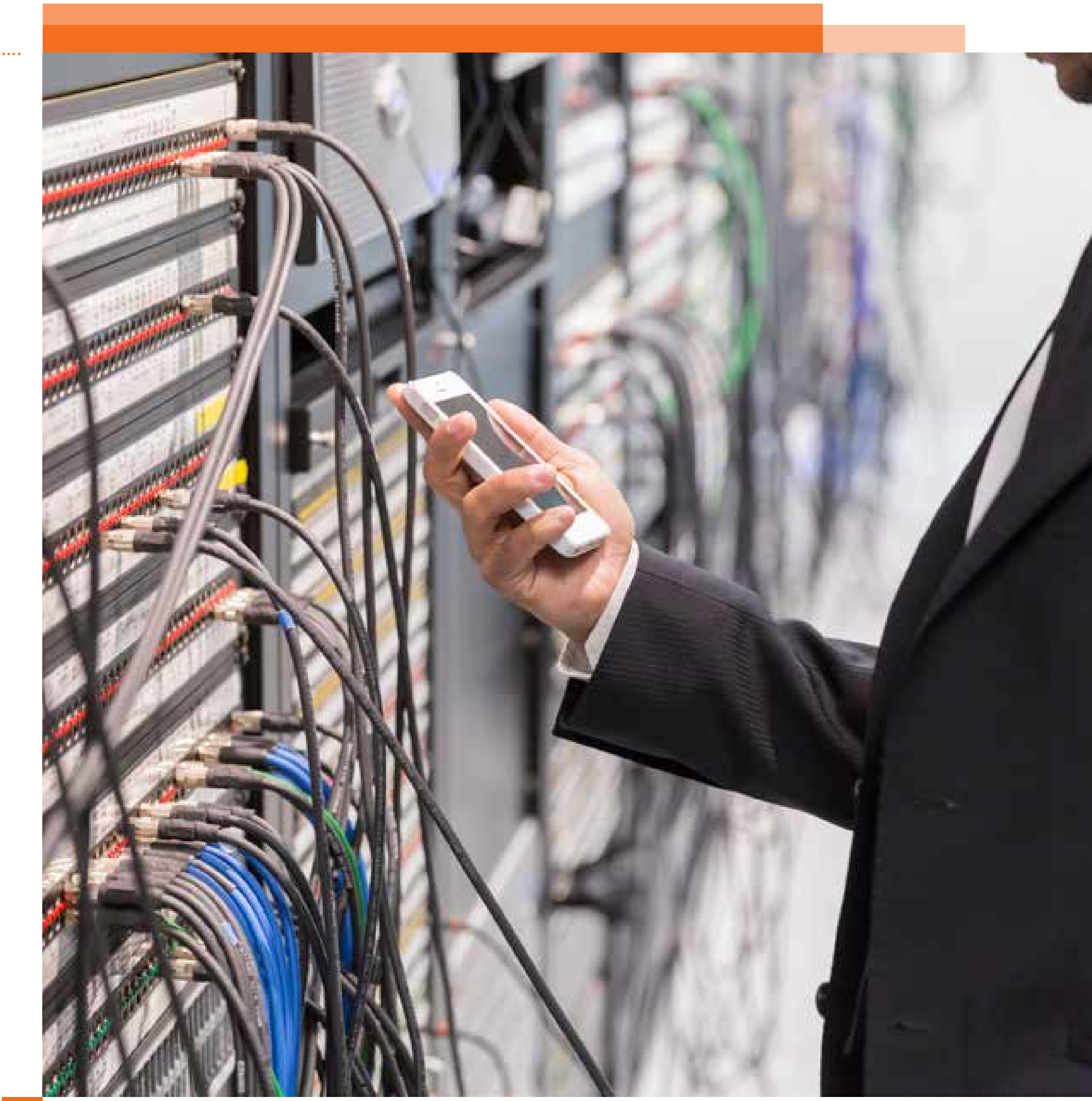
Key findings from the 2013 US State of Cybercrime Survey

June, 2013

Cyberthreats have become so persistent, the attacks so pervasive, that organizations—and their leaders—have essentially become inured to what cybersecurity and US Government officials call an ever-increasing threat. When organizations fall victim to cyberattacks, only then do they realize the time to take action was yesterday.

Co-Sponsored by:

- The Software Engineering Institute CERT® Program at Carnegie Mellon University
- *CSO* Magazine
- United States Secret Service



Executive Summary

This year's cybercrime survey highlights what many in government and the cybersecurity industry have known for years: The cybercrime threat environment has become increasingly pervasive and hostile—and actions to stem the tide of attacks have had limited effect. We must accept that cyberattacks are now a routine part of doing business in today's uncertain world, and they likely will be a part of doing business going forward.

The survey results tell us that many organizational leaders do not know or appreciate what they are up against, lack a clear, real-time understanding of the nature of today's cyber-threats and those who pose these risks, and have made little headway in developing strategies to defend against both internal and external cyber-adversaries.

The survey also tells us that we collectively have a long way to go in coming to terms with the extent of the threat, its short- and long-term implications, and what actions should be taken to curtail the multi-faceted impact.

The entities that collaborated on preparing and analyzing this year's survey saw the emergence of three themes:

1. **Leaders do not know who is responsible for their organization's cybersecurity, nor are security experts effectively communicating on cyberthreats, cyberattacks, and defensive technologies.** If organizations fail to identify who is in charge, they will be left with identifying who is to blame in the wake of crippling attacks.

2. **Many leaders underestimate their cyber-adversaries' capabilities and the strategic financial, reputational, and regulatory risks they pose.** Despite indications that the Securities and Exchange Commission ("SEC"), Congress, and the White House appreciate the threat, many companies still have not adequately grasped the degree to which failure to address the digital threat environment may have wider repercussions.

3. **Leaders are unknowingly increasing their digital attack vulnerabilities** by adopting social collaboration, expanding the use of mobile devices, moving the storage of information to the cloud, digitizing sensitive information, moving to smart grid technologies, and embracing workforce mobility alternatives—without first considering the impact these technological innovations have on their cybersecurity profiles.

The news, however, is not entirely grim. In our view, most of these cybersecurity challenges can be addressed internally. The majority of attacks (roughly 80%) rely on exploits that companies can readily defend against, if *they focus their attention on fundamental cybersecurity education, properly maintained IT infrastructure, and effective monitoring.*

In addition, the *right cybersecurity strategy, awareness of the threat environment,* and a *solid asset identification and protection program* can help entities manage another 15% of attacks. The final 5% of attacks emanate from sophisticated—and often nation state-sponsored adversaries—who threaten our national security, and *should be faced in strong collaboration with government agencies.*

What makes this survey different?

This is the first year that PwC has partnered with *CSO* Magazine and the other co-sponsors to conduct and evaluate the 2013 US State of Cybercrime Survey. Together, we have applied our deep experience in data analytics to dig into the layers of data and identify central concepts we see as vital to organizations that are attempting to make sense of current and future cyberthreats and attacks. We have brought the issue into focus by going beyond the statistics and focusing on the factors that can impact an organization's cybersecurity stance, such as by considering:

- Strategy and execution of the cybersecurity program;
- Understanding changes in the threat environment;
- Identifying key organizational assets in need of protection; and
- Spreading that protection beyond the walls of the entity to encompass the enterprise ecosystem.

Additionally, we have placed special emphasis on the unique cybersecurity challenges posed by the insider threat.

CSO Magazine and its partners Carnegie Mellon University's Software Engineering Institute ("CMU SEI") and the United States Secret Service ("USSS") have again participated in this effort.

We have also brought to bear our experience in identifying security- and cyber- trends by drawing on results from PwC's annual Global CEO Survey and annual Global State of Information Security Survey.

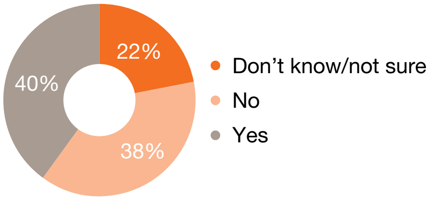
Key findings from the 2013 US State of Cybercrime Survey

In this 11th survey of cybercrime trends, over 500 US executives, security experts, and others from the public and private sectors provided their views on the state of cybercrime: who the internal and external threat actors are, what they are after, how well public-private collaboration supports cybersecurity, and what technologies are best able to defend and protect against cyberattacks.

The frog in the pot of hot water

There were no significant changes in C-Suite threat awareness, no spikes in spending on cyber-defense, no breakthroughs in the use of technology to combat cybercrime, and no significant change in the ability of organizations to measure the impact of both cybercrimes committed by insiders and those caused by external cyberattacks. (See Figure 1).

Figure 1: Do you have a methodology that helps you determine the effectiveness of your organization's security programs based on clear measures?



In reviewing the survey data from the past three years, we found little movement in key indicators. When we compare this with the almost daily reports of cyber-breaches against public and private organizations in the United States and globally, we are struck by the possibility that the threats have become so persistent, the attacks so pervasive, that organizations—and their leaders—have essentially become inured to what cybersecurity and US government officials call "an ever-increasing threat."

Many senior executives have become the proverbial "frog in the pot of hot water"—unaware of the ever increasingly hostile environment. When the pot boils over and their organization falls victim to cyberattacks, only then do they realize the time to take action was yesterday. Or as Ira Winkler, the president of the Information Systems Security Association ("ISSA"), put it, "We hear about wake-up calls, but people keep hitting the snooze button."[1] Perhaps part of the problem, to continue the analogy, is the failure on many companies' part to appreciate the strategic need to measure the temperature of the water in which one sits.

One goal of this paper is to drive an urgent call to action, to appreciate the need to bridge a gap that exists today among those who do not perceive cybersecurity as a strategic business issue and those who do, and to increase awareness as to the strategic implications of the cyber concerns we, as a collective, face.

Our in-depth analysis of the survey results identified four critical areas that have the most impact on organizational responses to cybercrime:

1) Understanding ecosystem-wide risks;

2) Integrating threat intelligence and information-sharing into proactive defense programs;

3) Identifying and mitigating cybercrime committed by trusted insiders; and

4) Understanding and using cybersecurity technology effectively.

Gaining a better understanding of these areas, combined with a strong grasp of a continuously organization's threat environment and an appreciation of its sensitive assets, should give senior executives a stronger basis for an adaptive cybersecurity strategy. The technical debt built up over the years, and the vulnerabilities created as a results, must also be acknowledged. (See Technical Debt on page 16)

[1] http://www.reuters.com/article/2013/05/16/us-cyber-summit-congress-idUSBRE94F06V20130516

Understanding risks across the ecosystem

In the cyber-arena, what you don't know can hurt both you and everything your organization touches. Advances in technology have interconnected businesses to partners, suppliers, customers, government entities, and even competitors. Cybercrime is an equal-opportunity event—it can affect every entity across a company's business ecosystem.

As a result, the entity's leaders should develop a thorough cybersecurity plan that encompasses all aspects of their global business ecosystem. Yet a significant number of respondents to this year's survey answered 'unknown' or 'I don't know' to important survey questions. Of particular concern, we noted that those who identified themselves as Chief Information Officers ("CIOs") or Chief Technology Officers ("CTOs") often were unfamiliar with key cornerstones of a strong cybersecurity program. (See Figure 2)

Figure 2: Percentage of responding CIOs (including CTOs) indicating "Don't Know" or "Not Sure"

22% responded: Don't know/ Not sure	When compared with the prior 12 months, how have monetary losses as a result of cybersecurity events in your organization changed?
22% responded: Don't know/ Not sure	When considering the financial losses or costs to your company from those targeted attacks aimed at your company, has the financial loss or cost increased or decreased when compared to the prior 12 months?
21% responded: Don't know/ Not sure	Which of the following proactive activities and techniques are you using to counter advanced persistent threats?
21% responded: Don't know/ Not sure	Which of the following groups posed the greatest cyber security threat to your organization during the past 12 months?
21% responded: Don't know/ Not sure	In general, what causes of electronic crimes were more costly or damaging to your organization?
17% responded: Don't know/ Not applicable	What was your organization's approximate annual budget for security products, systems, services and/or staff for each of the following areas during the last 12 months?
17% responded: Don't know	Please indicate all of the cybercrimes committed against your organization during the past 12 months, along with the source(s) of these cybercrimes to the best of your knowledge.
16% responded: Don't know	If you were to find it necessary to seek government assistance with cybercrime or a cyber security-related event, which organization(s) would you contact immediately?

Some survey respondents might not be in a position to have access to cybersecurity strategy and response information, or might not be directly involved in the company's insider threat or law enforcement liaison processes. But in our view, cybersecurity is everyone's business—employees, contractors, consultants, and senior executives should all have at a minimum, a basic understanding of how the company protects people and information from cyberattacks.

The good news from this year's survey? A strong strategy to protect the ecosystem starts with sensible IT security policies and processes. For cybersecurity to work across an ecosystem, all players need to know not only what the policies and processes are, but also why they need to adhere to them. In questions related to IT security processes, it appears that a solid majority of IT staff and IT leaders understand the policies and processes in place to protect corporate data.

The issue of establishing, communicating, and effectively evaluating cybersecurity policies and practices extends beyond organizational boundaries. Because of the interconnected nature of the ecosystem and today's reliance on global supply chains, organizations must integrate their vendors and suppliers into their cybersecurity strategy. This does not mean that all organizations in an ecosystem have to have the same strategy, tools, and technologies—but it does mean that individual organizations should have some confidence that their partners aren't passing on increased cyberrisks through the ecosystem web.

Companies grappling with cybersecurity should be prepared to address two types of supply chains:

1. The IT supply chain, which includes the software and hardware used to support corporate networks and operations; and

2. The more traditional supply chain that encompasses the parts and services that are integrated into the entity's customer offerings, be they physical products, data or services.

In today's interconnected ecosystem, both of these supply chain avenues are often direct freeways to compromise company assets. Not all companies recognize that supply chain vendors and business partners such as joint ventures, strategic partnerships, and franchisees can have lower—even non-existent—cybersecurity policies and practices, a situation that can increase cybercrime risks across any entity that partner or supplier touches. And those who do recognize the risk often fail to understand what mitigation steps should be taken.

Although supply chain risk management is a capability identified by respondents as something they use to address cyber-risk, only 22% of respondents actually conduct incident response planning with their third party supply chain. (See Figure 3) Additionally only 20% of respondents evaluate the security of third parties more than once a year. (See Figure 4)

Figure 3: Do you conduct incident response planning with your third-party supply chain?

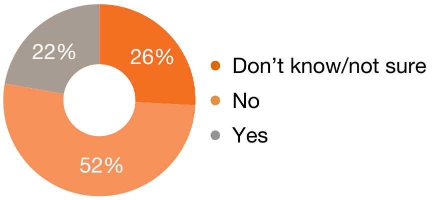
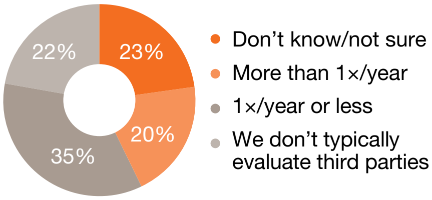


Figure 4: On average, how often do you evaluate the security of third-parties with which you share data or network access?



Previous PwC surveys support the view that the supply chain is a potential weak link in cybersecurity—both in the United States and globally. In the PwC 2013 Global CEO Survey, the inability to protect intellectual property ("IP") and customer data in the corporate supply chain was a concern for 36% of corporate leaders in the United States. Companies often struggle to get their suppliers to comply with privacy policies—a baseline indicator of data protection capabilities.

This is especially true for industries able to easily understand the tangible information types that are at risk, such as those industries focused on protecting personally identifiable information ("PII"), such as financial services, and those that are affected by the Health Insurance Portability and Accountability Act ("HIPAA") protected data, as well as those that manage Payment Card Industry ("PCI") information. Yet fewer than one-third of all industry respondents to PwC's 2013 Global State of Information Security Survey required third parties to comply with privacy policies.

Threat intelligence and information-sharing

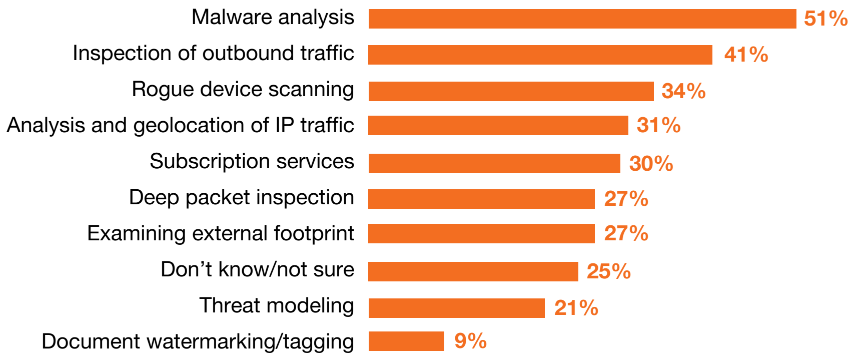
Threat Intelligence

While US cyberthreat anecdotes have become almost routine (keeping the media focused on this issue) the barrage of alarms has not significantly raised survey respondents' understanding of who these cyber adversaries are, what they target, and how they operate. Many C-Suite executives have neither adequate knowledge of who the most serious threat actors are, nor (logically given the foregoing) do they have a cybersecurity strategy to defend against them. Despite all the talk about cybercrime and cybersecurity, awareness of the threat environment is not increasing.

'Threat awareness'—the ability to understand cyberthreat actors' capabilities, motivations, and objectives—should be one of your organizations' starting points for developing an adaptive cybersecurity strategy, providing the contextual background against which organizations can identify key assets that will likely be of interest to your adversaries. Such awareness can also help make more efficient the organizations' assessment of their vulnerabilities to cyberattacks from the most likely threat actors.

We asked survey respondents which type of proactive tools they used to counter the Advanced Persistent Threat ("APT"), a commonly used term to define remote attacks employed by sophisticated threat actors, often nation states or their intelligence services. Only 21% of respondents said they used threat modeling, a relatively inexpensive tool that organizations can adapt to their particular threat environment and asset protection requirements. (See Figure 5)

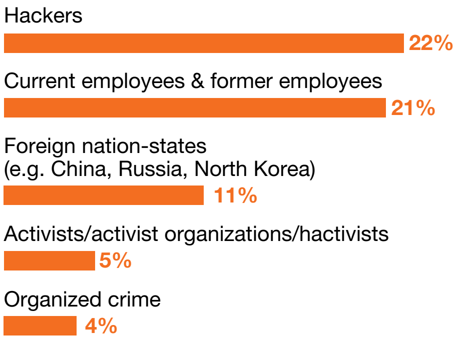
Figure 5: Which of the following proactive activities and techniques are you using to counter advanced persistent threats?



The majority of survey participants cited malware analysis and inspection of outbound traffic as a tool they currently have in place. While these technologies are effective in identifying intrusions and potential losses, if they are installed in the right place, they are after-the-fact techniques that can help organizations proactively only if the results are incorporated into an adaptive and forward-looking threat modeling strategy. As a result, these entities can be vulnerable to APTs seeking to access sensitive information surreptitiously over an extended period of time.

In fact, CIOs and Chief Security Officers (“CSOs”) do not agree on what constitutes the most significant threat to their operations. When asked in the survey to name the top threats facing their organization this year, CSOs, including Chief Information Security Officers (“CISOs”) pointed to hackers (26%) and foreign nation-states (23%). CIOs, including CTOs, however, were more concerned about insiders (27%)—current or former employees-but only 6% were concerned about nation-states. (See Figure 6) This lack of consensus, which likely contributes to a lack of action at the C-suite and board level, reflects differences in the threat landscape from industry-to-industry, or varying perspectives according to job responsibilities: the old but often true adage that “where you stand depends on where you sit” applies.

Figure 6: Which of the following groups posed the greatest cybersecurity threat to your organization during the past 12 months?



All respondents

How CSOs (including CISOs) compare:

1: Hackers

2: Foreign nation states

3: Current and former employees

How CIOs (including CTOs) compare:

1: Current and former employees

2: Hackers

3: Organized crime

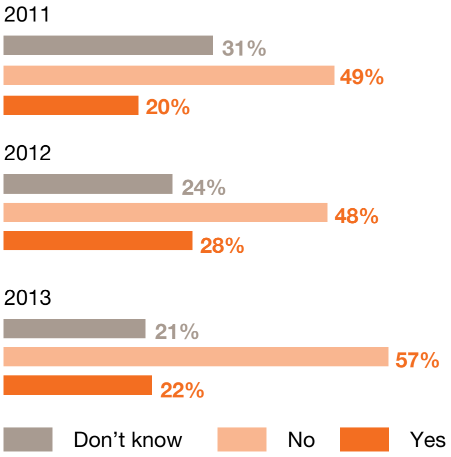
Information Sharing

A sensible approach to public-private partnerships should be a cornerstone of any cybersecurity strategy. And those who take advantage of available government sources of cyber-intelligence can gain a fuller picture of both the threats and the leading practices for defending against them. President Obama, in his February 2013 Executive Order on Cybersecurity, designated the Department of Homeland Security (“DHS”) as the focal point for intelligence-sharing with the private sector.

While DHS coordinates the process by which Information Sharing and Analysis Centers (“ISACs”) engage with key sectors of the US critical infrastructure, awareness and use of ISACs is particularly low and has not increased appreciably over the past three years, with the exception of the banking and finance industry, the survey showed. (See Figure 7) As we noted in our September 2012 ZoomLens article on cybersecurity[2], the Financial Services- ISAC (“FS-ISAC”) is often praised for its work in bringing public and private sector counterparts together, but with the myriad number of public-private information sharing groups available, companies are often unable to determine what government agencies to engage and what to expect from them.

[2] http://www.pwc.com/us/en/forensic-services/assets/zoomlens-cybersecurity.pdf

Figure 7: Does your organization participate in any Information Sharing and Analysis Center (ISAC) activities (http://www.isaccouncil.org/), if available in your industry sector?

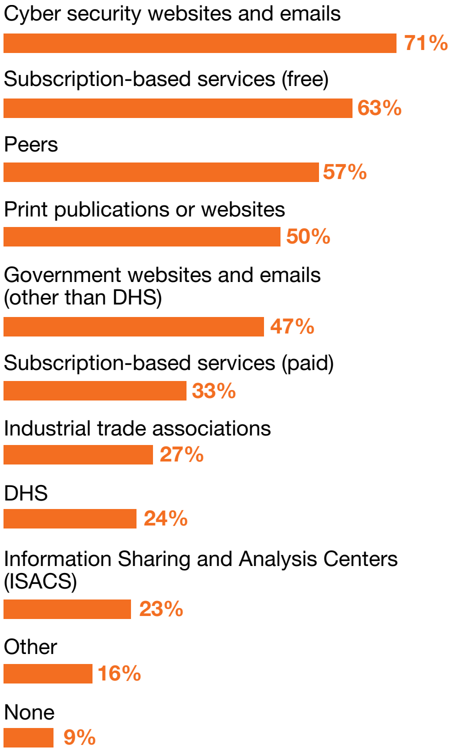


How company leaders get their information on threats might be part of the problem. Even though reporting on the severity and complexity of the threat has grown over the past few years, security and business executives are increasingly turning to publicly-available sources of information, such as free Internet websites, as their sources of information. Smaller numbers turn to subscription services, industry colleagues, and the US Government for information. (See Figure 8)

While open-source information can provide threat context to a cybersecurity strategy, these sources vary greatly in quality, accuracy, timeliness. At a 2011 conference on APT sponsored by RSA, attendees observed that, “…attackers seem to share intelligence more effectively than legitimate enterprises do.”[3] Organizations should have a robust, multi-source information collection and analysis strategy, drawing on a variety of external and internal data sources and integrating new information on both emerging threats and innovative technologies to create an agile cyberdefense.

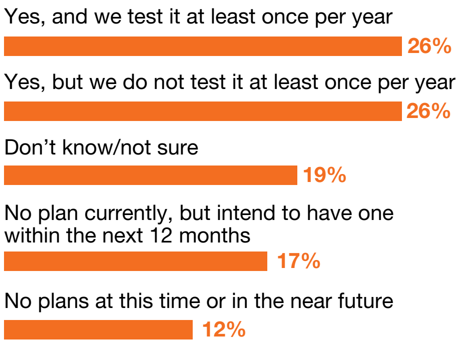
A cybersecurity strategy is the cornerstone of protecting sensitive business assets, yet nearly 30% of companies surveyed (see Figure 9) do not have a plan. And, of those that do, half fail to test it. Companies that understand what their key corporate assets are and then develop and constantly update their cybersecurity strategy based upon new intelligence to protect their assets will likely find themselves in a stronger position to defend against cyberattacks.

Figure 8: Please identify all sources you monitor to keep up with current with trends, threats, vulnerabilities, technology, and warnings



[3] http://www.rsa.com/innovation/docs/APT_findings.pdf

Figure 9: Does your organization have a formalized plan outlining policies and procedures for reporting and responding to cybersecurity events committed against your organization?



Additionally, many of the companies who lack or fail to test a cybersecurity plan are likely the same ones who report they don't know what government agency to contact when a cybercrime is suspected. Interestingly, there are differences between industries regarding which agencies are the top choices for such support. While many reach out to the FBI or the USSS, several industries still rely on local law enforcement for support.

The study reveals that the number of companies that reach out to the United States Computer Emergency Readiness Team ("US- CERT") remains quite low, an indicator that many organizations are unaware of the robust cybercrime-related information US-CERT makes available to the US private sector on a regular basis.

Deciding who within the government can best help your organization depends on your corporate experience, industry-specific considerations, the identity of likely threat actors, and the severity of the suspected crime. As a retired senior FBI cyber-official recently stated, "The government is…sharing information as fast as we can get it." The official continued, however, by saying that "when the government does provide information on a cybercrime, the agency hoped the company had already contemplated the potential for a cyberattack and has developed a response plan."[4] As noted above, our survey showed that most do not.

Cybercrime from within: Examining the insider threat

The Insider Threat

Insiders from anywhere within the business ecosystem can wreak havoc. The Software Engineering Institute CERT® Program at Carnegie Mellon University notes in its Common Sense Guide to Mitigating Insider Threats,[5] "…contractors, consultants, outsourced service providers, and other business partners should be considered as potential insider threats in an enterprise risk assessment."

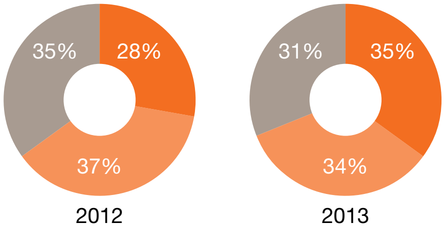
The threat of trusted organizational insiders committing cybercrime has received less media and public attention than other cyberthreats. And we see little shifting of respondent attitudes, despite a recent high-profile FBI campaign to raise awareness of instances of insiders stealing trade secrets.

Still, highly publicized research from Carnegie Mellon University cited the significant damage insiders have done to both private and public organizations. While most of the media cybercrime reporting has been on remote network attacks over the Internet, survey results show that among respondents answering insider-related questions, insiders were deemed more likely to be the sources of cyberattacks. For the second year in a row, a greater number of respondents identified insider crimes (34%) as causing more damage to an organization than external attacks (31%). (See Figure 10)

[4] http://www.ctlawtribune.com/PubArticleCT.jsp?id=1202601094171&slreturn=20130503094156

[5] http://www.sei.cmu.edu/reports/12tr012.pdf p. 27.

Figure 10: In general, electronic crimes were more costly or damaging to your organization when caused by:

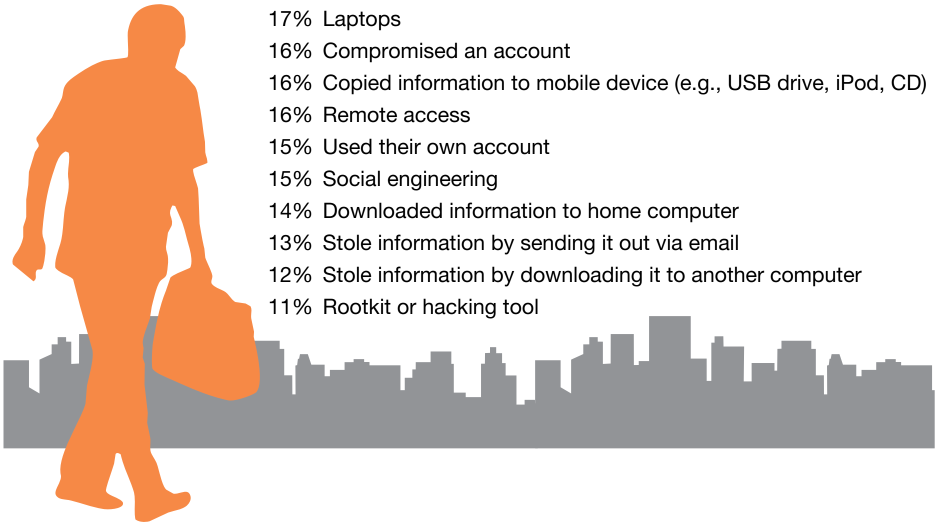


- ● Don’t know/not sure
- ● Insider: Current or former employee, service provider or contractor
- ● Outsider: Someone who has never had authorized access to an organization’s systems or networks

Many information security tools focus on access and authentication. However, these tools are less effective against insiders such as employees, contractors, and third parties who have been granted legitimate access to sensitive data and systems. (See Figure 11) These insiders are likely to be one step ahead of external threat actors because they tend to already know what the company’s crown jewels are: those assets that drive cash flows, competitive advantage, and shareholder value. They also know where they reside on the networks and how to gain access to them for the purposes of theft, disclosure, or destruction.

As we previously noted, what you don’t know can hurt both you and everything your organization touches. Similar to our ecosystem findings, the ‘don’t know’ answers related to the Insider Threat are concerning. Just as more than one-third of respondents said ‘don’t know’ when asked whether insiders or external actors could cause their organization more damage, the most popular answer to questions about the sources of cybercrime and the mechanisms insiders used was also ‘don’t know’. Twenty four percent of respondents who had suffered an insider attack did not know what the attack’s consequences were; 33% of respondents had no formalized insider

Figure 11: Please indicate all mechanisms used by insiders in committing cybercrimes against your organization in the past 12 months



Top 10 attack mechanisms reported by those who responded they experienced an attack conducted by an insider (excluding “don’t know”)

17%	Laptops
16%	Compromised an account
16%	Copied information to mobile device (e.g., USB drive, iPod, CD)
16%	Remote access
15%	Used their own account
15%	Social engineering
14%	Downloaded information to home computer
13%	Stole information by sending it out via email
12%	Stole information by downloading it to another computer
11%	Rootkit or hacking tool

Respondents indicated 29% of events they experienced during the past 12 months were known or suspected to have been conducted by Insiders.

threat response plan (See Figure 12); and, many were uncertain as to how their company handled investigating potential insider threat cases. (See Figure 13) Of those who did know what the insider threat handling procedures were, the majority reported that the cases were handled in-house, absent legal action or law enforcement involvement.

It remains unclear whether this stems from conscious decision making regarding the handling of insider cases or if it reflects a lack of understanding about how law enforcement agencies can support such investigations. It seems likely, however, that many organizations are not sufficiently incorporating the potential damage insiders can cause to corporate assets, business operations and reputations in deciding whether to pursue prosecution.

Insider Threat Management

While some companies seem to be aware of the damage insiders can cause, the survey shows that many respondents are not taking the threat seriously enough, nor doing a good enough job of responding to it.

A strong, enterprise-wide insider threat risk mitigation program is needed to:

- Recognize the risks posed by insider threats;
- Be capable of detecting them;
- Be capable of responding to them; and
- Be capable of effectively mitigating them.

To detect and manage the insider threat, the entity will need information and tools across a range of functions, including IT, information security, physical security, HR, and legal, which often handles privacy and internal investigation issues. Yet, the survey indicates only 14% of respondents handle the insider threat using an interdepartmental team. (See Figure 14)

Figure 12: Does your organization have a formalized plan for responding to insider security events committed against your organization?

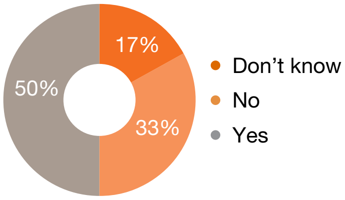


Figure 14: Who is responsible for responding to insider attacks in your organization?

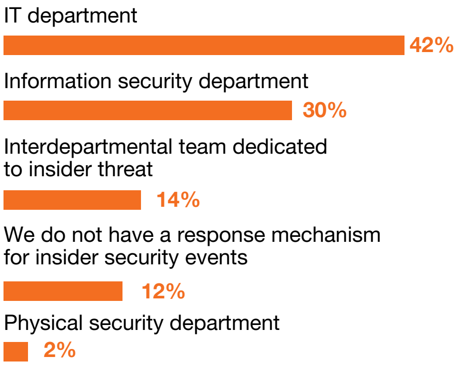
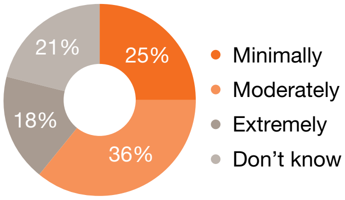


Figure 13: How effective is your organization in reporting managing and intervening in cyber threats with internal employees?



Our experience suggests that the lack of centralized collection and analysis of corporate data in these insider cases is a primary contributor to this general lack of knowledge. Pertinent information is often held in separate repositories owned by HR, legal, information security, and physical security. In addition, the legal and personnel implications of insider cases, along with training and awareness issues, indicates the importance of developing an insider threat management program, anchored by an interdepartmental team comprising representatives from IT, information security, physical security, legal, and HR, including training and ethics officers.

While significant technology advances in recent years enable security teams to identify and investigate potential insider threats quickly, non-technical collaboration among primary stakeholders is often pivotal in stopping a smart and motivated insider. Data from The Software Engineering Institute CERT® Program at Carnegie Mellon University Insider Threat Database, a repository of reported insider threat cases involving theft of IP using IT, IT sabotage, or fraud using IT, shows that 27% of the incidents in the database were detected by non-technical means. As an FBI insider threat analyst explained this at the February 2013 RSA conference, "…the risk from insider threats is not a technical problem, but a people-centric problem. So you have to look for a people-centric solution. People are multidimensional, so what you have to do is take a multidisciplinary approach."[6]

Another important element in defending against insider attacks is also likely one of the most cost-effective: employee training and awareness. Twice as many survey respondents indicated 'unintentional insiders'—those whose actions are not malicious—cause more sensitive data loss than those of malicious inside actors.

In responding to questions on perceived threats posed by insiders, the majority pointed to lost laptops and related devices, victims of social engineering, or violations of policies on attaching thumb drives or peripherals. Moreover, fellow employees and managers are in the best position to notice and report, and thus prevent damage caused by unintentional insiders, if they know what to look for and where to report it.

Employee training and awareness can be equally effective in mitigating malicious insider risks and damage. These cases often can be heralded by early warning signs such as poor work performance, issues with colleagues, disciplinary action, or living beyond their means; these are signs that employees and managers will notice, not IT security tools. This underscores the importance of training and awareness as a critical element of an insider threat management program, one that is integrated with current information security training and awareness, ethics training programs and the ombudsman process. This requires the participation of corporate functions: not just IT and information security, but also human resources, legal and physical security.

Breach consequences: Effective defense and organizational resilience

Many of the survey questions focus on the technologies organizations use to prevent and investigate cyber breaches, to improve organizational resilience once an attack compromises information systems, and to improve overall organizational cybersecurity capabilities. Entities can find themselves in a constant cycle of attack and defend. As novel attack vectors and methods enter the ecosystem, the security industry develops new technologies and techniques to counteract these methods.

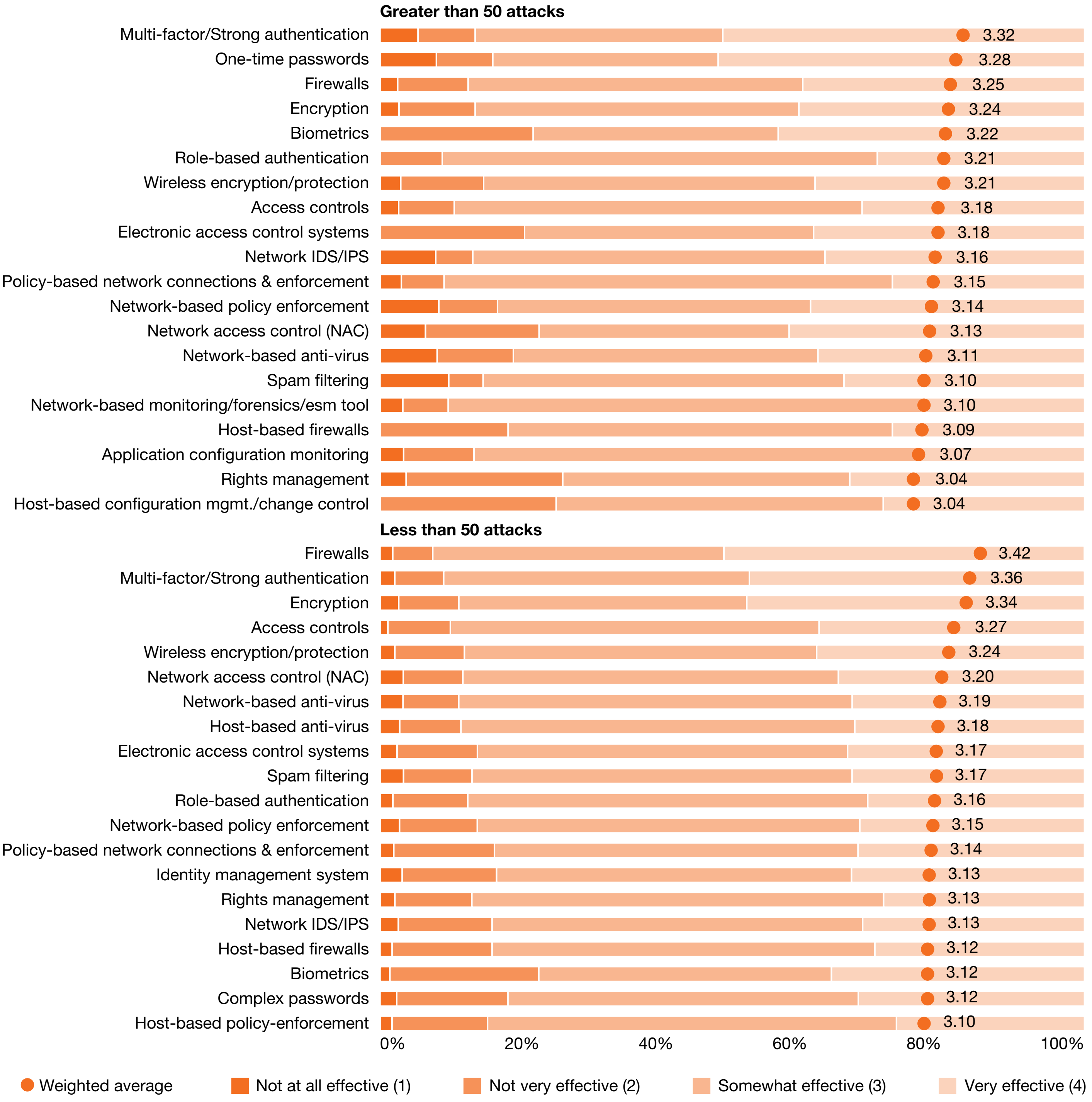
The result is a long list of technology classifications that are used to defend against every manner and type of attack. Respondents appear to be enthusiastic adopters of a variety of defensive, investigative, and mitigation technologies. But a closer look at the data reveals that organizations are not faring as well in assessing exactly what these technologies are supposed to be doing to protect their information—and how effective they are at actually doing that job.

In another sign that attitudes about cybersecurity have shifted little over the years, respondents this year continue to generally feel the same about the overall effectiveness of technologies, regardless of the number of reported attacks per year their organization experienced—*this was true for both IT professionals and non-IT professionals, who in theory should be more familiar with the effectiveness of the technologies.* This probably points to a lack of understanding about how specific technologies relate to different types of attacks and limited capabilities for assessing the effectiveness of one specific technology or a range of technologies. (See Figure 15)

Interestingly, when a breach does occur, companies reported no significant correlation between a targeted attack and financial loss. The ratio of targeted attacks to non-targeted attacks as identified by respondents remains the same, regardless of whether the attack resulted in a financial loss. We had expected to see more targeted attacks associated with financial losses. In fact, 96% reported cyber-related losses of less than US$1 million over the past year.

[6] http://www.darkreading.com/insider-threat/5-lessons-from-the-fbi-insider-threat-pr/240149745

Figure 15: Effective rating of technologies for respondents experiencing…



Still, some government officials, including NSA Director General Keith Alexander wrote in 2012 that "the ongoing cyber- thefts from the networks of public and private organizations, including Fortune 500 companies, represent the greatest transfer of wealth in human history."[7]

Similarly, the FBI estimates that all IP theft costs US businesses billions of dollars a year.[8] The recently released report by the Commission on the Theft of American Intellectual Property, a private advisory panel headed by former DNI Dennis Blair and former US Ambassador Jon Huntsman, found that IP theft was growing and costing the United States more than $300 billion each year.

This discrepancy between public statements on loss estimates and what organizations themselves estimate as losses is striking.

So why the disconnect? One explanation: organizations that have identified and even mitigated a cyberattack targeting IP still might lack an effective means of assessing what exactly has been stolen. According to a 2011 report on economic and industrial espionage in cyberspace published by the Office of the National Counterintelligence Executive ("ONCIX"), "Even in those cases where a company recognizes it has been victimized…calculation of losses is challenging and can produce ambiguous results."[9]

Another possibility: more sophisticated cyberattacks targeting IP might be going undetected by detection technologies. According to the retired senior FBI cyber official, "What happens with the FBI is right now, approximately 60 percent of the time, we are going out and telling a company that they have been intruded upon."[10] The survey, like many others that try to build cybercrime awareness and understanding, covers several types of cybercrime: denial of service attacks, credit card information thefts, website defacement, as well as IP thefts.

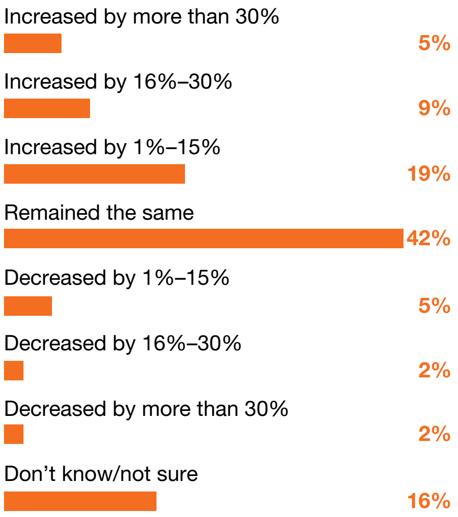
These latter attacks are designed to be less observable, longer lasting, and often sophisticated enough to avoid detection by current private sector cybersecurity technologies. Our view is that the 40% that are not notified are perhaps the most serious and significant thefts that are managed by a broader national security umbrella.

Losing ground?

From an organizational resiliency standpoint, companies appear to be losing ground in combating attacks. Although 90% of respondents reported fifty or fewer attacks in the past year, only 9% of respondents reported an overall decrease in the number of cyberevents over the previous year. About one-third reported an increase in events. And while reported losses still appear low, only 5% had been able to reduce their monetary losses from cyber events, with 19% stating that their monetary losses have actually increased.

Given this environment, it is hard to be optimistic about the future trajectory of information security. Clearly many companies have a poor understanding of how their technologies are deployed and how to properly gauge the effectiveness of those deployments. From an organizational resilience standpoint, things also appear to be trending in the wrong direction, as the number of successful events and monetary losses are both rising.

Figure 16: When compared with the prior 12 months, cybersecurity events in your organization have:



[7] http://www.nsa.gov/research/tnw/tnw194/article2.shtml

[8] http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr

[9] http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

[10] http://www.abajournal.com/news/article/what_law_firms_should_know_about_cyber_attacks_and_the_fbi/

A deeper dive into our data can help you protect yours

With this year's survey, we took a deeper dive into the data to explore what it means for protecting US public and private sector organizations amid increasing cybersecurity risks. Ignorance is far from bliss. Ignoring these threats will not keep the pot from boiling over.

Adversaries are more targeted and efficient than ever. A growing number of nation states are getting into the cyberattack game. Organized crime groups have advanced from small-scale monetary theft to large-scale multi-country simultaneous heists. Hactivists are working with sympathizers within organizations to gain better access.

Many entities are now conducting operations in unsafe regions around the world. And not just through customer locations. This includes places where they're conducting product development and innovation work, working with third parties who have the organization's crown jewels but aren't subject to their security policies.

Lines of business departments are using technologies and software that haven't been reviewed by the organization's information security department. Businesses are becoming intimately involved in ever-changing global ecosystems through activities such as global M&As, strategic partnerships with foreign competitors, and joint ventures that expose their most sensitive IP. More and more of their data is less and less protected.

At the same time, security budgets are misaligned to respond to yesterday's threats while companies are spending less on 'tried and true' security technologies—without understanding how effectively they are, or are not, in combating emerging cyberthreats. Meanwhile, business units are now working with new technologies without understanding the security consequences as they plan strategies for using social media; using public/private cloud services; and allowing employees to use personal devices.

- The C-suite and board should get directly involved with their organization's cybersecurity if they have not already done so.
- The C-suite, technology, and security leadership should establish a cross functional steering committee to foster collaboration and alignment.
- Security budgets should be allocated in line with business strategy.
- Organizations should put in place mechanisms to engage their entire ecosystem in security prevention and response.

Perhaps most importantly, organizations will be hard-pressed to manage cyber-related threats if they fail to understand their adversaries. Get to know how your business model can unintentionally open your entity's cyber-doors to those who will likely overstay their welcome while making off with precious jewels.

For the most part, the business world tends to underestimate cyberthreats. Neither corporate boards nor business unit leaders are paying enough attention to the negative business implications. According to PwC's Global CEO Survey, one-third of CEOs don't think a cyberattack would negatively impact their business. Yet 61% of consumers[11] would stop using a company's product or services after a breach. ***Think about it.***

[11] http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-consumer-privacy-and-information-sharing.pdf

Paying off the technical debt

Many organizations across the industry spectrum are suffering from substantive technology debt. It has been estimated this debt will soon exceed $1T. In effect, companies are spending their IT budgets on emerging business technologies while allowing their IT infrastructure to age and atrophy to the point that systems can't support basic data security functions. This is similar to a lack of funding to physical infrastructure in the US, such as roads, bridges, and other transportation infrastructure.

Annual spending in information technology does not appear to be keeping up with emerging threats. Technology's influence has grown rapidly, with many corporations adopting mobile solutions, social media, alternative workplace solutions, collaborative product innovation, digitized healthcare, and tele-medicine. This is happening amid a corresponding increase in regulatory controls associated with privacy controls, health information controls, financial data controls, intellectual property protection, and financial statement controls, and more. It's also happening at a time of increased awareness of cyber-campaigns targeting specific industries and organizations, and by adversaries who move from on-line industrial espionage to acts of destruction.

In the face of such intense demand and regulatory oversight, how is it that IT budgets are flat or declining?

Just as corporations should consider how much financial debt they are willing to take on and still maintain a credit rating worthy of its brand, they also should consider how much technical debt they're willing to take on in the face of increasing regulation, disclosure requirements, and consumer trust concerns. Technical debt, however, is not on the balance sheets and therefore the entity's leadership lacks the transparency required of management and boards to consider the risks associated with that debt.

It's not unusual for organizations to face trade-offs between the desire to keep pace with new technology-enabled services and the need to sustain existing services. Yet many executives remain in the dark about the infrastructure that can deliver emerging technology-fueled services. Still, the need to understand some fundamental technology issues should not be overlooked. Ask and consider:

1. How old are the firewalls that regulate what goes into and out of the corporate network?
2. Do they contain known vulnerabilities that our adversaries are exploiting?
3. What aspects of the identity-management system governing the role-based access are foundational to our control environment?
4. Is it current technology with a secure operating system and hardware, or did we choose the lowest cost alternative with known security issues?
5. Are the enterprise applications and their underlying databases current, or have we deferred maintenance and upgrades because they were highly customized, rendering the path to upgrade too costly to consider in our current economic climate?
6. Are the routers and switches that move data within our networks current, or have they been provided by a manufacturer that has installed 'back doors' into that equipment, allowing a copy of all corporate traffic to be taken without our knowledge?
7. Do we have known security vulnerabilities in key databases that we can't remediate because the applications that depend on those databases can't be modified?

While it's nothing new for businesses to defer maintenance and other basic technology needs as upgrades, security patches, and replacements, or to move to current generation technology. What is new is that adversaries have raised the risk for many corporations.

Cyber adversaries often exploit vulnerabilities (both known and unknown) in the technology 'stack' that underpins most businesses today. In the current environment, it's all too easy to amass substantive technical debt by deferring merger integrations, letting enterprise system upgrades lag, and expanding IT-enabled services—without making corresponding investments in the security infrastructure. This can open a toehold for cyber-adversaries who are hungry for system and data access to your valuable data assets.

About PwC's Cybersecurity Practice

As a part of the largest professional services Firm in the World, PwC has market leading strategic, technical, forensic, business process, and industry knowledge and experience. PwC's Cybersecurity consulting practice helps organizations understand, adapt and respond to dynamic cyber challenges and accelerating risks inherent to their business ecosystem. We enable our clients to preserve and protect their competitive advantage and shareholder value by prioritizing and protecting the most valuable assets fundamental to their business strategy. For more information on PwC's cybersecurity point of view, visit: www.pwc.com/cybersecurity.

About PwC US

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 158 countries with more than 180,000 people. We're 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/US.

www.pwc.com

To have a deeper conversation about how this subject may affect your business, please contact:

David Burg
Principal, PwC
703 918 1067
david.b.burg@us.pwc.com

Michael Compton
Principal, PwC
313 394 3535
michael.d.compton@us.pwc.com

Peter Harries
Principal, PwC
213 356 6760
peter.harries@us.pwc.com

John D Hunt
Principal, PwC
703 918 3767
john.d.hunt@us.pwc.com

Gary Loveland
Principal, PwC
949 437 5380
gary.loveland@us.pwc.com

Joseph Nocera
Principal, PwC
312 298 2745
joseph.nocera@us.pwc.com

David Roath
Partner, PwC
646 471 5876
david.roath@us.pwc.com

© 2013 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. LA-13-0317 SL/JM