www.pwc.com/gsiss2015

Managing cyber risks in an interconnected world

Key findings from The Global State of Information Security® Survey 2015

30 September 2014

pwc

Table of contents

01

Cyber risks: A severe and present danger

Cybersecurity is now a persistent business risk

It is no longer an issue that concerns only information technology and security professionals; the impact has extended to the C-suite and boardroom.

Awareness and concern about security incidents and threats also has become top of mind among consumers as well. In short, few risk issues are as all-encompassing as cybersecurity.

Media reports of security incidents have become as commonplace as the weather forecast, and over the past 12 months virtually every industry sector across the globe has been hit by some type of cyber threat.

Following are but a few: As incidents proliferate, governments are becoming more proactive in helping organizations fight cyber crime.

The US Federal Bureau of Investigation (FBI), for example, disclosed that it notified 3,000 companies—including banks, retailers, and defense contractors—that they had been victims of cybersecurity breaches in 2013.[1]

Subsequently, the US Department of Justice (DOJ) charged five Chinese military hackers with conducting cyber economic espionage against American companies in the nuclear power, metals, and solar energy sectors.[2] This marked the first time that the US has charged state officials with economic espionage using external cyber attacks under section 1831 of the Economic Espionage Act.

It's a trend that will likely continue, according to Sean Joyce, PwC principal and former deputy director of the FBI. "I think we will see the DOJ and FBI continue to pursue an aggressive strategy against nation-state actors that cause significant economic damage to the US economy," says Joyce.

Assaults on major retailers reached epic levels in the past year, resulting in the theft of hundreds of millions of customer payment card records, a rash of litigation, and a rush to adopt a new payment card standard in the US. In the UK, payroll information and bank account numbers of 100,000 employees of a supermarket chain were stolen by a company insider and published online.[3]

Stock exchanges also have become routine targets

A survey of 46 global securities exchanges conducted by the International Organization of Securities Commissions (IOSCO) and the World Federation of Exchanges Office found that **more than half (53%)** had experienced a cyber attack.[8]

Huge heists of consumer data were also reported in South Korea, where 105 million payment card accounts were exposed in a security breach.[4] And in Verden, Germany, city officials announced the **theft of 18 million** e-mail addresses, passwords, and other information.[5]

The retail attacks did much to elevate awareness of cyber threats, as did media coverage of the breach by former contractor Edward J. Snowden. The revelations of cyber surveillance of individuals, businesses, and nations has also prompted many international businesses and governments to reconsider purchase of products and services from companies that may be affiliated with government entities.

Other examples of state-sponsored espionage were uncovered by security firm Symantec, which discovered attacks against major European governments that has been under way for at least four years. Because of the chosen targets and sophisticated malware employed, Symantec believes a state-sponsored group is coordinating the attacks.[6]

Geopolitical discord, most notably between Russia and Ukraine, resulted in a volley of cyber attacks between the two nations that took down and defaced government websites on both sides of the conflict, as well as spread malware to the computers of embassies.

Financial services companies continued to be major targets

Cyber thieves plundered more than **$45 million** from worldwide ATM accounts of two banks in the Middle East.[7]

Other critical infrastructure providers are also under attack.

A hacker group successfully infiltrated a US public utility via the Internet and compromised its control system network, although the intrusion was halted before any damage was done.[9] And sophisticated state-backed cyber adversaries employed powerful malware to infect the industrial control systems of hundreds of energy companies across the US and Europe.[10]

One of the year's most far-reaching incidents was the Heartbleed defect, which impacted almost two-thirds of web servers around the world, including some of the most popular e-mail and social networking sites.[11] It is believed to have compromised millions of websites, online shopping destinations, and security applications, as well as software like instant messaging, remote access tools, and networking devices. In the first intrusion attributed to the Heartbleed defect, a US hospital chain reported theft of 4.5 million patient records in August.[12]

We also saw increases in attacks on connected consumer devices—such as baby monitors, home thermostats, and televisions—that comprise the Internet of Things, a nascent ecosystem of devices that interconnect information, operational, and consumer technologies. These Internet-connected devices are vulnerable to attack because they lack fundamental security safeguards, a point verified by a recent HP Fortify on Demand study.

HP reviewed 10 of the most commonly used connected devices and found that **70% contain serious vulnerabilities**.[13]

And the risks go beyond devices

Security firm IOActive has published research that demonstrates in detail how hackers can control the Electronic Control Units of specific automobiles and proposes mechanisms to detect attacks.[14]

Even those reporting the cybersecurity intrusions were not immune. Some of the world's most trusted news organizations, including *The New York Times*, *The Financial Times*, CNN, and Reuters—were taken down or compromised in the past year. Many of the most prominent attacks were carried out by hackers tied to a Middle Eastern government.

This list is by no means exhaustive. It will always be difficult to know exactly what organizations have been compromised because many simply don't realize that they have been attacked or are under attack. Others may be reluctant to reveal known compromises for very real fear of reputational damage, lawsuits, and regulatory investigations.

Indeed, regulators around the world are beginning to more proactively address cyber risks.

In an indicator of how the regulatory landscape is evolving, the US Securities and Exchange Commission (SEC Office of Compliance Inspections and Examinations (OCIE) recently announced that it plans to examine the cybersecurity preparedness of more than 50 registered broker-dealers and investment advisers.[15] In Asia, the Singapore Personal Data Protection Act establishes new standards for the collection, use, and disclosure of personal data.

Organizations that do not comply with the act are subject to financial penalties of **up to $1 million (SGD) or $788,995 (USD)**.[17]

The new guidance highlights several unique requirements, such as suggesting that organizations have cyber insurance and be able to produce a comprehensive inventory of all security incidents and breaches. SEC guidance also requires that businesses implement risk-assessment processes, as well as more effectively assess vendor risks and due diligence.

It was widely reported that automobiles, which contain dozens of computers that are often linked to one another and, in some cases, communicate wirelessly with the outside world, **can be hacked** to control the brakes, steering, and even engines.

Executives of multinational organizations are keeping an eye on European Union Data Protection Regulation, which is on track to be finalized in 2015. The regulation is expected to add new requirements for breach notification to individuals, require organizations that handle personal data to conduct risk assessments and audits, and increase fines for compromised businesses.[16]

The EU General Data Protection Regulation's breach notification requirements may increase disclosure of security incidents in Europe, according to John W. Woods, Jr., co-leader of the global cybersecurity practice for the law firm Baker & McKenzie LLP. "In the US, state data-breach notification statutes have resulted in the disclosure of a significant number of security breaches which in turn has raised the consciousness around cybersecurity issues," Woods says. "It will be interesting to see if the proposed EU data-breach notification has a similar impact. If it parallels the experience in the US, I think we very well may see a proliferation of incidents reported in Europe."

We have also seen new government efforts to help organizations improve their cybersecurity posture on a voluntary basis.

In the US, the President's 2013 Executive Order on improving cybersecurity produced the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Version 1.0 of the voluntary standard is being implemented by individual companies to assess and improve cybersecurity, as well as to create a common language for discussion and collaboration on security intelligence and response tactics.

Private-sector efforts to advance security include the launch of Google's Project Zero initiative, which aims to advance security by identifying and stopping zero-day threats (unknown and unpatched code flaws) before hackers can exploit them. Google says Project Zero researchers will work to enhance the security of widely used software, as well as study the motivations and techniques of attackers and conduct research into effective monitoring and mitigation of cyber compromises.[18]

Cybersecurity services market is expanding

In the wake of increased incidents and heightened regulations, corporations and government agencies are scrambling to safeguard their data and networks—a push that is catalyzing growth in the market for cybersecurity solutions and technologies.

Research firm Gartner predicts that global IT security spending will increase 7.9% to $71.1 billion in 2014, and grow an additional 8.2% to reach $76.9 billion in 2015, according to *The Wall Street Journal*.[19]

The upsurge in security incidents and the resulting media coverage has helped unleash a flood of venture capital investment in companies that provide cybersecurity software, solutions, and services.

During the first six months of 2014, venture capital firms invested $894 million in US cybersecurity startups, almost the same amount invested in all of 2013.[20] That puts the sector on track to post the highest investments in more than a decade. At the same time, the market capitalizations of some security firms hit new highs in the past year.

Network security provider FireEye, after a $304 million initial public offering (IPO) in 2013, now has a market cap of approximately

$4.6 billion[21]

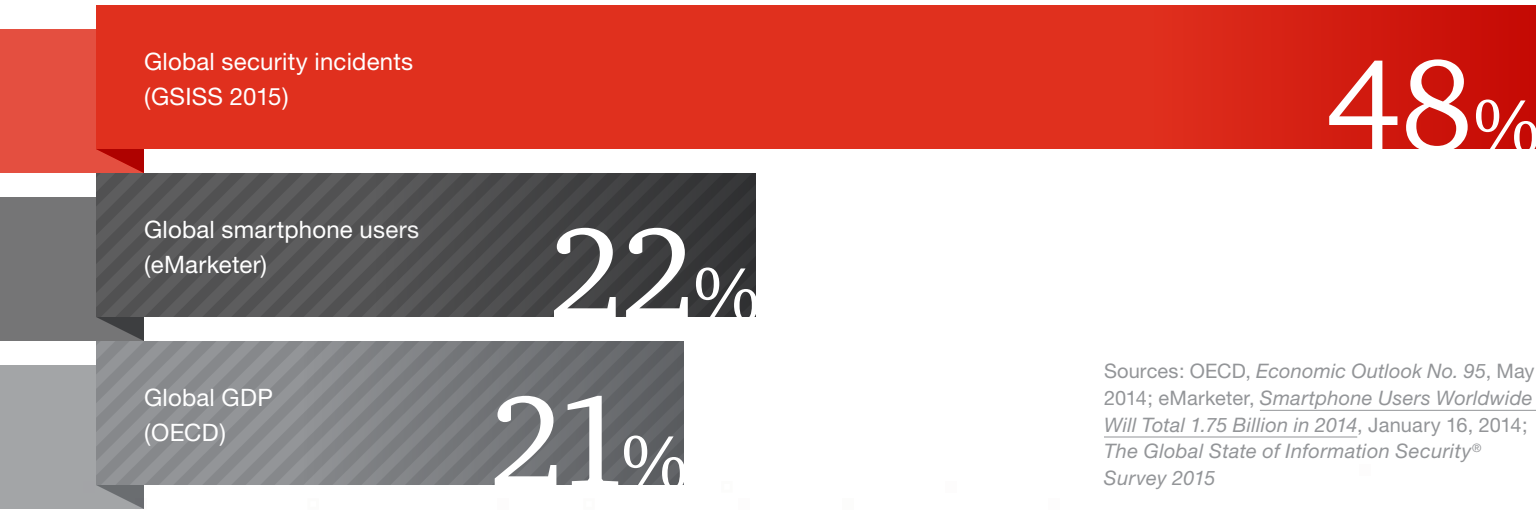
Enterprise firewall specialist Palo Alto Networks raised $260 million in a 2012 IPO and now has a market cap of approximately

$6.2 billion[21]

Figure 1

Security incidents outpace GDP and mobile phone growth

Year-over-year growth, 2013–2014



Sources: OECD, *Economic Outlook No. 95*, May 2014; eMarketer, *Smartphone Users Worldwide Will Total 1.75 Billion in 2014*, January 16, 2014; *The Global State of Information Security® Survey 2015*

At the height of the venture-funding boom, the valuation of some cybersecurity companies was five-to-ten times their annual revenues in 2013.

The market is starting to self-adjust, however, as investment in cybersecurity companies has cooled in recent months. As a result, some prominent firms have lost more than half of their previous market caps.

We believe the cybersecurity software, solutions, and services market is likely to remain a growth sector because executives and Boards recognize that cyber threats will never be completely eliminated, and regulatory and compliance requirements will likely become more stringent.

Against this backdrop of elevated risks, regulation, and market activity, we present the results of this year's survey.

Venture capital investments in cybersecurity firms are also accelerating in Europe.

London-based C5 Capital launched a cybersecurity-focused fund of

$125 million[22]

and announced an investment in IT security firm Balabit[22] of

$8.0 million[22]

Index Ventures, another venture capital firm, created a fund to invest in technology start-ups in Europe, Israel, and the US totalling

$550 million[23]

It has also been an active year for mergers and acquisitions of cybersecurity firms.

FireEye purchased Mandiant for approximately

$1.0 billion

Cisco Systems acquired Sourcefire for

$2.7 billion[24]

02

Incidents and financial impacts continue to soar

Continued year-over-year rise is no surprise

Given the nature and number of very prominent security breaches over the past year, it comes as no surprise that incidents reported by respondents to *The Global State of Information Security® Survey 2015* continued a year-over-year rise.

The annual survey of more than 9,700 security, IT, and business executives found that the total number of security incidents detected by respondents climbed to 42.8 million this year, an increase of 48% over 2013. That's the equivalent of 117,339 incoming attacks *per day, every day.*

Taking a longer view, our survey data shows that the compound annual growth rate (CAGR) of detected security incidents has increased 66% year-over-year since 2009.

These numbers are by no means definitive, however; they represent only the total incidents detected and reported. As noted, many organizations are unaware of attacks, while others do not report detected incidents for strategic reasons or because the attack is being investigated as a matter of national security.

Figure 2

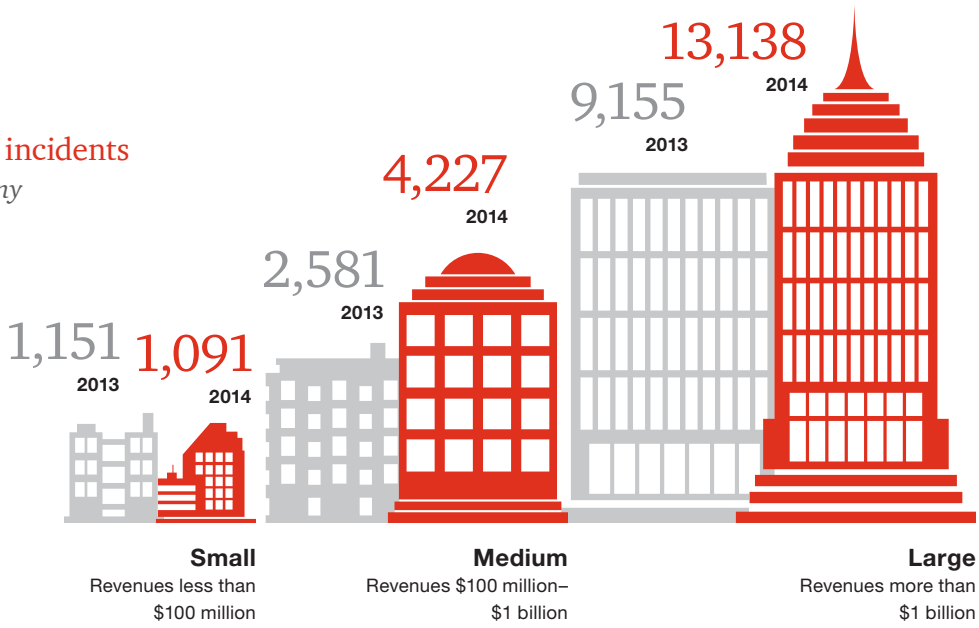
Security incidents grow 66% CAGR

Total number of detected incidents

Figure 3

Larger companies detect more incidents

Detected security incidents by company size (revenue)



It seems certain, given the technical sophistication of today's well-funded threat actors, that a substantial number of incidents are successful but not discovered. In fact, one cybersecurity firm recently estimated that as many as 71% of compromises go undetected.[25]

When it comes to discovering incidents, one thing is very clear: Large companies have the edge over smaller firms.

Among our global survey sample, large organizations (those with gross annual revenues of $1 billion or more) detected 44% more incidents compared with last year. The fact that big companies detect more incidents is not surprising.

Threat actors often target large organizations because they typically offer a rich trove of information—including trade-strategy documents, intellectual property related to product design, and large volumes of consumer data—that can be exploited, sold, or used for economic or military gain. Larger companies also typically have more mature security processes and technologies in place, which allows them to uncover more incidents.

As larger companies continue to implement more effective security safeguards, threat actors are increasingly stepping up their assaults on middle-tier companies, many of which may not have security practices that match the maturity of bigger businesses. That, in part, explains the 64% jump in the number of incidents detected by medium-size organizations (those with revenues of $100 million to $1 billion).

Small organizations proved the exception in discovering compromises. Companies with revenues of less than $100 million detected 5% fewer incidents this year. The reasons are not immediately clear, but one explanation may be that small companies are investing less in information security, which may leave them both incapable of detecting incidents and a more tempting target to cyber adversaries.

Small firms often consider themselves too insignificant to attract threat actors—a dangerous misperception. It's also important to note that sophisticated adversaries often target small and medium-size companies as a means to gain a foothold on the interconnected business ecosystems of larger organizations with which they partner. This dangerous reality is compounded by the fact that big companies often make little effort to monitor the security of their partners, suppliers, and supply chains.

The lack of due diligence into third parties has become so prevalent that an increasing number of regulators now require assessment of partner and supply-chain security capabilities. To catch up, small businesses might consider outsourcing elements of their cybersecurity programs to take advantage of economies of scale.

While big corporations may have the expertise and resources to build a sophisticated cybersecurity fusion center that enables sharing of threat intelligence and response techniques, that is not practical for smaller firms. But they can obtain the same benefits through managed security services. Another option to address risks might be purchase of cyber insurance.

Looking at security incidents across geographic regions, cybercrime is rising significantly in Europe, which reported a **41% jump** in the number of incidents detected over 2013.

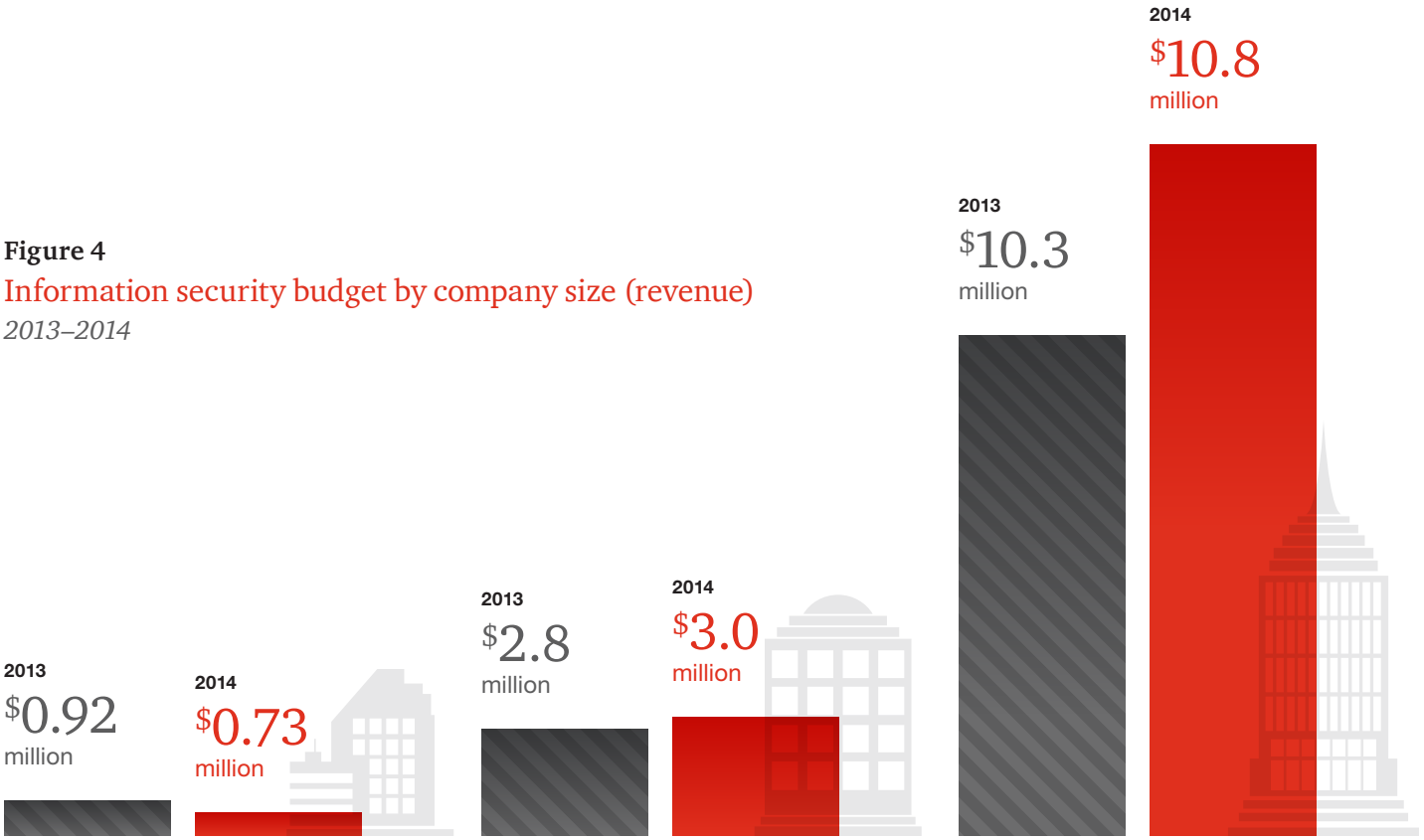
To improve their security posture, one option that small and medium companies might pursue is consideration of managed security services. This can enable them to employ sophisticated technologies and processes to detect security incidents in a cost-effective manner.

It very well may be that Europe leads in detecting incidents because the Continent reports a healthy 12% bump in security spending, among the highest of all regions.

In North America, respondents detected 11% more incidents this year. Asia Pacific respondents seem less adept at discovering incidents, reporting a 5% increase in detections.

South America was the only region to show a decline in the detection of compromises: The number of incidents dipped 9%. It's worth noting that information security spending dropped 24% in South America, significantly more than other regions.

Figure 4
Information security budget by company size (revenue)
2013–2014



Small
Revenues less than $100 million

Medium
Revenues $100 million–$1 billion

Large
Revenues more than $1 billion

Financial losses increase apace

As security incidents grow in frequency, the costs of managing and mitigating breaches also are rising.

Globally, the annual estimated reported average financial loss attributed to cybersecurity incidents was $2.7 million, a jump of 34% over 2013.

Not surprising in light of last year's prominent breaches, is the finding that big losses are more common: Organizations reporting financial hits of $20 million or more increased 92% over 2013.

The rise in security incidents would account for some of this increase in financial losses, of course. But another explanation might be that today's more sophisticated compromises often extend beyond IT to other areas of the business, according to William Boni, corporate information security officer for T-Mobile US.

"Financial losses may now include remediation for monitoring of external customer impacts, as opposed to just operational distructions inside an organization's firewall," says Boni.

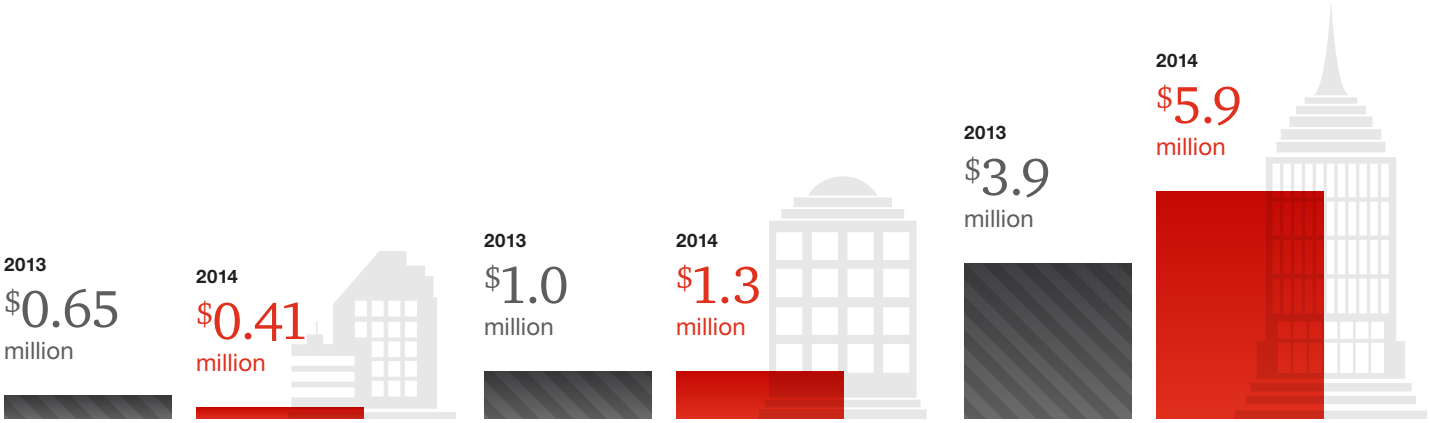
As with the total number of incidents, the global cost of cybercrime is ultimately unknowable because many attacks are not reported and the value of certain types of information, intellectual property in particular, is difficult to calculate. A recent study by the Center for Strategic and International Studies noted the difficulties in estimating financial impact but estimated that the annual cost of cybercrime to the global economy ranges from $375 billion to as much as $575 billion.[26]

If that figure seems high, it doesn't even approach the estimates of losses that can result from theft of trade secrets and intellectual property. The impact of this type of information loss can be measured by financial and non-financial indicators.

Figure 5

Incidents are more costly to large organizations

Average financial losses due to security incidents, 2013–2014



Small
Revenues less than $100 million

Medium
Revenues $100 million–$1 billion

Large
Revenues more than $1 billion

Financial impact may include decreased revenues, disruption of business systems, regulatory penalties, and erosion of customers.

Non-financial impact may include reputational damage, the pirating of products, diversion of research and development information, impacts to innovation, stolen product designs or prototypes, theft of business and manufacturing processes, as well as loss of sensitive information such as M&A plans and corporate strategy.

Using the World Bank's annual global GDP estimate of **$74.9 trillion** in 2013, loss of trade secrets may range from **$749 billion** to as high as **$2.2 trillion** annually.[28]

Measured across these vectors, financial damages can be significantly higher than traditional measures.

Consider that the Center for Responsible Enterprise And Trade (CREATe.org), in conjunction with PwC, estimated that the impact of trade-secret theft ranges from 1% to 3% of a nation's annual gross domestic product (GDP).[27] Potential losses seem even more menacing when the likelihood of cybersecurity compromise is factored in.

In its 2014 global risk report, the World Economic Forum rated cyber attacks among its **top five risks** in terms of likelihood.[29] The possibility of compromise is a threat that is not lost on many senior executives.

Almost **half (48%)** of respondents to PwC's 2014 Global Economic Crime Survey said the perception of cybercrime risk to their organization had increased in the past year, **up from 39%** in 2011.[30] In other words, executives clearly recognize that cyber threats have become a serious enterprise risk-management issue.

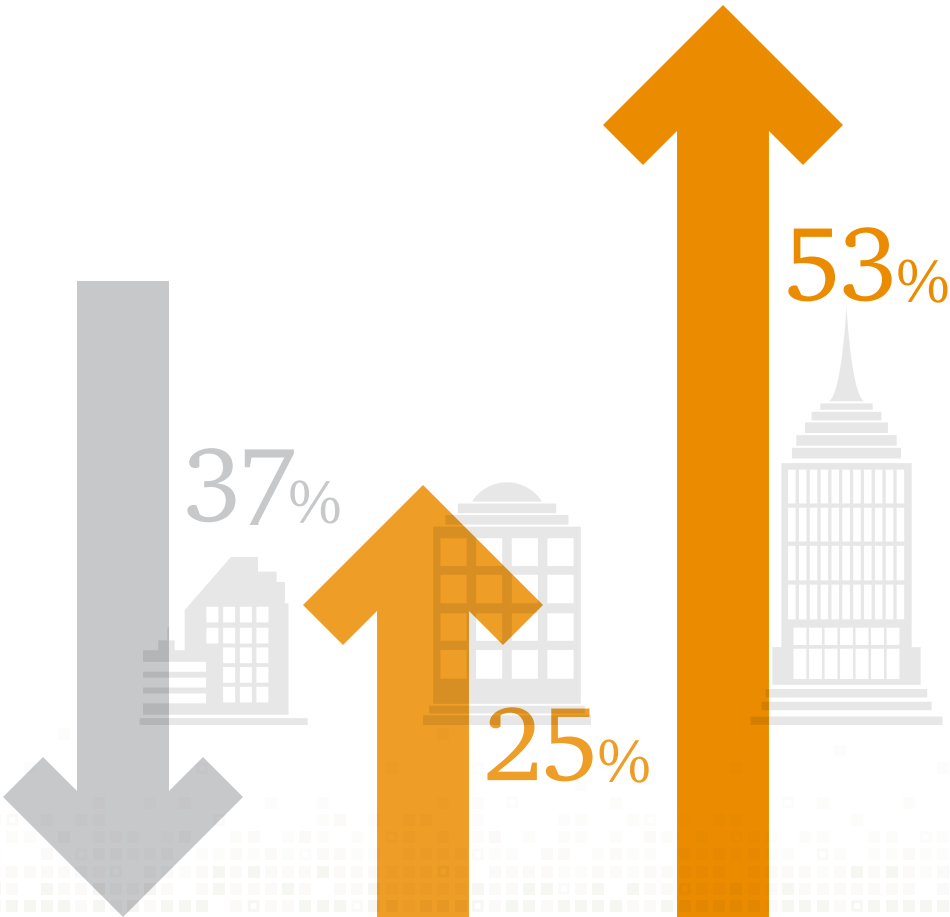
While risk has become universal, our security survey found that financial losses due to security incidents vary widely by organizational size. To understand these discrepancies, we looked into how organizations measure the financial impact of security incidents. Large companies typically spend more on information security and have a more mature program.

As a result, they are more likely to have the processes and knowledge to accurately calculate financial losses. Accordingly, they may consider a full range of possible impacts, including costs associated with loss of customer business, legal defense fees, court settlements, forensics, and reputational damage.

Larger organizations also take a more strategic approach to security by identifying sensitive assets and allocating spending to their most valuable data, and they are likely to understand third-party risks through the use of security baselines for partners.

Large companies tend to have the processes and technologies in place to actively monitor and analyze security intelligence; should anomalies be detected, they are in a better position to have an incident-response process at the ready.

And big organizations more frequently cultivate a culture of security through employee awareness and training programs, as well as by ensuring that senior executives broadcast the importance of cybersecurity across the enterprise.



Small companies report that the cost of incidents actually **decreased 37%** compared with last year, while large companies report a **53% jump** in financial damages. Medium-size organizations landed somewhere in the middle, reporting that the costs of incidents **rose 25%** over the year before.

03

Employees are the most-cited culprits of incidents

Nation-states, hackers, and organized crime groups are the cybersecurity villains that everybody loves to hate

10%

The percentage of respondents who point the finger at current employees jumped over 2013.

While there's no doubt that these actors are a force to be reckoned with, insiders—current and former employees, in particular—have become the most-cited culprits of cybercrime. That's not to say that all employees exhibit malicious behavior, however. In many cases, they may unwittingly compromise data through loss of mobile devices or targeted phishing schemes.

The jump in insider incidents may carry serious implications.

In the 2014 US State of Cybercrime Survey, we found that almost one-third (32%) of respondents said insider crimes are more costly or damaging than incidents perpetrated by outsiders.[31] Yet many companies do not have an insider-threat program in place, and are therefore not prepared to prevent, detect, and respond to internal threats.

It's a risk that PwC's Joyce has seen first hand. "Based on my experience with the [Chelsea] Manning and Snowden leaks, and with managing one of the leading insider program's within the intelligence community, I have seen that organizations sometimes overlook the threat from within their own business ecosystem," says Joyce. "The effects can be devastating."

Another threat lies in the fact that organizations often handle remediation of insider cybercrime internally. In fact, 75% of respondents to the US cybercrime survey said they did not involve law enforcement or bring legal charges in compromises committed by insiders.[32] In doing so, they may leave other organizations vulnerable to risks because those that hire these individuals in the future have no way to assess their threat potential.

Insiders

31% 35%
Current employees

27% 30%
Former employees

16% 18%
Current service providers/consultants/contractors

13% 15%
Former service providers/consultants/contractors

12% 13%
Suppliers/business partners

10% 11%
Customers

Outsiders

8% 10%
Terrorists

12% 15%
Organized crime

10% 16%
Activists/activist organizations/hacktivists

10% 16%
Information brokers

14% 24%
Competitors

6% 9%
Foreign entities & organizations

4% 7%
Foreign nation-states

6%
Domestic intelligence service

32% 24%
Hackers

24% 18%
Do not know

Figure 6
Insiders vs. outsiders
Sources of security incidents, 2013–2014

Employees are not the only source of rising insider threats, however.

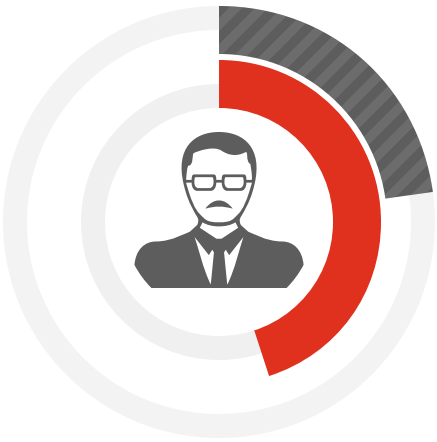
The percentage of incidents attributed to current and former service providers, consultants, and contractors increased to 18% and 15%, respectively, in 2014.

This is a threat that has been made all too apparent by a rampage of attacks on US retailers over the past year, some of which were achieved by criminals who gained access to the networks and point-of-sale systems of retailers through compromises of third-party suppliers and contractors.

Labeling 2013 as "the year of the retailer breach," Verizon counted 467 retailer breaches around the world in its annual Data Breach Investigations Report, noting that payment card data was the primary target in 95% of incidents within the retail industry.[33]

It looks as if 2014 will be another year of unprecedented breaches. As we prepared this report, news broke of another US retailer heist that resulted in the loss of 56 million payment card records.[34]

Among retailer and consumer companies, we found a noticeable jump in those who attribute security incidents to **current service providers and contractors (23%)** as well as **former partners (45%)**.



If there is an upside to these compromises, it's that they have spurred stakeholders in the US payment card industry to move from the existing magnetic-stripe technology to EMV, a more secure microprocessor-based standard that is less vulnerable to compromise.

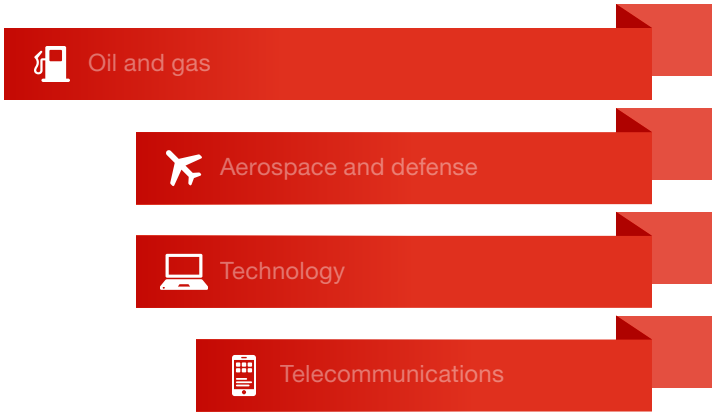
High growth in high-profile crimes

Cyber incidents that garner the most attention—compromises by nation-states, organized crime, and competitors—remain among the least frequent.

That's of little comfort, however, considering that our survey results show these attacks are among the fastest-growing threats.

It's a growing concern for many organizations, according to Lisa J. Sotto, a partner of the legal firm Hunton & Williams who specializes in cybersecurity and privacy issues. "I have seen a huge increase in the number of nation-state attackers who are seeking IP, blueprints, M&A data, and R&D," says Sotto. "The number of attacks by organized crime rings also appears to be at an all-time high, and the level of organization and infrastructure of these crime rings is unprecedented."

Nation-states often target critical infrastructure providers and suppliers to steal IP and trade secrets as a means to advance their own political and economic advantages. It isn't surprising, therefore, to find that nation-state incidents are most frequent among sectors such as **oil and gas (11%)**, **aerospace and defense (9%)**, **technology (9%)**, and **telecommunications (8%)**.



Survey results square with that assessment from the field. This year, we found an 86% increase in respondents who say they have been compromised by nation-states. Given the ability of nation-state adversaries to carry out attacks without detection, we believe the volume of compromises is very likely under-reported.

The boost in incidents attributed to nation-states may be due, in some part, to geopolitical events in Eastern Europe and the Middle East, which have coincided with an increase in distributed denial of service (DDoS) attacks and the use of sophisticated espionage spyware.

The battle against nation-state crime is compounded by the fact that timely sharing of cyber-threat intelligence is a challenge for most countries. Only a few, such as the US, Canada, the United Kingdom, Australia, and New Zealand, have the ability to effectively share cyber-attack information with companies headquartered in their respective countries.

Improvement of security intelligence-sharing capabilities could prove a significant economic advantage to both nations and their businesses. What's more, the combination of effective information sharing and the security research being conducted by private companies like Google may eventually make cybercrime less lucrative for adversaries by requiring that they invest more in technology and attack-process capabilities.

We also found a striking **64% jump** in security incidents attributed to competitors, some of whom may be backed by nation-states. Nowhere was this problem more acute than in Asia Pacific, and specifically in China. Almost **half (47%)** of respondents from China pointed to competitors as the source of security incidents, higher than any other nation.

The reason for this increase may be that companies are discovering that, as information is increasingly stored in digital formats, it is easier, cheaper, and quicker to steal IP and trade secrets than to develop capabilities themselves. In carrying out attacks, competitors often fuse sophisticated high-tech techniques with other methods such as recruiting employees of the targeted company, bribery, extortion, and the promise of a new job. The rise in cybercrimes attributed to nation-states and competitors is concurrent with an increase in theft of intellectual property and other types of sensitive information.

This year, IP theft increased 19% over 2013. Almost one-in-four (24%) respondents report theft of "soft" intellectual property, which includes information on processes and institutional knowledge. Fewer (15%) say "hard" intellectual property, such as strategic business plans, deal documents, and sensitive financial documents, was stolen.

This year, 15% of survey respondents cited organized crime as a source of incidents, up from 12% last year. By region, theft by organized criminals was particularly high in **Malaysia (35%)**, **India (22%)**, and **Brazil (18%)**.

IP theft is highest among respondents from aerospace and defense, an industry whose trade secrets can include sensitive information that may be critical to a country's national security.

This year, aerospace and defense respondents reported a **97% increase** in hard IP theft and a **66% jump** in soft IP compromise—higher by far than any other sector.

Compromises by organized crime also are on the rise.

Organized crime groups are typically motivated by financial gain. A successful cyber attack can net millions of payment card records that can be quickly monetized.

In addition to credit and debit card data, these criminals increasingly target patient health care data or other personally identified information that has considerable value in the underworld of information resellers.

In the US alone, financial losses due to personal identity theft, which includes misuse of payment cards, bank accounts, and personal information, totaled $24.7 billion in 2012, according to the Bureau of Justice Statistics.[35] The recent theft of more than a billion user credentials by organized criminals illustrates that these attacks are growing in scope.

In response, law-enforcement agencies across the world are beginning to band together to fight organized criminals, according to cybersecurity attorney Woods. "There has been an increased cross-border recognition of the need for more coordinated law-enforcement efforts to identify incidents caused by organized crime," he says. "I think this will accelerate in the coming years through organizations like Interpol."

Domestic intelligence: A new source of concern

Edward J. Snowden's disclosures of government surveillance have added a new adversary to the threat environment: domestic intelligence services.

As a result of the Snowden leaks, nations, businesses, and society in general have become increasingly skeptical of domestic surveillance and are concerned about potential impact on data privacy and security.

The headline-making nature of the Snowden revelations has resulted in considerable awareness and concern among business executives. Not only are they raising questions about government surveillance, but also regarding the telecommunications and technology companies that may have provided government access to data.

Globally, 59% of respondents say their organizations' executives are worried about government surveillance. Concerns are markedly higher in **China (93%)**, **India (83%)**, and **Brazil (77%)**.

This concern carries potentially broad implications for some telecommunications and high-technology companies. Firms in the US, in particular, and Europe have traditionally dominated the market for telecommunications and corporate networking equipment. But Asian companies are making inroads, and their prospects brightened after it was disclosed that the US government had collected sensitive information from some domestic technology and telecom firms.

As a result, organizations in some nations report they are reconsidering the procurement of equipment from certain manufacturers. In fact, 42% of respondents say the purchase of products and services originating in certain nations is under review, and 29% say they now purchase fewer products and services from some nations.

The "Snowden effect," which helped consumers understand the concept of Big Data analytics, has also raised a red flag among individuals. In fact, the Snowden leaks and the proliferation of Big Data have elevated the issue of personal privacy to a matter of public debate. The White House responded by publishing this year two high-profile papers on the impact of Big Data to the privacy of consumer information. These government studies underscore the importance of integrating a strategy for Big Data security and consumer privacy to protect information and gain competitive advantages.[36]

The issues that most worry executives?
The **privacy** of personal data, potential legal **risks**, and **loss** of intellectual property.

04

As incidents rise, security spending falls

Organizations are undoubtedly worried about the rising tide of cybercrime

PwC's Global Economic Crime Survey 2014 found that almost half (48%) of global respondents said their perception of cybercrime risk increased, up from 39% in 2011.[37]

At the same time, PwC's 2014 Annual CEO Survey reported that 48% of global CEOs are concerned about cyber threats to their organization, including a lack of data security.[38]

Despite elevated concerns, our survey found that global IS budgets actually decreased 4% compared with 2013. In fact, security spending as a percentage of IT budget has remained stalled at 4% or less for the past five years.

"Information security is a risk issue, not an IT issue," Sotto says. "Information security should be a distinct function, with a separate governance structure and a separate budget so that appropriate resources are given to information security. Having CISOs report to the head of IT is a vestige."

No matter where the security function reports, it seems counter-intuitive that, as threats become more frequent and costly, organizations have not stepped up investment in security initiatives. This finding is also puzzling in light of Gartner's forecast for a 7.9% increase in security spending for 2014.[39]

We found one explanation for the spending slow-down by looking at investment levels reported in last year's survey. In 2013, organizations reported very significant increases in spending over 2012, expanding IT investments by 40% and security spending by an even more substantial 51%. It could be that this year's respondents were hard-pressed to continue investments at that accelerated pace.

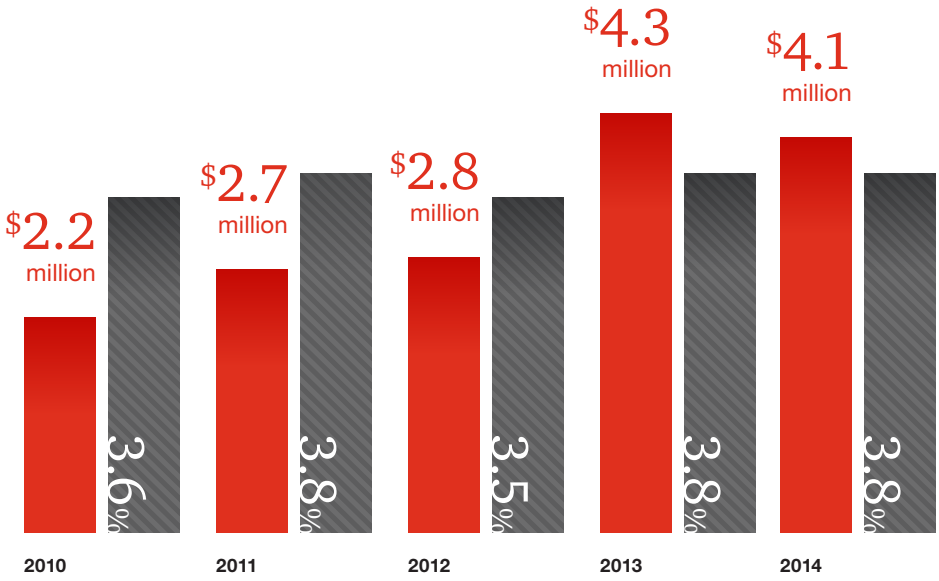


Figure 7

Overall, average security budgets decrease slightly, reversing a three-year trend

The average information security budget dipped to $4.1 million, down 4% over last year. Security spending remains stalled at only 3.8% of the overall IT budget.

% of IT budget spent on information security

Information security budget for 2014

Looking at security investment by company size also sheds some light on the anemic funding.

This year, companies with revenues less than $100 million say they reduced security investments by 20% over 2013, while medium and large companies report a 5% increase in security spending.

That represents a significant level of spending, according to T-Mobile's Boni. "One variable is a reluctance to increase spending during the recent economic recovery," says Boni. "I think a 5% increase is a pretty substantial level of attention since companies are starving other corporate areas and want to keep costs tightly under control."

Another explanation could be that more targeted security practices has enabled organizations to strategically optimize spending. "I think we are heading toward a paradigm shift in the way we spend on information security," says Fernando Camarotti, chief information security officer of Vale, a global metals and mining company based in Rio de Janeiro. "In the past, the big spending projects tended to lock down all the data, but that's no longer seen as effective. In addition to traditional information security controls for the entire company, we worked to find where we had confidential information that needed to be protected. When you do that, the security investment can be more effective and much smarter."

This diminished spending among small organizations begs the question: Are they simply giving up on cybersecurity? We can't be sure, but we certainly hope not. As noted, smaller businesses often believe they are too insignificant to draw the attention of serious hackers and organized crime. It also may be that rising risks, combined with an overabundance of security solutions, has resulted in "analysis paralysis," leaving smaller firms unable to make decisions and take action.

It could also be fatigue, says cybersecurity attorney Sotto. "The entire issue of cybersecurity is so daunting, particularly for small companies that don't have the appropriately skilled people, or credentialed people at the helm of the IS function," Sotto says.

It's also possible that, due to the ongoing shortage of experienced security professionals, the most skilled candidates are hired by bigger organizations with hefty budgets.

Among larger companies, an explanation for limited growth of security spending might be that, as the global economy continues to recover, more corporations are hoarding more cash and investing less in IT and security. It's obvious, however, that businesses are spending in some areas, most notably research and development.

Annual expenditures among the world's 1,000 biggest R&D spenders hit a record **$638 billion** in 2013, a 6% increase over the year before.[40]

We also believe many organizations struggle to understand how much to spend on security and how to determine the return on investments of their security outlay. In part, that's because there is no definitive data on current security risks to help inform a security spending strategy.

It also seems likely that, since only 40% of respondents say their Board is involved in security budget decisions, many may have trouble achieving robust funding in security. And, we also hear that many senior executives and Boards often find it difficult to understand how security technology works and identify the related tactical risks.

Looking at security investments by industry shows that spending is down in most sectors, with a few notable exceptions.

While the revenues and spending among airline manufacturers are up, for instance, defense spending is dropping among developing nations. This is particularly true in the United States after its pullout from Afghanistan and Iraq and subsequent defense budget cuts. And while the decline in the retail and consumer industry spending may seem puzzling given widely reported breaches, consider that 2014 security budgets may have been in place for the year before the incidents were reported.

Information security budgets are declining steeply among organizations in the **aerospace and defense (-25%)**, **technology (-21%)**, **automotive (-16%)**, and **retail and consumer products (-15%)** industries. In some sectors, overall business trends account for these drops.

"The typical CIO or CFO will spend money when there is documented proof a problem may result in real hurt," says Boni of T-Mobile. "When that is lacking, it's very difficult to accurately quantify the business impact of new technologies and unknown threats. Organizations must be very judicious about every nickel they spent on information security."

Industries reporting the most significant increases in security spending include healthcare providers and payers (66%), oil and gas (15%), and utilities (9%). The increase in spending among healthcare providers and payers is particularly striking—but certainly justifiable given current risks and trends. This year, healthcare providers and payers report a 60% increase in detected incidents, with financial losses skyrocketing 282% over 2013.

The explanation for this snowballing volume of incidents and financial losses may be that threat actors are targeting healthcare providers and payers for their increasingly valuable patient health data. A health record often comprises a full complement of information—financial, medical, family, and personal—that can be used to construct a complete identity.

A complete identity-theft kit containing comprehensive health insurance credentials can be worth hundreds of dollars or even $1,000 each on the black market, and health insurance credentials alone can fetch $20 each; stolen payment cards, by comparison, typically are sold for $1 each.[41]

These black markets for stolen data are growing in size and complexity.

While the number of websites on which data is sold is not known, the number of criminals who participate in these dark bazaars is likely to increase because it is becoming easier to get involved, according to the RAND Corp.[42] In part, that's because today's black market comprises increasingly more websites, forums, and chat channels in which goods can be bought and sold.

Healthcare providers and payers also may be boosting security investments to prepare for connected health-monitoring devices and the explosion of data that the Internet of Things will bring. Indeed, for healthcare providers and payers, the Internet of Things is not futuristic, nor are the risks theoretical.

Consider that almost half (47%) of healthcare provider and payer respondents say they have integrated consumer technologies such as wearable health-monitoring devices or operational technologies like automated pharmacy-dispensing systems with their IT ecosystem.

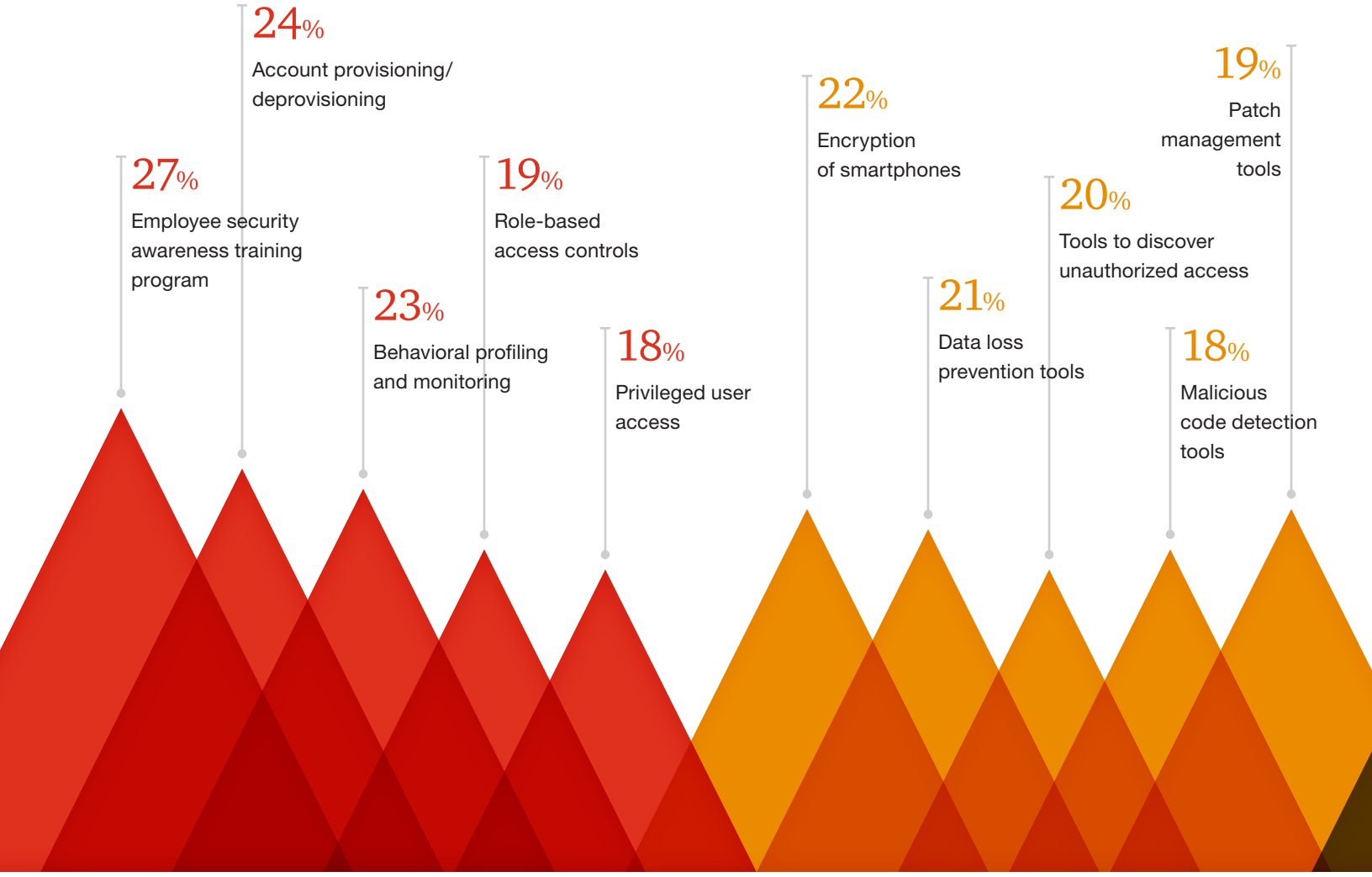
Yet they have not been as quick to ensure the security of these connected devices.

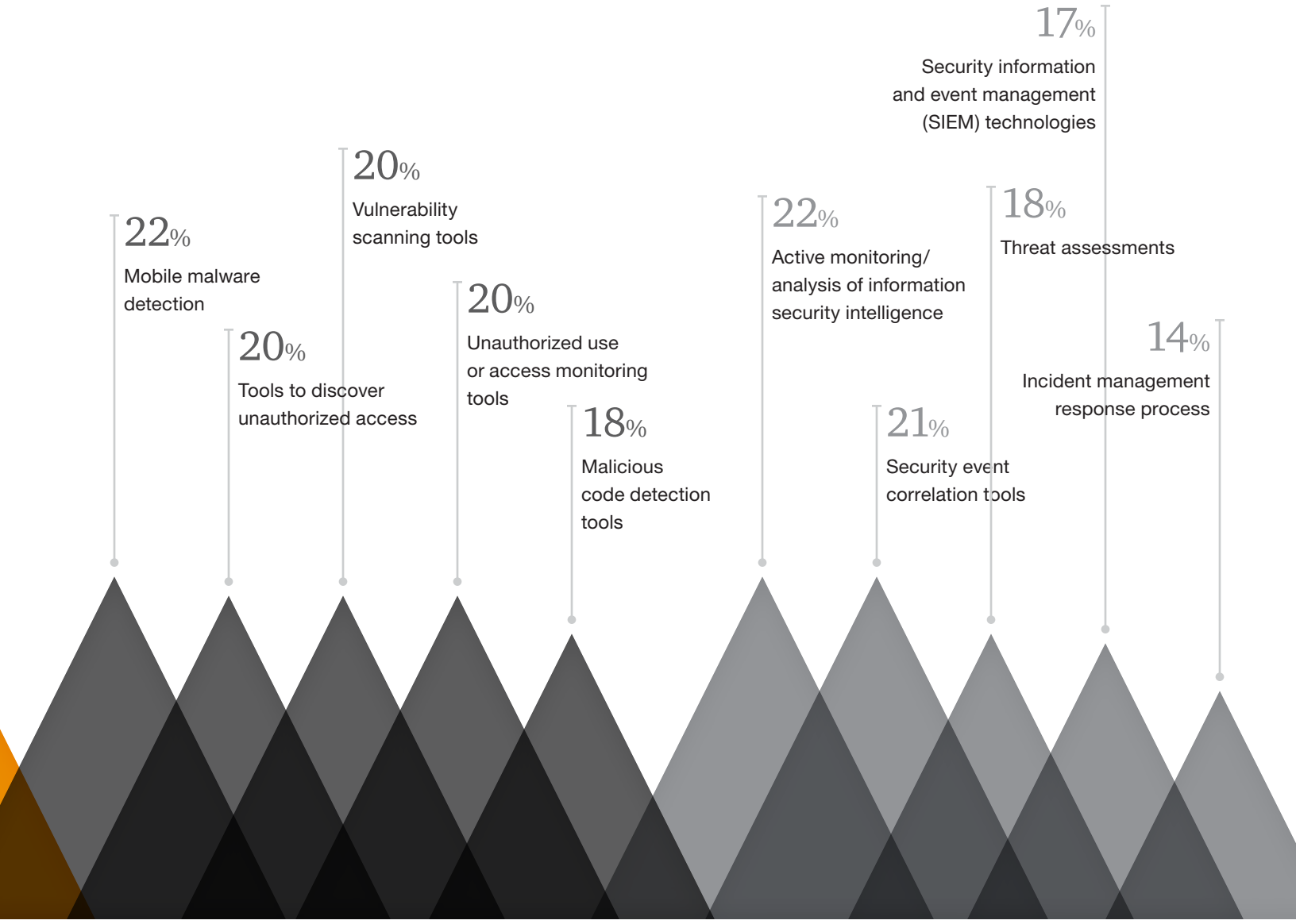
Just more than **one-third (34%)** have contacted device manufacturers to understand the equipment's security capabilities and risks, and **58%** have performed a risk assessment of the devices or technologies. Only **53%** have implemented security controls for these connected devices.

Figure 8

Top spending priorities over the next 12 months

Prevent, protect, detect, respond





Detect

Respond

05

Declines in fundamental security practices

Security practices must keep pace with constantly evolving threats and security requirements

Doing so will demand investments in the right processes and technologies to prevent, protect, detect, and respond to security risks. Overall, many organizations are failing to do so.

Given today's interconnected business ecosystem, in which exponentially more data is generated and shared with business partners and suppliers, an area of specific concern is the lack of policies and due diligence regarding third parties. It is worrisome that the focus on third-party security actually weakened in the past year in some very key areas—even as the number of incidents attributed to these insiders increased.

"We are seeing third-party vendors as a very significant source of cyber risk," says attorney Sotto. "You could have a moat around a heavily fortified castle but if the bridge is down to your vendors, then your fortifications become worthless." Sotto says organizations should anchor their third-party due diligence on three key practices:

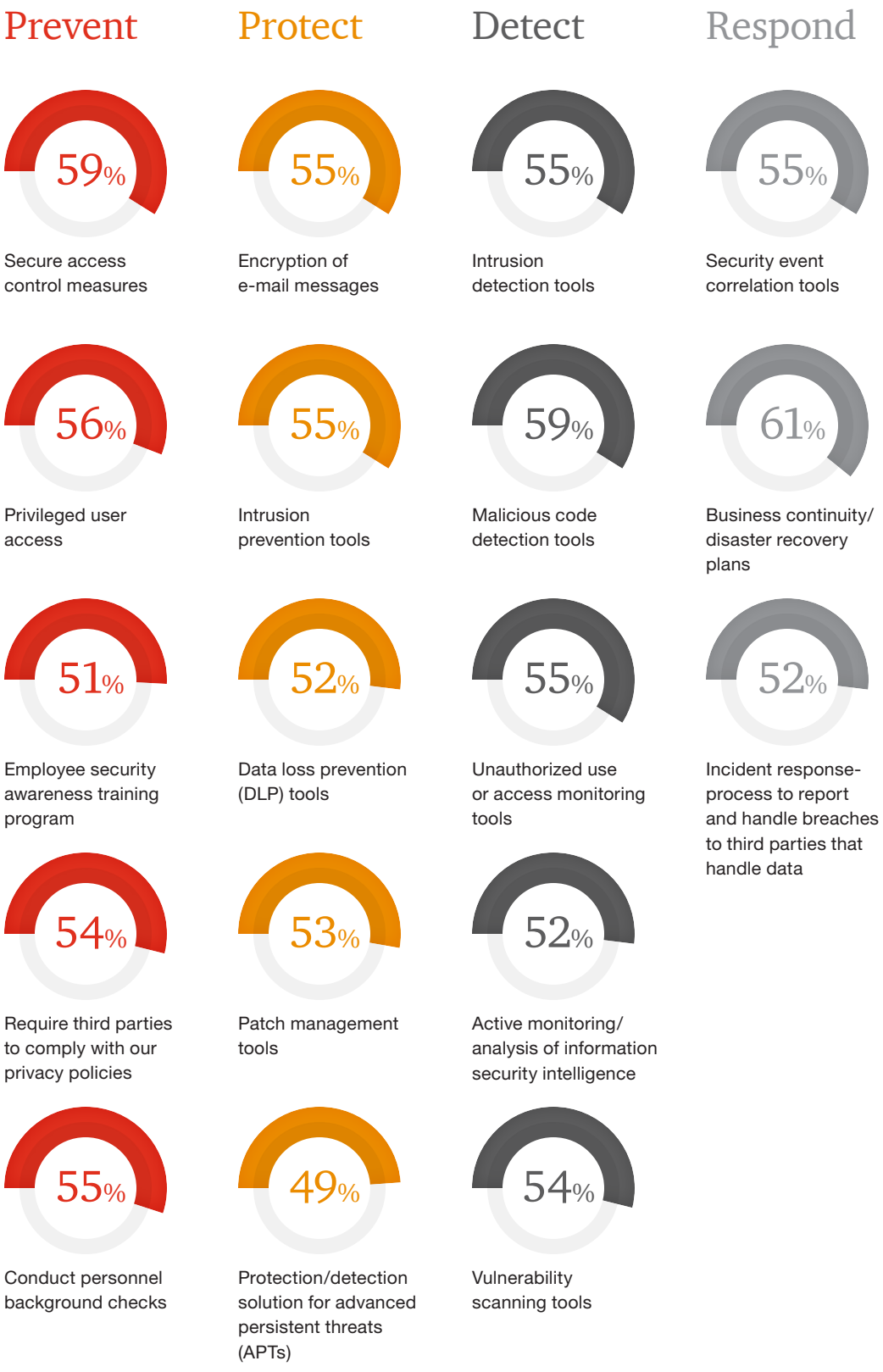
Perform appropriate protections of vendors to ensure that they have the ability to safeguard the information, have robust contractual protection, and conduct ongoing monitoring to ensure the third party is protecting the data.

Based on these criteria, many respondents are behind the curve. For instance, only 50% say they perform risk assessments on third-party vendors (down from 53% in 2013), and just 50% say they have conducted an inventory of all third parties that handle personal data of employees and customers. Just over half (54%) of respondents say they have a formal policy requiring third parties to comply with their privacy policies, down from 58% in 2013.

Figure 9

Failing to keep up with security threats

Prevent, protect, detect, respond



This year, **51%** of respondents said they have a security awareness and training program, down from **60%** last year. A slightly higher number, **57%**, say they require employees to complete training on privacy policies.

Employee training and awareness is a fundamental component of every program because the weakest link in the security chain is often human. Frequently, the disconnect comes down to how organizations engage their employees and generate awareness through their communications programs.

Consider that 84% of CEOs believe their strategic priorities will deliver on goals, but only 41% say their employees understand the strategy well enough to inform decision-making.[43]

Large organizations are more likely to recognize and act upon the importance of employee training. We found that 58% of big companies do so, compared with 47% of small firms.

Security training is most prevalent in North America and Asia Pacific, and is most likely to be embraced by organizations in the healthcare, industrial products, and financial services sectors.

Effective security awareness will also demand top-down commitment and communication, a tactic that is often lacking. Only 49% of respondents say their organization has a cross-organizational team that regularly convenes to discuss, coordinate, and communicate information security issues. It also will require that the C-suite and Board be directly involved.

Effective security awareness will require adequate funding, but perhaps more importantly it also will demand a commitment to maturity, says Gary Hayes, chief information officer of CenterPoint Energy, an electric and natural gas utility based in Houston. Accelerating investments is not enough" he says. "You have to mature your organization, your people, and your technologies, and that can be a more restraining factor than the availability of capital."

It is incumbent upon the executive team to take ownership of cyber risk and ensure that the Board understands how the organization will defend against and respond to cyber risks.

The barrage of incidents over the past year has resulted in a lot of discussion about Board involvement in security. Yet for all the chatter, organizations clearly have not elevated security to a Board-level discussion.

We know because we asked: Only 42% of respondents say their Board actively participates in the overall security strategy and 36% say the board is involved in security policies. Just 25% say Boards are involved in review of current security and privacy threats—a crucial component of effective information security.

That may be starting to change, however. Hayes of CenterPoint Energy notes that he attends regular meetings with CIOs of 22 large utility companies, and virtually all deliver security reports to the Board.

As does he. "I report to the broader Board twice a year, and I also report to the audit committee on a quarterly basis," Hayes says. "The Board definitely requests information about what's going on and how we are responding because cyber risks have been identified as among our top three enterprise risk-management issues."

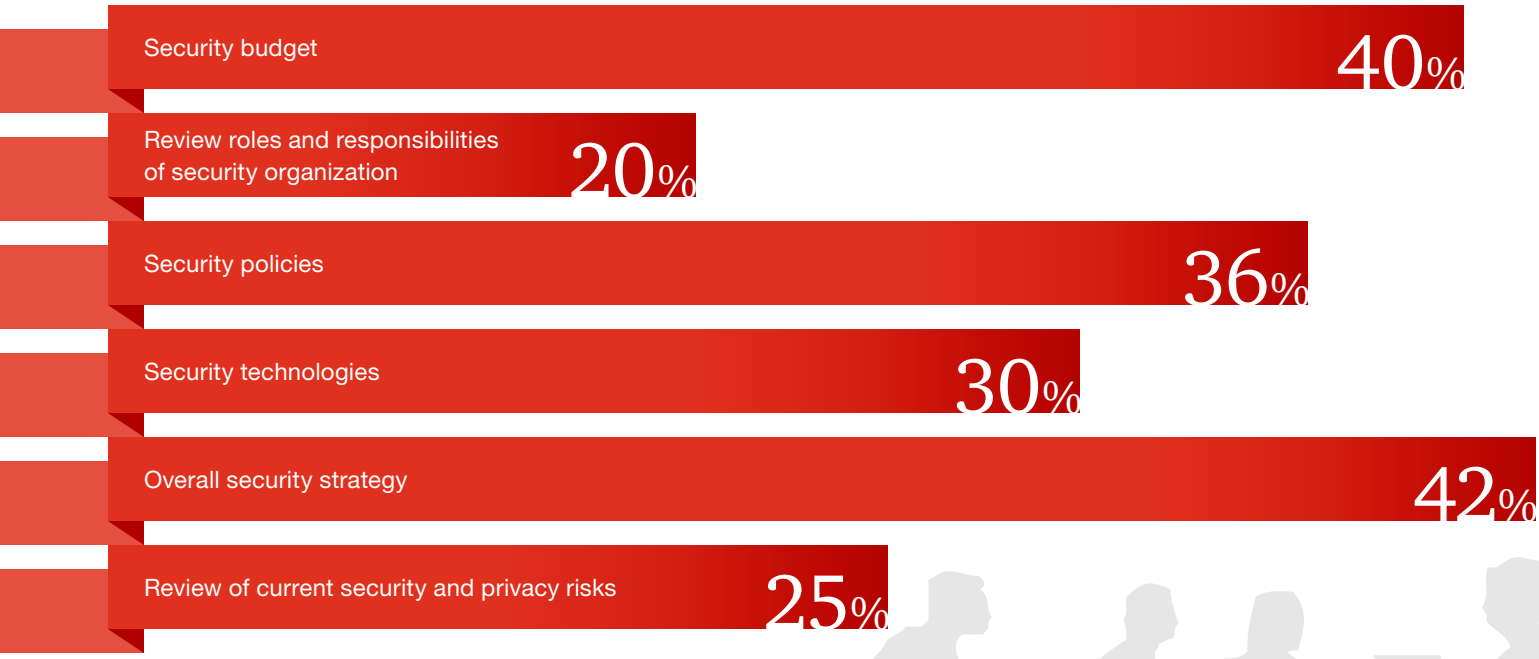


Figure 10

At most organizations, the Board of Directors does not participate in key information security activities.

Despite the high-profile security breaches in the past year, the Board of Directors is often not involved in critical initiatives such as security strategy, budget, and review of risks.

06

Gains in select security initiatives

While we found declines in some security practices, we also saw gains in important areas

Cyber risks, technologies, and vulnerabilities evolve at lightning speed, and sharing information among public and private entities regarding cyber threats and responses is central to a strong cybersecurity program.

Increasingly, organizations are embracing external collaboration to improve security and threat intelligence. Hayes of CenterPoint says his company actively collaborates with several Information Sharing and Analysis Centers (ISACs) and industry associations, as well as government agencies, an initiative that has proven to be "invaluable."

"If you are not connected to the conversations, you are going to be lost," he says. "In today's threat environment, there is no reason for not collaborating."

Survey respondents are starting to see the value of working with others.

This year, 55% of respondents say they collaborate with others to improve security, an increase of 12% over 2013. The larger the company, the more likely it is to collaborate with others: 66% of large organizations do so, compared with 49% of small firms. Collaboration is more common in regions in which growth in the development of IT infrastructure has been rapid over the past decade. Respondents from South America and Asia Pacific, for instance, are more likely to work with others to advance security intelligence.

As smartphones and tablets become ubiquitous, organizations have historically lagged in implementing security safeguards to counter mobile threats. This year we saw some notable advances. At the most basic level, 54% of respondents say they have implemented a mobile security strategy. Given the risks of mobility, that is still low but it represents an improvement over the 42% that had a mobile security strategy in 2013.

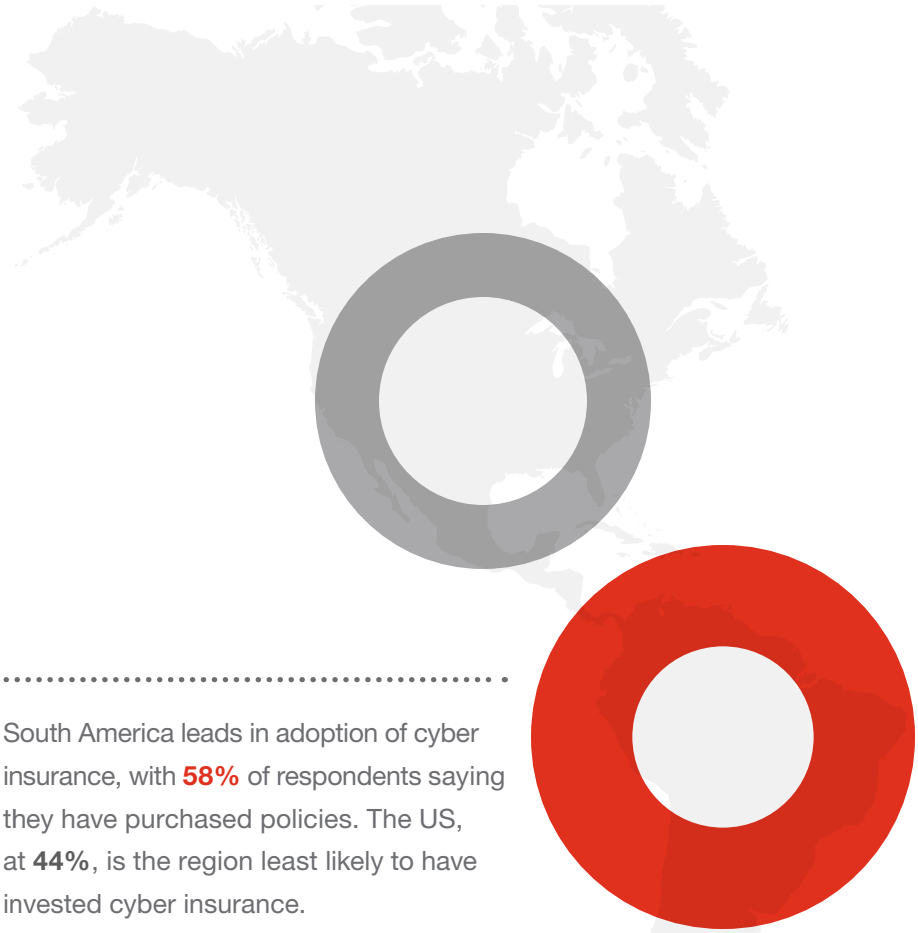
Similarly, mobile device management (MDM) and mobile application management (MAM) solutions are essential to securing a fleet of devices, whether owned by the enterprise or the individual. This year, 47% of respondents say they employ MDM/MAM solutions, an improvement from last year's 39% who did so. Nonetheless, there remains much opportunity for improvement.

Not surprisingly, advances in mobile security are more prominent among larger organizations, which tend to have more mature overall security programs in place. Financial services, telecommunications, and industrial products organizations have made the most progress in advancing their mobile security practices.

Another area of improvement can be seen in the adoption of cyber insurance as a tool to help manage the risks of cybercrime.

In the US, as noted, the SEC OCIE guidance has suggested that financial services organizations purchase cyber insurance as part of an effective cyber-risk management strategy. Given today's elevated threat environment and escalating costs of cybercrime, we believe that protecting against financial losses from cyber risks should rank as high as other insurable risks.

It's an approach that many organizations seem to understand. More than half (51%) of respondents say they have purchased cybersecurity insurance, up from 45% last year. Perhaps more significant is the finding that some companies are leveraging cyber insurance as a way to improve their security program. More than a third (36%) say they have taken steps to enhance their security posture in order to lower their insurance premium. Aerospace and defense, automotive, entertainment and media, and financial services companies are most likely to purchase cyber insurance.



South America leads in adoption of cyber insurance, with **58%** of respondents saying they have purchased policies. The US, at **44%**, is the region least likely to have invested cyber insurance.

07

Evolving from security to cyber risk management

As incidents continue to proliferate across the globe, it's becoming clear that cyber risks will never be completely eliminated

Today's interconnected business ecosystem requires a shift from security that focuses on prevention and controls to a risk-based approach that prioritizes an organization's most valuable assets and its most relevant threats.

It also will be critical to focus on rapid detection of security intrusions and an effective, timely response. To get there, businesses should reposition their security strategy by more closely linking technologies, processes, and people skills with the organization's broader risk-management activities. This remains a challenge for many businesses, according to Boni of T-Mobile.

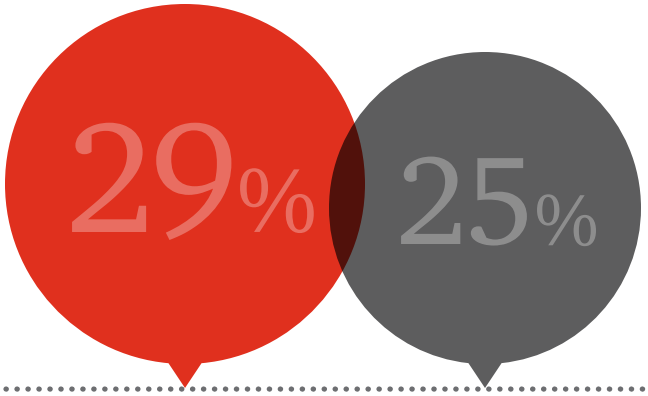
"It's rare that organizations have the practioners, tools, and executive leadership required to understand and respond to security challenges," Boni says. "Too many people still see information security as a principally technical problem and believe that simply buying the right software will cause the problem to go away. Information security involves people, processes, and technologies—getting all three in the right measure is the real art of a successful security program."

It also can help guide spending on information security. "There is a lot of uncertainty in return on investment for security. Companies often do not know if they are doing a good job," says Boni. "There is no generally accepted accounting procedure equivalent for baseline cybersecurity. Over time, the NIST standard should help create a common language and framework to help companies understand if they're doing a good job with their information security investments and programs."

Organizations seeking to implement the correct mix of people, processes, and technologies should consider the NIST Cybersecurity Framework. Even though the Framework targets US critical infrastructure providers, it offers an effective model for risk-based security for organizations across industries and across the globe.

We believe it is well worth adopting solely for its stated goal of improving security. "The NIST Framework is a great example of the public and private sector collaboration that provides an excellent agnostic framework to cybersecurity," says PwC's Joyce, who helped develop the executive order that mandated creation of the Framework.

Adoption of the Framework also can deliver ancillary benefits that include enhanced collaboration and communication of security posture among executives and industry organizations, as well as potential future improvements in legal exposure and even assistance with regulatory compliance.[44]



US organizations are already beginning to embrace the NIST Framework. We found that **29%** of American respondents say they have adopted the Framework, and an additional **25%** say adoption is a future priority.

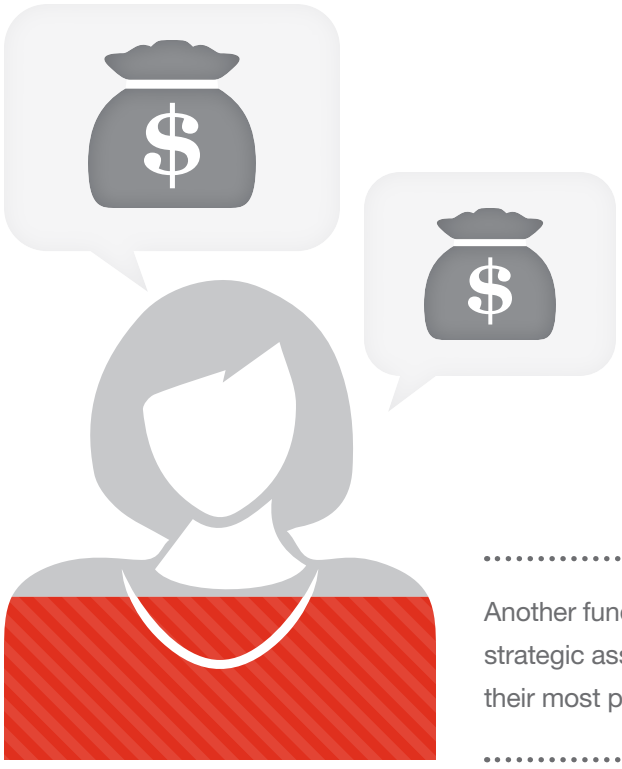
Organizations that participated in the development of the NIST Framework are typically early adopters of the guidelines. Hayes says CenterPoint personnel attended NIST workshops and developed a cyber incident response plan in tandem with creation of the Framework. With this head start, the company quickly adopted and enhanced its approach by leveraging the NIST Framework. "The process enabled us to enhance aspects of cybersecurity that we feel are applicable to our space," Hayes says. "We've used it to understand what we need to do, and to act on that."

Among the first steps NIST suggests is that organizations identify and classify their most valuable information assets, as well as determine where high-value data are located across the ecosystem and who has access to them.

For mining company Vale, this initial process created a solid foundation for its information security program. "One of the first things we did was to identify our confidential information and determine where it is stored." says Camarotti. "That gave us huge insights into the business side of information security, as well as an understanding of how our employees use confidential data. It also enabled us to determine specific levels of protection, and to understand areas in which we can be more lenient and areas in which we should be more strict."

Many of our survey respondents have not yet taken these steps, however: Only 54% have a program to identify sensitive assets, and just 56% have taken the effort to inventory the collection, transmission, and storage of sensitive data for employees and customers. This type of strategic approach to spending is most common among aerospace and defense, technology, telecommunications, and financial services organizations.

Regionally, respondents from South America and Asia Pacific are more likely to allocate security spending to their most valuable data. It is also essential that organizations align their security strategy with specific business needs, a step that 40% of respondents forgo. Industries most likely to link security and business strategies include industrial products, healthcare providers and payers, and financial services. Regionally, respondents from Asia Pacific and North America lead in this approach.



Another fundamental step is aligning security spending with the organization's strategic assets. Yet **34%** of respondents do not allocate security spending to their most profitable lines of business.

Strategic security spending also will demand that businesses identify and invest in cybersecurity practices that are most relevant to today's advanced attacks. It is essential to fund processes that fully integrate predictive, preventive, detective, and incident-response capabilities to minimize the impact.

Also critical is adequate investment in the people and process capabilities that allow businesses to rapidly respond to and mitigate incidents. Cybersecurity attorney Sotto says many of her clients are taking steps to improve response and mitigation. It will also be necessary to ensure adequate funding for comprehensive, ongoing employee training and awareness programs. The US State of Cybercrime Survey clearly demonstrated the merit of security awareness programs.

Businesses that have security awareness report significantly lower average financial losses from cybersecurity incidents.

And the savings can be significant: We found companies that do not have security training for new hires reported annual financial losses that are four times greater than those that do have training.[45]

Effective security also 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 understanding of leading cybersecurity practices. In the current environment of proliferating threats, risk-based security practices should be a primary component of an organization's overall enterprise risk-management framework.

"We have been approached many times since December to help companies develop together proactive programs to minimize the impact of a cyber attack should it happen," says Lisa Sotto, cybersecurity attorney. "Previously, that kind of proactive preparation was much more sparse."

While a well-designed cyber-risk management program will not totally eliminate risk, it can enable organizations to manage threats through an informed decision-making process, increase efficiencies in security practices, and create a more resilient security practice.

In the coming years, we believe that advances in computer science will help organizations better manage the risks and repercussions of cyber threats. Technology breakthroughs will likely help organizations reduce the complexity of cybersecurity, more quickly detect and remediate incidents, and improve their abilities to monitor and analyze digital activity. Until then, it is imperative that organizations, large and small, commit to understanding and managing the cybersecurity risks that have become top of mind for executive leaders, boards, and consumers across the globe.

Methodology

The Global State of Information Security® Survey 2015 is a worldwide study by PwC, CIO, and CSO

The 2015 survey was conducted online from March 27, 2014 to May 25, 2014; readers of *CIO*, *CSO*, and clients of PwC from around the globe were invited via e-mail to take the survey.

All figures and graphics in this report, unless noted otherwise, are sourced from The Global State of Information Security® Survey 2015 results. The margin of error is less than 1%.

The results discussed in this report are based on the responses of more than 9,700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, and directors of IT and security practices across more than 154 countries.

Asia Pacific
14%

North America
35%

South America
13%

Europe
34%

Africa, Middle East
4%

Endnotes & sources

01
Cyber risks: A severe and present danger

1 PwC, *The FBI says you've been breached by a nation-state. Now what?*, April 24, 2014

2 US Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014

3 BBC, *Wm Morrison supermarket suffers payroll data theft*, March 14, 2014

4 Symantec Corp., *Internet Security Threat Report 2014*, April 2014

5 TechWeek Europe, *Germany Investigating Data Breach Affecting 18 million*, April 7, 2014

6 Symantec Corp., *Turla: Spying tool targets governments and diplomats*, August 7, 2014

7 Cnet.com, *U.S. charges 8 in $45M global cybercrime scheme*, May 9, 2013

8 IOSCO and the World Federation of Exchanges Office, *Cyber-crime, securities markets and systemic risk*, July 2013

9 Department of Homeland Security, *ICS-CERT Monitor, January–April 2014*, May 2014

10 Financial Times, *Energy companies hit by cyber attack from Russia-linked group*, June 30, 2014

11 Ars Technica, *Critical crypto bug exposes Yahoo Mail, other passwords Russian roulette-style*, April 8, 2014

12 TrustedSec, *CHS Hacked via Heartbleed Vulnerability*, August 19, 2014

13 HP Fortify on Demand, *Internet of Things State of the Union Study*, July 2014

14 IOActive, *Adventures in Automotive Networks and Control Units*, August 2013

15 Securities and Exchange Commission, *National Exam Program Risk Alert*, April 15, 2014

16 Vormetric Data Security, *Security measures to go under spotlight as new Data Protection Directive approaches*, July 8, 2014

17 Singapore Personal Data Protection Commission, *Personal Data Protection Act Overview*, accessed August 23, 2014

18 Google Online Security Blog, *Announcing Project Zero*, July 15, 2014

19 The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014

20 The Wall Street Journal, *The Daily Startup: Venture Funding Soars for Cybersecurity Startups*, August 6, 2014

21 Quotes from wsj.com as of August 8, 2014

22 The Financial Times, *Europe's first cyber security-focused fund to launch*, June 18, 2014

23 TechCrunch, *Index Ventures Raises New $550M Early-Stage Fund For Europe, The US And Israel*, June 10, 2014

24 The Financial Times, *Investors flock to cyber security start-ups*, March 12, 2014

02
Incidents and financial impact continue to soar

25 Trustwave Holdings, *2014 Trustwave Global Security Report*, May 2014

26 Center for Strategic and international Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014

27 Create.org and PwC, *Economic Impact of Trade Secret Theft*, February 2014

28 World Bank, *World Development Indicators Database*, July 2014; PwC calculations

29 World Economic Form, *Global Risks 2014, Ninth Edition*, December 2013

30 PwC, *Economic Crime: A threat to business globally*, February 2014

31 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

03
Employees are the most-cited culprits of incidents

32 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

33 Verizon, *2014 Data Breach Investigations Report*, April 2014

34 The Financial Times, *Home Depot attack bigger than Target's*, September 19, 2014

35 Bureau of Justice Statistics, *Victims of Identity Theft*, 2012, December 2013

36 PwC, *Big Data: Big benefits and imperiled privacy*, June 2014

04
As incidents rise, security spending falls

37 PwC, *Economic Crime: A threat to business globally*, February 2014

38 PwC, *Fit for the future: Capitalizing on global trends*, April 2014

39 The Wall Street Journal, *Global Security Spending to Grow 7.9% in 2014, Gartner Says*, August 22, 2014

40 Booz & Co., *Highlights from the 2013 Global Innovation 1000 Study*, October 2013

41 Dell SecureWorks, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents, for over $1,000 Per Dossier*, July 15, 2013

42 RAND Corp., *Markets for Cybercrime Tools and Stolen Data*, 2014

05
Declines in fundamental security practices

43 PwC, *16th Annual Global CEO Survey*, January 2013

07
Evolving from security to cyber risk management

44 PwC, *Why you should adopt the NIST Cybersecurity Framework*, May 2014

45 *2014 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Division of the Software Engineering Institute at Carnegie Mellon University, PwC, and the US Secret Service, March–April 2014

Contacts by region

Australia

Andrew Gordon
Partner
andrew.n.gordon@au.pwc.com

Steve Ingram
Partner
steve.ingram@au.pwc.com

Belgium

Floris Ampe
Partner
floris.ampe@be.pwc.com

Brazil

Edgar D'Andrea
Partner
edgar.dandrea@br.pwc.com

Canada

Salim Hasham
Partner
s.hasham@ca.pwc.com

China

Ramesh Moosa
Partner
ramesh.moosa@cn.pwc.com

Kenneth Wong
Partner
kenneth.ks.wong@hk.pwc.com

Denmark

Christian Kjaer
Director
christian.x.kjaer@dk.pwc.com

Mads Nørgaard Madsen
Principal
mads.norgaard.madsen@dk.pwc.com

France

Philippe Trouchaud
Partner
philippe.trouchaud@fr.pwc.com

Germany

Derk Fischer
Partner
derk.fischer@de.pwc.com

Wilfried Meyer
Partner
wilfried.meyer@de.pwc.com

India

Sivarama Krishnan
Partner
sivarama.krishnan@in.pwc.com

Israel

Yaron Blachman
Partner
yaron.blachman@il.pwc.com

Italy

Fabio Merello
Partner
fabio.merello@it.pwc.com

Japan

Maki Matsuzaki
Partner
maki.matsuzaki@jp.pwc.com

Naoki Yamamoto
Director
naoki.n.yamamoto@jp.pwc.com

Middle East

Taha Khedro
Partner
taha.khedro@ae.pwc.com

Waddah Salah
Partner
waddah.salah@sa.pwc.com

Netherlands

Erwin de Horde
Partner
erwin.de.horde@nl.pwc.com

Gerwin Naber
Partner
gerwin.naber@nl.pwc.com

Otto Vermeulen
Partner
otto.vermeulen@nl.pwc.com

New Zealand

Adrian Van Hest
Partner
adrian.p.van.hest@nz.pwc.com

Norway

Tom Remberg
Director
tom.remberg@no.pwc.com

Poland

Rafal Jaczynski
Director
rafal.jaczynski@pl.pwc.com

Piotr Urban
Partner
piotr.urban@pl.pwc.com

Russia

Christopher Gould
Partner
chirstopher.gould@ru.pwc.com

Singapore

Vincent Loy
Partner
vincent.j.loy@sg.pwc.com

Kok Weng Sam
Partner
kok.weng.sam@sg.pwc.com

South Africa

Pierre Dalton
Partner
pierre.dalton@za.pwc.com

Mark Telfer
Partner
mark.telfer@za.pwc.com

Sidriaan de Villiers
Partner
sidriann.de.villiers@za.pwc.com

South Korea

Sung-Bae Cho
Director
sung-bae.cho@kr.pwc.com

Jae Hyeong Joo
Partner
jae-hyeong.joo@kr.pwc.com

Spain

Elena Maestre
Partner
elena.maestre@es.pwc.com

Javier Urtiaga Baonza
Partner
javier.urtiaga@es.pwc.com

Sweden

Emil Gullers
Partner
emil.gullers@se.pwc.com

Jacob Henricson
Partner
jacob.henricson@se.pwc.com

Switzerland

Thomas Koch
Director
thomas.koch@ch.pwc.com

Jan Schreuder
Partner
jan.schreuder@ch.pwc.com

Turkey

Burak Sadic
Senior Manager
burak.sadic@tr.pwc.com

United Kingdom

Richard Horne
Partner
richard.horne@uk.pwc.com

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

United States

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

Sean Joyce
Principal
sean.joyce@us.pwc.com

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

www.pwc.com/gsiss2015
www.pwc.com/cybersecurity