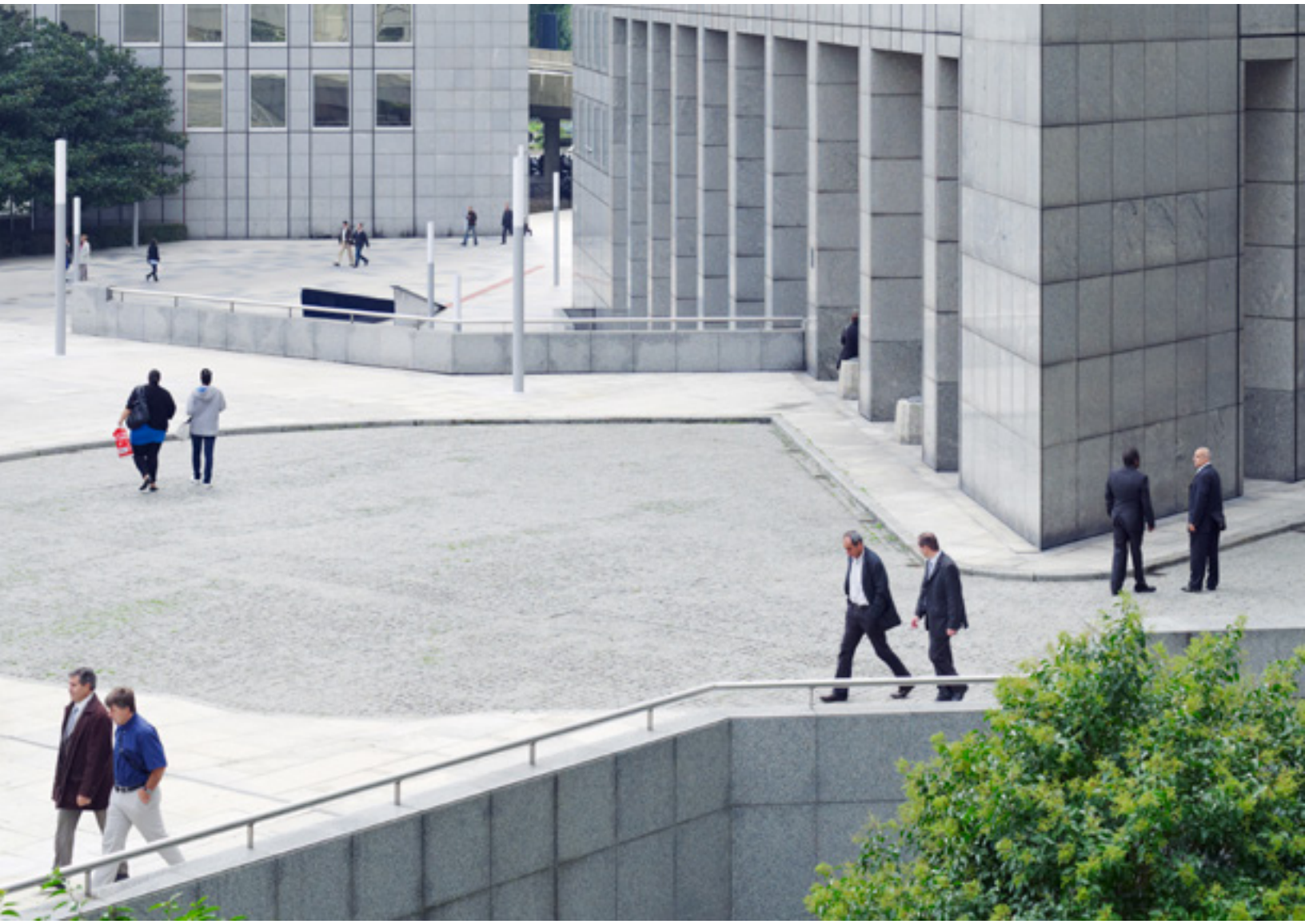
www.pwc.com/gsiss

Turnaround and transformation in cybersecurity

Key findings from The Global State of Information Security® Survey 2016



pwc

Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey 2016

Table of contents

Global responses to rising risks

38%

Increase in detected information security incidents

The numbers have become numbing. Year after year, cyberattacks continue to escalate in frequency, severity and impact. Prevention and detection methods have proved largely ineffective against increasingly adept assaults, and many organizations don't know what to do, or don't have the resources to combat highly skilled and aggressive cybercriminals.

"Many executives are declaring cyber as the risk that will define our generation," said Dennis Chesley, Global Risk Consulting Leader for PwC.

At the same time, technological change continues to disrupt how organizations compete and create value in ways that often alter operating models. Some of today's most significant business trends—the explosion of data analytics, the digitization of business functions and a blending of service offerings across industries, to name a few—have expanded the use of technologies and data, and that is creating more risk than ever before.

In addition, many executives see over-regulation as a prime long-term disruptive trend in their industries. Other government impacts, including nation-state use of state-directed capital to fund and execute cyberattacks, have increasingly serious implications for cybersecurity.

Together, these issues illustrate why cybersecurity risks have become top of mind for leaders in business and government. "Many executives are declaring cyber as the risk that will define our generation," said Dennis Chesley, Global Risk Consulting Leader for PwC. "As a result, businesses are taking an enterprise-wide business-oriented view of this important risk area."

Forward-leaning business leaders also are rethinking their cybersecurity practices and focusing on a nexus of innovative technologies that can reduce these risks and improve business performance. If there is one unifying element among these technologies, it is cloud computing. The cloud is central to today's interconnected digital ecosystem for individuals, businesses and governments. Furthermore, it is the platform that is enabling organizations of all sizes to leverage and link cloud-based cybersecurity tools, Big Data analytics and advanced authentication. The cloud also is the conduit that underpins new technology platforms like the Internet of Things (IoT) and mobile payment systems.

Simply put, cloud computing has had a towering impact on technology innovation in the past decade—and is likely to continue to do so. Research firm IDC predicts that spending on public cloud computing will soar to nearly $70 billion this year, and that the number of new cloud-based solutions will triple over the next four to five years.[1]

Technology alone won't turn around the state of cybersecurity, however. Smart organizations have always known that the human side of the security equation is equally essential. That's why many are moving toward a more collaborative approach to cybersecurity, one in which intelligence on threats and response techniques are shared with external partners in the public and private sectors.

Internally, businesses are expanding the roles of key executives and Boards of Directors to allow for enhanced communication of cyberthreat information and help build better-prepared, more resilient cybersecurity capabilities. They also are implementing awareness programs to help educate employees and executives about cybersecurity fundamentals and human vulnerabilities like spear phishing, which remains a very successful attack technique.

Another notable measure of progress is a willingness to invest in cybersecurity. This year, respondents to The Global State of Information Security® Survey 2016 reported they have boosted information security spending significantly, and many are gearing up to tackle the cybersecurity juggernaut head on. (For details on incidents, impacts and costs, see Appendix A). In this report, we'll show you how innovative businesses are going about this challenge, and how these efforts connect and intersect in ways that enable them to implement an integrated approach to protecting assets, reputation and competitive advantages.

1 IDC, *Public Cloud Computing to Reach Nearly $70 billion in 2015 Worldwide, According to IDC*, July 21, 2015

Reclaiming cybersecurity through innovation

Have adopted a risk-based cybersecurity framework

The rewards of risk-based frameworks

An effective cybersecurity program starts with a strategy and a foundation based on risks. So it was encouraging to find that the vast majority of organizations have adopted a security framework, or more often an amalgam of frameworks—often with very productive results.

The two most frequently implemented guidelines are ISO 27001 and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework. These guidelines enable organizations to identify and prioritize risks, gauge the maturity of their cybersecurity practices and better communicate internally and externally.

Risk-based frameworks also can help businesses design, measure and monitor goals toward an improved cybersecurity program that centers around the safety and security of client and organizational information. The Canadian Imperial Bank of Commerce (CIBC), for instance, has developed a scorecard based on framework controls that it uses to measure the maturity of its security program, according to Joe LoBianco, vice president of information security for the Toronto-based bank. "If we didn't have that framework providing the structure, progress would be difficult to measure year over year," he said.

Benefits of security frameworks

Harnessing the power of cloud-enabled cybersecurity

Cloud computing has emerged as a sophisticated tool for cybersecurity safeguards in recent years as cloud providers steadily invested in advanced technologies for data protection, privacy, network security and identity and access management. Many also have added capabilities that enable them to improve intelligence gathering and threat modeling, better block attacks, enhance collective learning and accelerate incident response.

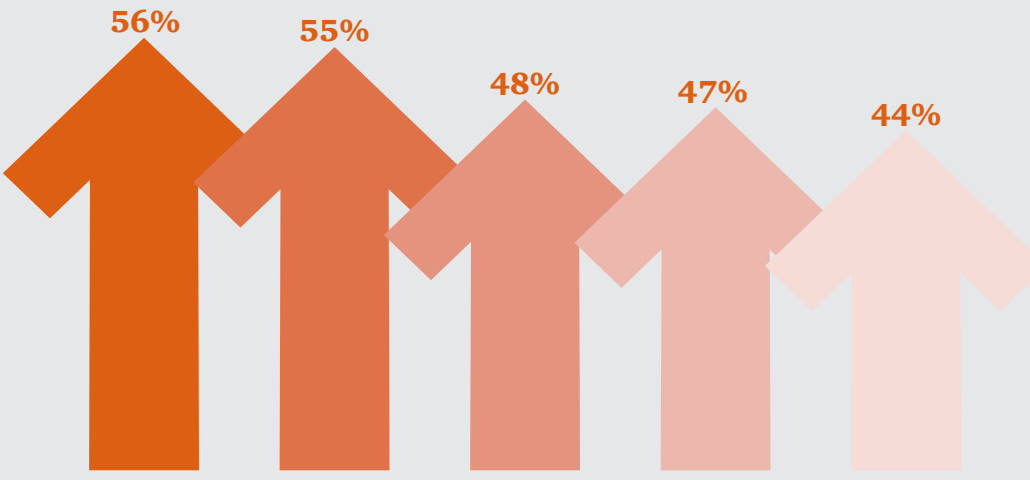
It's no wonder, then, that most survey respondents said they use cloud-based security services to help protect sensitive data and strengthen privacy. And they entrust a broadening range of critical services to the cloud, including real-time monitoring and analytics, advanced authentication and identity and access management.

For instance, Global Payments, a worldwide provider of payment technology services based in Atlanta, leverages private cloud managed services to handle threat monitoring and incident response. "We use a cloud-based solution that aggregates all of our alerts and threat information, and the solution then filters out events or alerts that are either considered not a security threat or are a false positive," said Guido Sacchi, the company's executive vice president and CIO. "It then communicates events that our Security Operations Center [SOC] needs to investigate." The cloud is ideal for this type of task because cloud providers have massive processing horsepower necessary to quickly sift through a huge volume of threat and event data, he said. In addition, cloud providers are likely to have internal expertise in building algorithms for analytics, which is a difficult skill set for most corporations to develop and grow.

Another example of adoption of cloud-based cybersecurity comes from Steelcase, the Grand Rapids, MI-based office furniture company. Steelcase employs a range of cloud-based managed services that include advanced authentication, penetration and vulnerability testing, security alert analysis and network behavior analysis, according to Stuart Berman, IT security architect

Use cloud-based cybersecurity services

Adoption of cloud-based cybersecurity services



and innovation fellow. These cloud services have helped the company build a security program that is capable as well as cost-effective. "The use of cloud-based managed security services, which require very deep and specific technical expertise, allows our full-time security employees to focus on identifying and managing security problems, rather than building and maintaining deep technical knowledge. That enables us to better manage costs based on risks," Berman said.

The big impact of Big Data

A growing number of organizations are leveraging Big Data analytics to model and monitor for cybersecurity threats, respond to incidents, and audit and review data to understand how it is used, by whom and when.

"Data analytics is an area that we're investing in right now," said LoBianco of CIBC. "I think it's going to be a significant growth area for us in the security space, one that will change how we do our work the most."

A data-driven approach can shift security away from perimeter-based defenses and enable organizations to put real-time information to use in ways that can help predict security incidents. Data-driven cybersecurity enables companies to better understand anomalous network activity and more quickly identify and respond to security incidents. It also can be effective in reducing or quickly detecting employee security incidents by monitoring their behavior for suspicious activity.

But Big Data analytics typically requires an enormous commitment to computing resources and software expertise. Companies like Global Payments address these challenges by using a cloud-based solution to analyze the aggregated system log data because the cloud can better handle the heavy computing demands of such analysis.

Data analytics also can be combined with existing security information and event management (SIEM) technologies to generate a more customizable and extensive view of network activity. CIBC is testing a new analytics-based threat detection and monitoring system to augment traditional rule-based SIEM, according to LoBianco. "This will essentially take data that we

The synergies of cloud and DevOps

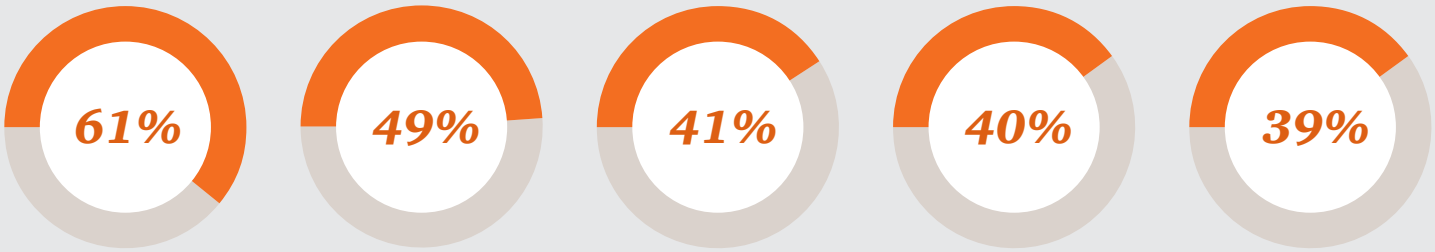
Web-based companies are enhancing and automating their cybersecurity programs through the adoption of DevOps, a software development model that promotes close collaboration between application developers and IT operations. This agile approach is particularly beneficial for companies that have thousands of active applications, as well as those that deploy code updates very frequently. Streaming media provider Netflix, for example, employs DevOps to automate tasks like identifying changes in configurations across dozens of cloud services accounts.[2]

When aligned with cloud-enabled services, DevOps can deliver powerful enhancements to cybersecurity programs. Here's what the fusion of DevOps and cloud-based cybersecurity could look like: When an intruder modifies application code, automated analytics and monitoring software identifies the breach, terminates connections and alerts developers. Cybersecurity engineers then pinpoint changes made by adversaries and repair the code. The system can then reroute all user traffic to the updated version and automatically issue a patch for all other vulnerable applications across the enterprise.

Leverage Big Data analytics for security

2 Netflix, *Announcing Security Monkey-AWS Security Configuration and Monitoring*, June 30, 2014

Benefits of data-driven cybersecurity



collect for SIEM, as well as some additional data, and provide a more open-ended and exploratory capability that will support our Security Operations Center in threat detection and monitoring," he said.

Other organizations are exploring the use of data analytics for identity and access management to monitor employee usage patterns and flag outliers. In this scenario, the data analysis solution looks for patterns around the employee access entitlements and then identifies unwanted access.

This kind of wide-open view can help companies improve systems in unexpected ways. Steelcase, for instance, deployed analytics to monitor for advanced persistent threats and insider risks, but it also found that Big Data helped identify unknown network performance issues. "Data analytics can help you find the needle in the haystack, and the needle in the haystack is not only the security needle, sometimes it's a performance needle," Berman said. "That's what Big Data analysis is really good at: Finding patterns you didn't know existed and not necessarily answering questions you have but answering questions you didn't have."

"Data analytics is an area that we're investing in right now," said Joe LoBianco of CIBC. "I think it's going to be a significant growth area for us in the security space, one that will change how we do our work the most."

91%

Use advanced authentication

Replacing passwords with advanced authentication

In an era in which passwords are generally considered inadequate, at best, it's easy to understand why many organizations are turning to advanced authentication to help manage access and improve trust among customers and business partners.

As noted above, many organizations are embracing advanced authentication as a cloud service. The reason is pretty apparent, considering that many high-profile hacks begin with compromised credentials. "If you're counting on passwords for security, you've got a problem," said Berman of Steelcase, which uses a combination of one-time passwords and hardware tokens with cloud-based authentication platforms.

Banks, in particular, are moving away from traditional passwords for both clients and employees. LoBianco of CIBC says one-time passwords sent to a client's mobile phone have proved popular with users and have enabled the bank to enhance its data security while trimming support desk costs. CIBC is also using two-factor authentication for employees with privileged access to networks and data. Many employees already have strong-authentication tokens for remote access, and the bank is leveraging the same token for privileged access wherever possible, he said.

Other businesses are developing and implementing more advanced on-premises authentication technologies such as biometrics. USAA, the San Antonio, TX-based financial services and insurance firm that caters to military veterans and service members, has implemented facial and voice recognition and fingerprint scanning for customer access to mobile apps.[3] Biometrics has enabled USAA to enhance security and customer service, reduce help desk calls and improve ease of use for customers.

Another approach is hardware-based authentication. Tech giant Google has developed a USB device called Security Key that provides highly secure two-factor authentication for its Google for Work applications.[4] Using the FIDO Alliance's Universal 2nd Factor (U2F) standard, the Security Key transmits an encrypted signature rather than a verification code to help ensure that credentials cannot be phished. To authenticate, users simply tap the Security Key, a method that is faster than requesting and entering an authentication code.

Benefits of advanced authentication

3 SecureID News, *Biometrics secure next generation of mobile banking apps,* July 7, 2015
4 Google, *The key for working smarter, faster, and more securely,* April 21, 2015

Starwood Hotels & Resorts has created an entirely different type of access key. The hospitality company's SPG Keyless service allows preregistered hotel guests to bypass the check-in desk and tap their smartphone or Apple Watch to unlock hotel room doors.[5] The app, available to members of Starwood's Preferred Guest (SPG) frequent traveler program, also provides guests with directions to the property from the airport, as well as information about individual hotel and frequent traveler account balances.

Use of these types of password-less authentication and apps will require that organizations rethink their approach to identity management and focus solutions on building identity trust relationships with users, said Suzanne Hall, Managing Director, PwC. "Businesses should design authentication solutions that marry the level of authentication to the risk of the access or transaction. Trust relationships between an enterprise and an individual recognize the balance between the information needed to validate and the need to protect."

Another critical factor is ease of use. "Consumers will adopt solutions that ease the burden of remembering passwords or carrying tokens. Authentication must be frictionless and easy to use," Hall said.

Gearing up for the Internet of Things

By now, the Internet of Things (IoT) needs no introduction. This ecosystem of Internet-connected devices, operational tools and facilities is poised to soar in the coming years. Research firm IDC predicts that the number of devices connected to the Internet will reach 30 billion in 2020, up from an estimated 13 billion this year.[6]

Most organizations understand that the Internet of Things will bring enormous advantages but also increase risks to data security and privacy. In fact, the number of survey respondents who reported exploits to IoT components such as embedded devices, operational systems and consumer technologies more than doubled in 2015.

The number of respondents who reported exploits of operational, embedded and consumer systems increased 152% over the year before.

5 Starwood Hotels & Resorts, *Starwood Hotels & Resorts Celebrates UK Launch of Keyless Check-In Through the SPG App for Apple Watch*, April 24, 2015
6 IDC, *Connecting the IoT: The Road to Success,* June 2015

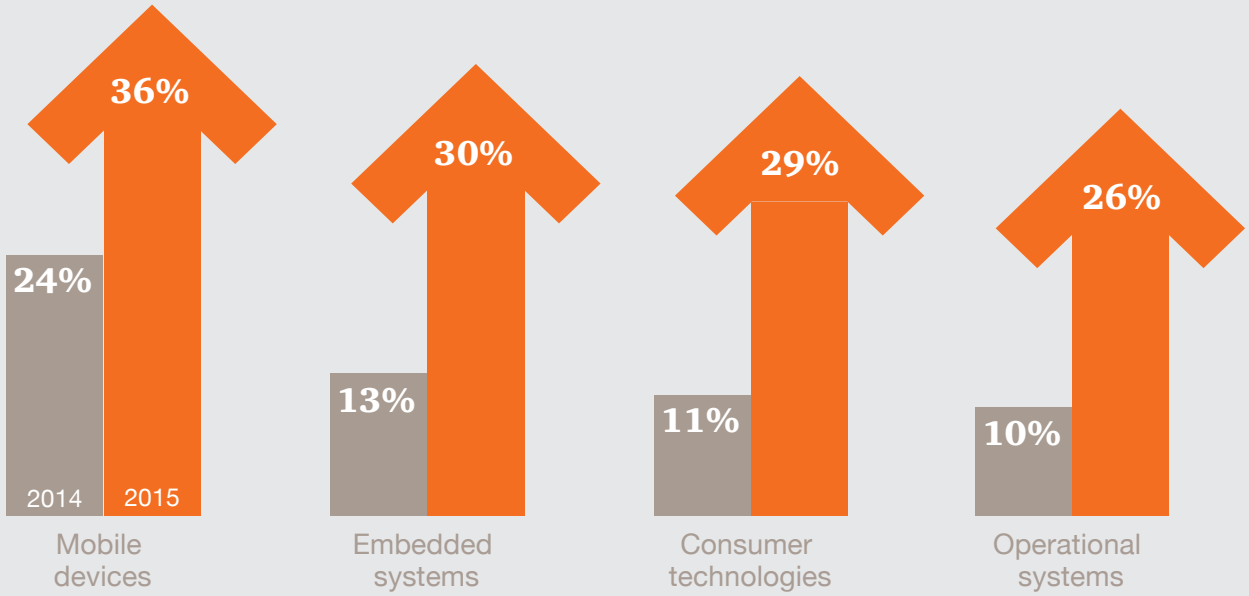
In the coming years, new vectors of access to IT and operational systems will be exposed as more businesses deploy connected sensor-based devices and machine-to-machine technologies. This type of equipment typically lacks the fundamental security safeguards of traditional enterprise IT, potentially enabling threat actors to penetrate an organization's systems and exploit data, disrupt operations and compromise the integrity of products and services.

Forward-thinking companies are beginning to understand the need for a common privacy and cybersecurity standard that can protect the business and its customers, and help earn user trust. Doing so will require that IoT stakeholders create and adhere to a privacy framework that addresses issues such as tested security controls, a common data format, policies for collection and use of customer data and appropriate disclosure controls.

Some organizations are beginning to build consensus on cybersecurity and privacy standards by collaborating with other players in the IoT ecosystem. Steelcase, for instance, has joined an Internet of Things accelerator called Seamless and partners with local start-ups and universities to help it understand the multiple moving parts and privacy requirements of converged technologies. This collaboration informs the company's initiative to develop an industrial IoT manufacturing platform as well as an "office" version that comprises smart facilities and connected spaces for customers. For both platforms, Steelcase is "designing in" strong security and privacy principles and controls, according to Berman.

But as the Internet of Things expands from plants and corporate facilities to civic environments, potential privacy issues will very likely proliferate. Consider "smart city" projects like the partnership between GE Lighting and US municipalities.

Attacks on IoT devices & systems



The initiative retrofits urban street lamps with LEDs that contain sensors and wireless transmitters that are linked to a central data collection and analysis platform.[7] Switching on this type of smart-city project can help municipal governments optimize traffic flow, trim energy costs and create safer pedestrian environments, among other benefits. It can even steer drivers toward available parking spaces.

But privacy advocates have raised concerns about surveillance and responsible use of data. Some worry that cities could employ video capabilities of connected streetlights for real-time monitoring of pedestrians and motorists, putting citizens in the spotlight of government surveillance and data collection—with no ability to opt out. Municipalities and businesses, therefore, should design systems that preserve the right to privacy from the very beginning.

This scenario illustrates the likelihood that the Internet of Things will introduce a welter of privacy issues that are as yet unimagined. "We are seeing the tension between the value these systems can bring and the privacy concerns that organizations and individuals have," said Berman of Steelcase. "The real barrier is between those expectations, what privacy, legal concerns, and technology used to mean, and what they may come to mean."

"The real barrier is between those expectations, what privacy, legal concerns, and technology used to mean, and what they may come to mean," said Stuart Berman of Steelcase.

7 GE Lighting, *GE Unveils LED-enabled Intelligent Environments, a Glimpse into The Connected Future,* May 5, 2015

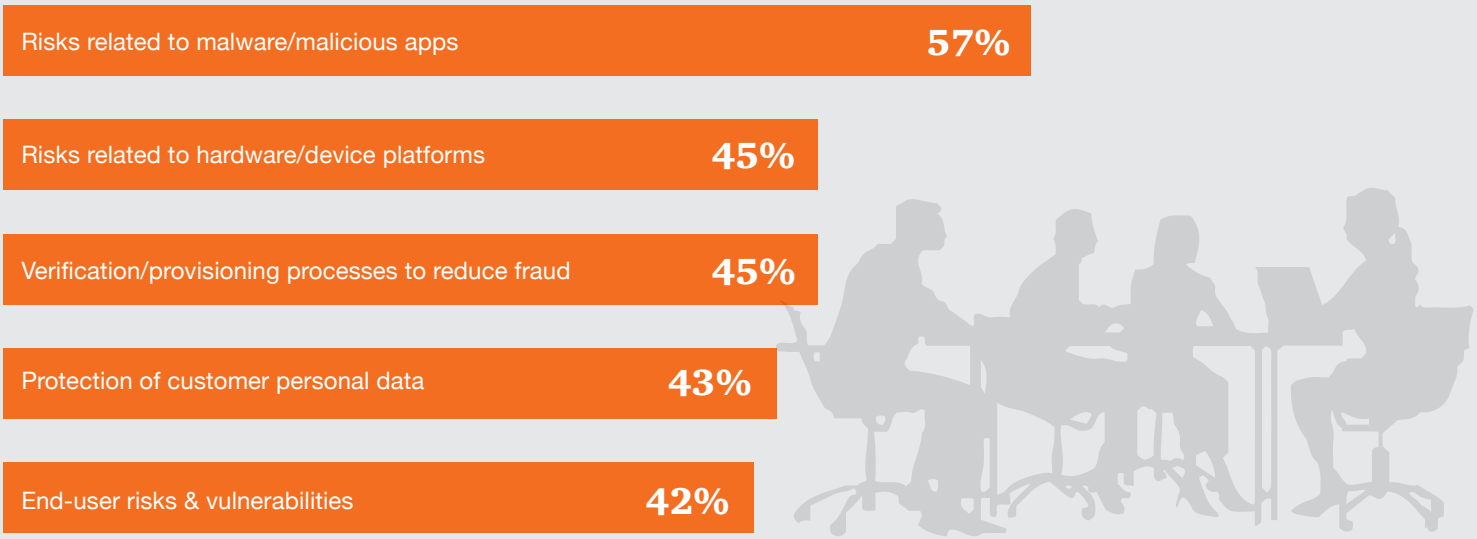
Going mobile with payments

This year, 57% of survey respondents said they have adopted mobile payment systems. While mobile payments is already mainstream, the ecosystem continues to rapidly evolve as new partnerships are formed among a constellation of technology, financial, retail and telecommunications firms. This shifting environment will likely bring unanticipated cybersecurity threats and broaden the cyberattack vector.

Risks can result from new technologies as well as processes, as demonstrated during the high-profile rollout of the Apple Pay service in the US. "Some of the initial challenges [of Apple Pay] weren't necessarily issues with the physical or logical security of the phone or the credentials, but rather the process around enrollment," said LoBianco of CIBC. "When you have these new payment models, you have to look at the end-to-end lifecycle of enrolling a user, transactions that flow through the system and de-enrolling users. When there are new processes, the bad guys will try to exploit human weaknesses just as much as technological weaknesses."

Mobile payment technologies that transmit a token to merchant systems are considered fundamentally secure because no credit card information is stored on the device or transmitted to retailer point-of-sale systems. But some believe smartphone-based payments are only an incremental step toward the future of transactions. Truly innovative mobile payments completely remove the payment process from the user experience, according to Sacchi of Global Payments, who cites the seamless process used by ride-hailing service Uber as a game-changer. The merchant uses a payment card on file, and customers' cards are automatically billed. "Uber has essentially made the payment step disappear from the entire user experience: You take your ride, you leave the car and you're done," said Sacchi. "If there is one thing that is a takeaway from all this, it's that you need to look at both security and user experience. The winners in the marketplace are going to be those that strike the best balance between the two."

Issues organizations are addressing to improve mobile payments security



Partnering up to sharpen cybersecurity intelligence

As more businesses share more data with an expanding roster of partners and customers, it makes sense that they also would swap intelligence on cybersecurity threats and responses. Indeed, over the past three years the number of organizations that embrace external collaboration has steadily increased.

And they cite clear benefits. Most organizations say external collaboration allows them to share and receive more actionable information from industry peers, as well as Information Sharing and Analysis Centers (ISACs). Many also report that information sharing has improved their threat awareness and intelligence.

Organizations that do not collaborate often cite the lack of an information-sharing framework and standards, as well as incompatible data formats and platforms among public and private entities. Another weakness in today's information-sharing ecosystem: Cybersecurity updates are not communicated at network speed.

What's more, policies and regulations on data privacy vary widely across the globe, and some organizations worry that sharing certain types of data could violate the privacy of customers, employees and other individuals. And, of course, validation of intelligence is a concern for all.

Despite the barriers, information sharing got a shot in the arm earlier this year when US President Barack Obama signed an executive order that encourages collaboration among public and private organizations. The president proposed creation of new Information Sharing and Analysis Organizations (ISAOs) designed to be more flexible than industry-specific ISACs, with the goal of enabling businesses and public-sector agencies to share information specific to individual industries as well as intelligence related to geographies, issues, events or specific threats.

These organizations are likely to help build out collaboration and information sharing capabilities for many businesses. "I believe ISAOs will fill certain gaps that current groups do not address and ultimately play a valuable role in contributing to a national cybersecurity immune system," said David Burg, Global and US Cybersecurity Leader for PwC. "That's why PwC is currently working with stakeholders from the White House, industry and academia to help resolve issues, encourage discussion and ultimately maximize the effectiveness of ISAOs."

The question is, how will organizations benefit from new ISAOs? Some businesses believe they can learn quite a bit from others across industries. For example, cybersecurity challenges often do not differ by sector but rather by an entity's size or constituency—a big bank might have much more in common with a large pharmaceutical company than it does with a regional bank.

Some organizations are taking a wait-and-see approach on cross-industry collaboration, however. In the banking and finance sector, for instance, some firms believe that the Financial Services ISAC meets the needs of participants and that involvement in multiple information-sharing groups might be superfluous—and unproductive. Attitudes will likely vary across industries, however, and because ISAOs are a new concept, most organizations do not yet know if they will participate. Nor can they predict the value of collaboration in these groups.

"I believe ISAOs will fill certain gaps that current groups do not address and ultimately play a valuable role in contributing to a national cybersecurity immune system," said David Burg, Global and US Cybersecurity Leader for PwC.

The US is not the only nation to emphasize the power of partnering, of course. The European Parliament has approved a Network and Information Security Directive that aims to improve cooperation and information sharing on cybersecurity initiatives among member states as well as between the public and private sectors.[9] The Directive requires that organizations in certain critical infrastructure sectors adopt risk-management practices and report major incidents to national authorities. It also calls for the European Network and Information Security Agency (ENISA) to work with standardization bodies and relevant stakeholders to develop specifications for incident reporting.

What can't be protected can be insured

Information sharing and advanced cybersecurity technologies will not stop all cyberattacks—by now it seems clear that technically adept adversaries will always find new ways to circumvent cybersecurity safeguards. That's why many businesses are purchasing cybersecurity insurance to help mitigate the financial impact of cybercrimes when they do occur.

Cybersecurity insurance is, in fact, one of the fastest-growing sectors in the insurance market: A recent PwC report forecasts that the global cyberinsurance market will reach $7.5 billion in annual sales by 2020, up from $2.5 billion this year.[10]

Today, first-party insurance products cover data destruction, denial of service attacks, theft and extortion; they also may include incident response and remediation, investigation and cybersecurity audit expenses. Other key areas of coverage include privacy notifications, crisis management, forensic investigations, data restoration and business interruption. The insurance industry is attempting to expand into policies that cover the value of lost intellectual property, reputation and brand image, as well as cyber-related infrastructure failures.

Benefits of external collaboration

9 European Commission, *Network and Information Security (NIS) Directive,* March 16, 2015
10 PwC, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience,* September 2015

In addition to mitigation of financial risks associated with cybercrime, companies that purchase insurance stand to gain a better understanding of their cyber-readiness. That's because insurers require a thorough assessment of current capabilities and risks as a precondition to purchasing a policy. These evaluations can help businesses better predict legal and regulatory exposures, costs of response, and potential brand damage related to cybersecurity risks.

For some, today's cybersecurity policies do not deliver the right mix of value and risk management. CIBC has been evaluating cybersecurity insurance for several years, and has been monitoring the policy landscape as it matures. "Our security and our corporate insurance teams analyze and review risks that our bank faces on an annual basis and views these in the context of available policies and associated costs. Based on this analysis, we have not selected cyberinsurance, primarily for its lack of readiness," said LoBianco. "The biggest concerns we have around cyberbreaches have to do with the safety and security of our clients' information and ensuring their utmost trust in our bank, and that's much more difficult to insure."

Another vexing issue for many organizations is determining how much cybersecurity insurance to purchase. There is no one-size-fits-all policy recommendation, however. "Generally, businesses should understand that they won't be able to insure the full risk of loss because the market just doesn't have the supply yet," according to PwC Principal Joseph Nocera. "Looking at some of the big breaches that have occurred in the past year or so, many large firms are trying to get $80 to $100 million policies, while smaller companies are settling on $10 million policies. There's no one answer, however, because there are an array of individual variables, such as company size, industry sector, types of data the organization stores, the maturity of security controls and individual risk tolerance. It's also important to remember that no insurance products will protect a firm's reputation or brand."

Have purchased cybersecurity insurance

"Generally, businesses should understand that they won't be able to insure the full risk of loss because the market just doesn't have the supply yet," said Joseph Nocera, PwC Principal.

Incident-related losses covered by cybersecurity insurance

"The biggest concerns we have around cyberbreaches have to do with the safety and security of our clients' information and ensuring their utmost trust in our bank, and that's much more difficult to insure," said Joe LoBianco of CIBC.

The evolving involvement of executives and the Board

54%

Have a CISO in charge of the security program

Leaps in technologies hold tremendous promise for contending with seemingly intractable cyberthreats. Yet the spotlight on technical advances can dim the focus on the roles, competencies and training of people—an often neglected yet very effective defense. That's starting to change.

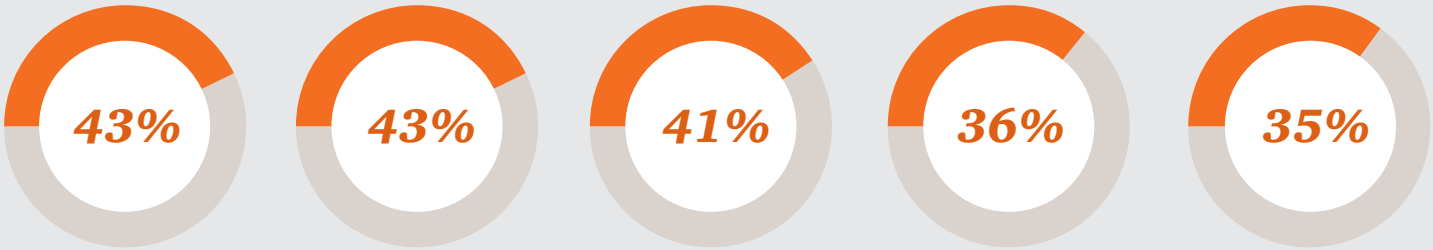
"Companies tend to have a more technology-centered view," said Claude Yoder, global head of analytics for insurance provider Marsh. "But I think as more and more information on cyber comes out, companies are expanding their technology-centered view to include people and processes."

When it comes to cybersecurity, there is no more pivotal player than the top information security officer, typically the Chief Information Security Officer (CISO) or Chief Security Officer (CSO). It is a role whose responsibilities and competencies have become increasingly visible and critical.

Today's CISO or CSO should be a senior business manager who has expertise not only in cybersecurity but also risk management, corporate governance and overall business objectives. He or she should have access to key executives to provide insight into business risks and should be able to competently articulate risk-based cybersecurity issues to the C-suite and Board. Put simply, the cybersecurity leader should have the ability to effect change on par with C-level executives.

"Today's security leader is a general manager with expertise in communications, presentation and business—in short, all the skills you would expect of a COO," said James Shira, Global CISO for PwC. "The CISO or CSO is responsible and accountable for risks, and is expected to deliver a minimum information security posture across the organization. Doing so demands a new level of management skills."

Skills & competencies of security leaders



This level of responsibility is more likely to be achieved when the top security leader reports to a corporate officer who has broad oversight of both risk and strategy, preferably the CEO or other C-suite executives. Among survey respondents, the most frequently cited reporting structure is the CEO, CIO, Board and CTO, in that order. In larger organizations, the information security function is more often organized under the CIO.

While there are some exceptions, we believe that CISOs and CSOs should be independent of CIOs to better allow for internal checks and balances, as well as the ability to escalate security issues to corporate leadership and the Board. Another concern is the cybersecurity budget: A CISO or CSO may be empowered with all the necessary skills and authority, but will be unable to do the job without adequate funding.

"Companies tend to have a more technology-centered view," said Claude Yoder of Marsh. "But I think as more and more information on cyber comes out, companies are expanding their technology-centered view to include people and processes."

Boards are more involved in cybersecurity

Today's cybersecurity incidents often leave behind a broad swath of operational, reputational and financial damages. Consequently, many Boards of Directors have begun to address cybersecurity as a serious risk-oversight issue that has strategic, cross-functional, legal and financial implications.

Guidelines from the National Association for Corporate Directors (NACD) advise that Boards should view cyber-risks from an enterprise-wide standpoint and understand the potential legal impacts.[11] They should discuss cybersecurity risks and preparedness with management, and consider cyberthreats in the context of the organization's overall tolerance for risk.

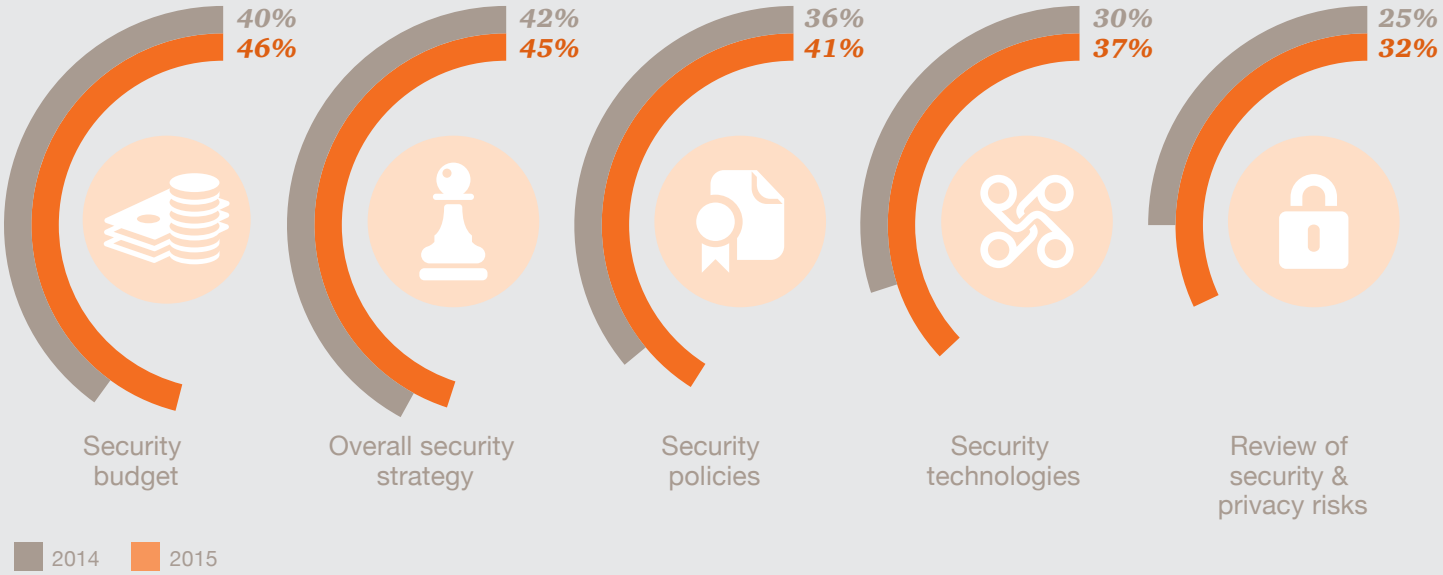
Boards appear to be listening to this guidance. This year we saw a double-digit uptick in Board participation in most aspects of information security. Respondents said this deepening Board involvement has helped improve cybersecurity practices in numerous ways. It may be no coincidence that, as more Boards participate in cybersecurity budget discussions, we saw a 24% boost in security spending. Other notable outcomes cited by survey respondents include identification of key risks, fostering an organizational culture of security and better alignment of cybersecurity with overall risk management and business goals.

45%

Boards participate in the overall security strategy.

11 NACD, *Cyber-Risk Oversight: Directors Handbook Series,* June 2014

Board participation in information security



Perhaps more than anything, however, Board participation has opened the lines of communication between the cybersecurity function and top executives and directors. "It's commonly understood that cybersecurity is an enterprise-wide priority requiring the active engagement of all internal stakeholders, from the business to risk and compliance, right up to the Board of Directors. We regularly provide updates to our Chief Risk Officer on any material developments around cybersecurity," said LoBianco of CIBC.

Today's Boards want more than a fear-factor report, however. "I absolutely will not go down the FUD road," said Berman of Steelcase, referring to the acronym for fear, uncertainty and doubt. "To me, it's about teaching the Board that security is not some hairy monster out there hiding in the dark. Instead, it's a risk that can be managed as an economic decision."

"To me, it's about teaching the Board that security is not some hairy monster out there hiding in the dark. Instead, it's a risk that can be managed as an economic decision," said Stuart Berman of Steelcase.

Due diligence of cybersecurity in M&As

As organizations continue to grow through mergers and acquisitions (M&As), the cybersecurity practices and potential liabilities of a target company have become serious risks.

Businesses that do not adequately assess the cybersecurity practices and capabilities of target companies may put themselves in jeopardy of attack. How so? Sophisticated cyberadversaries may infiltrate smaller companies with less secure cybersecurity capabilities and wait for them to be acquired by larger firms. When the companies' information systems are integrated, threat actors may attempt to gain a foothold on the networks of the acquiring firms to carry out attacks.

That's why due diligence of the target's cybersecurity capabilities and risks is becoming as essential as a careful audit of its financials. Yet many organizations do not thoroughly investigate how a target company protects its digital assets. In fact, a Freshfields survey of 214 global dealmakers found that 78% of respondents believe cybersecurity is not analyzed in great depth or specifically quantified as part of the M&A process.[12]

In assessing cybersecurity risks, three areas should be considered: The nations in which the target company is headquartered and operates, the organization's industry sector, and its individual cybersecurity practices and incident history. Operations in certain countries carry inherently more risk than others, and they also may be subject to more stringent cybersecurity and privacy regulations. The types of risks vary by industry as well.

By individual company, some of key areas of vulnerability include the target's data inventory and locations (including data for third-party suppliers), data collection processes, cybersecurity policies and controls, privacy policies and cybersecurity insurance coverage. It's also important to consider whether a target has incident-response and crisis-management plans in place, as well as whether it has detected breaches and how it responded to those incidents.

The challenge for many organizations is that they often have a very brief time frame to assess the cybersecurity performance of target companies. A well-planned strategy for due diligence will help provide an orderly and timely process to assess potential acquisitions.

Cybersecurity risks of target companies should be considered across three areas:

12 Freshfields Bruckhaus Deringer, *Cyber Security in M&A,* July 2014

Fit for the future of cybersecurity

The adoption of innovative cybersecurity safeguards explored in this paper will help organizations better defend against today's known vulnerabilities and threats. But as technologies evolve and adversaries sharpen their skills, how can businesses anticipate the risks of tomorrow?

That's not an easy question to answer. Prognostication is an imprecise discipline that yields an approximate view, at best. And it's exceedingly difficult to predict the future of a situation whose present state is uncertain and continually shifting. Nonetheless, we believe there are some assumptions that organizations should consider in preparing for cybersecurity over the next five years.

First, any discussion of the future should be predicated on the premise that personal lives will be increasingly digitized, creating an even greater avalanche of data that can be collected, analyzed and potentially compromised. Businesses, too, will continue to generate and share more information about people and processes, and the Internet of Things will unleash a torrent of machine-to-machine information. Amid this escalation of data, individual and corporate identity and privacy will begin to converge.

It's safe to assume that future threat actors will likely wield an attack kit of even more technically sophisticated tools and tactics. For governments and businesses, espionage and political hacking will merge as attack techniques become more nuanced and aggressive. At the same time, increasingly brazen attacks by nation-states and politically motivated hacktivists will likely result in economic sanctions or possibly even cyberwarfare. In fact, it's not entirely unlikely that a catastrophic cybersecurity incident will precipitate demand—and support—for government-controlled identity management.

Authentication and identity management are the juggernauts that pose the greatest perils to cybersecurity—and promise the greatest payoffs. Mustering the right defenses will require new solutions based on Bigger Data, cloud computing and heuristic modeling.

Forward-thinking companies are already shifting away from traditional perimeter defenses in favor of cloud-enabled cybersecurity that is based on real-time analysis of data and user-behavior patterns. As the Internet of Things continues to expand, analysis of machine-to-machine data and activity will become increasingly critical. In this type of data-centric environment, the importance of strong encryption cannot be underestimated.

It's unlikely that today's entrenched solutions vendors will be on the cutting edge of cybersecurity five years from now. Rather, innovative solutions will come from nimble small to medium-size tech companies and start-ups. Organizations will choose from a wide assortment of services and solutions provided by a panoply of vendors. As a result, businesses will require services that harmonize security and IT solutions across a very heterogeneous technology stack. Vendor lock-in will go the way of perimeter-based security, but the new collage of choices may overwhelm organizations.

In fact, enterprise IT as we know it will likely begin to fall away as personal and business identities merge. Lines of businesses will likely build and run their own apps on the cloud, with little to no involvement of IT.

Finally, governments are working to improve their ability to trace and directly attribute intrusions to responsible threat actors. Empty indictments of individual cybercriminals or governments hasn't worked in the past and will be similarly ineffective in the future. Enforceable international treaties will be a necessity.

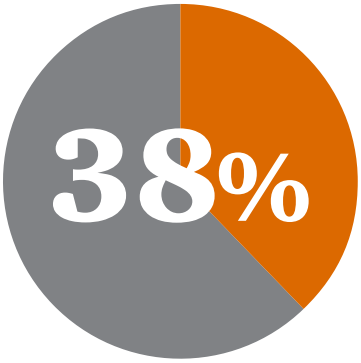
Snapping back to the present, we acknowledge that the future may or may not unfold as we have predicted. Five years is a very long time in the quicksilver evolution of cybersecurity, after all.

So while the utility of foresight ultimately may be questionable, forethought will be essential. Thinking ahead can help organizations stimulate discussion, explore possible scenarios and develop a strategy for cyber-resilience. Doing so will help businesses build a forward-looking cybersecurity program that is based on the right balance of technologies, processes and people skills—all supplemented with an ample measure of innovation. With these components in place, organizations will likely be better prepared for the future of cybersecurity, whatever it might bring.

Appendix A: Responding to rising cyber-risks

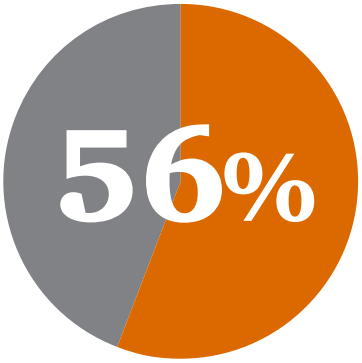
Insights from The Global State of Information Security® Survey 2016

Average number of security incidents



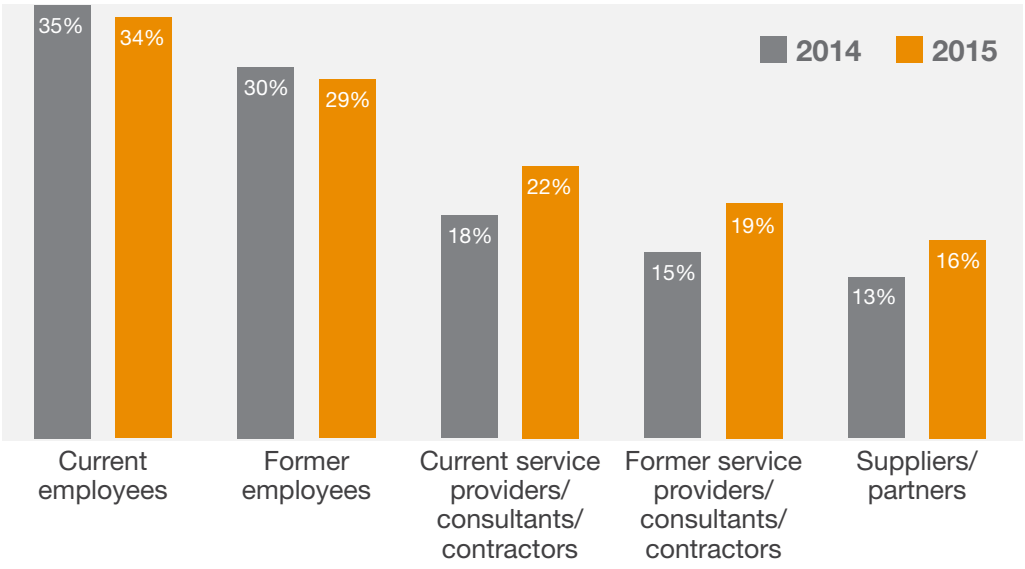
In 2015, **38%** more security incidents were detected than in 2014.

Impacts of security incidents



Theft of "hard" intellectual property increased **56%** in 2015.

Sources of security incidents



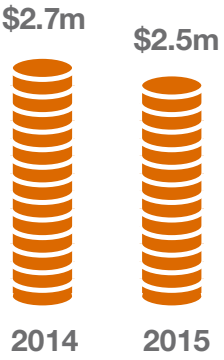
22%

While employees remain the most cited source of compromise, incidents attributed to business partners climbed **22%**.

Average information security budgets

Respondents boosted their information security budgets by 24% in 2015.

Average financial losses due to security incidents



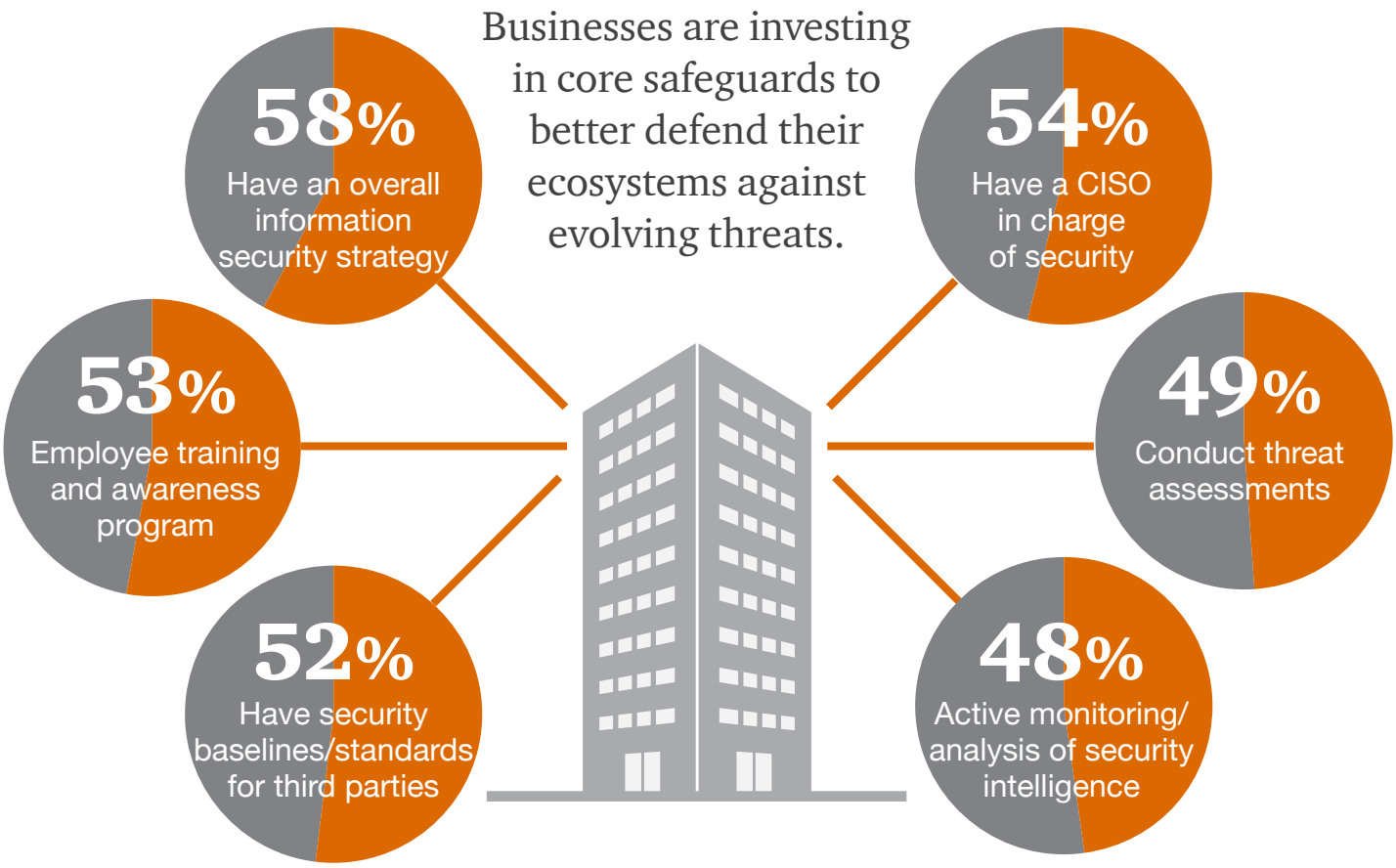
-5%

Financial losses decreased 5% from 2014 to 2015.

Adoption of strategic security initiatives

Many organizations are incorporating strategic initiatives to improve security and reduce risks.

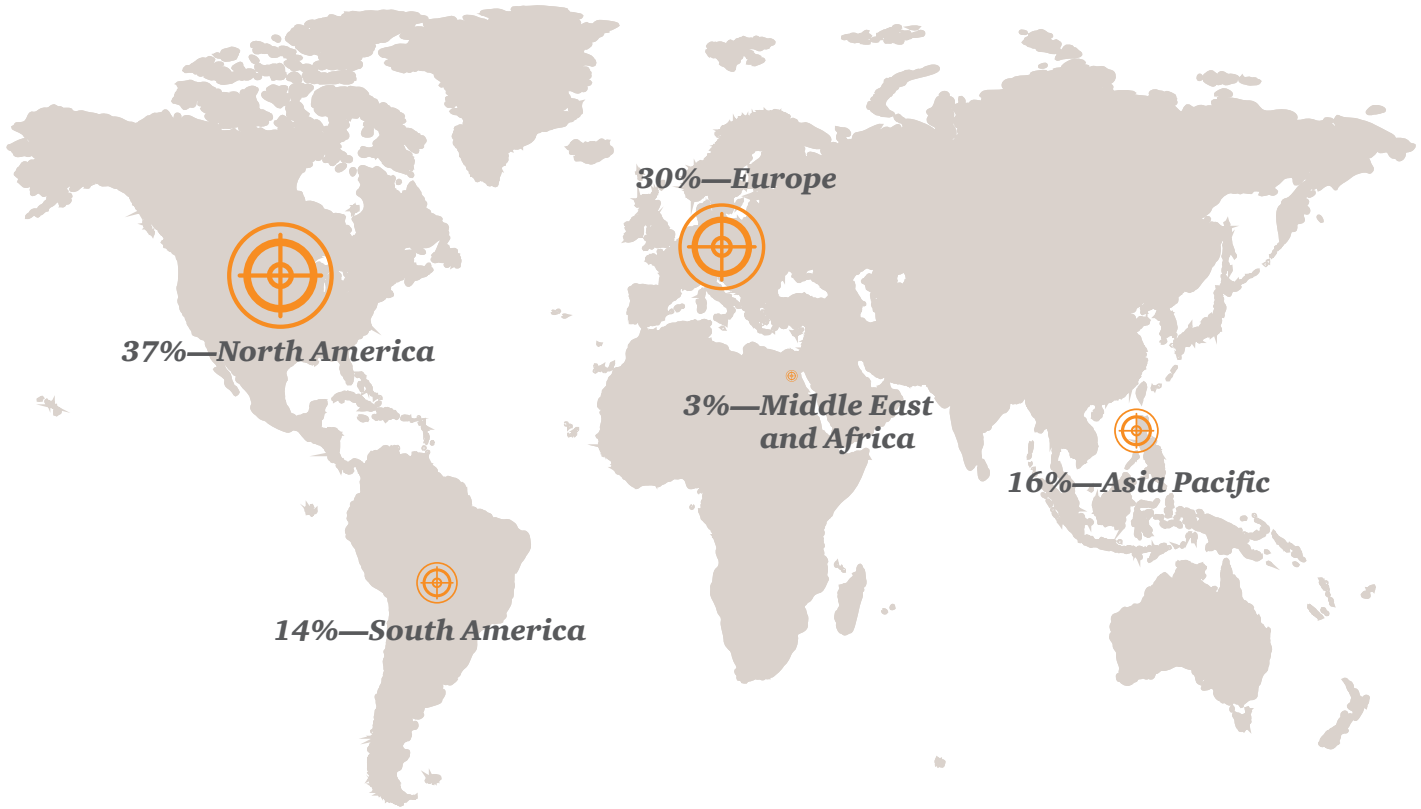
Implementation of key security safeguards



Methodology

The Global State of Information Security® Survey 2016 is a worldwide study by PwC, *CIO* and *CSO*. It was conducted online from May 7, 2015 to June 12, 2015. Readers of *CIO* and *CSO* and clients of PwC from around the globe were invited via email to participate in the survey.

The results discussed in this report are based on responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 127 countries.



The margin of error is less than 1%.

All figures and graphics in this report were sourced from survey results.

PwC cybersecurity and privacy contacts by country

Australia

Richard Bergman
Partner
richard.bergman@au.pwc.com

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

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

Austria

Christian Kurz
Senior Manager
christian.kurz@at.pwc.com

Belgium

Filip De Wolf
Partner
filip.de.wolf@be.pwc.com

Brazil

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

Canada

Sajith (Saj) Nair
Partner
s.nair@ca.pwc.com

China

Megan Haas
Partner
megan.l.haas@hk.pwc.com

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

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

Denmark

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

Mads Nørgaard Madsen
Partner
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

Yuji Hoshizawa
Partner
yuji.hoshizawa@jp.pwc.com

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

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

Korea

Soyoung Park
Partner
s.park@kr.pwc.com

Luxembourg

Vincent Villers
Partner
vincent.villers@lu.pwc.com

Middle East

Mike Maddison
Partner
mike.maddison@ae.pwc.com

Patrick MacGloin
Director
patrick.macgloin@ae.pwc.com

Netherlands

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

Bram van Tiel
Director
bram.van.tiel@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

Jacek Sygutowski
Director
jacek.sygutowski@pl.pwc.com

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

Russia

Tim Clough
Partner
tim.clough@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

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

Elmo Hildebrand
Director/Partner
elmo.hildebrand@za.pwc.com

Busisiwe Mathe
Partner/Director
busisiwe.mathe@za.pwc.com

Spain

Jordi Juan Guillem
Director
jordi.juan.guillem@es.pwc.com

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

Sweden

Martin Allen
Director
martin.allen@se.pwc.com

Rolf Rosenvinge
Director
rolf.rosenvinge@se.pwc.com

Switzerland

Rodney Fortune
Manager
rodney.fortune@ch.pwc.com

Chris Hemmi
Manager
christoph.hemmi@ch.pwc.com

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

Turkey

Burak Sadic
Director
burak.sadic@tr.pwc.com

United Kingdom

Neil Hampson
Partner
neil.r.hampson@uk.pwc.com

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

United States

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

Scott Dillman
Principal
scott.dillman@us.pwc.com

Chris O'Hara
Principal
christopher.ohara@us.pwc.com

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

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

www.pwc.com/gsiss
www.pwc.com/cybersecurity

PwC helps organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 184,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2015 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

The Global State of Information Security® is a registered trademark of International Data Group, Inc.

71224-2016 JP