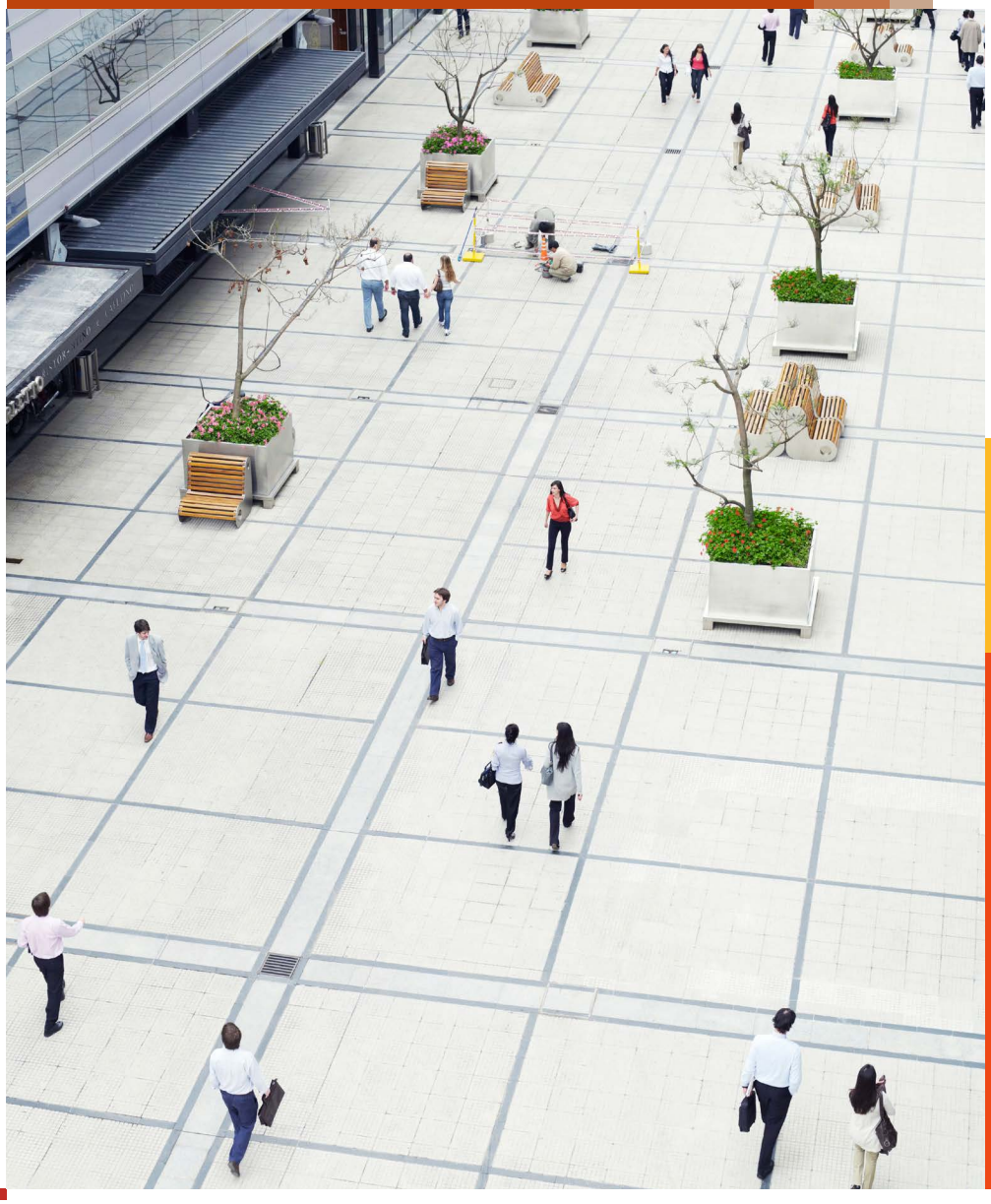
US cybercrime: Rising risks, reduced readiness

Key findings from the 2014 US State of Cybercrime Survey



June 2014

As cybersecurity incidents multiply in frequency and cost, the cybersecurity programs of US organizations do not rival the persistence and technological prowess of their cyber adversaries.

Organizations do not adequately address employee and insider vulnerabilities, nor do they assess the security practices of third-party partners and supply chains.

Most do not strategically invest in cybersecurity and ensure that it is aligned with their overall business strategy.

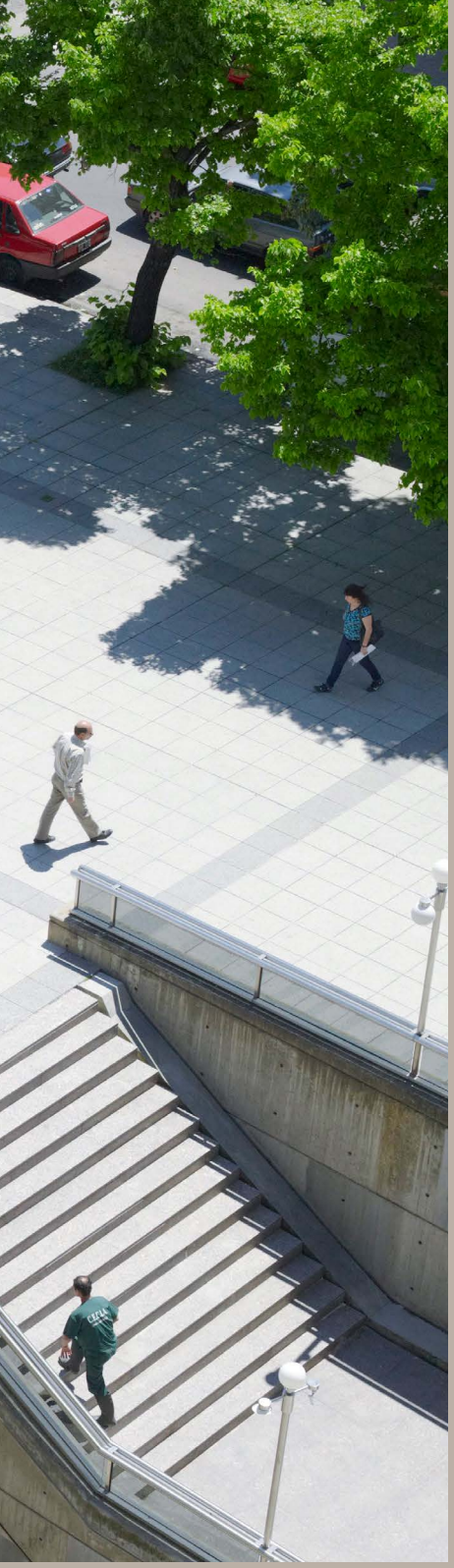
Co-sponsored by

The CERT® Division of the Software Engineering Institute at Carnegie Mellon University

CSO *magazine*

United States Secret Service

pwc



About the 2014 US State of Cybercrime Survey

The 2014 US State of Cybercrime Survey was co-sponsored by PwC, ***CSO*** magazine, 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 identified requirements for effective cybersecurity and evaluated these practices against current and evolving adversaries, threats, and known attacks across the digital ecosystems of private and public organizations.

Additionally, we compared survey responses with the Core processes, practices, and technologies prescribed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework to determine how respondents' security programs compare with the best practices recommended by NIST.

In addition to analysis of the survey results, this report also draws on previous PwC research that includes PwC's 2014 Global CEO Survey, the 2014 Global Economic Crime Survey, and The Global State of Information Security® Survey 2014. We leveraged these surveys to provide a more thorough and balanced look into the current state of cybersecurity and cyber threats.

Table of contents

The risks and repercussions of cybercrime

One thing is very clear: Most organizations' cybersecurity programs do not rival the persistence, tactical skills, and technological prowess of today's cyber adversaries.

In this 12th survey of cybercrime trends, more than 500 US executives, security experts, and others from the public and private sectors offered a look into their cybersecurity practices and state of risk and readiness to combat evolving cyber threats and threat agents.

One thing is very clear: The cybersecurity programs of US organizations do not rival the persistence, tactical skills, and technological prowess of their potential cyber adversaries. Today, common criminals, organized crime rings, and nation-states leverage sophisticated techniques to launch attacks that are highly targeted and very difficult to detect. Particularly worrisome are attacks by tremendously skilled threat actors that attempt to steal highly sensitive—and often very valuable—intellectual property, private communications, and other strategic assets and information.

It is a threat that is nothing short of formidable. In fact, the US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction.[1] Underscoring the threat, the FBI last year notified 3,000 US companies—ranging from small banks, major defense contractors, and leading retailers—that they had been victims of cyber intrusions.

"The United States faces real [cybersecurity] threats from criminals, terrorists, spies, and malicious cyber actors," said FBI Director James B. Comey at a recent security conference.[2] "The playground is a very dangerous place right now."

Nation-state actors pose a particularly pernicious threat, according to Sean Joyce, a PwC principal and former FBI deputy director who frequently testified before the US House and Senate Intelligence committees. "We are seeing increased activity from nation-state actors, which could escalate due to unrest in Syria, Iran, and Russia," he said. "These groups may target financial services and other critical infrastructure entities."

In today's volatile cybercrime environment, nation-states and other criminals continually and rapidly update their tactics to maintain an advantage against advances in security safeguards implemented by businesses and government agencies. Recently, for instance, hackers engineered a new round of distributed denial of service (DDoS) attacks that can generate traffic rated at a staggering 400 gigabits per second, the most powerful DDoS assaults to date.

[1] Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Committee, January, 2014
[2] Federal Bureau of Investigation, The FBI and the private sector: Closing the gap in cybersecurity, Feb. 26, 2014

69%

of US executives are worried that cyber threats will impact growth.

— PwC, 17th Annual Global CEO Survey

Similarly, the US Secret Service has reported a marked increase in the quality, quantity, and complexity of cyber crimes targeting both private industry and critical infrastructure, according to William Noonan, deputy special agent in charge for the US Secret Service Criminal Investigative Division.[3]

"The increasing level of collaboration among cyber criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors and allowing for development of expert specialization," Noonan said in testimony before a House of Representatives subcommittee. "These specialties raise the complexity of investigating these cases, as well as the level of potential harm to companies and individuals."

Critical infrastructure systems used in electrical power distribution, oil and gas pipelines, water supplies, and transportation are particularly vulnerable because their legacy architecture may be easier to compromise. Similarly, the coming year could bring a new wave of strikes on industries that have not migrated critical systems from the Windows XP operating system, which Microsoft no longer supports with security updates. Despite a six-year advance notice that Microsoft would end XP support in April 2014, utility companies continue to run the outdated operating system. Many cash ATMs also use Windows XP, although some employ a simplified embedded version that Microsoft will support until January 2016.[4]

Another evolving area of risk lies in physical objects—industrial components, automobiles, home automation products, and consumer devices, to name a few—that are being integrated into the information network, a trend typically referred to as the "Internet of Things." The interconnection of billions of devices with IT and operational systems will introduce a new world of security risks for businesses, consumers, and governments.

Given the potentially serious impact of these threats, it's not surprising that US business leaders are increasingly concerned about cybercrime—much more so than their global counterparts. PwC's Annual Global CEO Survey 2014 found 69% of US respondents reported they were worried about the impact of cyber threats to their growth prospects, significantly higher than 49% of global CEOs who reported the same unease.[5]

One reason for the heightened concern is the high financial costs of cybercrime. PwC's 2014 Global Economic Crime Survey found that 7% of US organizations lost $1 million or more due to cybercrime incidents in 2013, compared with 3% of global organizations; furthermore, 19% of US entities reported financial losses of $50,000 to $1 million, compared with 8% of worldwide respondents.[6]

Another reason for worry: In the wake of data breaches among US retailers, many believe the risk of legal liability and costly lawsuits will escalate. Today, claims by businesses that they are unaware of cybercrime risks and the need to invest in updated cybersecurity safeguards have become increasingly unconvincing. "I think there will be a lot more litigation than we've seen in the past," said Tom Ridge, chief executive officer of security firm Ridge Global and the first secretary of the US Department of Homeland Security. "These high-profile attacks have the attention of every board of directors."

[3] http://www.dhs.gov/news/2014/03/05/written-testimony-usss-house-financial-services-subcommittee-financial-institutions
[4] MSDN, What does the end of support for Windows XP mean for Windows Embedded? Feb. 17, 2014
[5] PwC, 17th Annual Global CEO Survey, January 2014
[6] PwC, Global Economic Crime Survey 2014, February 2014

Working together to advance security

82%

of companies with high-performing security practices collaborate with others to deepen their knowledge of security and threat trends.

The global risks and repercussions of cybercrime may seem overwhelming for any single organization, no matter how great its resources. Understanding that there is strength in numbers, private and public organizations are starting to band together to combat cybercrime and gain intelligence about current security threats and effective responses.

It's an approach that leading security executives have embraced. In The Global State of Information Security® Survey 2014, we found that 82% of companies with high-performing security practices collaborate with others to deepen their knowledge of security and threat trends.[7] One of the most effective collaboration approaches is participation in Information Sharing and Analysis Centers (ISACs) forums, which have gained traction in security-forward industries like financial services and technology.

The need for this type of teamwork has been bolstered by the release of the NIST Cybersecurity Framework, a compendium of best practices and security standards developed by the National Institute of Standards and Technology (NIST). (See sidebar "How current cybersecurity compares with the NIST Framework.") The framework very strongly encourages information-sharing as a means to stimulate conversations about security threats and response tactics. It provides a common language to promote an open dialogue on cybersecurity, both internally and with external entities such as third-party service providers and partners.

"Cybersecurity is a shared responsibility," said Secretary of Homeland Security, Jeh Johnson, at the White House unveiling of the Framework. "So everyone needs to work on this: Government officials and business leaders, security professionals, and utility owners and operators."[8]

This call for enhanced collaboration can also be heard from the private sector. In the aftermath of last year's retailer breaches, the CEO of JPMorgan Chase urged companies to unite across industries to help prevent future intrusions. "All of us have a common interest in being protected, so this might be a chance for retailers and banks to for once work together, as opposed to sue each other like we've been doing the last decade," James Dimon said earlier this year on an earnings call.[9]

A united response may very likely prove to be an indispensable strategy in advancing the state of cybersecurity, but there is much more to be done. We hope the following report will help organizations determine what action to take now to protect themselves from cyber criminals in the year ahead.

[7] PwC, *CSO* magazine, *CIO* magazine, *The Global State of Information Security® Survey 2014,* September 2013

[8] Department of Homeland Security, Remarks by Secretary of Homeland Security Jeh Johnson at The White House Cybersecurity Framework Event, Feb. 12, 2014

[9] Seeking Alpha, JPMorgan Chase CEO Discusses Q4 2013 Results – Earnings Call Transcript, Jan. 14, 2014

Incidents and monetary losses continue to mount

59%

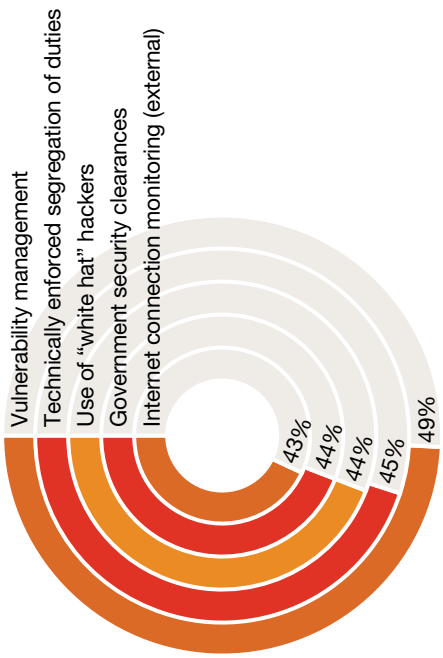
of respondents said that they were more concerned about cybersecurity threats this year than in the past.

You've heard it before: The number of detected cybersecurity incidents is surging, as are the financial costs associated with these events.

This year, three in four (77%) respondents to the US State of Cybercrime Survey detected a security event in the past 12 months, and more than a third (34%) said the number of security incidents detected increased over the previous year. So it's no surprise that more than 59% of respondents said that they were more concerned about cybersecurity threats this year than in the past.

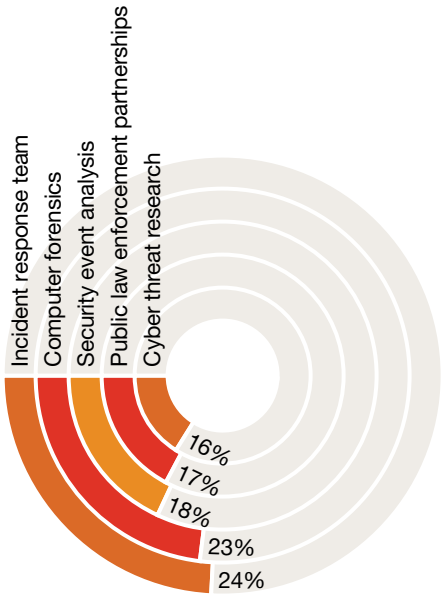
We're not talking about a handful of intrusions: The average number of security incidents detected in 2013 was 135 per organization. This does not account for incidents that go undetected, a potentially significant number given the 3,000 companies mentioned above that were unaware of cyber intrusions until notified by the FBI. When we asked about monetary losses attributed to cybercrime, 14% of respondents reported losses have mounted in the past year—but the costs of these incidents remain largely unknown. That's because more than two-thirds (67%) of those who detected a security incident were not able to estimate the financial costs. Among those that could, the average annual monetary loss was approximately $415,000.

Policies & procedures most likely to help deter a criminal*



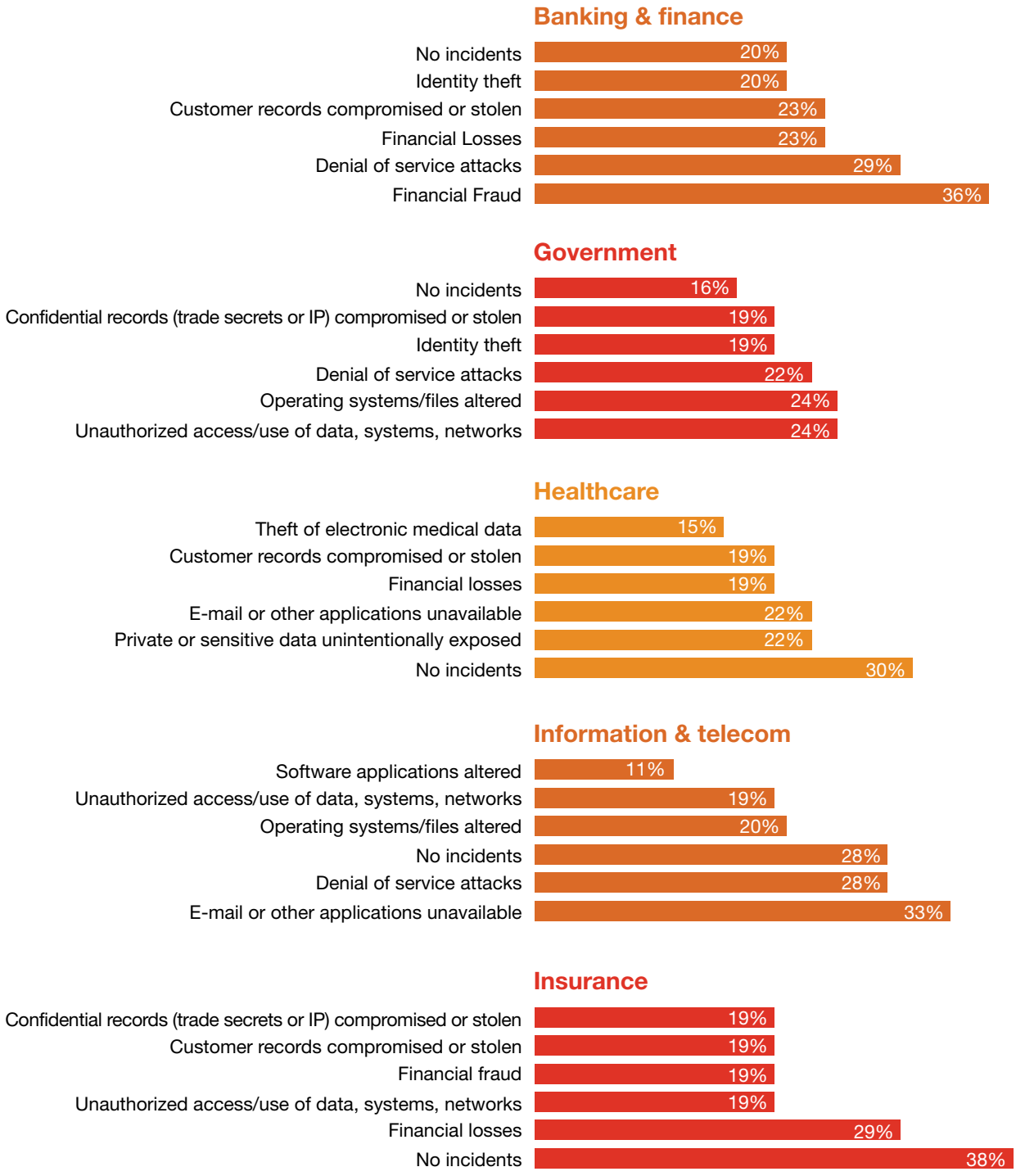
* *Respondents who said these policies & procedures helped deter a potential criminal*

Policies & procedures most likely to help detect a criminal*



* *Respondents who said these policies & procedures helped detect a potential criminal*

Figure 1: Significant detected incidents across industries



The most frequent types of incidents comprise a greatest hits list of cybercrime: malware, phishing, network interruption, spyware, and denial of service attacks. Beyond these top five, we found some intriguing variances by sector. (Figure 1). In banking and finance, for instance, the second most-cited type of incident was financial fraud. Among government services, unauthorized access to information, systems, or networks was reported by 24% of respondents. For healthcare, the number of respondents who reported unintentional exposure of private or sensitive information was 83% higher than overall respondents and a critical shortcoming for a highly regulated industry that deals in sensitive personal information.

Nation-states often target valuable IP, the theft of which many organizations are reluctant to report—if, in fact, they are aware this information has been stolen. Often there is no legal or regulatory requirement to do so, and the consequences of disclosing IP loss may, in some cases, cripple a business.

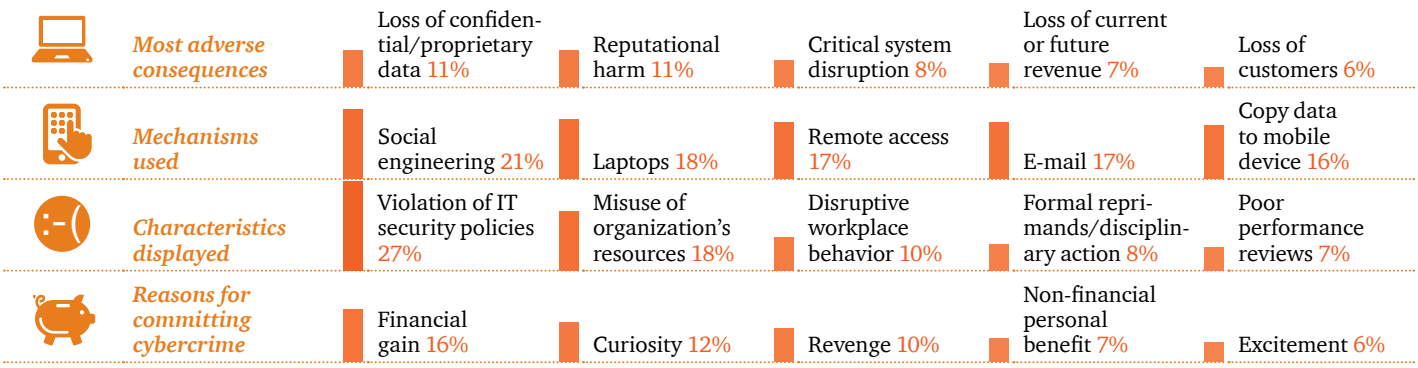
It is also quite difficult to quantify the consequences of IP loss. Unlike payment card heists, in which the financial losses are reported quickly and are fairly straightforward to calculate, victims of IP theft may not know exactly what has been stolen. What's more, trade secrets often are not monetized by adversaries in an immediately noticeable way, and the impact may remain undetected for years.

When it comes to the sources of cybersecurity incidents, the highest percentage of respondents (72%) cite outsiders such as hackers. Other highly publicized sources of incidents—nation-states (7%) and organized crime (8%)—are in fact less likely culprits, although larger companies are more likely to be concerned about these threat actors. It's worth noting that these types of incidents are comparatively uncommon, yet they are often sensational in nature and generate media attention that is disproportionate to their frequency. Also consider that a great deal of uncertainty exists about incidents: We found that 26% of respondents that had detected a cybersecurity incident could not identify the source of the attack.

The incidents that typically fly under the media radar are insider events. We found that 28% of respondents pointed the finger at insiders, which includes trusted parties such as current and former employees, service providers, and contractors. Almost one-third (32%) say insider crimes are more costly or damaging than incidents perpetrated by outsiders. The larger the business, the more likely it is to consider insiders a threat; larger businesses also are more likely to recognize that insider incidents can be more costly and damaging. Despite this, however, only 49% of all respondents have a plan for responding to insider threats.

Many insider incidents result from employee vulnerabilities such as social engineering and loss of devices—risks that could very well be mitigated by employee training. Organizations can also prevent insider incidents by monitoring employees for certain negative behaviors. For instance, respondents said that insiders who had perpetrated cybercrimes most often displayed behaviors such as violation of IT policies, disruptive behavior, and poor performance reviews. They also said most insider incidents are conducted for financial gain. (Figure 2.)

Figure 2: The causes and consequences of cybercrime committed by insiders*



** A current or former employee, service provider, authorized user of internal systems, or contractor*

49%

of all respondents have a plan for responding to insider threats.

Smaller businesses assign management of insider attacks to the IT department, most likely because they lack an information security function. We found, for instance, that only 20% of small companies rely on a security function to handle insider attacks, compared with 62% of large organizations. That means it's very likely that companies with 500 employees or fewer may have only one person responsible for managing information security and IT.

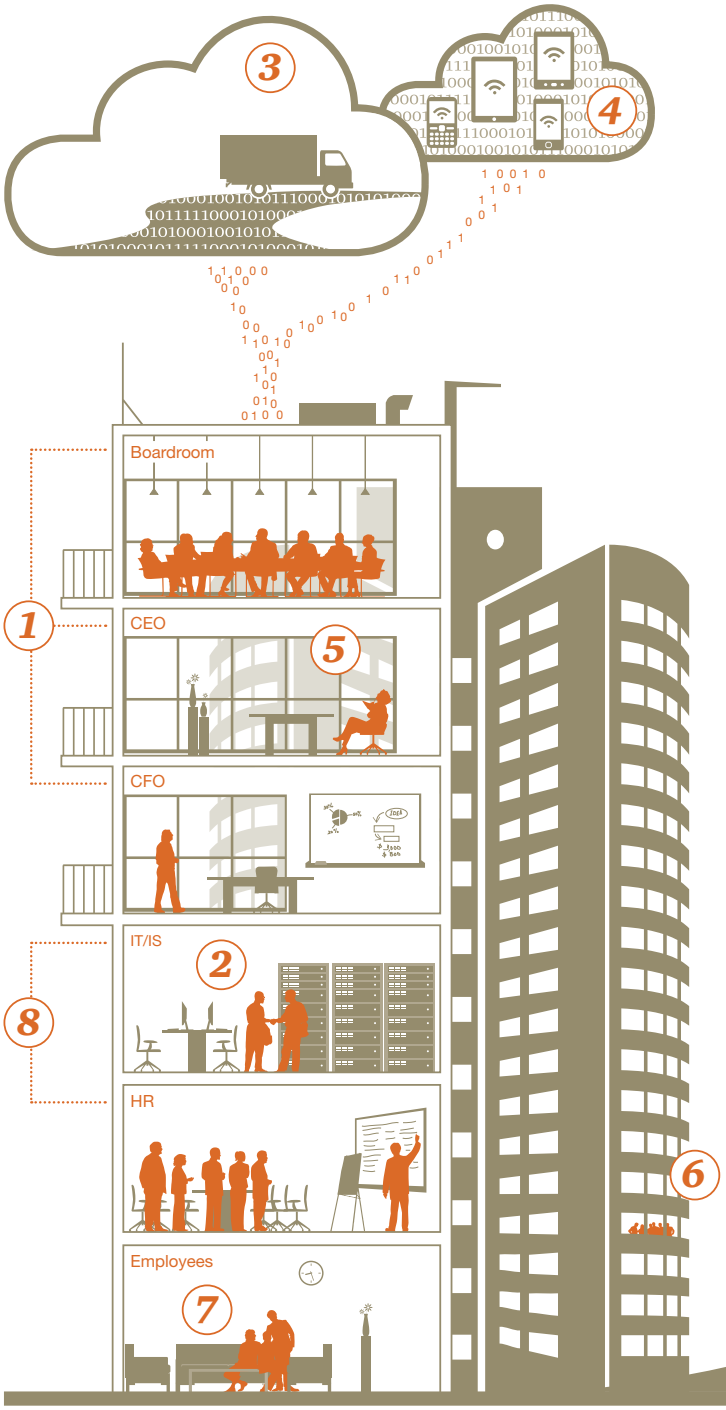
Interestingly, this year the number of overall respondents who said their organization relies on an interdepartmental team for responding to insider attacks dropped to 6% from 14% in 2013, and 14% have no response mechanism for insider incidents. This does not bode well for effective mitigation of insider attacks, since doing so requires an enterprise-wide effort and monitoring across functions that include IT, information security, physical security, human resources, and legal counsel. Consequently, it is no surprise that almost one-quarter (23%) said their organization is merely minimally effective in dealing with insider events.

Beyond employees, trusted partners also perpetrate insider incidents, as last year's high-profile government-contractor data leaks and retailer breaches so conclusively proved. Indeed, criminals have found that third-party partners may provide relatively easy access to confidential data. It's an indirect path to criminal profit that is increasingly successful because most organizations make no effort to assess the cybersecurity practices of their partners and supply chains.

In fact, organizations that have a process for evaluating third parties before they launch business operations has dropped to 44% from 54% last year. The implications are astounding: Two-thirds of organizations that, for instance, push a process to a third-party cloud-computing provider may be doing so without a proper cybersecurity evaluation.

Similarly, only 41% of companies have a process for assessing the cybersecurity of third-party industries with which they share data or networks before launching business operations. The smaller the company, the less likely it is to evaluate cybersecurity of partners.

Cyber insecurity
8 cybersecurity issues that should concern you



1. *Spending with a misaligned strategy isn't smart*

Strategy should be linked to business objectives, with allocation of resources tied to risks.

38% prioritize security investments based on risk and impact to business
17% classify the business value of data[1]

2. *Business partners fly under the security radar*

Recent contractor data leaks and payment card heists have proved that adversaries can and will infiltrate systems via third parties, but most organizations do not address third-party security.

44% have a process for evaluating third parties before launch of business operations
31% include security provisions in contracts with external vendors and suppliers

3. *A missing link in the supply chain*

Flow of data to supply chain partners continues to surge, yet they are not required to comply with privacy and security policies.

27% conduct incident-response planning with supply chain partners
8% have supply chain risk-management capability

4. *Slow moves in mobile security*

Mobile technologies and risks are proliferating but security efforts are not keeping up.

31% have a mobile security strategy
38% encrypt devices
36% employ mobile device management

5. *Failing to assess for threats is risky business*

Organizations typically include cyber risks in enterprise risk-management programs but do not regularly assess threats.

47% perform periodic risk assessments
24% have an objective third party assess their security program

6. *It takes a team to beat a crook*

External collaboration is critical to understanding today's threats and improving cybersecurity but most don't work with others.

25% participate in Information Sharing and Analysis Centers (ISACs)
15% work with public law enforcement agencies

7. *Got suspicious employee behavior?*

Cybersecurity incidents carried out by employees have serious impact, yet are not addressed with the same rigor as external threats like hackers.

49% have a formal plan for responding to insider events
75% handle insider incidents internally without involving legal action or law enforcement

8. *Untrained employees drain revenue*

Employee vulnerabilities are well known, but businesses do not train workers in good cybersecurity hygiene.

20% train on-site first responders to handle potential evidence
76% less is spent on security events when employees are trained, yet
54% do not provide security training for new hires

1. PwC, *CSO* magazine, *CIO* magazine, *The Global State of Information Security® Survey 2014*, September 2013

And it gets worse: A low 31% of respondents include security provisions in contract negotiations with external vendors and suppliers. It is imperative that organizations hold third-party partners to the same—or higher—cybersecurity standards that they set for themselves. Compliance should be mandated in contracts.

Finally, an organization's size matters when it comes to handling insider threats of all types. Larger organizations not only understand the potential impacts of insider incidents, but they also tend to have more mature security practices than smaller companies and, as a result, are also more likely to have an information security department that is in charge of responding to incidents. We also found that large organizations (those with 10,000 or more employees) use advanced technologies such as malware analysis, threat subscription services, and threat modeling to address overall cybersecurity risks.

The link between spending and cybersecurity

$2,500
per employee
Median maximum amount that banking and finance organizations invest in cybersecurity.

$400
per employee
Median maximum amount that retail and consumer products businesses invest in cybersecurity.

This year's US State of Cybercrime survey revealed a significant correlation between the level of spending on cybersecurity and the number of events detected. In other words, the more you spend, the more incidents you will detect.

Consider, for instance, the generalization that organizations operating in highly regulated sectors typically have high-performing cybersecurity programs. They also invest considerably more in cybersecurity than organizations from other sectors. This year, banking and finance respondents spent as much as $2,500 per employee (median) on cybersecurity, while retail and consumer products businesses invested up to $400 per employee (median) and education respondents invested a maximum of $200 per employee (median).

Similarly, organizations that have experienced a cybercrime are more cautious and exhibit more maturity in their security practices than those that have not. We found that 37% of respondents who had not suffered a security incident did not know what groups posed the greatest threat to their organization, compared with 18% of those who had experienced an incident.

What's more, organizations that have detected attacks are considerably more likely to employ security capabilities such as vulnerability management, cyber threat intelligence analysis, intrusion detection tools, and Security Information and Event Management (SIEM) technologies. They are also more likely to include cyber risks in the enterprise risk-management program and to prioritize security spending based on the level of risk a threat presents to the overall business strategy.

The takeaway: Those that demonstrate a more advanced cybersecurity posture are not necessarily smarter. They have simply invested more and have learned from experience.

Toward strategically smart cybersecurity spending

38%

have a methodology to prioritize cybersecurity investments based on risk to the business.

While organizations are more concerned about cyber threats, our research finds they have done very little to strategically invest in cybersecurity and ensure that it is aligned with the overall business strategy.

Cybersecurity spending will be most productive when the allocation of resources is based on specific business risks. It's a concept that seems clear-cut, yet most organizations do not take this type of strategic approach: Only 38% of survey respondents said they have a methodology to prioritize security investments based on greatest risk and impact to the organization's business strategy.

There is no one-size-fits-all methodology for strategic spending, but allocation of resources based on risk is an approach all organizations should adopt, regardless of industry and geography.

Cybersecurity programs also should be designed with flexibility and agility to enable the organization to quickly address cyber threats as they multiply and evolve. In practical terms, the scope and duration of cybersecurity initiatives should be designed and funded for shorter terms than the typical three- to five-year business plans.

A strategic investment also will require that organizations identify and invest in cybersecurity practices that are most relevant to today's advanced attacks. Rather than an emphasis on prevention mechanisms, for instance, it is essential to fund processes that fully integrate predictive, preventive, detective, and incident-response capabilities to minimize the impact. In particular, we find that many organizations fail to invest in the people and process capabilities that allow them to rapidly respond to and mitigate incidents.

Similarly, it is critical that organizations invest in resources to identify and classify their most valuable information assets, as well as determine where high-value assets are located across the ecosystem and who has access to them. These "crown jewels" will vary by industry, of course. A retailer's high-value data, for instance, would include customers' financial information, while the lifeblood of pharmaceutical companies is often trade secrets for developing new medications.

Identification and classification of assets will help security and business executives determine how much to invest in cybersecurity. It is equally important to consider the quality and end-to-end strategy of the investment. For instance, it's not enough to simply deploy network-monitoring technologies; you should also ensure adequate funding for data analytics that enable cybersecurity personnel to uncover patterns in anomalous network behavior and the people resources to act on this insight.

Once identified and located, organizations should then prioritize protection of high-value information across the enterprise and allocate resources in correlation with the greatest risks. Doing so will require a certain amount of knowledge about existing and potential adversaries, including their motives, resources, and methods of attack. This will not happen without a budget for threat analysis and monitoring, as well as a commitment of time and resources for collaborating with government agencies, peers, law enforcement, and other third parties to gain an understanding of leading cybersecurity practices.

These practices will vary by industry and market. A strategic approach to spending will require knowledge of best-in-class cybersecurity programs of companies that are similar in size, product offerings, operations, markets, and customer base. At the same time, it's advantageous to assess the programs of organizations that operate in different industries but are similar in size and other attributes. In other words, the key to learning from others is understanding which cybersecurity lessons apply to your organization.

"Cybercrime is a clear, present, and permanent danger. While it's a permanent condition, however, the actors, threats, and techniques are very dynamic."

— Tom Ridge, CEO of Ridge Global and first secretary of the US Department of Homeland Security

It will also be necessary to ensure adequate funding for comprehensive, ongoing employee training and awareness programs. The merit of awareness programs is quite clear: 42% of respondents said security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence.

The financial value of employee awareness is even more compelling. Organizations that do not have security awareness programs—in particular, training for new employees—report significantly higher average financial losses from cybersecurity incidents. Companies without security training for new hires reported average annual financial losses of $683,000, while those do have training said their average financial losses totaled $162,000.

At the other end of the organization chart, strategic spending will require a deep engagement with, and commitment from, the highest executive levels. To get there, security leaders must be prepared to persuasively articulate to executive leadership, the audit committee, and the Board the benefits of immediate—and sustained—investment in cybersecurity.

This discussion will be most effective when framed in the vocabulary of risk management, a context that is familiar to executive leaders and Board members. A risk-based discussion will enable security leaders to more effectively articulate the criticality and goals of cybersecurity, as well as set the agenda for prioritizing and validating investments based on risk-management strategies.

The time to start the conversation is now.

By all accounts, the severity of cyber threats will continue to intensify as threat actors evolve and sharpen their skills and techniques. "Cybercrime is a clear, present, and permanent danger," according to Tom Ridge. "While it's a permanent condition, however, the actors, threats, and techniques are very dynamic. "

So if history—and responses to this survey—are a guide, more organizations will fall victim to more costly cybercrime in the coming year. Don't be one of them. Organizations that take a strategic approach to cybersecurity spending can build a more effective cybersecurity practice, one that advances the ability to detect and quickly respond to incidents that are all but inevitable.

How current cybersecurity compares with the NIST Framework

The NIST Cybersecurity Framework may be voluntary, but it offers potential advances for organizations across industries.

The NIST Cybersecurity Framework, which was drafted by the Commerce Department's National Institute of Standards and Technology (NIST), is a voluntary risk-based compilation of guidelines that aims to help organizations identify, implement, and improve their cybersecurity stance.

The Framework Core defines standardized cybersecurity activities, desired outcomes, and applicable references that constitute sound cybersecurity. It is organized by five continuous functions:

- **Identify:** An understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities.
- **Protect:** The controls and safeguards necessary to protect assets or deter cybersecurity threats.
- **Detect:** Continuous monitoring to provide proactive and real-time alerts of cybersecurity-related events.
- **Respond:** The policies and activities necessary for prompt responses to cybersecurity incidents.
- **Recover:** Business continuity plans to maintain resilience and recover capabilities after a cyber breach.

To compare how the security programs of survey respondents achieve these recommended guidelines, we identified key responses to survey questions that correspond with best practices as prescribed by the Framework's Core functions.

The result: We found that the vast majority of respondents' cybersecurity programs fall very short of the NIST guidelines. Following is a look at organizations' adoption of 45 practices, policies, and technologies that correspond with the NIST Framework.

Identify	*Respondents have adopted*
Business environment	
Process for evaluating cybersecurity of third parties with which share data/network access	56%
Process for evaluating cybersecurity of third parties before doing business with them	44%
Include security in contract negotiations with vendors/suppliers	31%
Regular security communication from management	29%
Conduct incident response planning with third-party supply chain	27%
Have an intellectual property agreement	27%

Identify	*Respondents have adopted*
Governance	
Hired a Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	28%
Risk assessment	
Cyber risks included in enterprise risk-management program	81%
Have vulnerability management	46%
Conduct cyber threat analysis	23%
Employ threat modeling	14%
Have supply chain risk management	8%
Risk management strategy	
Prioritize security investments based on risk/impact to overall business strategy	38%
Protect	
Access control	
Account/password-management policies	59%
Intrusion prevention system	58%
Identity management	49%
Technically enforced segregation of duties	26%
Awareness and training	
New employee security training	46%
Periodic security education & awareness programs	44%
Employees required to review & accept written inappropriate use policy on periodic basis	40%
Data security	
Data Loss Prevention technology	44%
Information protection processes & procedures	
Employee/contractor background check	48%
Periodic risk assessments	47%
Penetration testing	42%
Incident response team	31%
Regular information audits	27%
Storage & review of e-mail or computer files	24%
Onsite first responders trained to handle digital evidence	20%

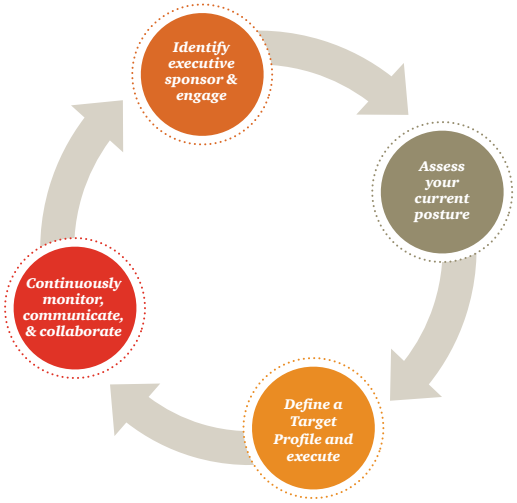
Detect	Respondents have adopted
Anomalies & events	
Intrusion detection system	62%
Security event analysis	40%
Use SIEM technologies	26%
Security continuous monitoring	
Regularly monitor, inspect, & compare outbound network traffic against threat intelligence	52%
Regular system log monitoring to identify intrusion attempts	49%
Monitor Internet connections	42%
Vulnerability management	40%
Conduct regular security audits	36%
Cyber threat intelligence analysis	33%
Required internal reporting of misuse or abuse of computer access by employees or contractors	32%
Employee monitoring	28%
Respond	
Response planning	
Have a formalized plan outlining policies & procedures for reporting and responding to cyber events	54%
Communications	
Participate in Information Sharing & Analysis Center (ISAC) activities	25%
Public law enforcement partnerships	15%
Analysis	
Computer forensics	25%
Recover	
Improvements	
Have a methodology to determine the effectiveness of security programs	53%
Have satisfactory outside communications firms (PR, crisis management)	20%

Taking action to implement the Framework

The NIST Cybersecurity Framework represents a tipping point in the evolution of cybersecurity, one that emphasizes and encourages a proactive risk-management approach that builds on standards and compliance. While the Framework is voluntary, we believe that organizations—across industries—should adopt the guidelines as a key tool to manage and mitigate cyber risk to their business, in combination with other risk-management tools and processes such as cyber insurance.

Doing so will not only help organizations improve cybersecurity programs, but also potentially advance their regulatory and legal standing for the future. Following are four steps your organization can take to get started:

The Framework can help organizations more effectively collaborate on security issues, as well as potentially advance their future regulatory and legal standing.



1. ***Identify your executive business sponsor and engage:*** Although not specifically included in the Framework, executive alignment and business context for your organization's desired cybersecurity posture is critical for appropriate implementation of the Framework.

2. ***Assess your current posture:*** Use a risk-based approach to assess your cybersecurity practices against the Framework Core industry standards and guidelines. This will help you determine the elements to include as desired control objectives.

3. ***Define a Target Profile and execute:*** Based on your assessment, establish a Current Profile of cybersecurity activities and risk-management practices. Using a combination of the Framework Core and business-specific requirements that have been endorsed by your executive sponsor, create a baseline to guide cybersecurity risk-management activities. Next, determine a Target Profile to identify gaps and draft a prioritized action roadmap and execution program to achieve the Target Profile.

4. ***Continuously monitor, communicate, and collaborate:*** In a reiterative process, continuously monitor and routinely assess your critical infrastructure asset's Current Profile against the business-defined Target Profile. Share information about the Target Profile with your executive sponsor, who can help transform progress toward the Target Profile into a business context. Use this business context to inform internal stakeholders, general counsel, internal audit functions, lines of business, and the board of directors, if necessary.

www.pwc.com/cybersecurity

Cybersecurity leadership team

David Burg
Principal, US & Global
Cybersecurity Leader
david.b.burg@us.pwc.com

Michael Compton
Principal, Cybersecurity Strategy
& Operations
michael.d.compton@us.pwc.com

Peter Harries
Principal, Health Industries
peter.harries@us.pwc.com

John Hunt
Principal, Public Sector
john.d.hunt@us.pwc.com

Mark Lobel
Principal, Technology, Entertainment,
Media & Communications
mark.a.lobel@us.pwc.com

Gary Loveland
Principal, Consumer and Industrial
Products & Services
gary.loveland@us.pwc.com

Joe Nocera
Principal, Financial Services
joseph.nocera@us.pwc.com

Dave Roath
Partner, Risk Assurance
david.roath@us.pwc.com

Contributing authors

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

Neal Pollard
Director
neal.a.pollard@us.pwc.com

Laurie Schive
Director
laurie.a.schive@us.pwc.com