Enterprise Strategy Group | Getting to the bigger truth.™

Research Report

Cyber Supply Chain Security Revisited

By Jon Oltsik, Senior Principal Analyst

With Bill Lundell, Senior Research Analyst and Jennifer Gahm, Senior Project Manager

September 2015

Contents

List of Figures

List of Tables

Executive Summary

Overview

The cyber supply chain is defined as follows:

> *The entire set of key actors involved with/using cyber infrastructure: system end-users, policy makers, acquisition specialists, system integrators, network providers, and software/hardware suppliers. The organizational and process-level interactions between these constituencies are used to plan, build, manage, maintain, and defend the cyber infrastructure."*

While most cybersecurity incidents are attributable to online attacks, countless examples used insecure cyber supply chains, introducing new types of risks, threats, vulnerabilities, and even cyber-attacks. For example:

- In 2008, the FBI seized $76 million of counterfeit Cisco equipment. According to an FBI presentation, the fake Cisco routers, switches, and cards were sold to the U.S. Navy, the U.S. Marine Corps., the U.S. Air Force, the U.S. Federal Aviation Administration, and even the FBI itself. One slide referred to the counterfeit Cisco equipment as a "critical infrastructure threat."
- Security researchers who analyzed the 2010 Stuxnet attack on Iranian nuclear facilities believe that malware used to infect programmable logic controllers (PLCs) and modify Siemens Step 7 software was likely carried into the facilities by third-party contractors working with the Iranian government. These third-party contractors were identified, attacked, and compromised and then unknowingly transported Stuxnet into the Iranian nuclear facilities, most likely through the use of USB thumb drives.
- In 2012, the Chairman and Ranking Member of the House Intelligence Committee, Mike Rogers (R-MI) and C.A. Dutch Ruppersberger (D-MD), released a report recommending that U.S. companies avoid using telecommunications equipment manufactured by Chinese telecommunications companies Huawei and ZTE. The report highlighted U.S. critical infrastructure interconnectivity and went on to warn of the heightened threat of cyber-espionage and predatory disruption or destruction of U.S. networks if U.S-based telecommunications networks were built by companies with known ties to the Chinese state, a country known to "aggressively steal valuable trade secrets and other sensitive data from American companies."
- According to documents leaked by Edward Snowden, the National Security Agency (NSA) intercepted networking equipment built in the United States, added backdoors for remote access capabilities, and then shipped these devices to their recipients abroad. When the hacked networking equipment was deployed online, it was programmed to phone home to NSA-controlled servers. "In one recent case, after several months a beacon implanted through supply-chain interdiction called back to the NSA covert infrastructure," said Glenn Greenwald, a reporter at the Guardian at the time. Greenwald further quoted the leaked NSA report: "This call back provided us (i.e., NSA) with access to further exploit the device and survey the network."
- The 2013 data breach at U.S. retailer Target exposed the personal and credit card data of more than 110 million consumers. Security researchers believe that this attack began with a spear phishing attack on a Target HVAC contractor, Fazio Mechanical, of Sharpsburg, PA. Cyber-attackers used an e-mail message to compromise a PC at Fazio Mechanical a few months before the attack and then downloaded password-stealing malware onto the system. The perpetrator then used legitimate Fazio credentials to log onto the Target network and ultimately carry out the attack.

While cyber supply chain security incidents like these threaten businesses and consumers alike, any type of cyber-attack on critical infrastructure organizations could result in massive societal disruption threatening national security. These concerns are exacerbated by numerous events such as:

- **The Siberian gas pipeline explosion of 1982.** In 1982, CIA agents learned of a Russian plot to steal western technologies for updating its outdated gas pipeline system. Armed with this knowledge, the CIA intervened with a covert operation. Unbeknownst to Soviet agents, software stolen in France was actually boobytrapped by the CIA and programmed to create havoc in a series of pumps, values, and turbines and increase pressure across the entire pipeline. Once installed, the malicious software caused a massive explosion. Leaked government documents referred to this event as, "the most monumental non-nuclear explosion ever seen from space," in the summer of 1982.

- **The Aurora test of 2007.** In 2007, Idaho National Labs ran an experiment called Aurora. The experiment simulated a cyber-attack and used a computer program to rapidly open and close a diesel generator's circuit breakers so they were out-of-phase from the rest of the electric grid. In a now famous video, this remote attack caused a 2.25 megawatt diesel generator to bounce, shake, smoke, and eventually blow up. The entire process took less than three minutes, but researchers believe that a true cyber-attack could have destroyed the generator in less time. This experiment proved that a knowledgeable cyber-adversary could cause massive disruptions to the U.S. power grid. Furthermore, a diesel generator like the one destroyed in this experiment could take months to build, ship, and replace, meaning that a cyber-attack like Aurora could have long-term national security implications.
- **The cyber-attacks on Estonia in 2007.** In 2007, the Estonian government removed a Soviet-era statue, the Bronze Soldier of Tallinn, from the city. This action was taken as an insult by Russian nationals within Estonia and some members of the Russian cybersecurity community within and outside the government. In April 2007, the small Baltic nation experienced a wave of devastating distributed denial-of-service (DDOS) attacks that disrupted the services of the Estonian banks, broadcasters, ministries, newspapers, and parliament. The Estonian attacks are sometimes referred to as the first documented acts of cyberwar.
- **The cyber-theft of the F-35 Joint Strike Fighter and other military secrets.** In 2015, NSA documents leaked by former contractor, Edward Snowden, revealed that cyber-attackers in China obtained more than 50 terabytes of data from U.S. defense contractors and government networks. This data included detailed plans about the F-35 Joint Strike Fighter's stealth radar and engine. By learning about these and other design points, Chinese defense companies were able to include similar designs and technologies in China's new stealth jet, the J-20. The secret also could allow Chinese air defenses to target the F-35 in a future conflict.

The potential for a devastating cyber-attack on U.S. critical infrastructure has had Washington's attention for a number of years. In 1998, Deputy Defense Secretary John Hamre cautioned the U.S. Congress about critical infrastructure protection (CIP) by warning of a potential "cyber Pearl Harbor." Hamre stated that a devastating cyber-attack "… is not going to be against Navy ships sitting in a Navy shipyard. It is going to be against commercial infrastructure."

After taking office, President Obama stated:

> *"From now on, our digital infrastructure, the networks and computers we depend on every day will be treated as they should be; as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy, and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."*

In 2012, defense secretary, Leon Panetta, echoed these earlier warnings, stating that the U.S. faced a potential "cyber Pearl Harbor," and was vulnerable to an increasing number of foreign hackers who could disrupt U.S.-based power grids, transportation networks, financial systems, and the government itself. Finally, in February 2015 at a cybersecurity summit held at Stanford University, President Obama announced five priorities to strengthen the U.S. approach to cybersecurity threats:

1. Protecting the country's critical infrastructure—our most important information systems—from cyber-threats.
2. Improving the country's ability to identify and report cyber-incidents so that we can respond in a timely manner.
3. Engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace.

4. Securing federal networks by setting clear security targets and holding agencies accountable for meeting those targets.
5. Shaping a cyber-savvy workforce and moving beyond passwords in partnership with the private sector.

There is clear evidence that the U.S. critical infrastructure faces a state of constant cyber-attack and a successful breach could have devastating consequences. Are critical infrastructure organizations adequately prepared to defend themselves? Do they have the right controls and oversight in place for cyber supply chain security? Are government agencies providing critical infrastructure organizations with the right programs and support? This ESG research report is intended to explore the answers to these important questions.

Report Conclusions

ESG surveyed 303 IT and cybersecurity professionals representing large midmarket (500 to 999 employees) organizations and enterprise-class (1,000 employees or more) organizations in the United States within 16 vertical industries designated as critical infrastructure by the U.S. Department of Homeland Security (DHS).

The survey focused on critical infrastructure organizations' current cybersecurity processes in general and cyber supply chain security awareness and safeguards in particular. Based on the data collected, ESG concludes:

- **The threat landscape has grown more dangerous for critical infrastructure organizations**. Nearly one-third (31%) of critical infrastructure organizations believe that the threat landscape (i.e., cyber-adversaries, cyber-attacks, exploits, malware, etc.) is much worse today than it was two years ago, while another 36% say that the threat landscape has grown somewhat worse in the past two years. Alarmingly, only 37% of critical infrastructure organizations rate their cybersecurity policies, processes, and technology safeguards as excellent and capable of addressing almost all of today's threats. The remaining 63% aren't nearly as confident.

- **Critical infrastructure organizations are under attack**. A majority (68%) of critical infrastructure organizations have experienced various cybersecurity incidents over the past two years, including compromises of an employee system, data breaches due to lost or stolen equipment, insider attacks, and breaches of physical security. Over one-third (36%) of these security incidents resulted in the disruption of a business process and/or critical operations. The ramification is clear: Cyber-attacks are already impacting critical infrastructure operations and could certainly disrupt services.

- **Cyber supply chain security is growing more difficult.** A majority (60%) of critical infrastructure organizations believe that cyber supply chain security is much more difficult or somewhat more difficult than it was two years ago. Of those that believe that cyber supply chain security has become more difficult, 44% equate this change to new types of IT initiatives that increased the cyber supply chain security attack surface, 39% say that they have more IT suppliers than two years ago, and 36% have consolidated IT and operational technology (OT) security, increasing cyber supply chain complexity.

- **IT vendor cybersecurity audits remain haphazard.** While more critical infrastructure organizations audit their IT supplier's security processes and metrics today than five years ago, audit processes remain somewhat ad-hoc. For example, only 14% of the critical infrastructure organizations surveyed audit the cybersecurity practices of all strategic IT infrastructure vendors, use standard processes for these IT vendor audits, and use the results of these audits as formal guidelines for IT procurement decisions. In spite of progress in IT security auditing over the past five years, many critical infrastructure organizations still treat IT vendor security as a check-box exercise rather than a serious risk management requirement.

- **Critical infrastructure organizations continue to employ risky IT technologies.** As evidence of continuing cyber supply chain security risk, 58% of critical infrastructure organizations admit that they use products or services from IT vendors that have product and/or internal process security issues that are cause for concern.

- **Third-party IT relationships exacerbate cyber supply chain risk.** Critical infrastructure services often rely on a vast network of connected organizations. Fifty eight percent of the organizations surveyed claim that they use IT services or business applications provided by third parties, while 48% provide IT service or business application access to third-party business partners. Of those critical infrastructure organizations with these types of external IT relationships, 38% provide IT access to more than 100 third-party organizations, while 27% consume IT services and business applications from more than 100 third parties. Most critical infrastructure organizations protect these third-party IT relationships with security controls and some oversight, but these safeguards are not nearly as formal or process-oriented as they should be.

- **Software security remains a major concern.** One-third of critical infrastructure organizations have experienced some type of security incident directly related to the compromise of internally developed software. This is particularly concerning since critical infrastructure services depend upon specialized processes often requiring homegrown software. To address software vulnerabilities, many critical infrastructure organizations have put secure software development processes in place, but only half of these firms implement these methodologies across the entire enterprise.
- **Critical infrastructure organizations want more help from Washington.** Only 22% of cybersecurity professionals working at critical infrastructure organizations believe that the U.S. government's cybersecurity strategy is extremely clear and thorough, while the remaining 88% are somewhat confused by Washington. Additionally, 45% believe that the U.S. government should be significantly more active with cybersecurity strategies and defenses. Those on the critical infrastructure cybersecurity front lines would like Washington to create better methods for sharing security intelligence with the private sector, black list IT vendors with poor cybersecurity track records, and limit government IT purchases to those vendors with demonstrably superior product and process security.

Introduction

Research Objectives

In order to explore cyber supply chain security practices and challenges further, ESG surveyed 303 IT and information security professionals representing large midmarket (500 to 999 employees) organizations and enterprise-class (1,000 employees or more) organizations in the United States within vertical industries designated as critical infrastructure by the U.S. Department of Homeland Security (DHS). All respondents were familiar with/responsible for their organization's information security policies and procedures, especially with respect to the procurement of IT products and services. Respondents also had to be familiar with cyber supply chain security as defined previously.

The survey was designed to answer the following questions:

1. Risk management
   - Has the organization experienced any security breaches? If so, what was the impact?
   - How would respondents rate the security threat landscape now compared with two years ago? Do respondents expect the threat landscape to get worse over the next two years?
   - How well prepared is the organization for the current threat landscape?
   - Is executive management supporting and investing in cybersecurity?
2. Procurement
   - How important are IT vendors' security processes in customers' procurement decisions?
   - Do critical infrastructure organizations audit the development processes of vendors before purchasing IT products? If so, is there a common model for these audits? Are these standard activities and processes across the enterprise?
   - Are vendor cybersecurity audits a critical component of IT procurement or do purchasing managers have the discretion to purchase from IT vendors with sub-par product and process security?
3. Software development
   - Do critical infrastructure organizations include security considerations as part of their standard software development processes?
   - Have organizations experienced any security breaches related to internally developed software vulnerability?
   - Do critical infrastructure organizations require their internal developers to be trained in secure software development?
   - When organizations outsource their software development, are secure development processes a requirement for external outsourcers and contractors?
4. External IT security
   - To what extent do critical infrastructure organizations currently open their IT systems to external parties such as customers, suppliers, and business partners?
   - To what extent do critical infrastructure organizations currently consume IT services and applications provided by external parties such as customers, suppliers, and business partners?
   - How are these relationships secured? Are there formal processes and safeguards in place?
5. The role of the U.S. Federal Government

- Do cybersecurity professionals working at critical infrastructure organizations understand the U.S. government's cybersecurity strategy?
- Do critical infrastructure organizations believe that the Federal Government should do more or less in terms of cybersecurity defenses and strategies?
- What if any specific actions should the Federal Government take?

Survey participants represented industries designated as critical infrastructure by the U.S. Department of Homeland Security (DHS). These industries include agriculture and food, banking and finance, communications, defense industrial base, energy (utilities, oil, and gas), transportation systems, water supply, health care, etc. For more details, please see the *Research Methodology* and *Respondent Demographics* sections of this report.

Research Findings

The Critical Infrastructure Cybersecurity Landscape

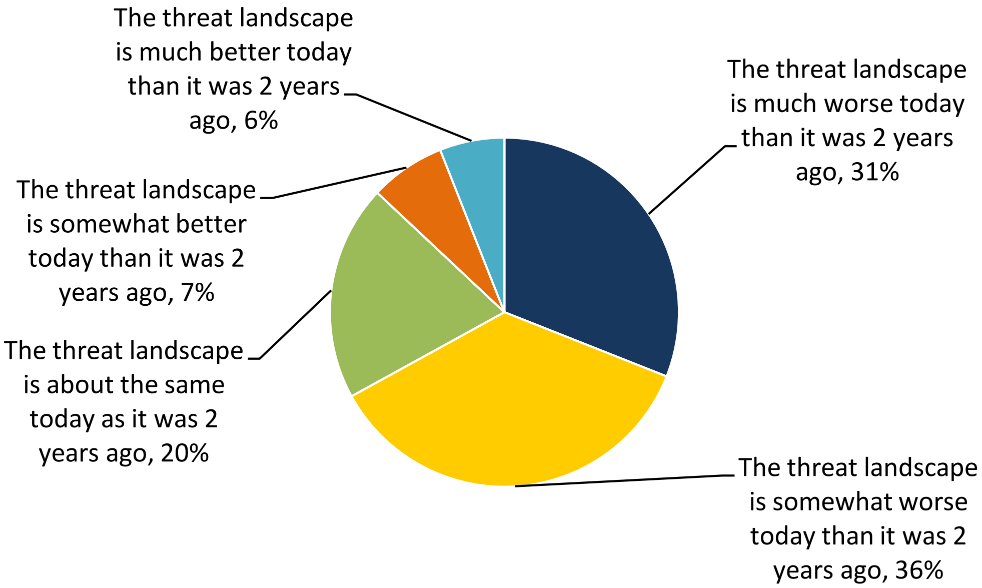
Today's Outlook on Cybersecurity Threats More Bleak than in 2013

Defending against cyber-attacks represents a perpetual battle for critical infrastructure organizations facing an increasingly dangerous threat landscape. In fact, 31% of security professionals working at critical infrastructure organizations believe that the threat landscape today is much worse than it was two years ago, while another 36% say it is somewhat worse (see Figure 1).

It is interesting to note that ESG asked this same question in its 2010 research project,[1] and it produced strikingly similar results—68% of respondents said that the threat landscape was worse in 2010 compared with 2008. Clearly, the threat landscape is getting more hazardous on an annual basis with no letup in sight. ESG finds this data particularly troubling. U.S. citizens depend upon critical infrastructure organizations for the basic necessities of modern society like food, water, fuel, and telecommunications services. Given the increasingly dangerous threat landscape, critical infrastructure organizations are tasked with maintaining important everyday services *and* defending their networks from a growing army of cyber-criminals, hacktivists, and nation state actors.

Figure 1. Current Threat Landscape Sentiment

How would you rate the current threat landscape (i.e., potential security threats such as malicious code attacks, DDoS, targeted attacks, cybercrime, state sponsored industrial espionage, etc.) faced by critical infrastructure industry organizations as compared to the last 2 years? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

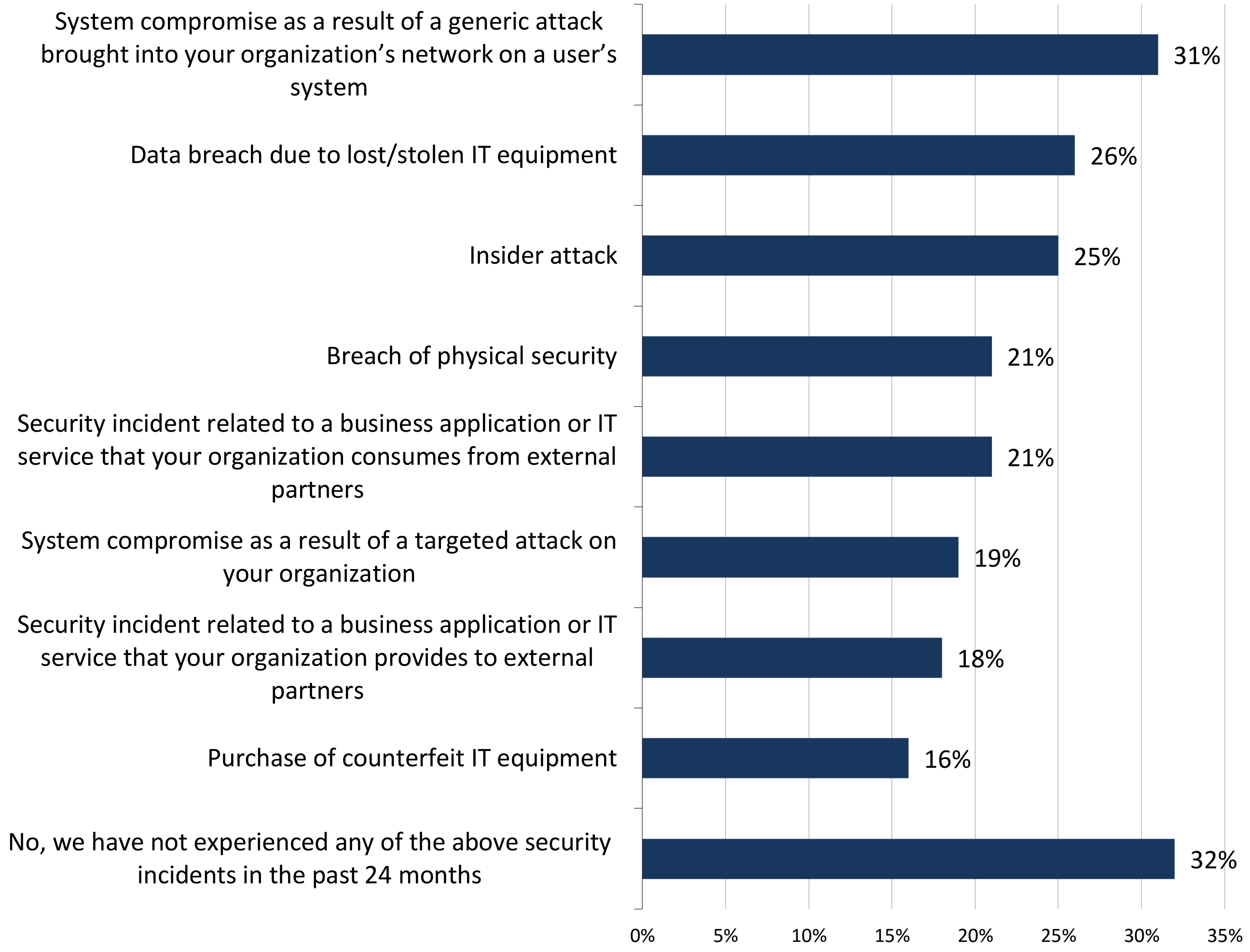
These beliefs about the increasingly dangerous threat landscape go beyond opinions alone as many critical infrastructure organizations face constant cyber-attacks. A majority (68%) of critical infrastructure organizations experienced a security incident over the past two years, with nearly one-third (31%) experiencing a system compromise as a result of a generic attack (i.e., virus, Trojan, etc.) brought in by a user's system, 26% reporting a data breach due to lost/stolen equipment, and 25% of critical infrastructure organizations suffering some type of

[1] Source: ESG Research Report, *Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure*, November 2010.

insider attack (see Figure 2). Alarmingly, more than half (53%) of critical infrastructure organizations have dealt with at least two of these security incidents since 2013.

Figure 2. Security Incidents Organizations Have Experienced Over the Past 24 Months

To the best of your knowledge, has your organization experienced any of the following security incidents over the past 24 months? (Percent of respondents, N=303, multiple responses accepted)



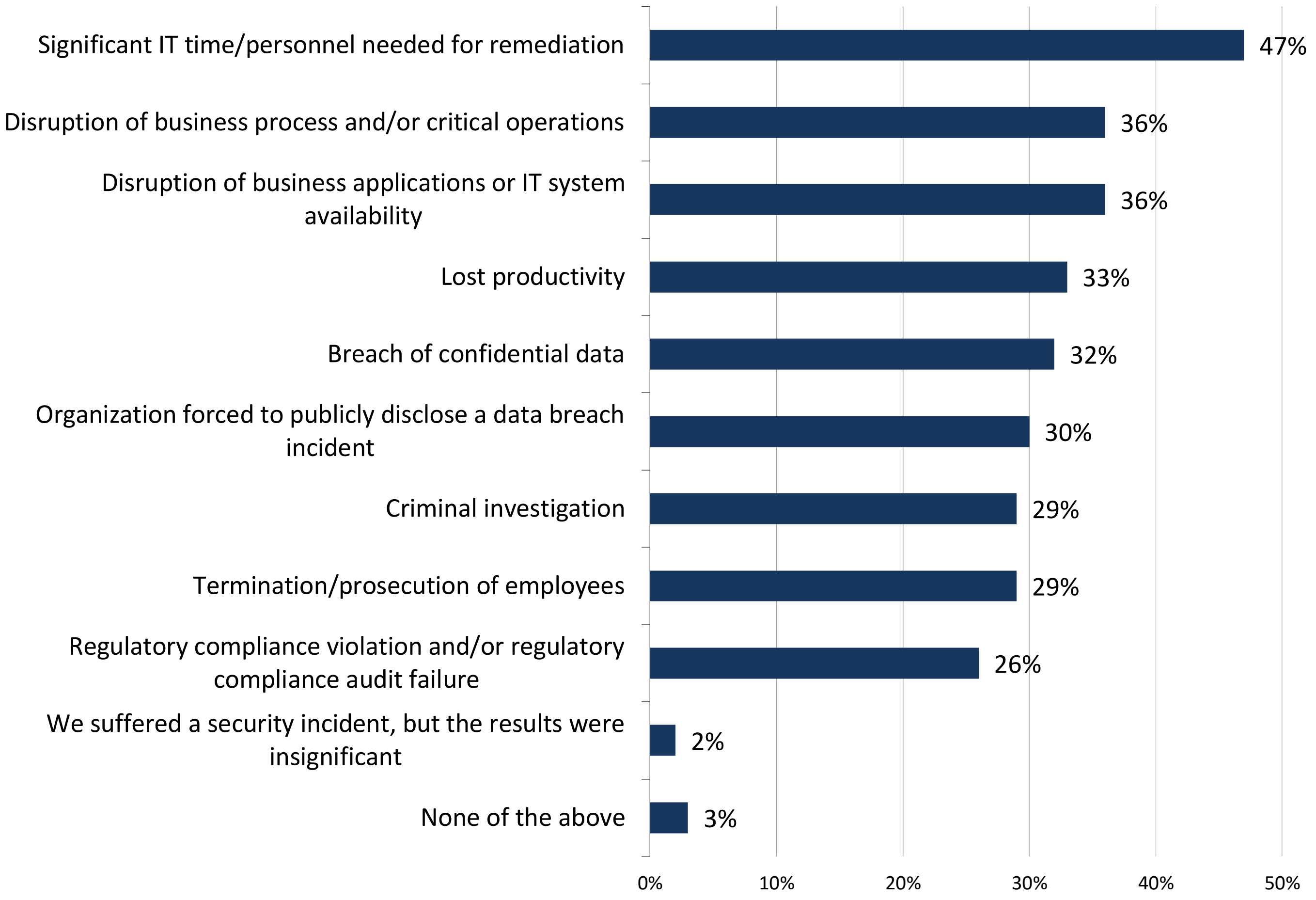
Source: Enterprise Strategy Group, 2015.

Security incidents always come with ramifications associated with time and money. For example, nearly half (47%) of cybersecurity professionals working at critical infrastructure organizations claim that security incidents required significant IT time/personnel for remediation. While this places an unexpected burden on IT and cybersecurity groups, other consequences related to security incidents were far more ominous—36% say that security incidents led to the disruption of a critical business process or business operations, 36% claim that security incidents resulted in the disruption of business applications or IT systems availability, and 32% report that security incidents led to a breach of confidential data (see Figure 3).

This data should be cause for concern since a successful cyber-attack on critical infrastructure organizations' applications and processes could result in the disruption of electrical power, health care services, or the distribution of food. Thus, these issues could have a devastating impact on U.S. citizens and national security.

Figure 3. Consequences of the Security Incidents Organizations Have Experienced Over the Past 24 Months

Which – if any – of the following consequences did your organization experience as a result of this security incident(s)? (Percent of respondents, N=203, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Cybersecurity at Critical Infrastructure Organizations

Do critical infrastructure organizations believe they have the right cybersecurity policies, processes, skills, and technologies to address the increasingly dangerous threat landscape? The results of that inquiry are mixed at best. On the positive side, 37% rate their organizations' cybersecurity policies, processes, and technologies as excellent and capable of addressing almost all of today's threats. It is worth noting that the overall ratings have improved since 2010 (see Table 1). While this improvement is noteworthy, 10% of critical infrastructure security professionals still rate their organization as fair or poor.

Being able to deal with most threats may be an improvement from 2010, but it is still not enough. This is especially true given the fact that the threat landscape has grown more difficult at the same time. Critical infrastructure organizations are making progress, but defensive measures are not progressing at the same pace as the offensive capabilities of today's cyber-adversaries and this risk gap leaves all U.S. citizens vulnerable.

Table 1. Respondents Rate Organization's Cybersecurity Policies

How would you rate your organization's security policies, procedures,and technology safeguards in their ability to address the current threat landscape?		
	2010 (N=285)	2015 (N=303)
Excellent, capable of addressing almost all of today's threats	22%	37%
Good, capable of addressing most of today's threats	56%	54%
Fair, capable of addressing only some of today's threats	18%	9%
Poor, capable of addressing few of today's threats	2%	1%
Don't know/no opinion	2%	0%

Source: Enterprise Strategy Group, 2015.

Given the national security implications of critical infrastructure, it is not surprising that cybersecurity risk has become an increasingly important board room issue over the past five years. Nearly half (45%) of cybersecurity professionals today rate their organization's executive management team as excellent, while only 25% rated them as highly in 2010 (see Table 2). Alternatively, 10% rate the executive management team's cybersecurity commitment as fair or poor in 2015, where 23% rated them so in 2010. These results are somewhat expected given the visible and damaging data breaches of the past few years. Critical infrastructure cybersecurity is also top of mind in Washington with legislators, civilian agencies, and the executive branch. For example, the 2014 National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) was driven by an executive order and is intended to help critical infrastructure organizations measure and manage cyber-risk more effectively. As a result of all of this cybersecurity activity, corporate boards are much more engaged in cybersecurity than they were in the past, but whether they are doing enough or investing in the right areas is still questionable.

Table 2. Respondents Rate Organization's Executive Management Team with Regard to Cybersecurity Initiatives

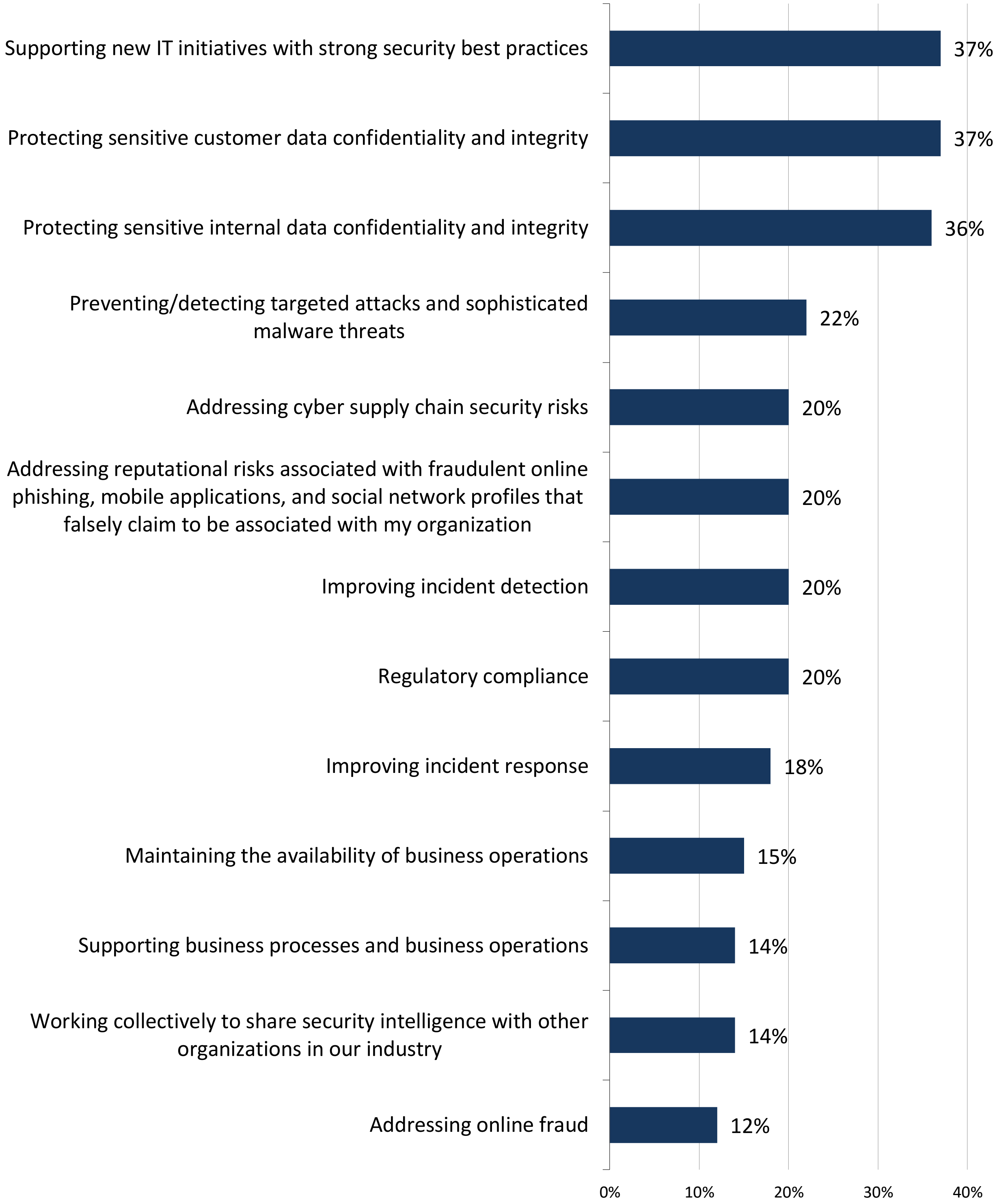
In your opinion, how would you rate your organization's executive management team on its willingness to invest in and support cybersecurity initiatives?		
	2010 (N=285)	2015 (N=303)
Excellent, executive management is providing the optimal level of investment and support	25%	45%
Good, executive management is providing an adequate level of investment and support, but we could use more	49%	45%
Fair, executive management is providing some level of investment and support, but we could use much more	21%	9%
Poor, executive management is not providing the right level of investment and support and we could use much more	2%	1%
Don't know/no opinion	3%	0%

Source: Enterprise Strategy Group, 2015.

Critical infrastructure organizations are modifying their cybersecurity strategies for a number of reasons. For example, 37% say that their organization's infosec strategy is driven by the need to support new IT initiatives with strong security best practices. This likely refers to IT projects for process automation that include Internet of Things (IoT) technologies. IoT projects can bolster productivity, but they also introduce new vulnerabilities and thus the need for additional security controls. Furthermore, 37% point to protecting sensitive customer data confidentiality and integrity, and 36% call out the need to protect internal data confidentiality and integrity (see Figure 4). These are certainly worthwhile goals, but ESG was surprised that only 22% of critical infrastructures say that their information security strategy is being driven by preventing/detecting targeted attacks and sophisticated malware threats. After all, 67% of security professionals believe that the threat landscape is more dangerous today than it was two years ago, and 68% of organizations have suffered at least one security incident over the past two years. Since critical infrastructure organizations are under constant attack, ESG feels strongly that CISOs in these organizations should be assessing whether they are doing enough to prevent, detect, and respond to modern cyber-attacks.

Figure 4. Primary Drivers of Organization's Cybersecurity Strategy

Which of the following factors are the primary drivers of your organization's information cybersecurity strategy? (Percent of respondents, N=303, three responses accepted)



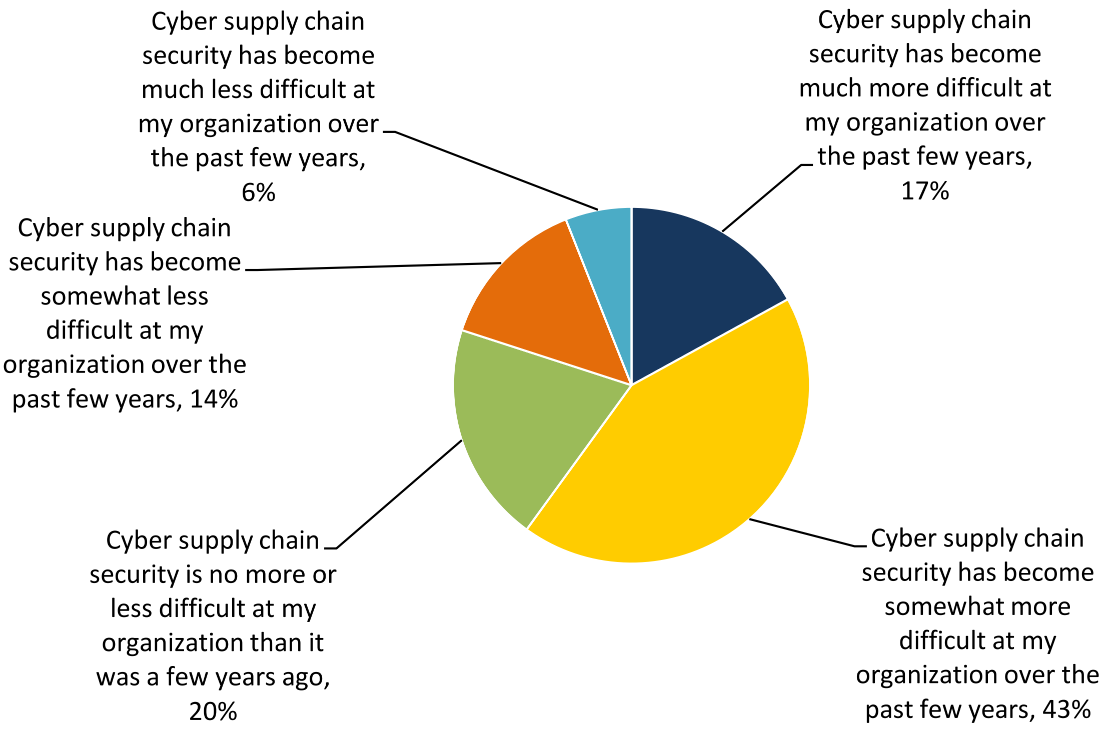
Source: Enterprise Strategy Group, 2015.

Cyber Supply Chain Security

Like many other areas of cybersecurity, cyber supply chain security is growing increasingly cumbersome. In fact, 60% of security professionals say that cyber supply chain security has become either much more difficult (17%) or somewhat more difficult (43%) over the last two years (see Figure 5).

Figure 5. Cyber Supply Chain Security Sentiment

Which of the following statements best reflects your opinion on the state of cyber supply chain security today? (Percent of respondents, N=303)

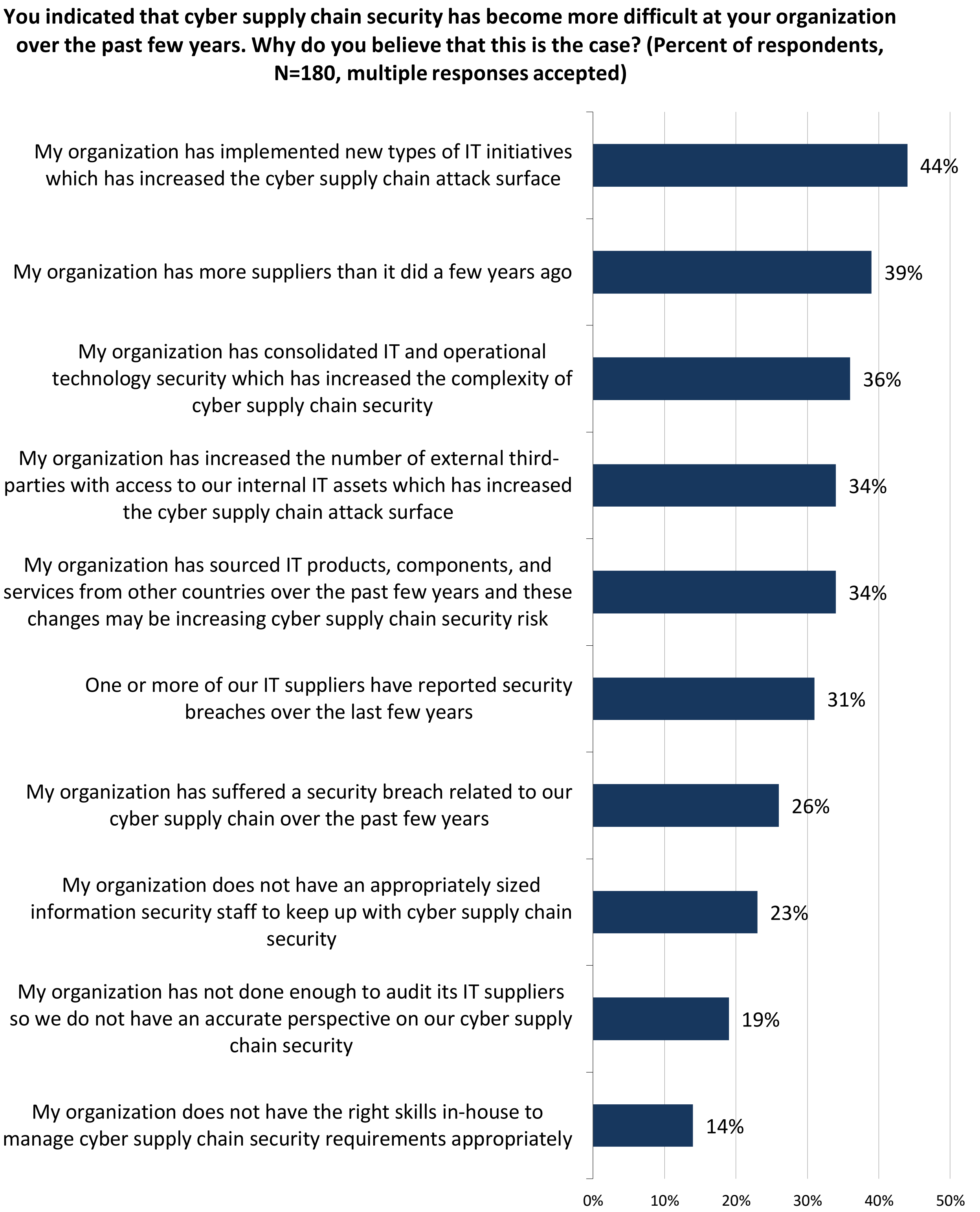


Source: Enterprise Strategy Group, 2015.

Why has cyber supply chain security become more difficult? Forty-four percent claim that their organizations have implemented new types of IT initiatives (i.e., cloud computing, mobile applications, IoT, big data analytics projects, etc.), which have increased the cyber supply chain attack surface; 39% say that their organization has more IT suppliers than it did two years ago; and 36% state that their organization has consolidated IT and operational technology security, which has increased infosec complexity (see Figure 6).

This data is indicative of the state of IT today. The fact is that IT applications, infrastructure, and products are evolving at an increasing pace, driving dynamic changes on a constant basis and increasing the overall cyber supply chain attack surface. Over-burdened CISOs and infosec staff find it difficult to keep up with dynamic cyber supply chain security changes, leading to escalating risks.

Figure 6. Why Organizations Believe Cyber Supply Chain Security Is Becoming More Difficult



Source: Enterprise Strategy Group, 2015.

Cyber Supply Chain Security and Information Technology

Cybersecurity protection begins with a highly secure IT infrastructure. Networking equipment, servers, endpoints, and IoT devices should be "hardened" before they are deployed on production networks. Access to all IT systems must adhere to the principle of "least privilege" and be safeguarded with role-based access controls that are audited on a continuous or regular basis. IT administration must be segmented through "separation of duties." Networks must be scanned regularly and software patches applied rapidly. All security controls must be monitored constantly.

These principles are often applied to internal applications, networks, and systems but may not be as stringent with regard to the extensive network of IT suppliers, service providers, business partners, contractors, and customers that make up the cyber supply chain. As a review, the cyber supply chain is defined as:

> *The entire set of key actors involved with/using cyber infrastructure: system end-users, policy makers, acquisition specialists, system integrators, network providers, and software/hardware suppliers. The organizational and process-level interactions between these constituencies are used to plan, build, manage, maintain, and defend the cyber infrastructure."*

To explore the many facets of cyber supply chain security, this report examines:

- The relationships between critical infrastructure organizations and their IT vendors (i.e., hardware, software, and services suppliers as well as system integrators, channel partners, and distributors).
- The security processes and oversight applied to critical infrastructure organizations' software that is produced by internal developers and third parties.
- Cybersecurity processes and controls in instances where critical infrastructure organizations are either providing third parties (i.e., suppliers, customers, and business partners) with access to IT applications and services, or are consuming IT applications and services provided by third parties (note: throughout this report, this is often referred to as "external IT").

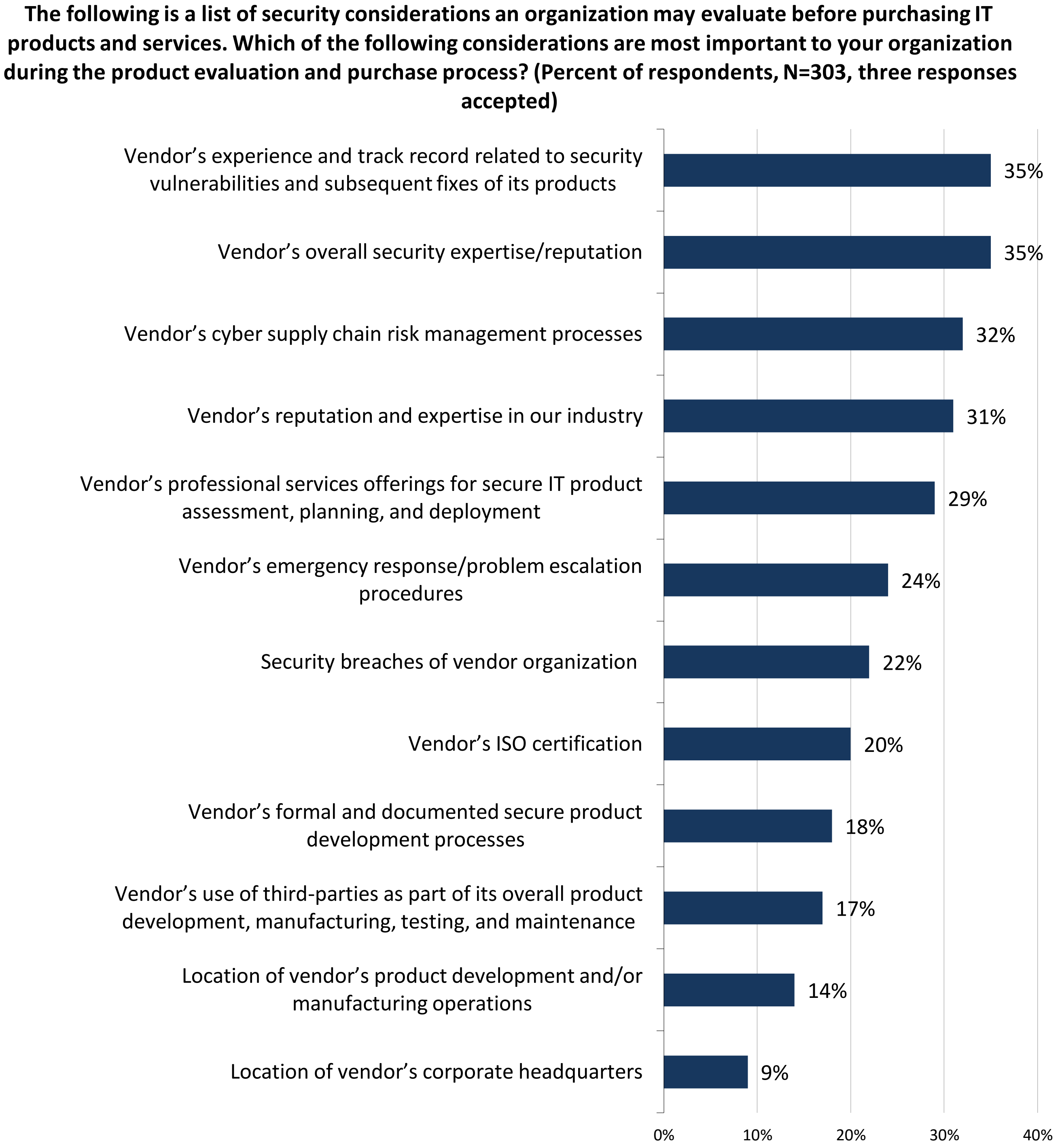
Cyber Supply Chain Security and IT Suppliers

Cybersecurity product vendors, service providers, and resellers are an essential part of the overall cyber supply chain. Accordingly, their cybersecurity policies and processes can have a profound downstream impact on their customers, their customers' customers, and so on. Given this situation, critical infrastructure organizations often include cybersecurity considerations when making IT procurement decisions.

Just what types of cybersecurity considerations are most important? More than one-third (35%) of organizations consider their vendors' experience and track record related to security vulnerabilities and subsequent fixes. In other words, critical infrastructure organizations are judging vendors by the quality of their software and their responsiveness in fixing software vulnerabilities when they do arise. Another 35% consider their vendors' overall security expertise and reputation. Close behind, 32% consider their vendors' cyber supply chain risk management processes, while 31% contemplate their vendors' reputation and industry expertise (see Figure 7).

Clearly, critical infrastructure organizations have a number of cybersecurity considerations regarding their IT vendors, but many of these concerns, such as vendor reputation and expertise, remain subjective. To counterbalance these soft considerations, CISOs should really establish a list of objective metrics such as the number of CVEs associated with specific ISV applications and the average timeframe between vulnerability disclosure and security patch releases. These types of metrics can be helpful when comparing one IT vendor's security proficiency against another's.

Figure 7. Most Important Security Considerations During Product Evaluation and Purchasing Processes



Source: Enterprise Strategy Group, 2015.

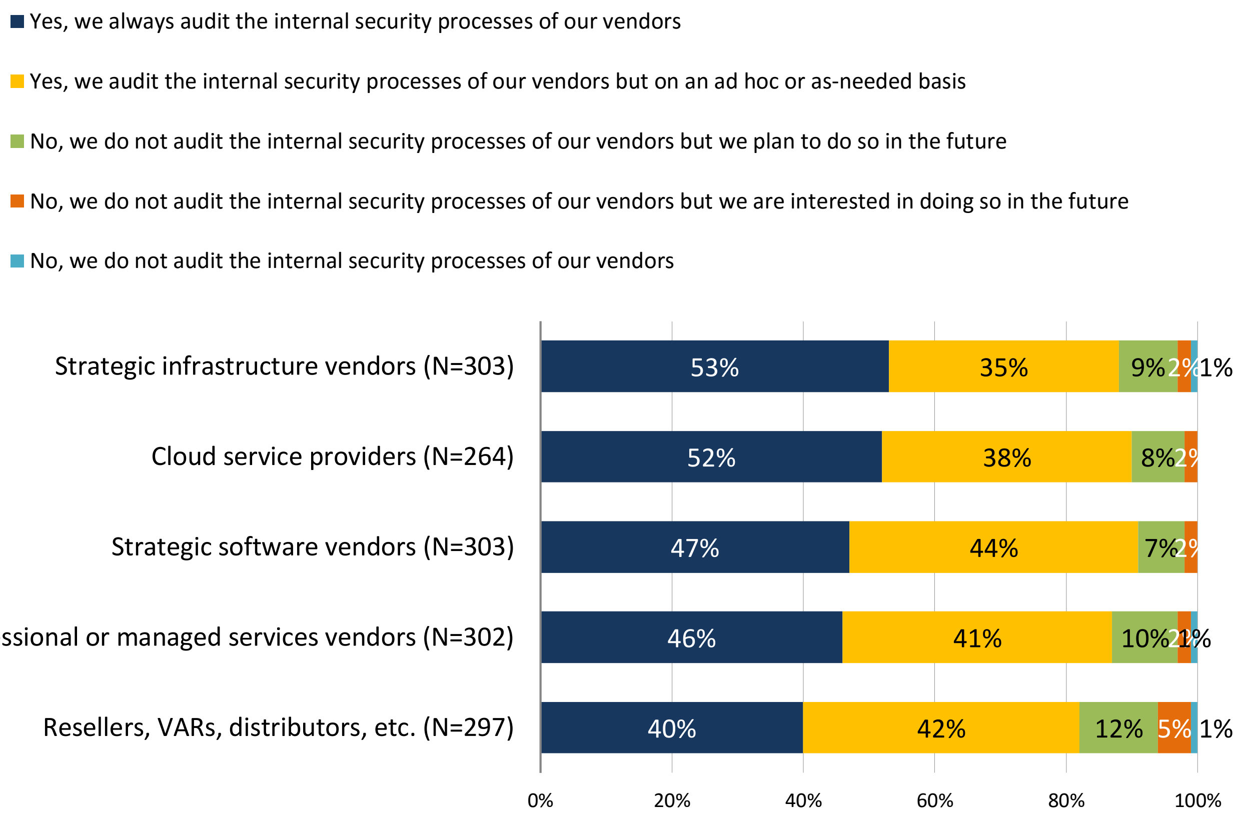
Cyber supply chain security best practices dictate that organizations assess the security processes, procedures, and technology safeguards used by all of their IT suppliers. In order to measure the cybersecurity practices of IT vendors, some critical infrastructure organizations conduct proactive security audits of cloud service providers, software providers, hardware manufacturers, professional services vendors that install and customize IT systems, and VARs/distributors that deliver IT equipment and/or services.

Are these security audits standard practice? ESG research reveals mixed results. On average, just under 50% of critical infrastructure organizations always audit all types of IT suppliers, a marked improvement from 2010 when

28% of critical infrastructure organizations always audited their IT suppliers. Nevertheless, there is still plenty of room for improvement. For example, 18% of organizations do not audit the security processes and procedures of resellers, VARs, and distributors at present. As the Snowden incident indicates, these IT distribution specialists can be used for supply chain interdiction for introducing malicious code, firmware, or backdoors into IT equipment to conduct a targeted attack or industrial espionage (see Figure 8).

Figure 8. Audits of Strategic Suppliers

Aside from assessing the security of IT products, some organizations audit the internal security processes and procedures of their strategic IT vendors. Audits can include areas such as vendors' software development security processes, vendors' supply chain security, and so on. To the best of your knowledge, does your organization audit the security processes and procedures of the following types of strategic IT vendors? (Percent of respondents)



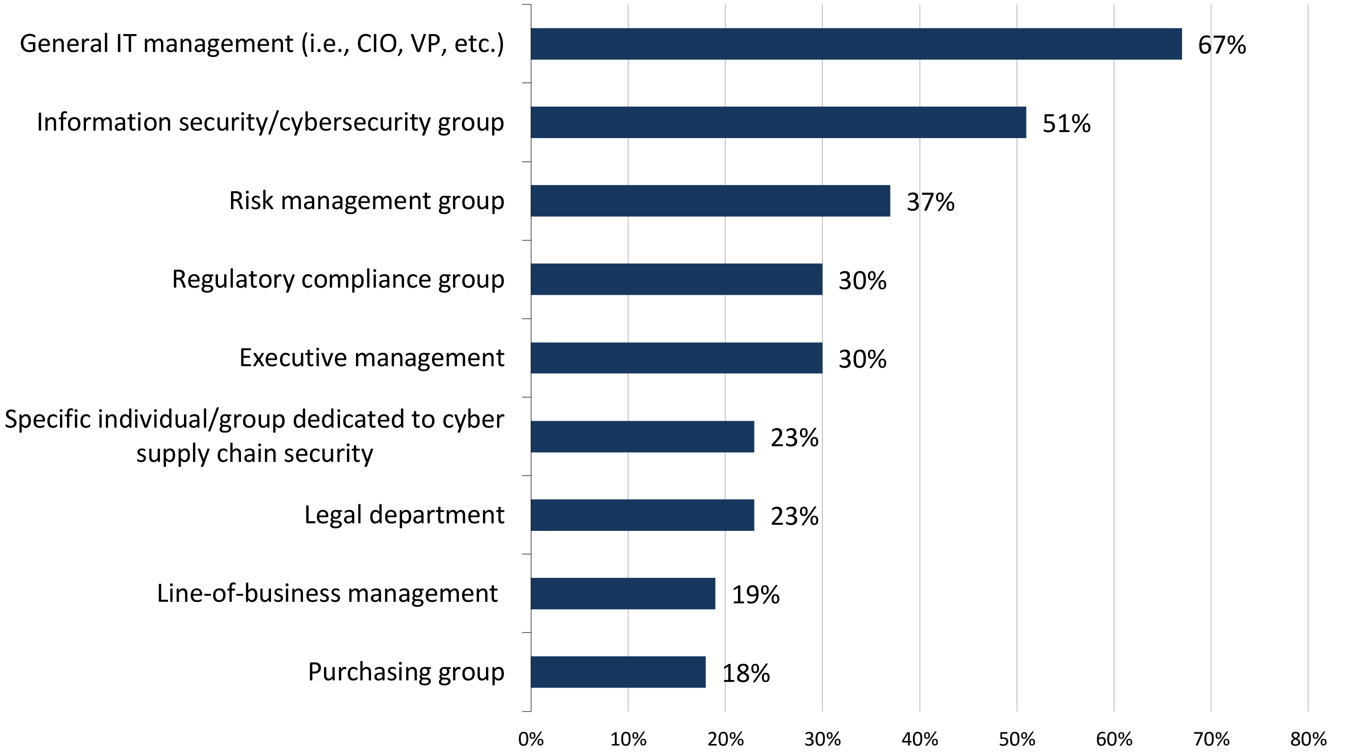
Source: Enterprise Strategy Group, 2015.

IT vendor security audits appear to be a shared responsibility with the cybersecurity team playing a supporting role. General IT management has some responsibility for assessing IT vendor security at two-thirds (67%) of organizations, while the cybersecurity team is responsible in just over half (51%) of organizations (see Figure 9).

These results are somewhat curious. After all, why wouldn't the cybersecurity team be responsible for IT vendor security audits in some capacity? Perhaps some organizations view IT vendor security audits as a formality, part of the procurement team's responsibility, or address IT vendor security audits with standard "checkbox" paperwork alone. Regardless of the reason, IT vendor security audits will provide marginal value without hands-on cybersecurity oversight throughout the process.

Figure 9. Internal Groups Responsible for IT Vendor Security Audit Processes

In your organization, which of the following groups are responsible for conducting, overseeing, and assessing IT vendor security audits? (Percent of respondents, N=294, multiple responses accepted)

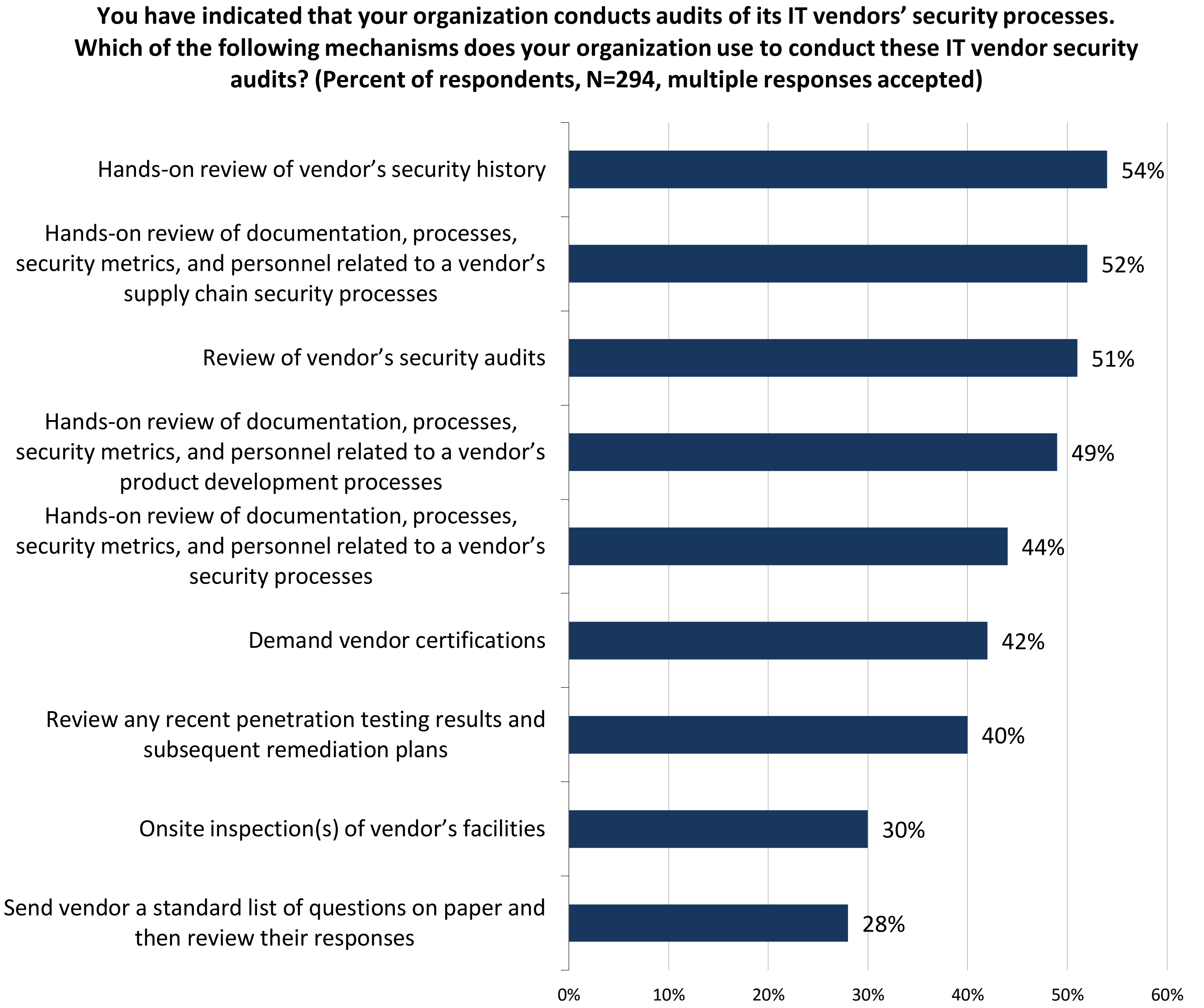


Source: Enterprise Strategy Group, 2015.

IT vendor security audits vary widely in terms of breadth and depth, so ESG wanted some insight into the most common mechanisms used as part of the audit process. Just over half (54%) of organizations conduct a hands-on review of their vendors' security history; 52% review documentation, processes, security metrics, and personnel related to their vendors' cyber supply chain security processes; and 51% review their vendors' internal security audits (see Figure 10).

Of course, many organizations include several of these mechanisms as part of their IT vendor security audits to get a more comprehensive perspective. Nevertheless, many of these audit considerations are based upon historical performance. ESG suggests that historical reviews be supplemented with some type of security monitoring and/or cybersecurity intelligence sharing so that organizations can better assess cyber supply chain security risks in real time.

Figure 10. Mechanisms Used to Conduct IT Vendor Security Audits



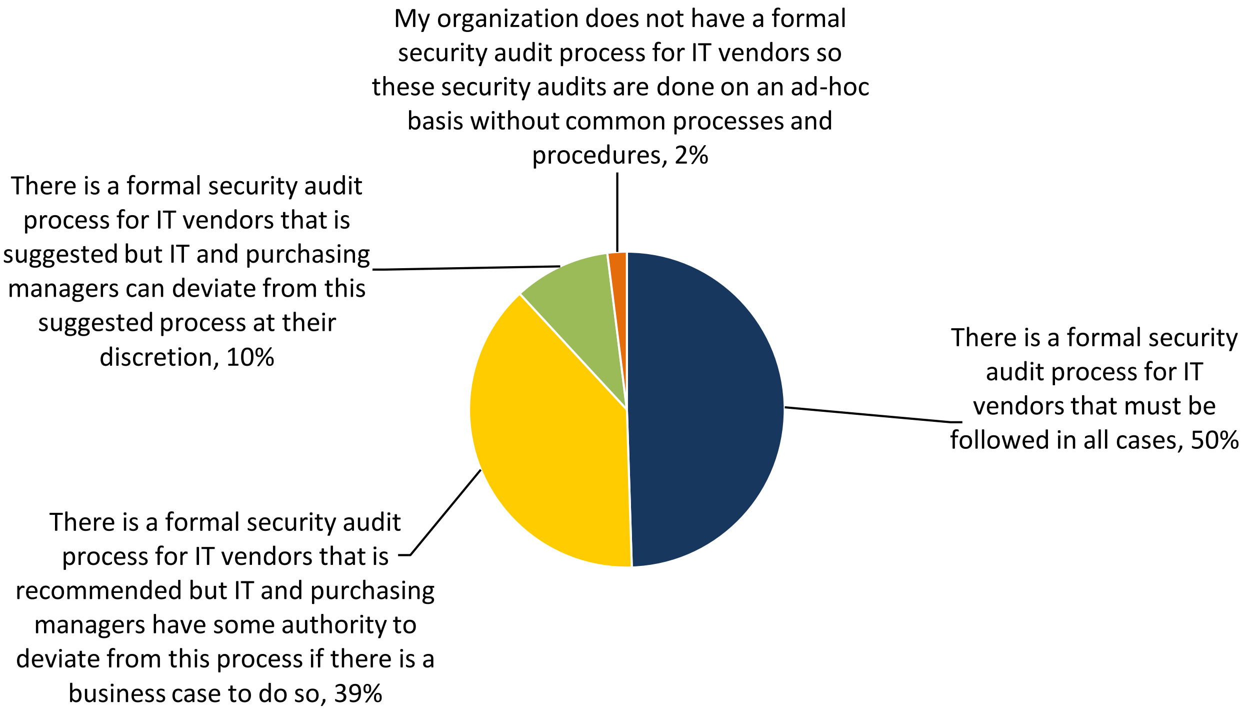
Source: Enterprise Strategy Group, 2015.

To assess the cybersecurity policies, processes, and controls with consistency, all IT vendor security audits should adhere to a formal, documented methodology. ESG research indicates that half of all critical infrastructure organizations conduct a formal security audit process in all cases, while the other half have some flexibility to deviate from formal IT vendor security audit processes on occasion (see Figure 11). It is worth noting that 57% of financial services organizations have a formal security audit process for IT vendors that must be followed in all cases, as opposed to 47% of organizations in other industries. This is another indication that financial services firms tend to have more advanced and stringent cybersecurity policies and processes than those from other industries.

IT vendor security audits involve data collection, analysis, evaluations, and final decision-making. From a scoring perspective, just over half (51%) of critical infrastructure organizations employ formal metrics/scorecards where IT vendors must attain a certain cybersecurity profile to qualify as an approved supplier. The remainder of critical infrastructure organizations have less stringent guidelines—32% have a formal vendor review process but no specific metrics for vendor qualification, while 16% conduct an informal review process (see Figure 12).

Figure 11. Current IT Vendor Security Audit Process

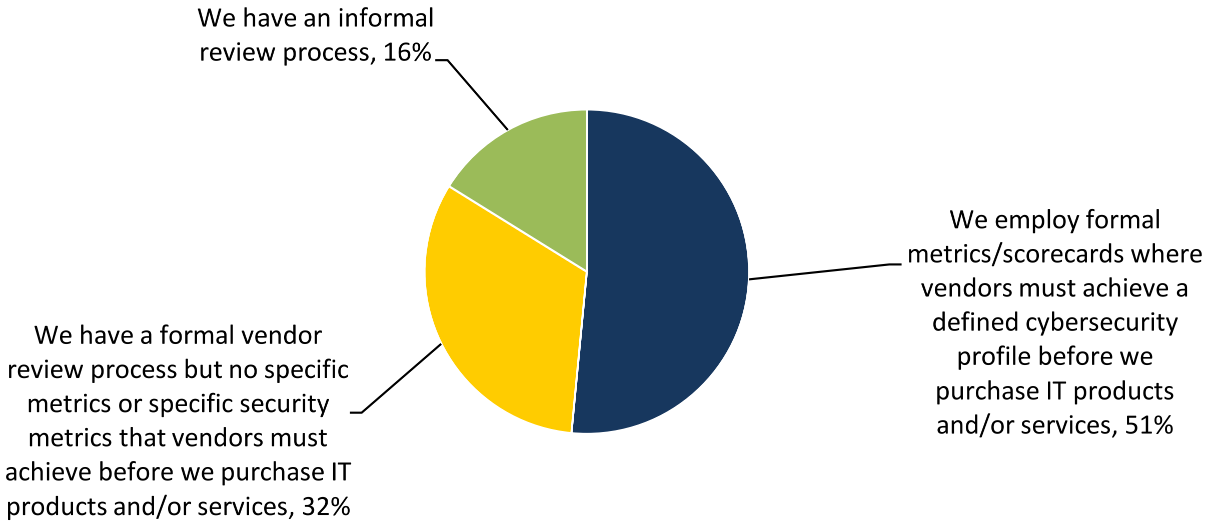
Which of the following statements best reflects your organization's current IT vendor security audit process? (Percent of respondents, N=294)



Source: Enterprise Strategy Group, 2015.

Figure 12. Measurement of IT Vendor Security Audits

How does your organization measure the results of these IT vendor cybersecurity audits? (Percent of respondents, N=294)



Source: Enterprise Strategy Group, 2015.

Overall, ESG research indicates that many critical organizations are not doing enough due diligence with IT vendor cybersecurity audits. To minimize the risk of a cyber supply chain security incident, vendor audit best practices would have to include the following three steps:

1. Organization *always* audits the internal security processes of strategic IT vendors.
2. Organization uses a formal standard audit process for all IT vendor audits.
3. Organization employs formal metrics/scorecards where IT vendors must exceed a scoring threshold to qualify for IT purchasing approval.

When ESG assessed critical infrastructure organizations through this series of IT vendor audit steps, the results were extremely distressing. For example, on average, only 14% of the total survey population adhered to all three best practice steps when auditing the security of their strategic infrastructure vendors (see Table 3). Since strategic infrastructure vendors are audited most often, it is safe to assume that less than 14% of the total survey population follows these best practices when auditing the security of software vendors, cloud service providers, professional services firms, and distributors.

Table 3. Incidence of Best Practices for IT Vendor Security Audits

Best Practice Step	Percentage of Total Survey Population
Organization *always* audits the internal security processes of strategic infrastructure vendors.	53%
Organization *always* audits the internal security processes of strategic infrastructure vendors AND organization uses a formal audit process for all vendor audits.	27%
Organization *always* audits the internal security processes of strategic infrastructure vendors AND organization uses a formal audit process for all vendor audits AND organization employs formal metrics/scorecards where IT vendors must exceed a scoring threshold to qualify for IT purchasing approval.	14%

Source: Enterprise Strategy Group, 2015.

It is also worth noting that ESG data shows marginal improvements regarding IT vendor security auditing best practices in the last five years. In 2010, only 10% of critical infrastructure organizations followed all six best practice steps, while 14% do so in 2015. Clearly, there is still a lot of room for improvement.

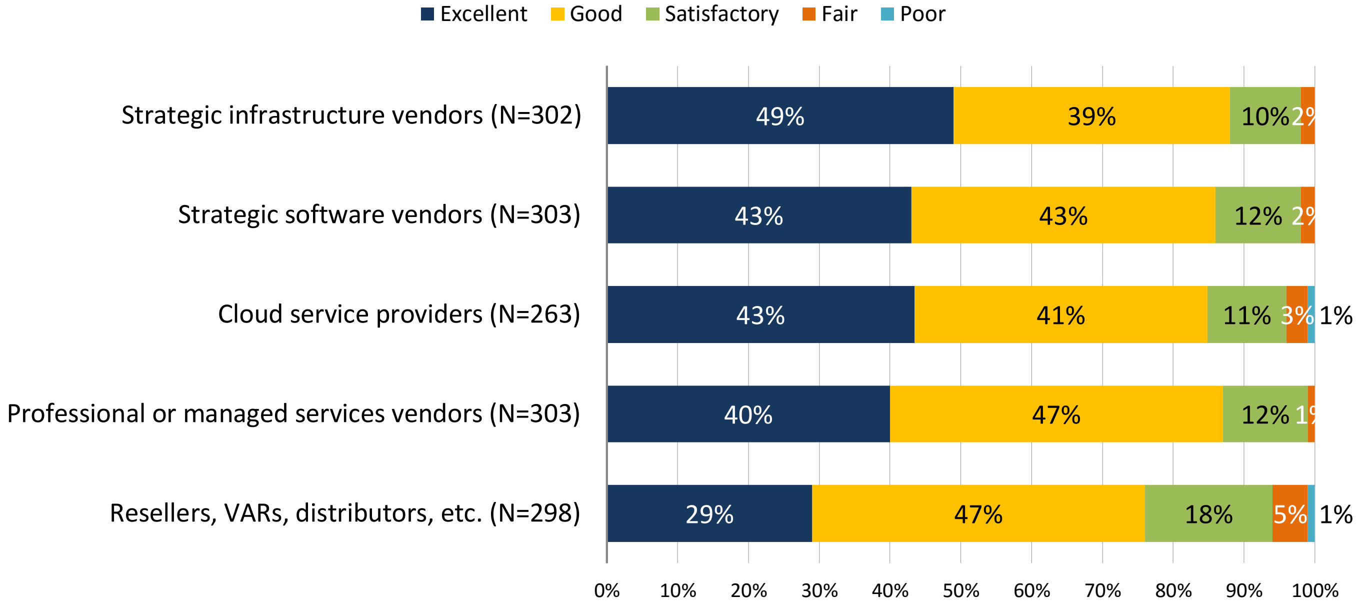
Regardless of security audit deficiencies, many critical infrastructure organizations are somewhat bullish about their IT vendors' security. On average, 41% of cybersecurity professionals rate all types of IT vendors as excellent in terms of their commitment to and communications about their internal security processes and procedures, led by strategic infrastructure vendors achieving an excellent rating from 49% of the cybersecurity professionals surveyed (see Figure 13).

Critical infrastructure organizations gave their IT vendors more positive security ratings in 2015 compared with 2010. For example, only 19% of critical infrastructure organizations rated their strategic infrastructure vendors as excellent in 2010 compared with 49% in 2015. Many IT vendors have recognized the importance of building cybersecurity into products and processes during this timeframe and are much more forthcoming about their cybersecurity improvements. Furthermore, critical infrastructure organizations have increased the amount of vendor security due diligence over the last five years, leading to greater visibility and improved vendor ratings.

The news isn't all good as at least 12% of critical infrastructure organizations are only willing to give their IT vendors' internal security processes and procedures a satisfactory, fair, or poor rating. ESG is especially concerned with ratings associated with resellers, VARs, and distributors since 24% of critical infrastructure organizations rate their internal security processes and procedures as satisfactory, fair, or poor. This is especially troubling since Figure 10 reveals that 18% of critical infrastructure organizations do not perform security audits on resellers, VARs, and distributors. Based upon all of this data, it appears that critical infrastructure organizations remain vulnerable to cybersecurity attacks (like supply chain interdiction) emanating from resellers, VARs, and distributors.

Figure 13. Respondents Rate IT Vendors' Commitment to/Communications about Internal Security Processes and Procedures

In your opinion, how would you rate your current IT vendors' commitment to and communications about their internal security processes and procedures? (Percent of respondents)



Source: Enterprise Strategy Group, 2015.

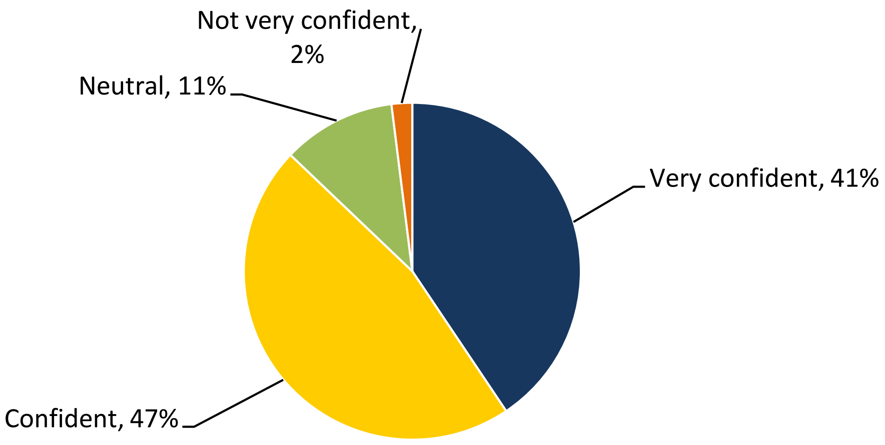
IT hardware and software is often developed, tested, assembled, or manufactured in multiple countries with varying degrees of patent protection or legal oversight. Some of these countries are known "hot beds" of cybercrime or even state-sponsored cyber-espionage. Given these realities, one would think that critical infrastructure organizations would carefully trace the origins of the IT products purchased and used by their firms.

ESG's data suggests that most firms are at least somewhat certain about the geographic lineage of their IT assets (see Figure 14). It should also be noted that there have been measurable improvements in this area as 41% of critical infrastructure organizations are very confident that they know the country in which their IT hardware and software products were originally developed and/or manufactured compared with only 24% in 2010. Once again, ESG attributes this progress to improvements in IT vendor security due diligence, greater supply chain security oversight within the IT vendor community, and increased overall cyber supply chain security awareness across the entire cybersecurity community over the past five years.

While cybersecurity professionals gave positive ratings to their IT vendors' security and are fairly confident about the origins of their IT hardware and software, they remain vulnerable because of insecure hardware and software that somehow circumvent IT vendor security audits, fall through the cracks, and end up in production environments. In fact, the majority (58%) of critical infrastructure organizations admit that they use insecure products and/or services that are a cause for concern (see Figure 15). One IT product or service vulnerability could represent the proverbial "weak link" that leads to a cyber-attack on the power grid, ATM network, or water supply.

Figure 14. Confidence Level in Organization's Knowledge of the Purchasing Origin of Hardware and Software

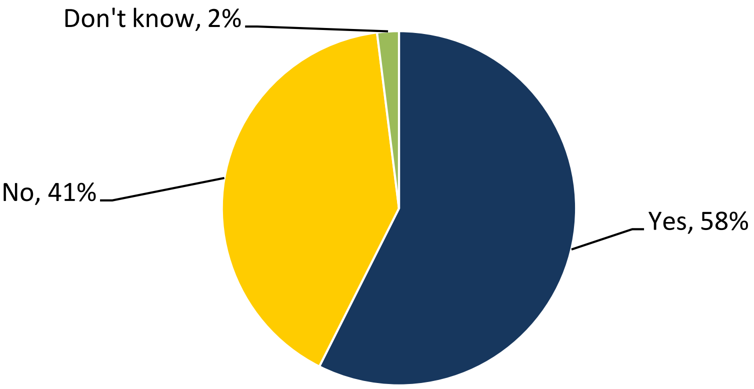
In your opinion, how confident are you that your organization knows where the IT hardware and software products it purchases (and all the sub-components of the software and hardware it purchases) were physically developed and/or manufactured (i.e., country of origin)? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

Figure 15. Use of Suspect Vendors

Does your organization use products or services from any IT vendors that have product and/or internal process security issues that are cause for concern to your organization? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

Cyber Supply Chain Security and Software Assurance

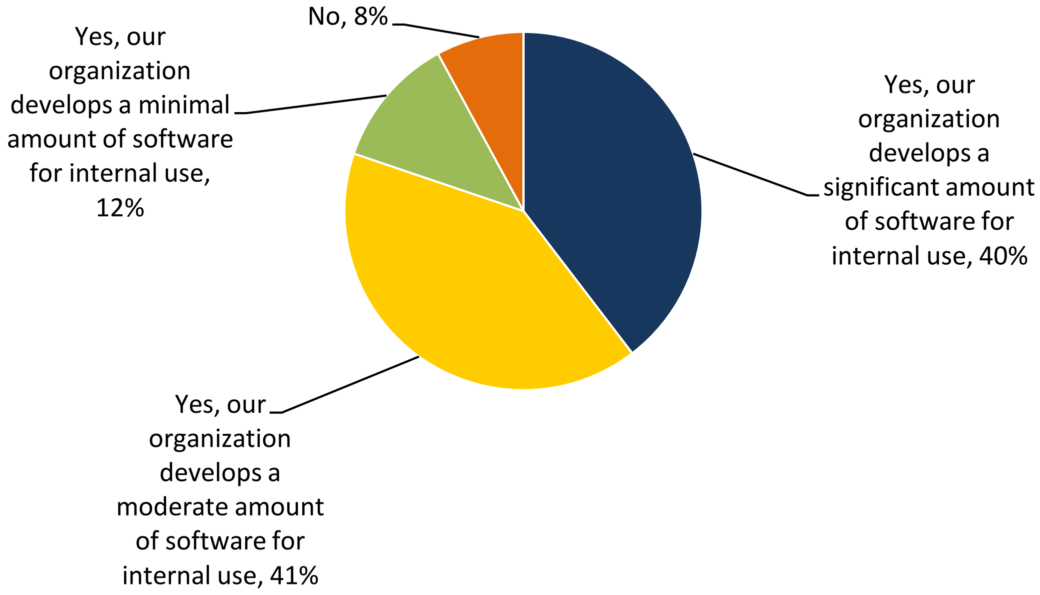
Software assurance is another key tenet of cyber supply chain security as it addresses the risks associated with a cybersecurity attack targeting business software. The U.S. Department of Defense defines software assurance as:

"The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner."

Critical infrastructure organizations tend to have sophisticated IT requirements, so it comes as no surprise that 40% of organizations surveyed develop a significant amount of software for internal use while another 41% of organizations develop a moderate amount of software for internal use (see Figure 16).

Figure 16. Internal Software Development

Does your organization write its own software in order to develop custom business applications for its own internal use? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

Software vulnerabilities continue to represent a major threat vector for cyber-attacks. For example, the [2015 Verizon Data Breach and Investigations Report]found that web application attacks accounted for 9.4% of incident classification patterns within the confirmed data breaches. Since any poorly written, insecure software could represent a significant risk to business operations, ESG asked respondents to rate their organizations on the security of their internally developed software. The results vary greatly: 47% of respondents say that they are very confident in the security of their organization's internally developed software, but 43% are only somewhat confident and another 8% remain neutral (see Figure 17).

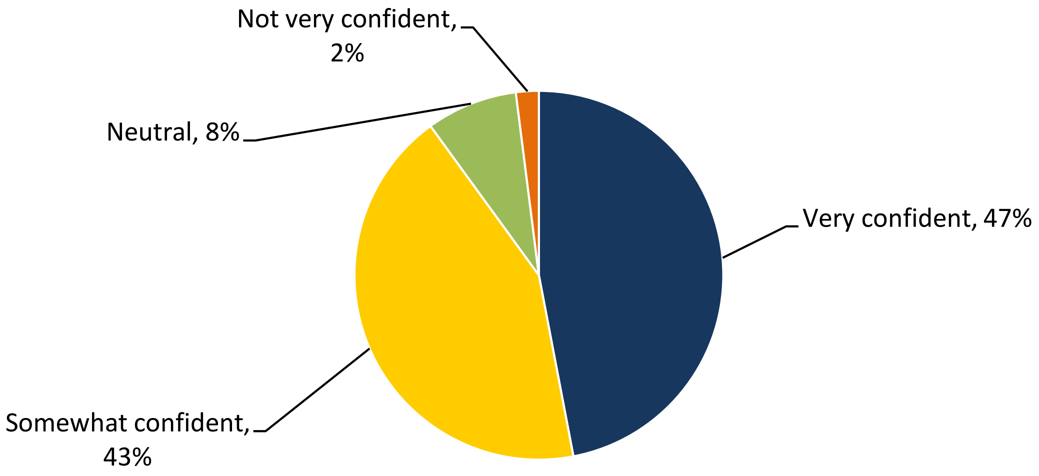
There is a slight increase in the confidence level over the past five years as 36% of cybersecurity professionals working at critical infrastructure organizations were very confident in the security of their organization's internally developed software in 2010 compared with 47% today. But this is a marginal improvement at best.

To assess software security more objectively, ESG asked respondents whether their organization ever experienced a security incident directly related to the compromise of internally developed software. As it turns out, one-third of critical infrastructure organizations have experienced one or several security incidents that were directly related to the compromise of internally developed software (see Figure 18).

From an industry perspective, 39% of financial services firms have experienced a security incident directly related to the compromise of internally developed software compared with 30% of organizations from other critical infrastructure industries. This happens in spite of the fact that financial services tend to have advanced cybersecurity skills and adequate cybersecurity resources. ESG finds this data particularly troubling since a cyber-attack on a major U.S. bank could disrupt the domestic financial system, impact global markets, and cause massive consumer panic.

Figure 17. Confidence Level in Security of Internally Developed Software

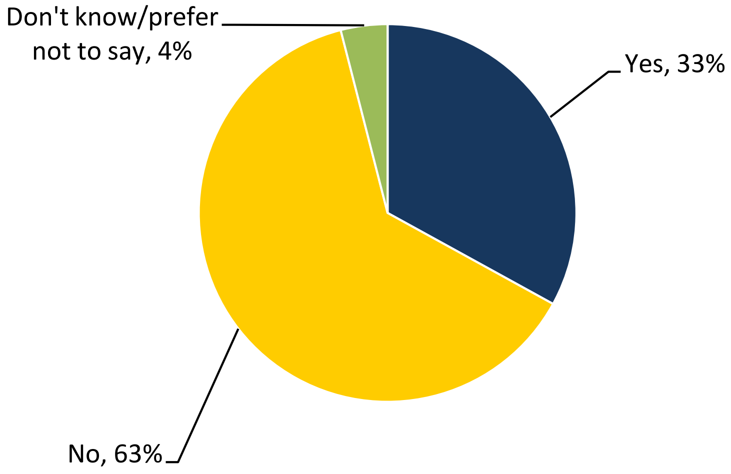
In general, how confident are you in the security of your organization's internally developed software (taking into account considerations such as secure design, attack surface area, coding quality, vulnerabilities, etc.)? (Percent of respondents, N=280)



Source: Enterprise Strategy Group, 2015.

Figure 18. Security Incidents Related to the Compromise of Internally Developed Software

To the best of your knowledge, has your organization ever experienced a security incident directly related to the compromise of internally developed software? (Percent of respondents, N=280)

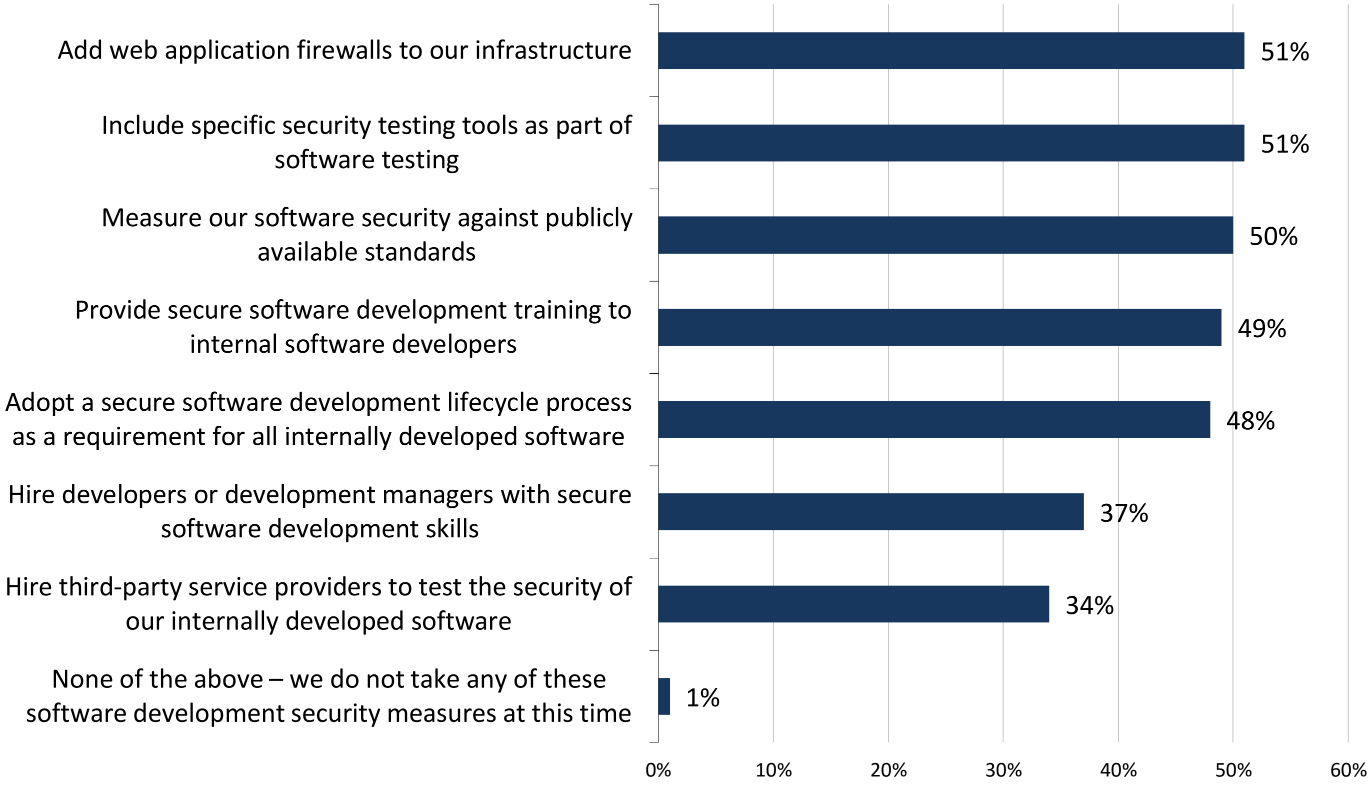


Source: Enterprise Strategy Group, 2015.

Critical infrastructure organizations recognize the risks associated with insecure software and are actively employing a variety of security controls and software assurance programs. The most popular of these is also the easiest to implement as 51% of the organizations surveyed have deployed application firewalls to block application-layer cyber-attacks such as SQL injections and cross-site scripting (XSS). In addition to deploying application firewalls, about half of the critical infrastructure organizations surveyed also include security testing tools as part of their software development processes, measuring their software security against publicly available standards, providing secure software development training to internal developers, and adopting secure software development lifecycle processes (see Figure 19). Of course, many organizations are engaged in several of these activities simultaneously in order to bolster the security of their homegrown software.

Figure 19. Security Activities Included as Part of the Software Development Process

Does your organization currently include any of the following security activities as part of its software development process? (Percent of respondents, N=280, multiple responses accepted)



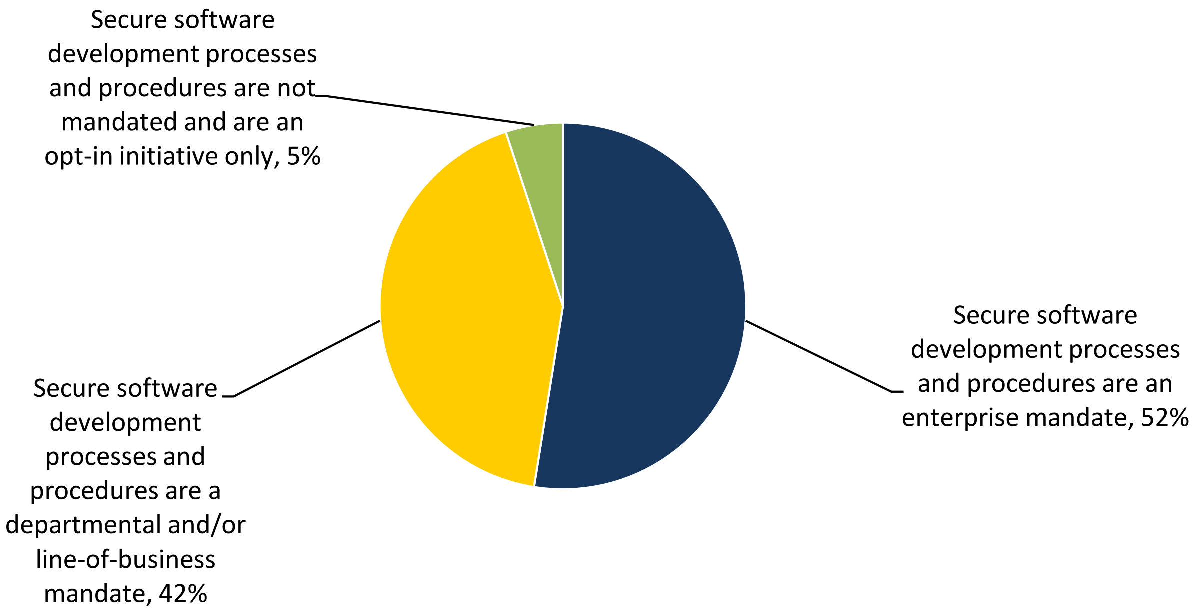
Source: Enterprise Strategy Group, 2015.

Secure software development programs are certainly a step in the right direction, but software assurance effectiveness is a function of two factors: the types of programs employed and the consistency of these programs. ESG research reveals that just over half of critical infrastructure organizations treat secure software development processes and procedures as an enterprise mandate, so it's likely that these firms have a consistent secure software development methodology across the organization.

Alternatively, 42% of the critical infrastructure organizations surveyed implement secure software development processes and procedures as departmental or line-of-business mandates (see Figure 20). Decentralized software security processes like these can lead to tremendous variability where some departments institute strong software assurance programs while others do not. Furthermore, secure software development programs can vary throughout the enterprise where one department provides training and formal processes while another simply deploys an application firewall. As the old saying goes, "One bad apple can spoil the whole bunch"—a single department that deploys insecure internally developed software can open the door to damaging cyber-attacks that impact the entire enterprise and disrupt critical infrastructure services like food distribution, health care, or telecommunications.

Figure 20. Secure Software Development Initiatives

Which of the following best describes the extent of your organization's secure software development initiatives? (Percent of respondents, N=279)



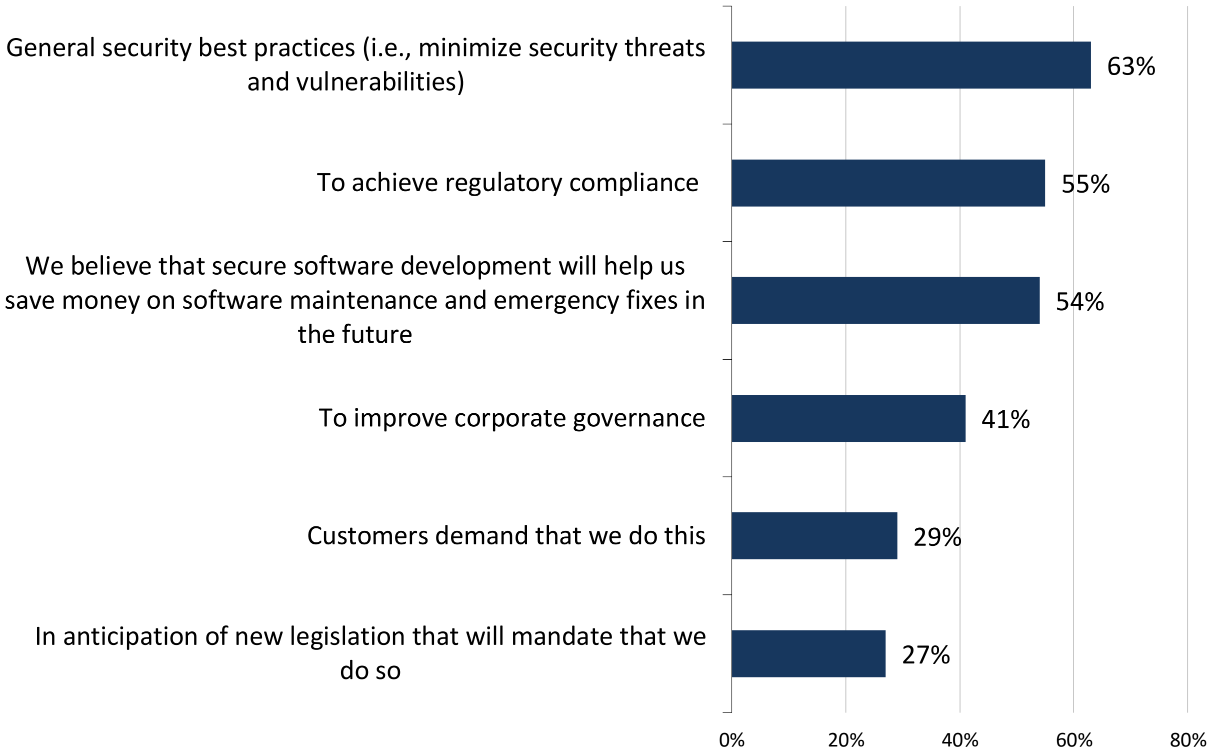
Source: Enterprise Strategy Group, 2015.

Critical infrastructure organizations are implementing secure software development programs for a number of reasons, including adhering to general cybersecurity best practices (63%), meeting regulatory compliance mandates (55%), and even lowering costs by fixing software security bugs in the development process (see Figure 21).

It is also worth noting that 27% of critical infrastructure organizations are establishing secure software development programs in anticipation of new legislation. These organizations may be thinking in terms of the NIST cybersecurity framework (CSF) first introduced in February 2014. Although compliance with the CSF is voluntary today, it may evolve into a common risk management and regulatory compliance standard that supersedes other government and industry regulations like FISMA, GLBA, HIPAA, and PCI-DSS in the future. Furthermore, the CSF may also become a standard for benchmarking IT risk as part of cyber insurance underwriting and may be used to determine organizations' insurance premiums. Given these possibilities, critical infrastructure organizations would be wise to consult the CSF, assess CSF recommendations for software security, and use the CSF to guide their software security processes and controls wherever possible.

Figure 21. Why Organizations Chose to Establish a Secure Software Development Program

In general, what would you say were the major reasons why your organization has chosen to establish a secure software development program? (Percent of respondents, N=279, multiple responses accepted)



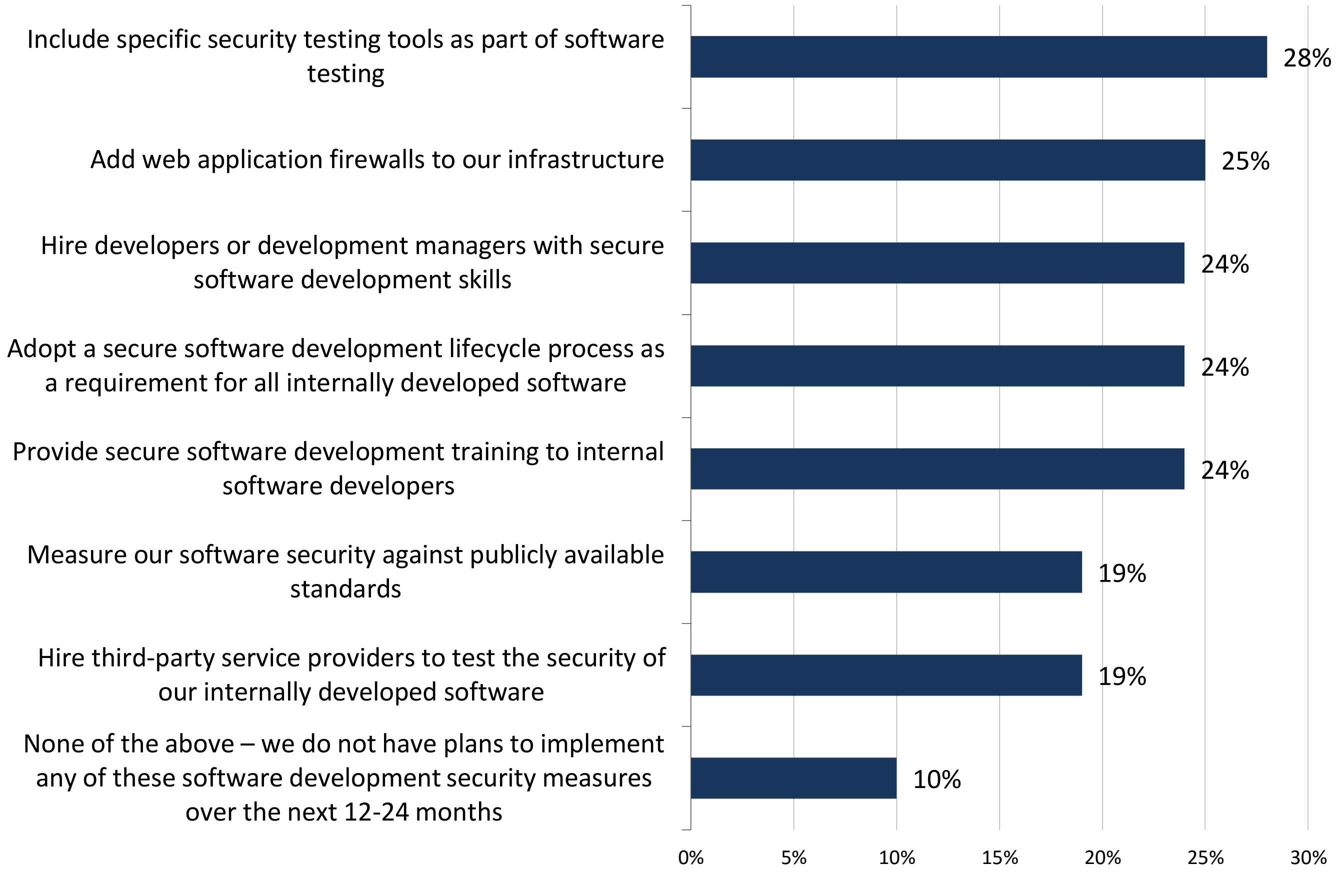
Source: Enterprise Strategy Group, 2015.

Aside from the ongoing software security actions taken today, critical infrastructure organizations also have future plans—28% plan to include specific security testing tools as part of software development, 25% will add web application firewalls to their infrastructure, and 24% will hire developers and development managers with secure software development skills (see Figure 22). These ambitious plans indicate that CISOs recognize their software development security deficiencies and are taking precautions in order to mitigate risk.

Some software development, maintenance, and testing activities are often outsourced to third-party contractors and service providers. This is the case at half of the critical infrastructure organizations that participated in this ESG research survey (see Figure 23).

Figure 22. Plans to Include Security Activities as Part of the Software Development Process

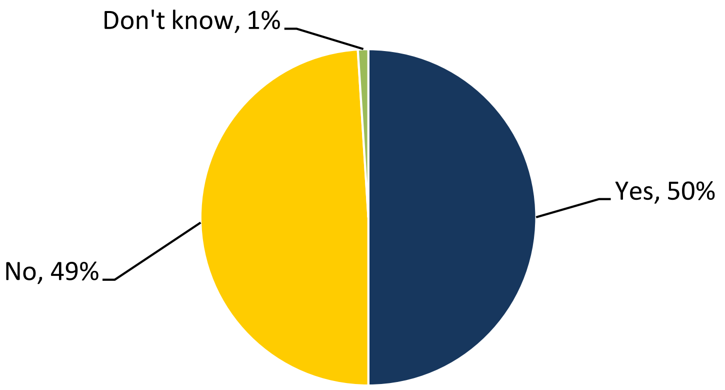
Will your organization include any of the following security activities as part of its software development process over the next 12 to 24 months? (Percent of respondents, N=271, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Figure 23. Outsourcing of Software Maintenance or Development Activities

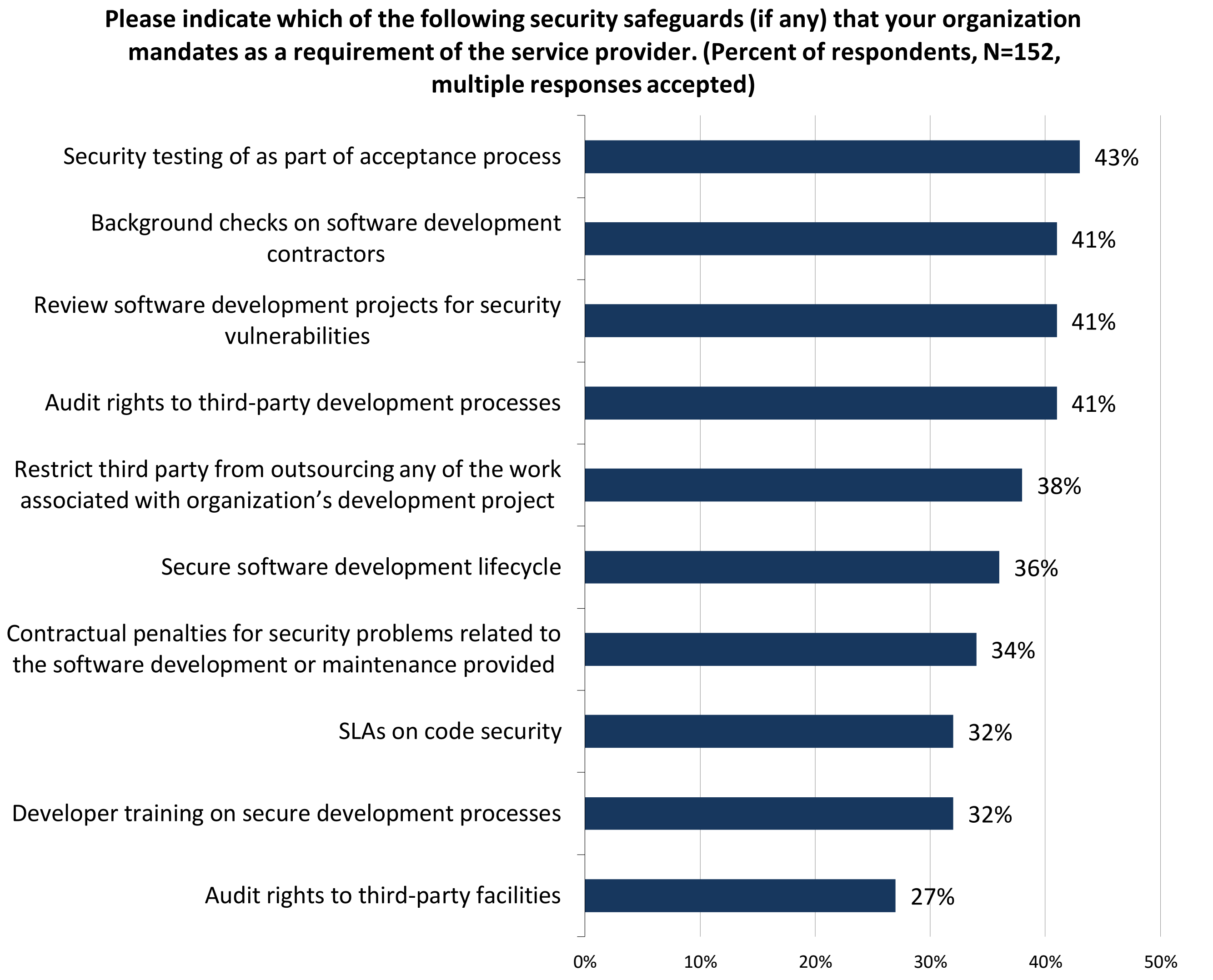
Does your organization outsource any of its software maintenance or development activities to third-party consultants, outsourcers, or service providers? (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

As part of these relationships, many critical infrastructure organizations place specific cybersecurity contractual requirements on third-party software development partners. For example, 43% mandate security testing as part of the acceptance process, 41% demand background checks on third-party software developers, and 41% review software development projects for security vulnerabilities (see Figure 24).

Figure 24. Security Safeguards Mandated of Service Providers



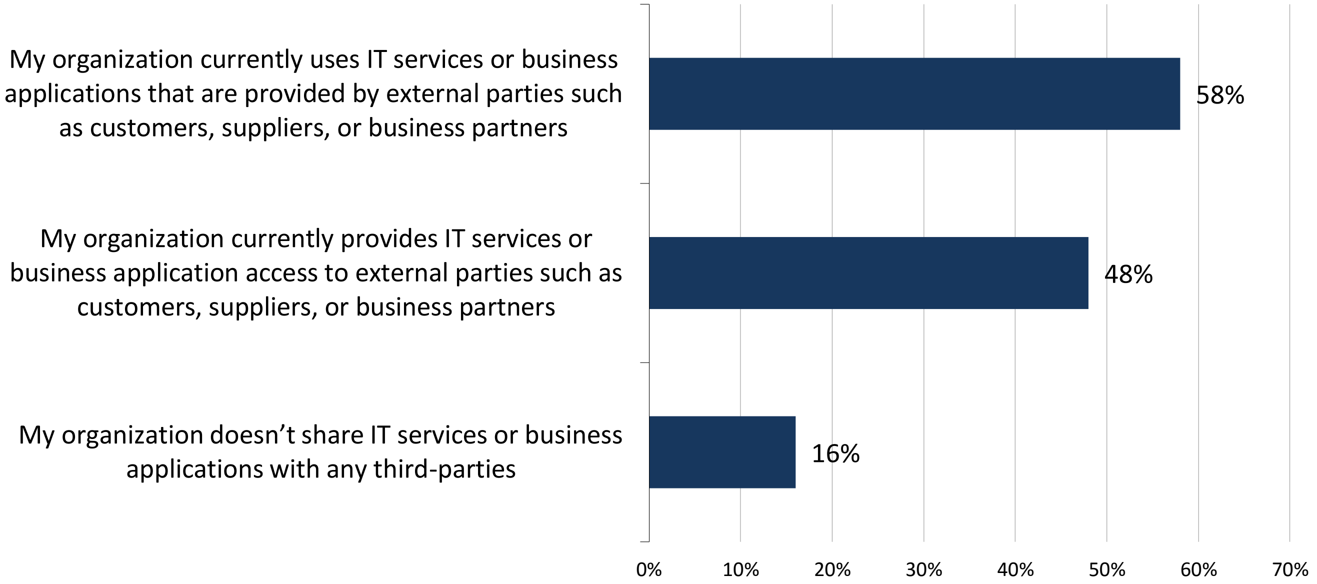
Source: Enterprise Strategy Group, 2015.

Information Technology Sharing Relationships

Critical infrastructure industry cyber supply chains can be extremely intricate where service delivery depends on a network of Internet-connected suppliers, customers, business partners, and other external parties supplying or consuming IT services from one another. This is certainly true with regard to the critical infrastructure organizations surveyed—58% of respondents say that their organization consumes IT services or business applications provided by external parties, while 48% of organizations provide IT services or business application access to external parties (see Figure 25). These relationships may be critical to producing products or delivering services but they also introduce a complex fabric of cyber supply chain risk.

Figure 25. Sharing of IT Services or Business Applications with Third Parties

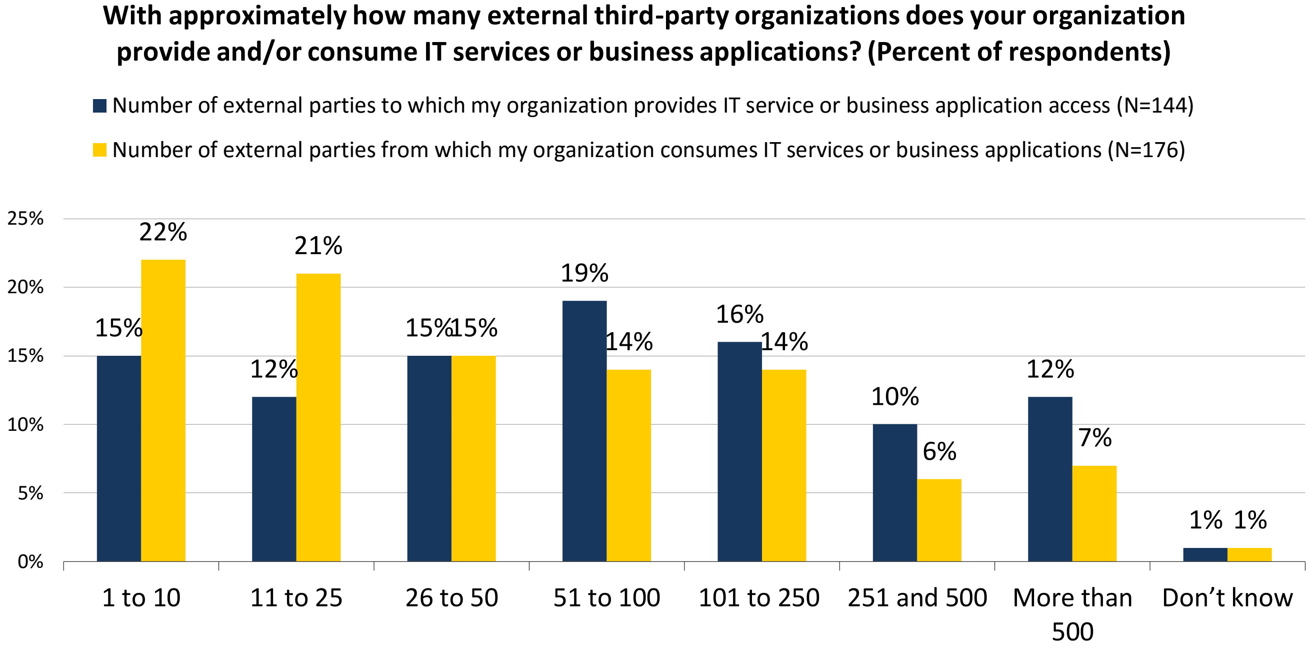
Please indicate which of the following statements are true for your organization. (Percent of respondents, N=303, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

According to ESG research, critical infrastructure organizations typically face extensive cyber supply chain security risk as 47% of those surveyed provide IT services and/or business application access to 50 or more external parties, while 41% of critical infrastructure organizations consume IT services and/or business application access from 50 or more external parties (see Figure 26).

Figure 26. Approximate Number of External Third Parties with which Respondent Organizations Share IT Services or Business Applications

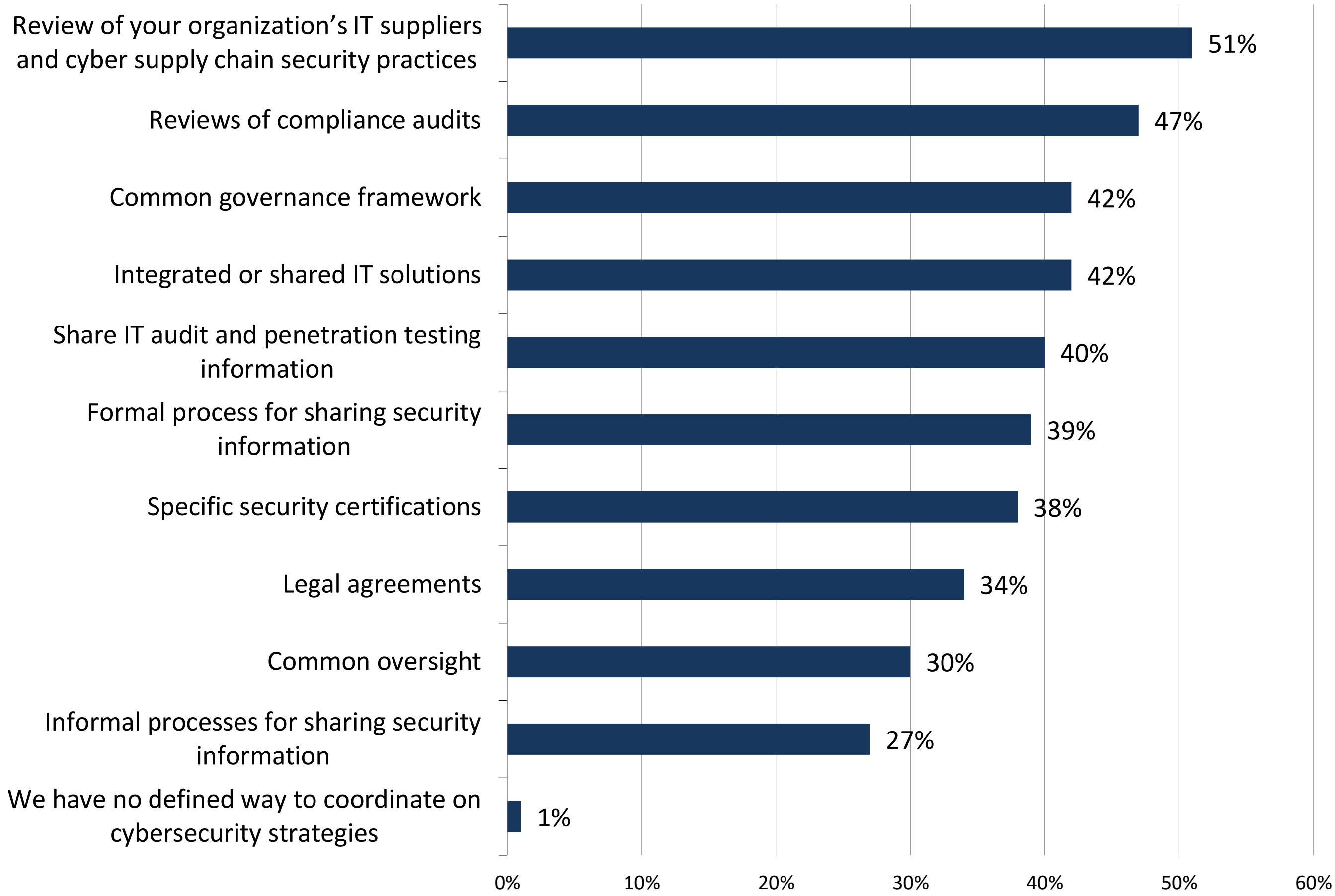


Source: Enterprise Strategy Group, 2015.

Third-party CISOs do have some security controls in place to mitigate the cyber supply chain risk associated with critical infrastructure organization connections. When critical infrastructure organizations are providing access to applications and services, third-party partners often require security controls such as a review of the organization's IT suppliers and cyber supply chain security practices (51%), review third-party organizations' regulatory compliance audits (47%), and mandate some type of common governance framework (42%) stipulating cybersecurity rules of engagement between the two parties (see Figure 27).

Figure 27. Security Controls Partners Require When Receiving IT Services or Business Applications from Critical Infrastructure Organizations

When your organization is providing IT services or business applications to external parties such as customers, suppliers, and business partners, which of the following security controls do your customers and partners typically require? (Percent of respondents, N=144, multiple responses accepted)



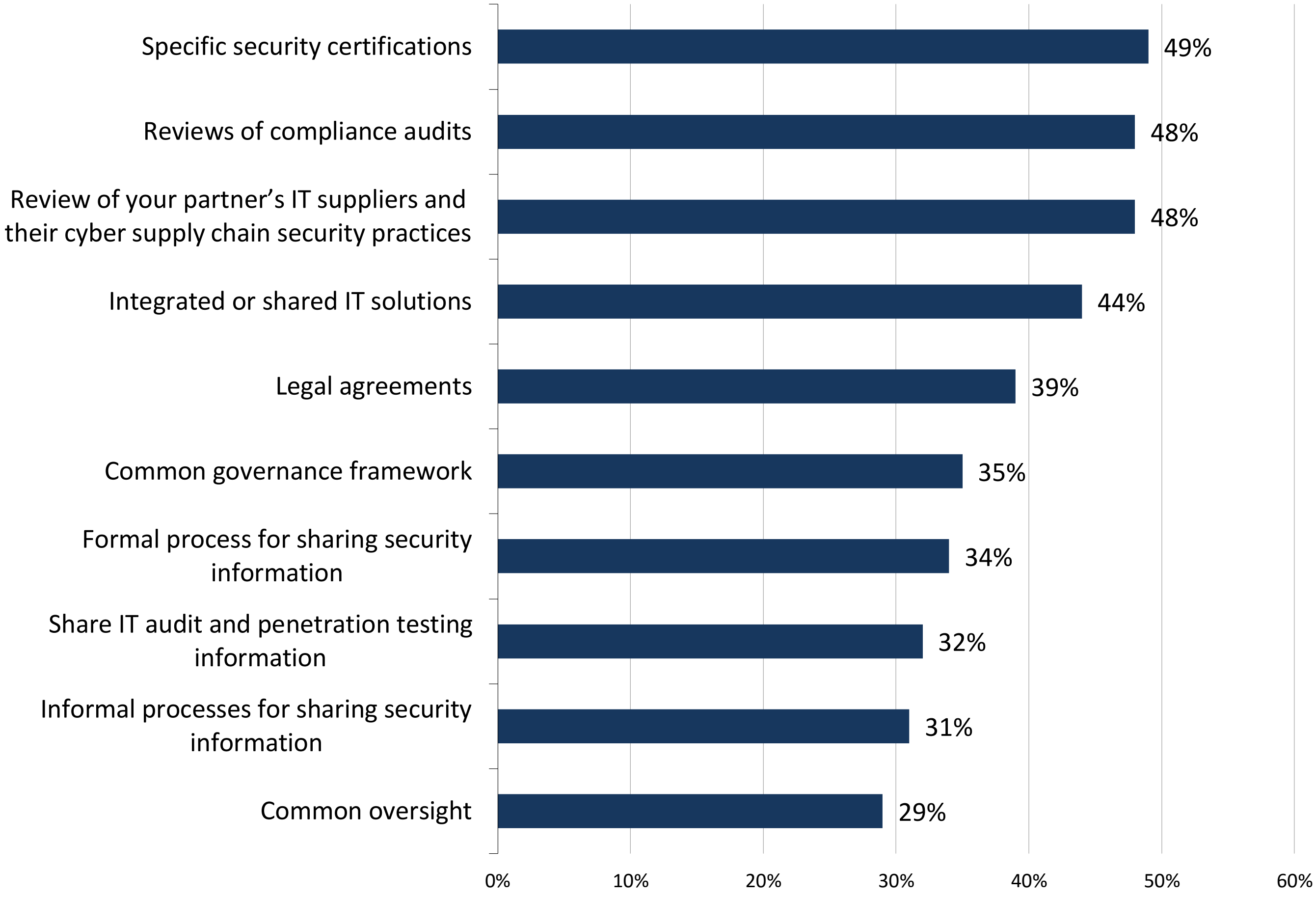
Source: Enterprise Strategy Group, 2015.

Critical infrastructure organizations have slightly different requirements when the roles are reversed and they are consuming IT services and business application access from third parties. Just under half (49%) require specific security certifications (i.e., ISO 9000, SAS 70, etc.), 48% ask for a review of compliance audits, and 48% review their partners' IT suppliers and cyber supply chain security practices (see Figure 28).

Certainly, many critical organizations have some oversight of third-party IT relationships, but the data points to haphazard oversight and policy enforcement once again. Business goals may be taking precedence over cybersecurity protection, exacerbating cyber supply chain risk.

Figure 28. Security Controls Critical Infrastructure Organizations Require When Using IT Services or Business Applications from Third Parties

When your organization is using IT services or business applications provided by external parties such as suppliers, and business partners, which of the following security controls does your organization typically require? (Percent of respondents, N=176, multiple responses accepted)



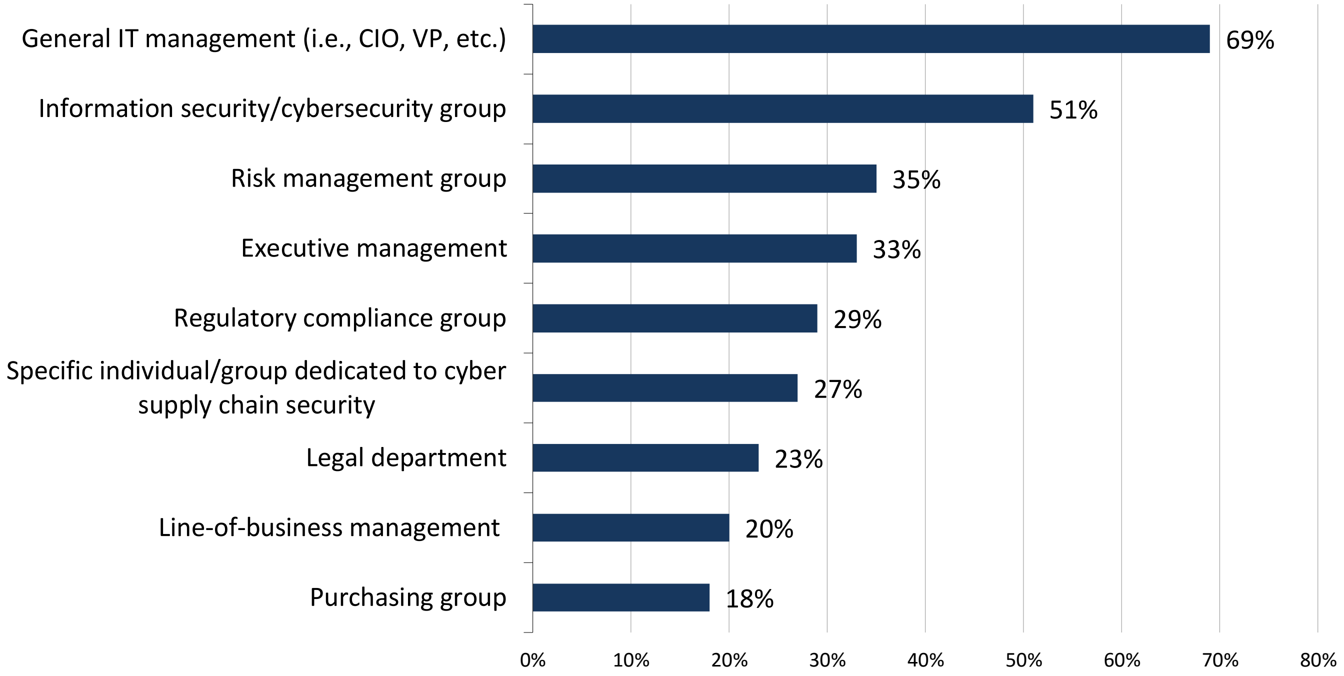
Source: Enterprise Strategy Group, 2015.

Just who is responsible for defining these cyber supply chain security requirements? It appears that this is a collective effort dominated by general IT management (69%), and information security/cybersecurity groups (51%, see Figure 29). ESG was somewhat surprised that other constituencies from risk management, regulatory compliance, and legal departments were less involved. This situation will likely change as cyber supply chain security evolves further as a board-level issue.

ESG data also points to another area where there is a fair amount of cyber supply chain discretion–less than half (45%) have formal policies, processes, and technology safeguards established for external third-party IT partners that must be utilized in all cases (see Figure 30). In other cases, business managers have some discretion to modify cyber supply chain security policies, processes, and technology safeguards. While there may be a business justification for some cyber supply chain security adjustments, ESG believes that this should be the exception and not the rule. Variation in third-party cyber supply chain security policies, processes, and technology safeguards can only increase the risk of human error, vulnerabilities, and potentially devastating cyber-attacks.

Figure 29. Groups Responsible for Security Policies and Safeguards for Interaction with Third Parties

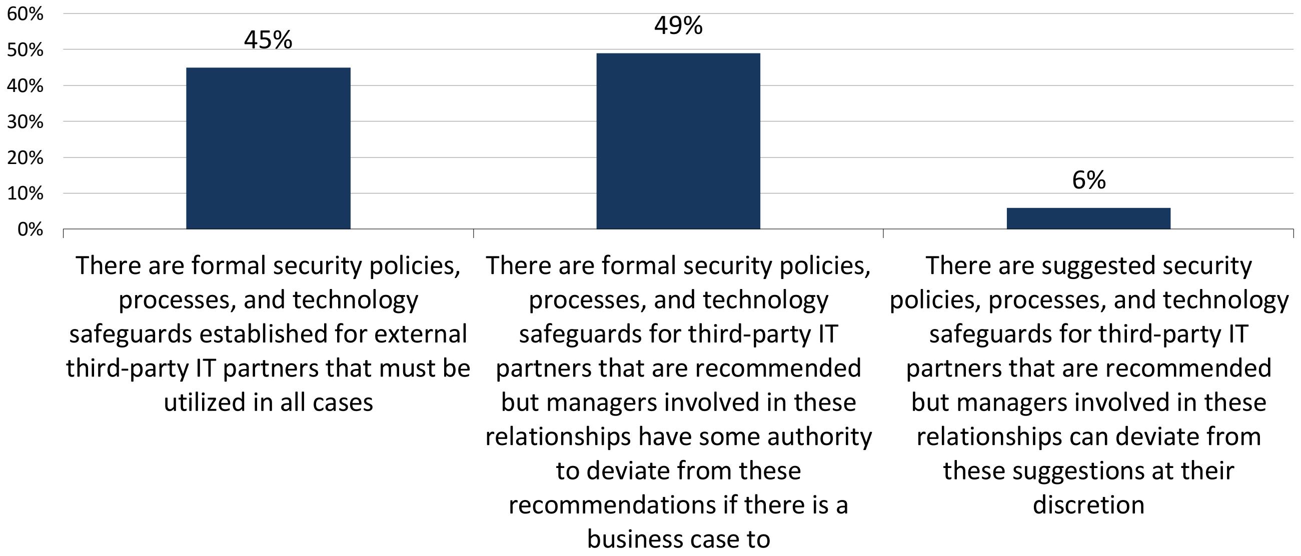
In situations where your organization is either providing IT services to or using IT services from an external party, which of the following groups are responsible for defining the security policies and safeguards between the two parties? (Percent of respondents, N=254, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Figure 30. Establishment of Security Policies and Safeguards for Interaction with Third Parties

In situations where your organization is either providing IT services to or using IT services from an external party, which of the following best describes how your organization establishes cooperative security policies, processes, and technology safeguards between the two parties? (Percent of respondents, N=254)



Source: Enterprise Strategy Group, 2015.

Cybersecurity, Critical Infrastructure Security Professionals, and the U.S. Federal Government

ESG research indicates a pattern of persistent cybersecurity incidents at U.S. critical infrastructure organizations over the past few years. Furthermore, security professionals working in critical infrastructure industries believe that the cyber-threat landscape is more dangerous today than it was two years ago.

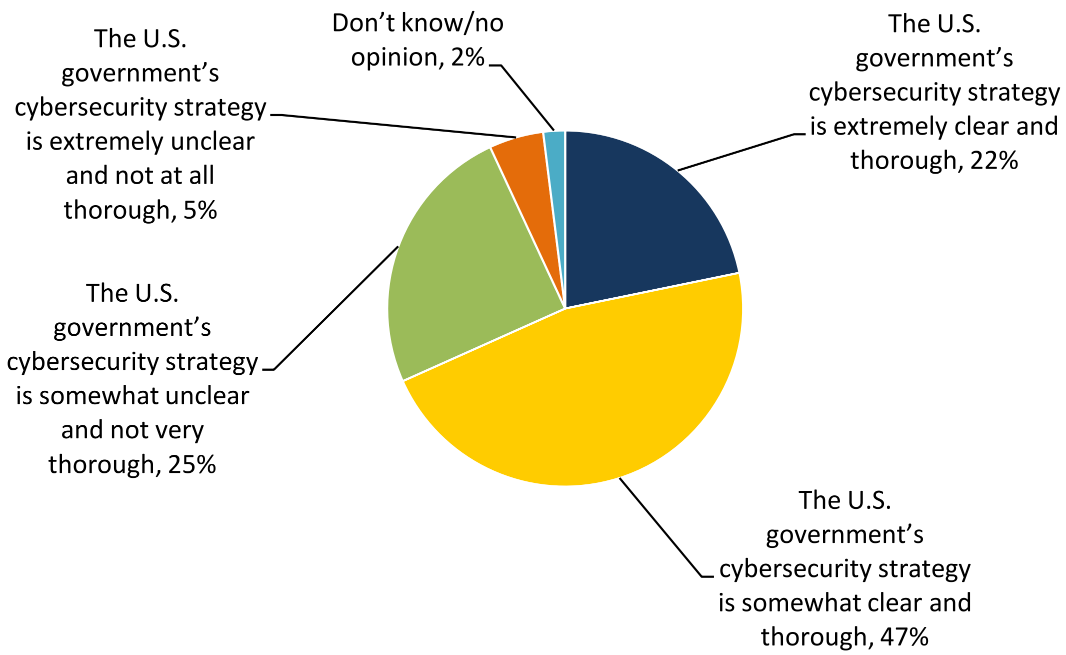
To address these issues, President Obama and various other elected officials proposed several cybersecurity programs such as the NIST cybersecurity framework and an increase in threat intelligence sharing between critical infrastructure organizations and federal intelligence and law enforcement agencies. Of course, federal cybersecurity discussions are nothing new. Recognizing a national security vulnerability, President Clinton first addressed critical infrastructure protection (CIP) with Presidential Decision Directive 63 (PDD-63) in 1998. Soon thereafter, Deputy Defense Secretary John Hamre cautioned the U.S. Congress about CIP by warning of a potential "cyber Pearl Harbor." Hamre stated that a devastating cyber-attack, "… is not going to be against Navy ships sitting in a Navy shipyard. It is going to be against commercial infrastructure."

Security professionals working at critical infrastructure industries have been directly or indirectly engaged with U.S. Federal Government cybersecurity programs and initiatives through several Presidential administrations. Given this lengthy timeframe, ESG wondered whether these security professionals truly understood the U.S. government's cybersecurity strategy. As seen in Figure 31, the results are mixed at best. One could easily conclude that the data resembles a normal curve where the majority of respondents believe that the U.S. government's cybersecurity strategy is somewhat clear while the rest of the survey population is distributed between those who believe that the U.S. government's cybersecurity strategy is very clear and those who say it is unclear.

ESG views the results somewhat differently. In spite of over 20 years of U.S. federal cybersecurity discussions, many security professionals remain unclear about what the government plans to do in this space. Clearly, the U.S. Federal Government needs to clarify its mission, its objectives, and its timeline with cybersecurity professionals to gain their trust and enlist their support for public/private programs.

Figure 31. Respondents' Opinion of the U.S. Federal Government's Cybersecurity Strategy

Which statement best reflects your opinion on the cybersecurity strategy of the U.S. Federal Government? (Percent of respondents, N=303)

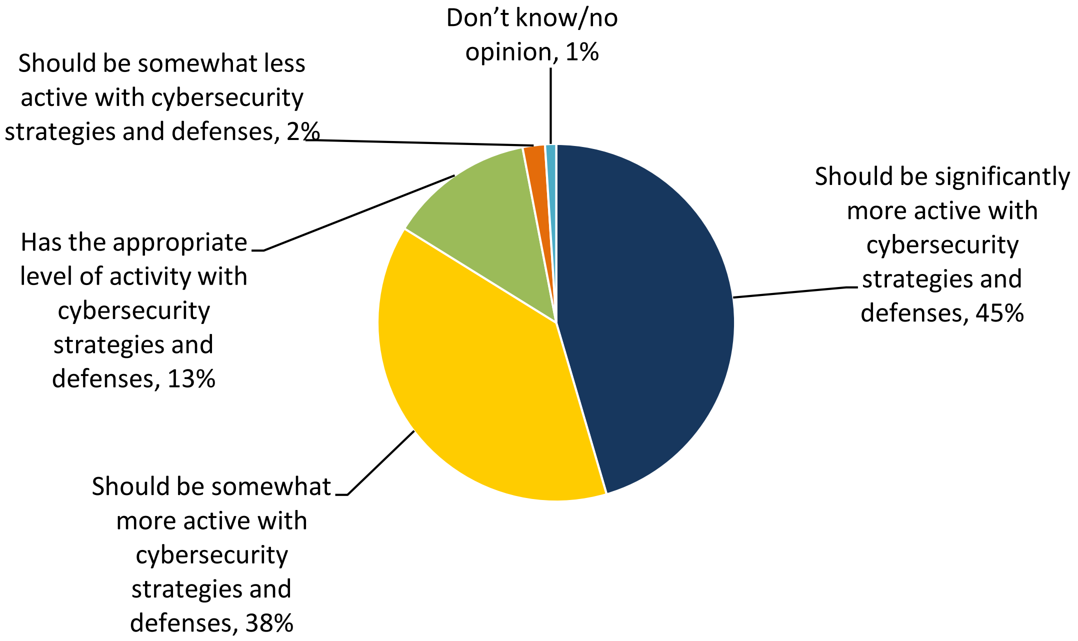


Source: Enterprise Strategy Group, 2015.

While critical infrastructure security professionals may be uncertain about the U.S. Federal Government's strategy, they would also like to see Washington become more engaged. Nearly half (45%) of critical infrastructure organizations believe that the U.S. Federal Government should be significantly more active with cybersecurity strategies and defenses while 38% believe that the U.S. Federal Government should be somewhat more active with cybersecurity strategies and defenses (see Figure 32).

Figure 32. Role of the U.S. Federal Government with Regard to Cybersecurity

Please complete the following statement by selecting one of the responses below. In my opinion, the U.S. Federal Government: (Percent of respondents, N=303)



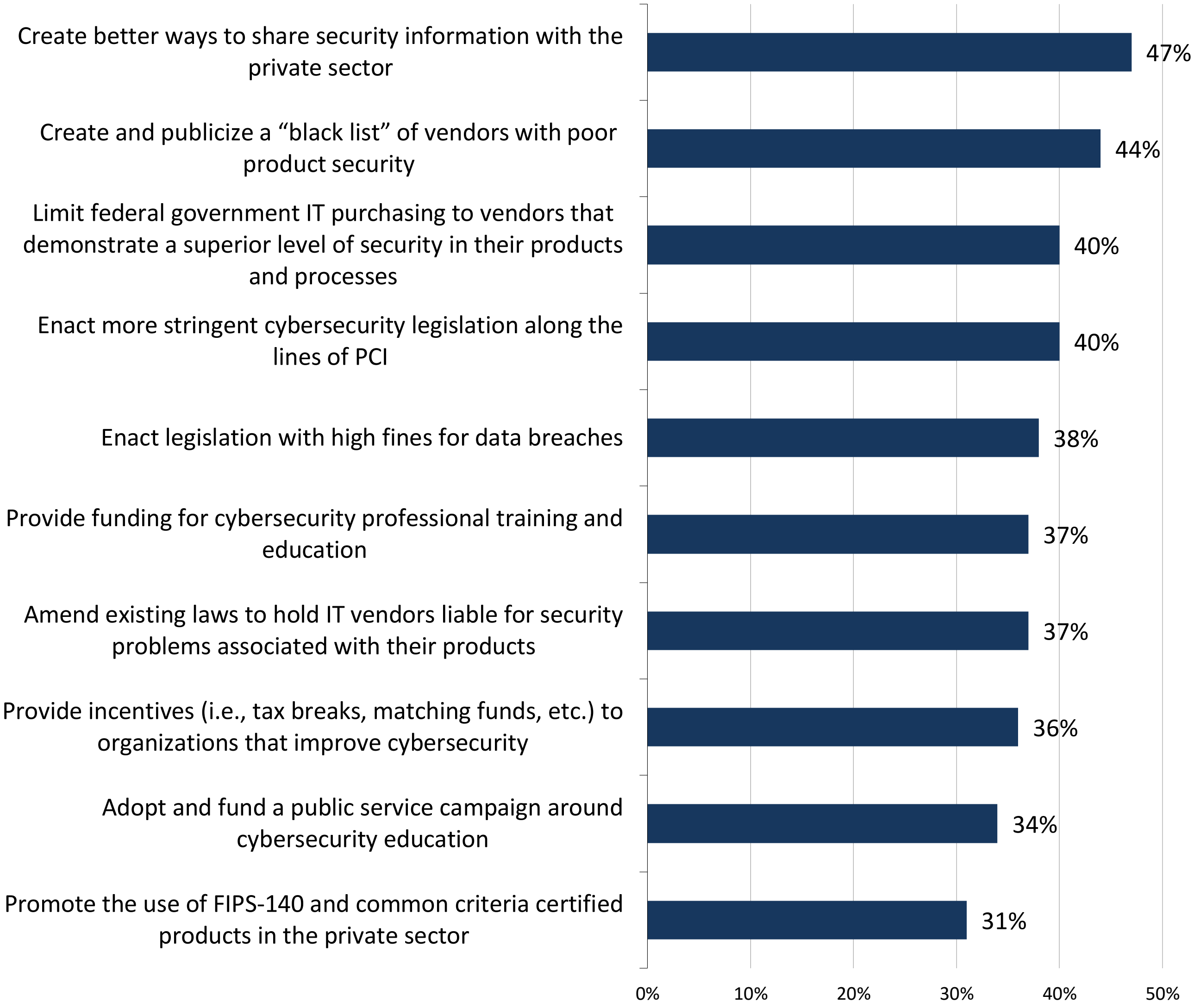
Source: Enterprise Strategy Group, 2015.

Finally, ESG asked the entire survey population of security professionals what types of cybersecurity actions the U.S. Federal Government should take. Nearly half (47%) believe that Washington should create better ways to share security information with the private sector. This aligns well with President Obama's executive order urging companies to share cybersecurity threat information with the U.S. Federal Government and one another. Cybersecurity professionals have numerous other suggestions as well. Some of these could be considered government cybersecurity enticements. For example, 37% suggest more funding for cybersecurity education programs while 36% would like more incentives like tax breaks or matching funds for organizations that invest in cybersecurity. Alternatively, many cybersecurity professionals recommend more punitive or legislative measures—44% believe that the U.S. Federal Government should create a "black list" of vendors with poor product security (i.e., the cybersecurity equivalent of a scarlet letter), 40% say that the U.S. Federal Government should limit its IT purchasing to vendors that display a superior level of security, and 40% endorse more stringent regulations like PCI DSS or enacting laws with higher fines for data breaches (see Figure 33).

Of course, it's unrealistic to expect draconian cybersecurity policies and regulations from Washington, but the ESG data presents a clear picture: Cybersecurity professionals would like to see the U.S. Federal Government use its visibility, influence, and purchasing power to produce cybersecurity "carrots" and "sticks." In other words, Washington should be willing to reward IT vendors and critical infrastructure organizations that meet strong cybersecurity metrics and punish those that cannot adhere to this type of standard.

Figure 33. Suggested Actions for the U.S. Federal Government with Regard to Cybersecurity

If the U.S. Federal Government were to become more involved with cybersecurity, which of the following actions do you believe it should take? (Percent of respondents, N=293, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

Conclusion

Although cyber supply chain security has improved somewhat over the last five years, there is still cause for concern. IT and information security professionals at critical infrastructure organizations believe that the threat landscape is getting worse and that cyber supply chain security is growing more difficult. Furthermore, more than two-thirds of critical infrastructure organizations have experienced a multitude of types of security incidents, including those emanating from vulnerabilities in software they developed in-house. Finally, many critical infrastructure organizations are pursuing new types of IT initiatives like cloud computing, mobile applications, and IoT projects. These technologies are in their genesis phase and may be fraught with vulnerabilities. Meanwhile, cybersecurity best practices and skills around IT innovation also lag behind.

All of these factors add up to continuing cyber supply chain security complexities. Based upon the research data presented herein, ESG offers the following recommendations for critical infrastructure organizations, IT technology vendors, and the U.S. Federal Government.

For Critical Infrastructure Organizations

ESG's research indicates that not only are critical infrastructure organizations inadequately prepared for the current threat landscape, but most are compounding this problem by not doing enough to mitigate the risks associated with cyber supply chain security. To address these shortcomings, critical infrastructure organizations should:

- **Assess cyber supply chain risk across the organization.** Since the cyber supply chain includes a broad range of participants, including IT vendors, suppliers, business partners, and contractors, many critical infrastructure organizations delegate cyber supply chain security management to a variety of internal groups and individuals. While this makes sense at an operational level, it makes it impossible to get a comprehensive perspective of cyber supply chain security or accurately measure cyber supply chain risk. To alleviate this unacceptable situation, CISOs and risk officers should take the time to map out their entire cyber supply chain—every partner, IT equipment vendor, SaaS provider, supplier, etc. Clearly, this will take time and require ample resources, but an end-to-end and up-to-date map of the cyber supply chain is an essential foundation for situational awareness and proactive risk management.
- **Integrate cyber supply chain security into new IT initiatives**. When asked why cyber supply chain security has become more difficult, 44% of cybersecurity professionals blamed new IT initiatives that have increased the cyber-attack surface. This isn't surprising given massive adoption of technologies like cloud computing, IoT, and mobile applications over the past few years. Unfortunately, new IT initiatives often prioritize business objectives at the expense of strong cybersecurity. Given today's threat landscape, this type of laissez-faire approach to cybersecurity must be expunged from the organization. To address and mitigate cyber supply chain risk, CEOs must lead by example with the goal of building a corporate culture that inculcates strong cybersecurity into all business processes, programs, and supporting IT initiatives.
- **Fully integrate security into IT procurement.** ESG data demonstrates that processes and procedures governing IT vendor security audits lack consistency and usefulness. As mentioned, best practices for IT vendor security audits should include the following steps:
    - Audit all strategic IT vendors (including service providers, cloud service providers, and distributors).
    - Follow a standard process for all vendor audits.
    - Implement a corporate policy where IT vendor security audit metrics have a significant impact for all procurement decisions.

A stringent audit process should pay for itself by lowering cyber supply chain risk over time. It will also send a clear message to IT vendors: Adhere to strong cybersecurity policies and procedures or hawk your insecure products and services elsewhere.

- **Address all aspects of software assurance**. As in other findings in this report, critical infrastructure organizations have made progress on software assurance since 2010, but these improvements are based on additional tactical actions rather than an end-to-end strategic approach. Software assurance must be anchored by a secure software development lifecycle and the right skill set for secure software development. Furthermore, software assurance best practices must be followed with no exceptions. This demands an enterprise program for internally developed software as well as stringent controls on third-party software development, maintenance, and testing. Leading companies will also impose testing and quality standards on all commercial software.
- **Formalize external IT security.** When it comes to cyber supply chain security, risk associated with working with third-party partners must be managed and mitigated with the same care as internal activities like vulnerability scanning and patch management. In fact, strong cyber supply chain security has become an SEC mandate and will likely find its way to other industries beyond financial services. Once again, this demands a consistent, documented, and measurable approach for third parties that provide IT services to or consume them from an organization. Aside from legal contracts, governance frameworks, and certifications, CISOs should explore new types of cyber intelligence designed for monitoring third-party risk from vendors like BitSight and SecurityScorecard.
- **Push for more help from Washington.** Like many other critical issues, cybersecurity has been relegated into partisan politics and pork barrel programs. Critical infrastructure organizations should work together, come up with legislative recommendations, lobby for action, and make sure to keep the public aware of any partisan behavior or stalling in Washington.

For the IT Industry

IT product and service providers should view this report as a harbinger of things to come. Critical infrastructure organizations have much work ahead, but ESG data does indicate clear progress since 2010. It is therefore wise to recognize that critical infrastructure organizations are slowly but surely making strong cybersecurity a requirement for all IT vendors. To prepare for this security transition, the entire IT industry must:

- **Build comprehensive internal cybersecurity programs.** Several large IT vendors including Cisco, IBM, Microsoft, Oracle, and VMware have not only created strong cybersecurity programs internally, but also published details about these programs for customer review. Typically, these programs include features like cyber supply chain security management, secure product design, security testing, employee training, IT security, and security services and support. All IT vendors should study and emulate these programs to the best of their abilities.
- **Take a solutions focus to cyber supply chain security.** As secure as any one vendor's products and processes are, business applications and IT infrastructure are composed of a myriad of connected piece parts working together. This means that IT vendors should take a proactive approach to engaging with product and services partners and participate fully in cybersecurity testing, deployment, and operations for complex IT solutions.
- **Include strong security as part of customer engagements.** Even the most diligent customers may not be aware of the cybersecurity intricacies of individual IT products. Smart vendors will work with customers to answer questions, recommend reference architectures, help them harden their products, and maintain a constant stream of communications.

For the U.S. Federal Government

While cybersecurity continues to be topical in the halls of Congress, this and other ESG research reveals a growing gap between cybersecurity professionals and Washington. To alleviate this disconnect and truly engage with the cybersecurity community, the U.S. Federal Government should:

- **Start with clear and concise communications.** ESG research indicates that only 22% of cybersecurity professionals working at critical infrastructure organizations have a clear understanding of the government's cybersecurity agenda. This may be because there are too many cybersecurity voices at different agencies, an abundance of programs with confusing acronyms, and far more rhetoric than action. The U.S. government can only rectify this situation by developing a comprehensive strategy for cybersecurity for critical infrastructure industries. Of course, there is no shortage of documents and programs that claim to do this, but the cybersecurity community at large is looking for one program, bipartisan support, strong and cogent communication, and a visible government leader who actually "owns" cybersecurity. Sadly, many cybersecurity professionals view Washington as part of the problem rather than part of the solution. Government officials will not reverse this cynicism without an honest two-way dialogue, a mutually beneficial partnership, and a clear long-term strategy.
- **Treat cybersecurity as a national security rather than a political issue.** After years of political wrangling, the Cybersecurity Act of 2012 received bipartisan support in the Senate Homeland Security and Governmental Affairs Committee. Unfortunately, the bill never proceeded to the senate floor for a vote. Why? It was a presidential election year, so finger pointing took precedence over collaboration. The cybersecurity legislation remains. In August 2015, the senate left Washington for recess without passing a pending cybersecurity bill on public/private threat intelligence sharing. While politicians continue to give stump speeches about data breaches, cyber-adversaries, and national security concerns, cybersecurity legislation continues to languish. Frustrated by this inactivity, President Obama issued several executive orders in this area. One of these led to the promising NIST cybersecurity framework—a good addition but more of a suggestion than anything else. The U.S. has faced an unprecedented wave of cybercrime and cyber-espionage over the past few years with no end in sight. It's time for the President and congress to:
    - Fund cybersecurity education programs.
    - Expand the Cyber Corps program as a way to exchange cybersecurity training and tuition funding for public service.
    - Improve the hiring process and compensation structure for federal cybersecurity professionals.
    - Create incentives for cybersecurity investments.
    - Work as an equal partner with the cybersecurity community at large. Make sure that federal cybersecurity programs in this area are equally accessible to all cybersecurity professionals in all industries and locations—not just within a few hundred miles of Washington D.C.
    - Create and promote standards like STIX and TAXII for threat intelligence sharing.
    - Share threat intelligence and best practices.
    - Limit liabilities to organizations that truly commit to strong cyber supply chain security.
    - Impose penalties on organizations that continue to minimize cybersecurity.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of IT and information security professionals from private- and public-sector industries designated by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR) in the United States between February 2, 2015 and February 11, 2015. To qualify for this survey, respondents were required to be familiar with/responsible for their organization's information security policies and procedures, especially with respect to the procurement of IT products and services. Respondents also had to be familiar with the cyber supply chain risk management model. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 303 IT and information security professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

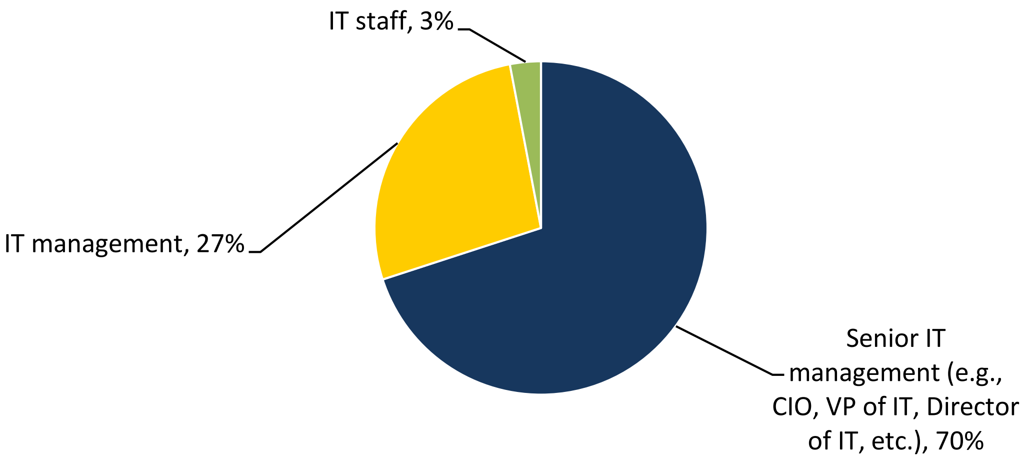
The data presented in this report is based on a survey of 303 qualified respondents. Figures 34-37 detail the demographics of the respondent base, including individual respondents' current job function, as well as respondent organizations' total number of employees, primary industry, and annual revenue.

Respondents by Current Job Function

Respondents' current job functions within their organizations is shown in Figure 34.

Figure 34. Survey Respondents by Current Job Function

Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=303)



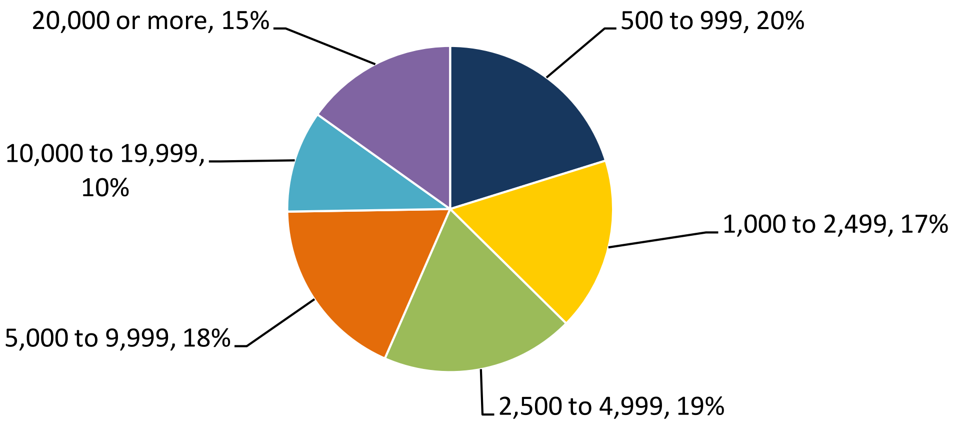
Source: Enterprise Strategy Group, 2015.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 35.

Figure 35. Survey Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of employees, N=303)

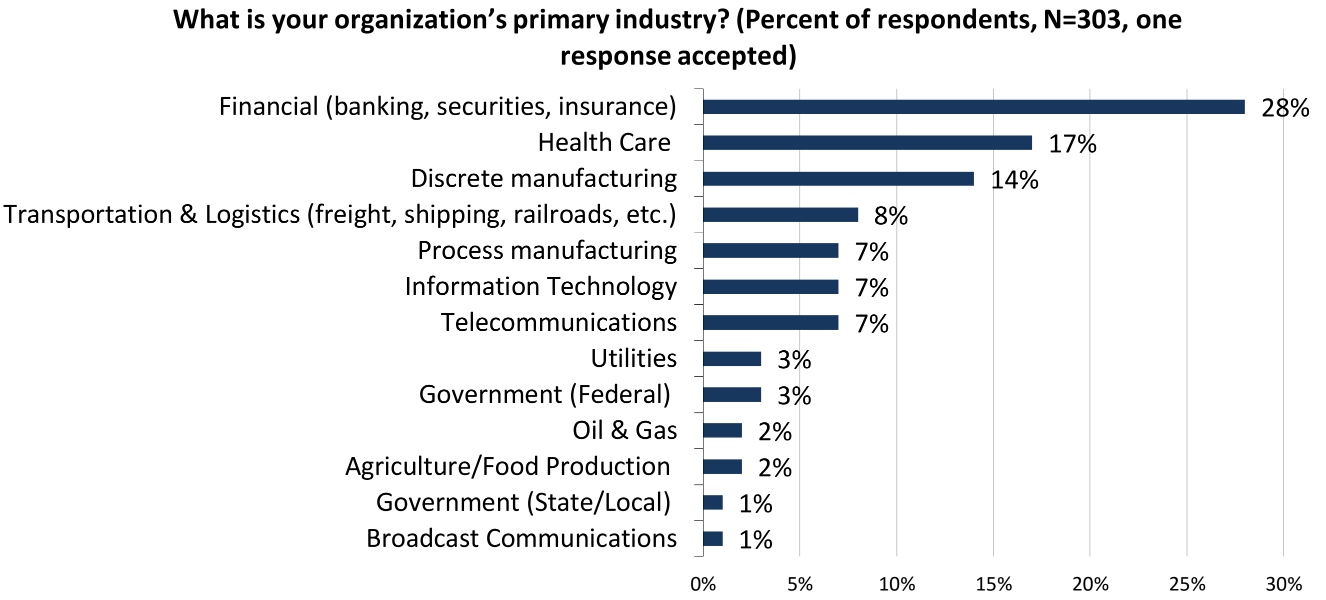


Source: Enterprise Strategy Group, 2015.

Respondents by Industry

Respondents were asked to identify their organization's primary industry. All respondent organizations were required to be part of industries categorized by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR), as shown in shown in Figure 36.

Figure 36. Survey Respondents by Industry

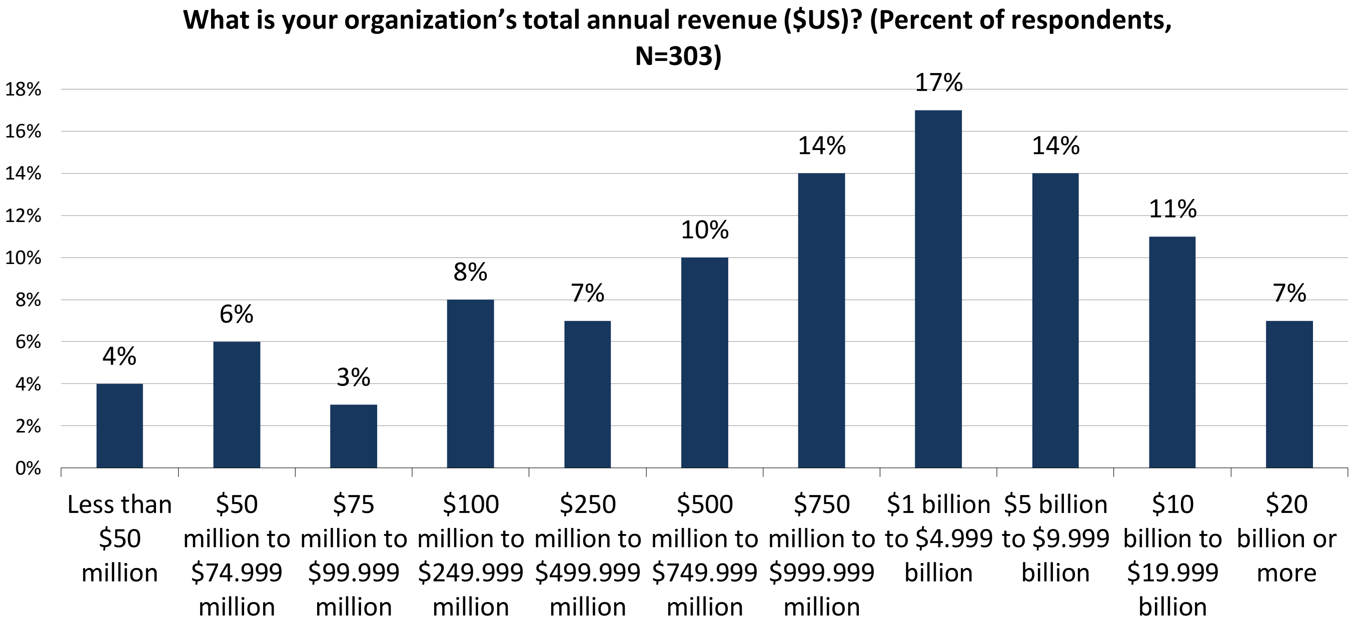


Source: Enterprise Strategy Group, 2015.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 37.

Figure 37. Survey Respondents by Annual Revenue



Source: Enterprise Strategy Group, 2015.

ESG Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0128 | www.esg-global.com