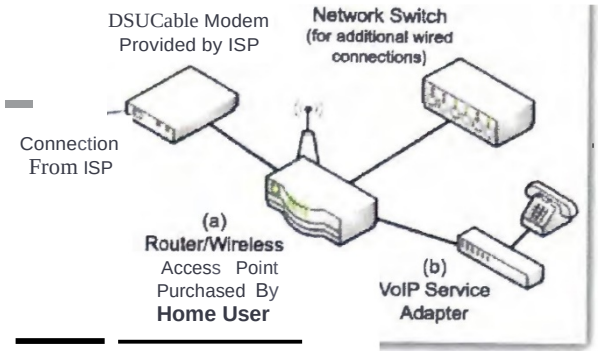
Mob\le devices such as laptops, smartphones, and tablets pose additional concerns due to their ease of use and portability. To protect against theft of the device and the information on the device, maintain physical control when possible, enable automatic screen locking after a period of inactivity, and use a hard-to-guess password or PIN. If a laptop must be left behind in a hotel room while travelling, power it down and use FOE as discussed above.

Network Recommendations

Home network devices include modems/ routers, wireless access points (WAPs), printers, and IP telephony devices. These devices control the flow of information into and out of your network, and should be carefully secured.

1. Configure a Flexible Home Network

Your Internet Service Provider (ISP) likely provides a modem/router as part cit your service contract. To maximize administrative control over the routing and wireless features of your home network, use a personally-owned routing device that connects to the ISP-provided modem/router. Figure 1 depicts a typical small office/home office (SOHO) network configuration that provides the home user with a network that supports multiple systems as well as wireless networking and IP telephony services.



Fi g ure 1: Typical SOHO Configuration

2. Disable Internet Protocol Version 6 (1Pv6) Tunneling

Both 1Pv6 and its predecessor, 1P v4, are used to transfer communications on the Internet. Most modern operating systems use 1Pv6 by default. If 1Pv6 is enabled on your device, but not supported by other systems/networks to which you are communicating, some OSes will attempt to pass 1Pv6 traffic in an 1Pv4 wrapper using tunneling capabilities such as Teredo, 6to4, or ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Because attackers could use these tunnels to create a hidden channel of communication to and from your system, you should disable tunneling mechanisms. In Windows, you can disable these through Device Manager (be sure to select "View hidden devices" under the View menu).

3. Provide Firewall Capabilities

To prevent attackers from scanning your network, ensure your personally-ownedrouting device supports basic firewall capabilities. Also verify that it supports Network Address Translation (NAT) to prevent internal systems from being accessed directly from the Internet. Wireless Access Points (WAPs) generally do not provide these capabilities so it may be necessary to purchase a wireless router, or a wired router in addition to the WAP. If your ISP supports 1Pv6, ensure your router supports 1Pv6 firewall capabilities in addition to 1Pv4.

4. Implement WPA2 on the Wireless Network

To keep your wireless communication con fidential, ensure your personal or ISP-provided WAP is using Wi-Fi Protected Access 2 (WPA2.) instead of the much weaker, and easily broken Wired Equivalent Privacy (WEP) or the original WPA. When configuring WPA2, change the default key to a complex, hard-to -guess passphrase. Note that older client systems and access points may not support WPA2 and will require a software or hardware upgrade. When identifying a suitable replacement, ensure the device is WPA2-Personal certified.

5. Limit Administration to the Internal Network

To close holes that would allow an attacker to access and make changes to your network, on your network devices, disable the ability to perform remote/external administration. Always make network configuration changes from within your internal network.

6. Implement an Alternate DNS Provider

The Domain Name System (DNS) associates domain names (e.g. www.example.com) with their numerical IP addresses. The ISP DNS provider likely does not provide enhanced security services such as the blocking and blacklisting of dangerous web sites. Consider using either open source or commercial DNS providers to enhance web browsing security.

7. Implement Strong Passwords on all Network Devices

In addition to a strong and complex password on your WAP, use a strong password on any network device that can be managed via a web interface, including routers and printers. For instance, many network printers on the market today can be managed via a web

interface to configure services, determine job status, and enable features such as e-mail alerts and logging. Without a password, or with a **weak** or default password , attackers could leverage these devices to gain access to your other internal systems.

Home Entertainment Device Recommendations

Home entertainment devices, such as blu-ray players, set-top video players (e.g. Apple TV®[11]), and video game controllers, are capable of accessing the Internet via wireless or wired connection. Although connecting these types of devices to a home network generally poses a low security risk, you can implement security measures to ensure these don't become a weak link in your network.

1. Protect the Device within the Network

Ensure the device is behind the home router/ firewall to protect it from unfettered access from the Internet. In the case of a device that supports wireless, follow the Wireless LAN security guidance in this document.

2. Use Strong Passwords for Service Accounts

Most home entertainment devices require you to sign up for additional services (e.g. Playstation®[12] Network, Xbox Live®[13], Netflix®[14], Amazon Prime®[15], iTunes®[16]). Follow the password guidance later in this document when creating and maintaining service accounts.

3. Disconnect When Not in Use

To prevent attackers from probing the network via home entertainment devices, if possible, disconnect these systems from the Internet when not in use. Some ISP modems/routers have a standby button you can use to disable the Internet connection.

Internet Behavior Recommendations

In order to avoid revealing sensitive information about your organization or personal life, abide by the following guidelines while accessing the Internet.

1. Exercise Caution when Accessing Public Hotspots

Many establishments, such as coffee shops , hotels , and airports, offer wireless hotspots or kiosks for customers to access the Internet. Because the underlying infrastructure of these is unknown and security is often weak, these hotspots are susceptible to adversarial activity. If you have a need to access the Internet while away from home, follow these recommendations:

- If possible, use the cellular network (that is, mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.
- Set up a confidential tunnel to a trusted virtual private network (VPN) service provider (for example, StrongSwan's StrongVPN) . This option can protect your traffic from malicious activities such as . monitoring. However, use of a VPN carries some inconvenience , overhead , and often cost. Additionally, you are still vulnerable during initial connection to the public network before establishing the VPN.
- If using a hotspot is the only option for accessing the Internet, limit activities to web browsing. Avoid accessing services such as banking websites that require user credentials or entering personal information.

2. Do Not Exchange Home and Work Content

The exchange of information (e.g. e-mails, documents) between less-secure home systems and work systems via e-mail or removable media may put work systems at an increased risk of compromise. If possible, use organization-provided laptops to conduct all work business from home. For those business interactions that are solicited and expected, have the contact send work-related correspondence to your work, rather than personal, e-mail account.

3. Be Cognizant of Device Trust Levels

Home networks consist of various combinations of wired and wireless devices and computers. Establish a level of trust based not only on a device's security features, but also its usage. For example, children typically are less savvy about security than adults and may be more likely to have malicious software on their devices. Avoid using a less savvy user's computer for online banking, stock trading , family photograph storage, and other sensitive functions.

4. Be Wary of Storing Personal Information on the Internet

Personal information historically stored on a local computing device is steadily moving to on-demand Internet storage called the cloud. Information in the cloud can be difficult to permanently remove. Before posting information to these cloud-based services, ask yourself who will have access to your information and what controls do you have over how the information is stored and displayed. In addition , be aware of personal information already published online by periodically performing a search using an Internet search engine.

5. Take Precaustions on Social Networking Sites

Social networking sites are a convenient means for sharing personal information with family and friends. However, this convenience also brings a level of risk. To protect yourself, do the following:

- Think twice about posting information such as address , phone number, place of employment, and other personal information that can be used to target or harass you.
- If available, limit access of your information to "friends only" and attempt to verify any new sharing requests either by phone or in person.
- Take care when receiving content (such as third-party applications) from friends because many recent attacks deliver malware by taking advantage of the ease with which content is generally accepted within the social network community.
- Periodically review the security policies and settings available from your social network provider to determine if new features are available to protect your personal information. For example, some social networking sites now allow you to opt-out of exposing your personal information to Internet search engines.
- Follow friends' profiles to see whether information posted about you might be a problem.

6. Enable the Use of SSL Encryption

Application encryption (SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit when logging into web based applications such as webmail and social networking sites. Fortunately, most web browsers enable SSL support by default.

When conducting sensitive personal activities such as account logins and financial transactions, ensure the web site uses SSL. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser. Additionally, many popular web applications such as Facebook®[17] and Gmail®[19] have options to force all communication to use SSL by default.

7. Follow E-mail Best Practices

Personal e-mail accounts, either web-based or local to the computer, are common attack targets. The following recommendations will help reduce exposure toe-mail-based threats:

- Use different usernames for home and work e-mail addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.
- To prevent reuse of compromised passwords, use different passwords for each of your e-mail accounts.
- Do not set out-of-office messages on personal e-mail accounts, as this can confirm to spammers that your e-mail address is legitimate and can provide information to unknown parties about your activities.
- To prevent others from reading e-mail while in transit between your computer and the mail server, always use secure e-mail protocols (Secure IMAP or Secure POP3), particularly if using a wireless network. You can configure these on most e-mail clients, or select the option to "always use SSL" for web-based e-mail.
- Consider unsolicited e-mails containing attachments or links to be suspicious. If the identity of the sender cannot be verified, delet the e-mail without opening . For those e-mails with embedded links, open a browser and navigate to the web site directly by its well-known web address or search for the site using an Internet search engine.
- Be wary of any e-mail requesting personal information such as a password or social security number as any web service with which you currently conduct business should already have this information.

8. Protect Passwords

Ensure that passwords and challenge responses are properly protected since they provide access to personal information.

- Passwords should be strong, unique for each account , and difficult to guess. Consider using a passphrase that you can easily remember, but which is long enough to make p ssword cracking more difficult.
- Disable the feature that allows web sites or programs to remember passwords.
- Many online sites make use of password recovery or challenge questions. Your answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question , assuming the response is unique and memorable.
- Use two-factor authentication when available for accessing webmail , social networking , and other accounts. Examples of two-factor authentication include a one-time password verification code sent to your phone, or a login based on both a password and identification of a trusted device.

9. Avoid Posting Photos with GPS Coordinates

Many phones and newer point-and-shoot cameras embed GPS location coordinates when a photo is taken. An attacker can use these coordinates to profile your habits/pattern of life and current location. Limit the exposure of these photos on the Internet to be viewable only by a trusted audience or use a third-party tool to remove the coordinates before uploading to the Internet. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Additional Guidance

Social Networking :
http://www.nsa.gov/ia/_files/factsheets/173-021R-2009.pdf

Mitigation Monday -
Defense Against Malicious E-mail Attachments:
http:l/www.nsa.gov/ia/_files/factsheets/MitigationMonday.pdf

Mitigation Monday #2 -
Defense Against Drive By Downloads:
http:l/www.nsa.gov/ia/_files/factsheets/1733-011R-2009.pdf

Hardening Tips

Mac OSX 10.6 Hardening Tips:
http://www.nsa.gov/ia/_files/factsheets/macosx_10_6_hardeningtips.pdf

Enforcing No Internet or E-mail from Privileged Accounts :
http://www.nsa.gov/ia/_files/factsheets/Final 49635NonInternetsheet91.pdf

Hardening Tips for the Default Installation of Red Hat Enterprise Linux 5:
http://www.nsa.gov/ia/_files/factsheets/rhel5-pam phlet-i731.pdf

Internet Protocol Version 6:
http://www.nsa.gov/ia/_files/factsheets/Factsheet-IPv6.pdf

Security Tips for Personally-Managed Apple iPhones and iPads:
http://www.nsa.gov/ia/_files/factsheets/iphonetips-image.pdf

Security Highlights of Windows 7:
http://www.nsa.gov/ia/_fi1es/os/win7/win7_security_highlights.pdf

References

[1] McAfee® is a registered trademark of McAfee, Inc.

[2] Norton® is a registered trademark of Symantec

[3] Symantec® is a registered trademark of Symantec

[4] ChromeTM is a trademark of Google

[5] Safari® is a registered trademark of Apple

[6] Adobe® is a registered trademark of Adobe Systems, Inc.

[7] Foxit® is a registered trademark of Foxit Corp.

[8] eEye Digital Security® is a registered trademark of eEye, Inc.

[9] Bitlocker® is a registered trademark of Microsoft

(1OJ Filevault® is a registered trademark of Apple

(11] Apple lV® is a registered trademark of Apple

(12] Playstation® is a registered trademark of Sony

(13] Xbox Live® is a registered trademark of Microsoft

(14] Netflix® is a registered trademark of Netflix.com , Inc.

(15] Amazon Prime® **is a** registered trademark of Amazon Technologies, Inc.

(16] iTunes® is a registered trademark of Apple

(17] Facebook® **is a** registered trademark of Facebook

[18] Gmail® **is a** registered trademark of Google