Enterprise Strategy Group | Getting to the bigger truth.™

Research Report

Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure

By Jon Oltsik, Principal Analyst

With John McKnight and Jennifer Gahm

November 2010

Contents

List of Figures

List of Tables

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. Copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482.0188.

Executive Summary

The Enterprise Strategy Group (ESG), a leading IT analyst, consulting, and research organization, has conducted a research project to assess whether organizations categorized by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR) were vulnerable to security attacks due to weaknesses in cyber supply chain security. For the purposes of this project, 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. These users/providers' organizational and process-level interactions to plan, build, manage, maintain, and defend cyber infrastructure."*[1]

This research project was sponsored in part by Hewlett-Packard Corporation and Microsoft Corporation. The objectives of this project were:

- **To provide real research on CIKR vulnerabilities.** Recognizing a national security vulnerability, President Clinton first addressed Critical Infrastructure Protection (CIP) with Presidential 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." Since this declaration, there has been a general acceptance that CIKR organizations are extremely vulnerable to cyber attack, yet little to no research backing up this claim with real data existed. The data presented in this report is meant to bridge this gap.

- **To assess the current security status of CIKR organizations**. ESG wanted to assess the current security status of CIKR organizations and whether critical infrastructure firms were externalizing security policies, procedures, and technology safeguards for cyber supply chain security.

- **To understand CIKR organizations' cyber supply chain security awareness and activities.** Cyber supply chain security is not a new concept; the U.S. Department of Defense (DOD) has been engaging in programs like the Defense Integrated Circuits Strategy (DTICS) since 2003. In 2009, SAIC and the University of Maryland's Robert H. Smith School of Business published the seminal paper on the topic, *Building a Cyber Supply Chain Assurance Reference Model*, that brought further visibility. In this report, ESG wanted to determine whether CIKR organizations are familiar with cyber supply chain security concepts, whether they recognize the risks associated with the cyber supply chain, and whether they are instituting the right levels of governance and oversight to adequately secure their cyber supply chains.

- **To highlight software assurance.** There is an abundance of data exposing the number of existing and new vulnerabilities introduced by poorly-written and insecure software. Do CIKR organizations understand this problem? Are they addressing these weaknesses? Once again, there is very little research available exploring these issues. As such, this report specifically analyzes issues related to software assurance.

Based on primary research with 285 U.S.-based CIKR organizations, ESG concludes that critical infrastructure firms realize they are under attack. ESG found that the vast majority of CIKR firms participating in the survey suffered at least one security breach over the past two years. Survey respondents believe that the current threat landscape is worse than it was two years ago and will grow even more insidious between 2010 and 2012. In spite of increasing security risks, ESG found abundant security vulnerabilities: about 20% of survey respondents don't believe their organizations are prepared to meet today's cyber security challenges.

In analyzing the data, ESG also found an ironic and somewhat frightening correlation: CIKR organizations with the best cyber security preparation, knowledge, and technology defenses were also the most likely to experience the highest number of security incidents. This introduces an important question: Are less secure organizations finding fewer security attacks because they aren't occurring or because these organizations lack the skills, processes, and

[1] Source: *Building a Cyber Supply Chain Assurance Model*, SAIC and the Supply Chain Management Center (SCMC), Robert Smith School of Business, June 2009.

tools to know what to look for? The frightening implication here is that many CIKR organizations may already be compromised.

ESG concludes that CIKR organizations are off to a good start with cyber supply chain security, but there is a lot of room for improvement. For instance, few organizations are doing thorough due diligence on their IT vendors' security, so CIKR firms may be buying hardware and software with security vulnerabilities "baked-in." Many critical infrastructure organizations are employing some types of secure software development programs, but these are often instituted haphazardly. Finally, CIKR companies are sharing IT systems with business partner employees and systems, but most lack formal cyber supply chain governance and oversight. As a result, secure CIKR organizations are increasing their security risks through electronic business processes with insecure partners.

ESG's research also uncovers an important cry for help: 71% of the CIKR organizations surveyed believe the Federal Government should be more active with cyber security strategies and defenses. Critical infrastructure organizations want to see more public/private information sharing, incentives for cyber security investment, and more stringent regulations with substantial penalties for compliance violations.

The December 2008 Center for Strategic and International Studies (CSIS) paper, *Securing Cyberspace for the 44th Presidency,* stated: "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration … it is a battle we are losing." After taking office, President Obama echoed the CSIS paper when in May 2009 he 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."*

There has been some cyber security progress during the Obama administration. For example, the Protecting Cyberspace as a National Asset Bill (S.3480) seeks to centralize oversight of the U.S. Critical Infrastructure under DHS and even encourages cyber supply chain security in the form of federal procurement reform. Unfortunately, political elections and congressional cycles continue to slow cyber security initiatives while CIKR organizations remain vulnerable.

Over the past few years, there have been real cyber attacks against national financial systems (Estonia, 2007), electric power grids (Brazil 2005, 2007), and nuclear facilities (i.e., the 2010 Stuxnet attack aimed at Iran). In a video leaked by DHS in 2007, security researchers at Idaho National Labs launched a network attack to compromise a control system which led to the destruction of an expensive electric power generator (note: this attack is often referred to as the Aurora vulnerability).

Based upon these research findings, CIKR organizations may be vulnerable to similar types of cyber attacks. Given this, ESG believes that federal cyber security initiatives focused on critical infrastructure protection are extremely timely and should remain a high priority in the near future.

Report Conclusions

ESG conducted an in-depth survey of 285 security professionals working at CIKR organizations. According to the 2009 DHS National Infrastructure Protection Plan, Critical Infrastructure and Key Resources sectors include:

- Agriculture and Food
- Defense Industrial Base
- Energy
- Health Care and Public Health
- National Monuments and Icons
- Banking and Finance
- Water
- Chemical
- Commercial Facilities (as designated by the DHS Office of Infrastructure Protection)
- Critical Manufacturing
- Dams
- Emergency Services
- Nuclear Reactors, Materials, and Waste
- Information Technology
- Communications
- Postal and Shipping
- Transportation Systems
- Government Facilities

The survey focused on CIKR organizations' current cyber security processes in general and cyber supply chain security awareness and safeguards in particular. Survey participants represented large midmarket (i.e., 500 to 999 employees) and enterprise-class (i.e., 1,000 employees or more) CIKR organizations in the United States.

Based on the research collected for this report, ESG concludes that:

- **Cyber security protection is directly related to regulatory compliance**. About one-third of the CIKR organizations surveyed are obligated to comply with more than three industry/government regulations. This group had consistently better security policies, procedures, and safeguards than those required to comply with less than three regulations. ESG concludes there is a cumulative security effect from multiple regulations that changes an organization's cyber security requirements while simultaneously improving skills and preparation.
- **Critical infrastructure organizations face constant cyber attacks.** Sixty-eight percent of CIKR organizations surveyed suffered at least one security breach over the past 24 months. Alarmingly, the organizations with the strongest security policies, procedures, and technical safeguards were also the ones with the highest number of security incidents. It is certainly possible that security-challenged CIKR organizations are under attack but lack the skills and tools to detect and remediate security incidents.
- **Threats continue to escalate.** Twenty-eight percent of CIKR organizations believe that the threat landscape is much worse today than it was 24-36 months ago, while another 40% believe that the threat landscape is somewhat worse. Additionally, 71% of respondents believe that the threat landscape will be even worse two years from now. It is worth noting that CIKR organizations with the strongest security policies,

procedures, and technical safeguards are the ones most likely to say that the threat landscape is getting much worse.

- **Some organizations are in bad shape.** Alarmingly, 20% of the CIKR organizations surveyed rated their organization's security policies, procedures, and technology safeguards as "fair" or "poor." Furthermore, 23% of organizations rate their executive management's support for and investment in cyber security as "fair" or "poor." This group needs help soon.

With regard to cyber supply chain security issues specifically, survey respondents from CIKR organizations report that:

- **IT vendor security audits are performed inconsistently and are rarely thorough.** Cyber supply chain security begins with careful and thorough security audits of IT vendors, service providers, and distributors. The goal? Assess IT vendor security practices, pinpoint threats and vulnerabilities, and then use this information to add security considerations into IT procurement decisions. While most CIKR organizations are doing some IT vendor due diligence, ESG found that IT security audits are done haphazardly and lack real depth. In some cases, CIKR organizations conduct IT security audits that have little impact on IT procurement. To achieve best practices for IT vendor security audits, all vendors would need to be audited with standard audit procedures. The results of these IT security audits would then be a critical factor for ongoing IT procurement. Unfortunately, only 10% of CIKR follow these best practices for IT vendor audits.
- **Software assurance is a work in progress.** Many cyber security problems are rooted in poorly-written software, so ESG focused special attention on CIKR organizations' software development practices. The good news is that many firms are employing technology safeguards, developer training, software security testing, and/or secure development lifecycles. The bad news is that these programs are fairly new and relatively random. For example, only 33% of CIKR organizations are providing secure software development training to their internal software developers. This is especially disconcerting since 30% of CIKR organizations experienced a security incident directly related to the compromise of internally-developed software within the past two years.
- **External IT relationships lack appropriate security.** To improve productivity, most CIKR organizations have opened internal IT systems to third parties like suppliers, customers, and business partners. While these relationships can help improve efficiency, increase revenue, and/or cut costs, they can also introduce cyber security vulnerabilities. The CIKR organizations surveyed seem to recognize this risk but lack the right level of skills, governance, oversight, or executive support to mitigate risks correctly. ESG found that external IT relationships are secured on a case-by-case basis. This informal structure is less than optimal.
- **Critical infrastructure organizations want help from the Federal Government.** Rather than an anti-government mindset, 71% of the CIKR organizations surveyed believe that the U.S. Federal Government should be a more active participant in cyber security strategies and defenses. Survey respondents would like to see the Federal Government institute programs to identify IT vendors with poor security, create better methods for public/private security data sharing, enact more stringent cyber security legislation, and provide incentives to organizations for improving their cyber security.

In aggregate, this research illustrates that many CIKR organizations are behind with *basic* security protection, let alone more advanced cyber supply chain security defenses. Many lack the skills or resources, while others need guidance and help with establishing best practices. There is also a visible cyber security communications gap between grass roots security professionals and executive managers who either don't understand or don't care about escalating cyber security risks. ESG believes that this situation leaves the U.S. critical infrastructure vulnerable to a cyber attack.

The report also suggests an increasing role for the U.S. Federal Government that includes both "carrots" and "sticks." CIKR organizations want to see tighter security regulations with strict penalties for violations, but they also need financial and technical help. This help will be especially important with regard to more advanced security concepts like cyber supply chain security.

Introduction

Research Objectives

The primary objective of this ESG research study was to survey CIKR organizations in order to qualify and quantify the current status of their existing security profiles as well as their awareness of and programs dealing with cyber supply chain security.

To assess cyber supply chain assurance, ESG asked 285 security professionals to respond to questions in areas such as:

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 as compared to 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 cyber security?
2. Procurement
   - How important are IT vendors' security processes in customers' procurement decisions?
   - Do CIKR 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?
   - Do IT vendors assume any liabilities for faulty or compromised products?
   - Do CIKR organizations hold system integrators accountable for the overall security of the systems they design, deploy, operate, and manage? If so, how?
   - To the best of their knowledge, have CIKR organizations purchased any counterfeit IT hardware/software over the past 12 months?
3. Software development
   - Do CIKR organizations include security considerations in their standard software development processes?
   - Have organizations experienced any security breaches related to internally-developed software vulnerability?
   - Do CIKR 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 CIKR organizations currently open their IT systems to external parties such as customers, suppliers, and business partners?
   - If so, how are these relationships secured? Are there formal processes and safeguards in place?
5. The role of the U.S. Federal Government
   - Do CIKR organizations believe that the Federal Government should do more or less in terms of cyber security defenses and strategies?
   - What specific actions should the Federal Government take?

Market Overview

Many Organizations are Unfamiliar with Cyber Supply Chain Security

"Cyber Supply Chain Security" is a concept that originated with the NSA's Trusted Product Evaluation initiative in the 1980s, expanded by the U.S. Department of Defense (DoD) in the early 2000s. According to a research report published by SAIC and the Supply Chain Management Center (SCMC), Robert Smith School of Business,[1] 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. These users/providers' organizational and process-level interactions to plan, build, manage, maintain, and defend cyber infrastructure."* [2]

In simpler terms, cyber supply chain security is meant to extend internal risk management and information security best practices to external parties that provide IT equipment, services, or business applications to an organization. If an internal IT organization follows secure development lifecycle processes for internally-developed software, then third party software suppliers should adhere to the same types of secure development practices. If internal IT operations teams are mandated to patch vulnerable systems within 24 hours of a critical update, then external partners and SAAS vendors providing business application access to the organization's employees should be required to do the same.

The assumption with regard to cyber supply chain security is that organizations have an existing baseline of information security and risk management best practices in place. Cyber supply chain security simply layers additional policies, processes, requirements, and security controls on top this strong foundation. Alternatively, cyber supply chain security won't provide much incremental protection to organizations with sub-standard information security knowledge, skills, policies, processes, and resources.

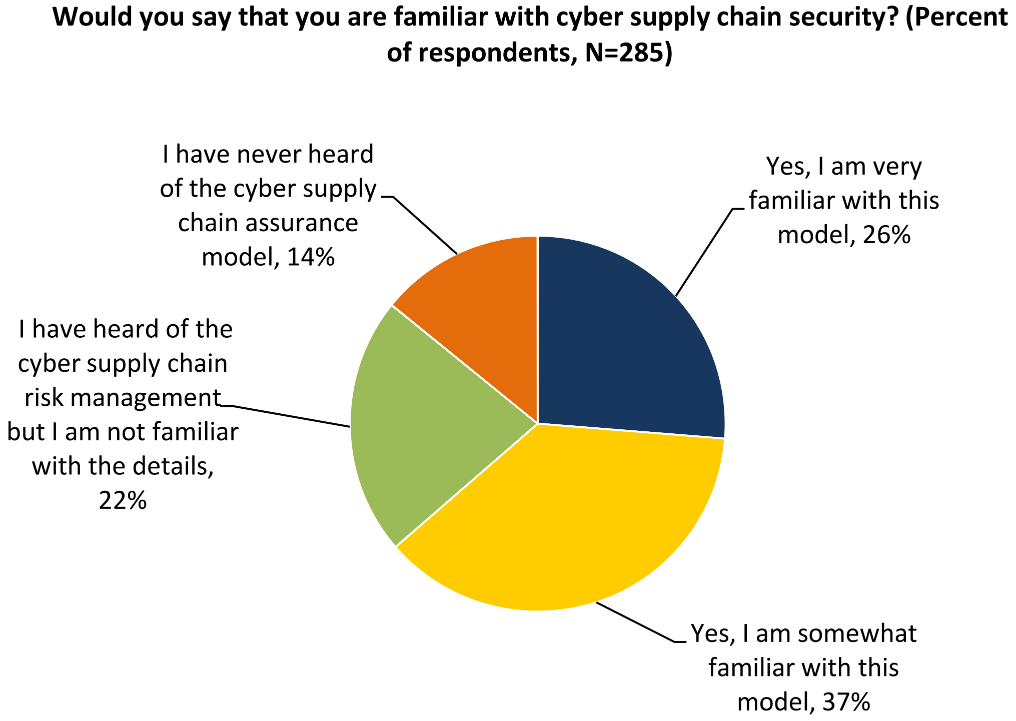
ESG research respondents work in industries considered to be Critical Infrastructure Key Resources (CIKR) by DHS. Obviously, these organizations work closely with cabinet-level agencies (i.e., Dept. of Energy, Dept. of Agriculture, Dept. of the Treasury, etc.) and with DHS itself. Given this, ESG assumed that the concept of cyber supply chain security would be somewhat familiar. To assess cyber supply chain security knowledge, respondents were provided with the following simple definition:

> *There is a relatively new cyber security best practices methodology known as cyber supply chain security. Simply defined, cyber supply chain security supplements internal security controls by mandating specific security requirements for any business partner or technology supplier providing IT products or services to an organization.*

Respondents were then asked: "Based on this definition, would you say that you are familiar with this model?" Surprisingly, only 26% said they were "very familiar" with this cyber supply chain security (see Figure 1).

[2] Source: *Building a Cyber Supply Chain Assurance Model*, SAIC and the Supply Chain Management Center (SCMC), Robert Smith School of Business, June 2009.

Figure 1. Familiarity with Cyber Supply Chain Security



Source: Enterprise Strategy Group, 2010.

What types of organizations are "very familiar" with cyber supply chain security?

- **Small and large firms.** Interestingly, the data dispels the assumption that cyber supply chain security knowledge would skew toward larger organizations. In fact, 32% of respondents working at critical infrastructure organizations with less than 1,000 employees were very familiar with cyber supply chain security while only 22% of respondents working at critical infrastructure organizations with more than 20,000 employees were very familiar with cyber supply chain security.
- **Financial services firms are most familiar with cyber supply chain security.** Based upon the sample size, ESG was able to analyze data from four vertical industries: financial services, health care, process manufacturing, and telecommunications. Thirty-six percent of respondents from the financial services industry were very familiar with cyber supply chain security, 24% of respondents from both the health care and process manufacturing industries were very familiar with cyber supply chain security, and 19% of respondents from the telecommunications industry were very familiar with cyber supply chain security.
- **Highly regulated organizations were most familiar.** Thirty-four percent of respondents working at critical industry organizations obligated to comply with more than three government or industry regulations (i.e., FISMA, HIPAA, GLBA, PCI DSS, etc.) said that they were very familiar with cyber supply chain security. Alternatively, 24% percent of respondents working at critical industry organizations required to comply with less than three government or industry regulations said that they were very familiar with cyber supply chain security.

Segmenting and Rating CIKR Organizations on Cyber Supply Chain Security Readiness

Cyber supply chain security is made up of a number of policies, processes, and controls that extend internal security protection to IT product vendors, software developers, and external organizations sharing business applications or IT services. Consequently, it is safe to assume that CIKR organizations adopting cyber supply chain security best practices have better overall cyber security protection than more *laissez-faire* firms. In other words, firms embracing cyber supply chain security are most likely to have:

- Superior understanding of the threat landscape.
- A cyber security culture that spans the organization and includes executive management.
- Strong cyber security policies, processes, technology defenses, and monitoring.
- Significant experience in the areas of security event detection, isolation, and remediation.

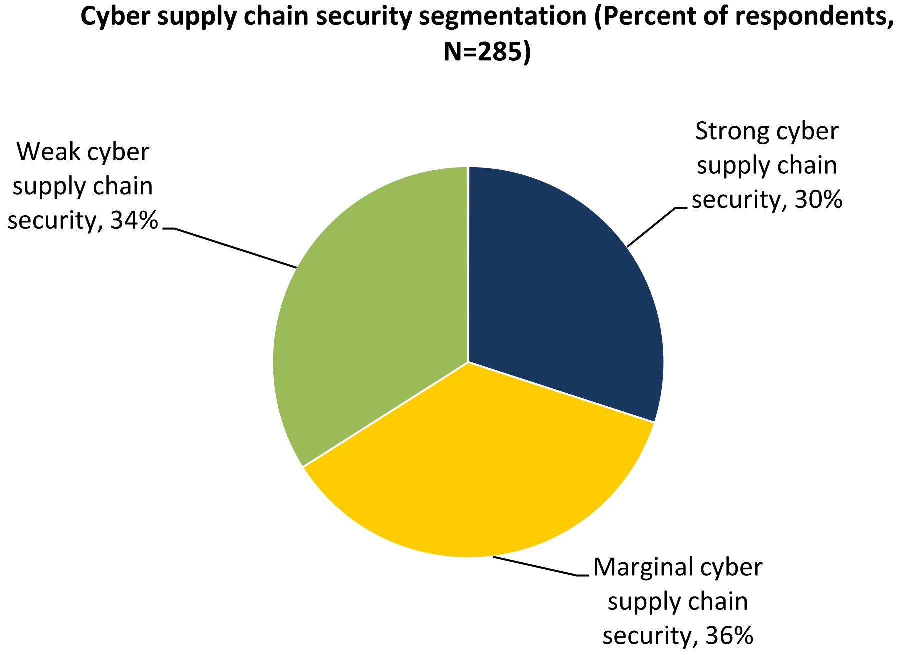
These assumptions certainly make sense, but are they really true? In order to answer this question, ESG developed a cyber supply chain security model that segments the CIKR organizations surveyed across four dimensions that characterize overall cyber supply chain security sophistication. These dimensions are based upon:

1. **Standard IT vendor security audits.** A value for this dimension was calculated based on CIKR organizations' IT vendor security audit standards. ESG assigned a higher cyber supply chain security value to critical infrastructure organizations that adhere to standard security auditing policies and procedures applied to all IT vendors.
2. **The impact of IT vendor security audits on IT purchasing decisions.** A value for this dimension was calculated based on the degree of influence that vendor security audit results had on IT procurement decisions. ESG assigned a higher cyber supply chain security value to critical infrastructure organizations claiming that vendor security audit results had a "significant" impact on IT purchasing decisions—i.e., they acted on the results of their audits as opposed to conducting them and then ignoring or discounting the results.
3. **The cyber security controls established for external IT relationships.** A value for this dimension was dependent upon the adoption of formal and standard cyber security policies, processes, and technology safeguards used to secure business applications or IT services shared between CIKR and external organizations. A higher value was assigned to organizations that mandate standard and formal cyber security policies, processes, and technology safeguards for all external IT relationships.
4. **The extent of software assurance programs.** A value for this dimension was based upon the scope of CIKR organizations' secure software development initiatives. A higher value was assigned to organizations that established software assurance programs as enterprise standards.

As indicated above, ESG used the survey data to assign every respondent organization a score for each of the four dimensions that comprise ESG's cyber supply chain security model. The maximum possible score was 20 points and the minimum was zero. Based on a respondent organization's aggregate score, that organization was then classified as either having "strong" cyber supply chain security (15 or more points), "marginal" cyber supply chain security" (10 to 14 points), or "weak" cyber supply chain security (less than 9 points).

Using this segmentation model, 30% of ESG the CIKR organizations can be identified as having "strong" cyber supply chain security, 36% have "marginal" cyber supply chain security, and 34% have "weak" cyber supply chain security" (see Figure 2).

Figure 2. Percent of Organizations Classified by ESG as Having "Strong," "Marginal," or "Weak" Cyber Supply Chain Security



Source: Enterprise Strategy Group, 2010.

Analysis of the research data by this market segmentation reveals clear and profound differences among CIKR organizations, demonstrating the correlation between cyber supply chain security and general cyber security best practices. For example, 38% of CIKR organizations with "strong" cyber supply chain security rate their organization's security policies, processes, and technology safeguards as "excellent," as compared to 16% of CIKR organizations with "weak" cyber supply chain security. ESG's cyber supply chain security segmentation will be used for data analysis purposes throughout this report to illustrate varying degrees of cyber security behavior amongst the groups. In aggregate, the data is indicative of a diverse population where about one-third of CIKR organizations are well protected while the remaining two-thirds remain vulnerable.

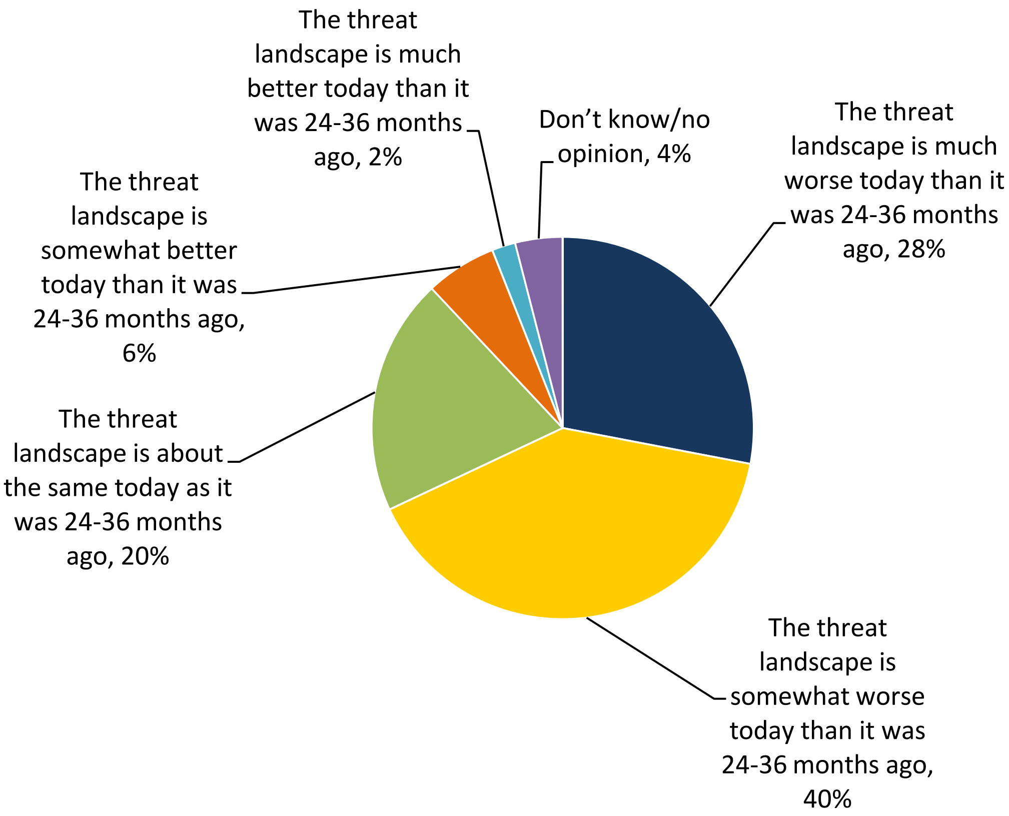
The Current Security Landscape

ESG's research finds a foreboding and increasingly threatening security environment. When asked to rate the current cyber security threat landscape compared to 24-36 months ago, 28% of respondents believe it has grown much worse while another 40% believe it is somewhat worse (see Figure 3).

This data is even more alarming when analyzed further: 42% of organizations with "strong" cyber supply chain security believe that the threat landscape is much worse today than it was 24-36 months ago as compared to 23% of those with "weak" cyber supply chain security. In other words, the most secure members of the CIKR survey population are also most likely to believe that the threat landscape has become much worse.

Figure 3. Rate Current Cyber Security Threat Landscape

How would you rate the current cyber security threat landscape compared to the threat landscape 24-36 months ago? (Percent of respondents, N=285)



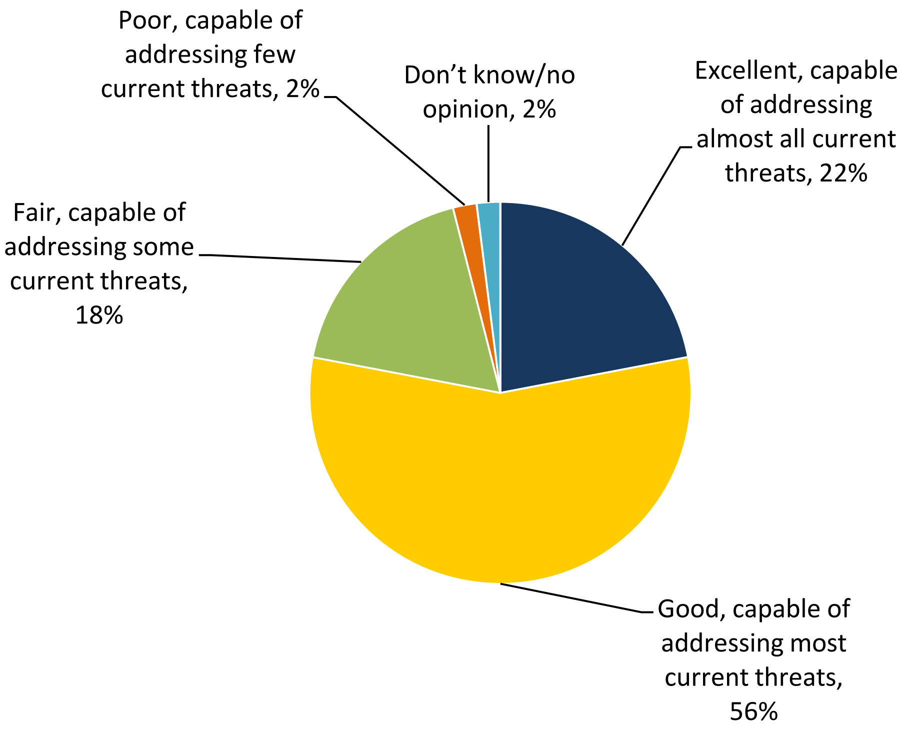
Source: Enterprise Strategy Group, 2010.

How are organizations standing up to this increasingly ominous threat landscape? The data suggests that one-fifth of respondents give their critical infrastructure organization's security policies, procedures, and technology safeguards a rating of "fair" or "poor" (see Figure 4).

Again, these results can vary widely. Eight percent of respondents working at critical infrastructure organizations with "strong" cyber supply chain security gave their organization a rating of "fair" or "poor," while 27% of respondents working at critical infrastructure organizations with "weak" cyber supply chain security rated their organization as rating of "fair" or "poor."

Figure 4. How Organizations Rate Their Security Policies, Procedures, and Technology Safeguards

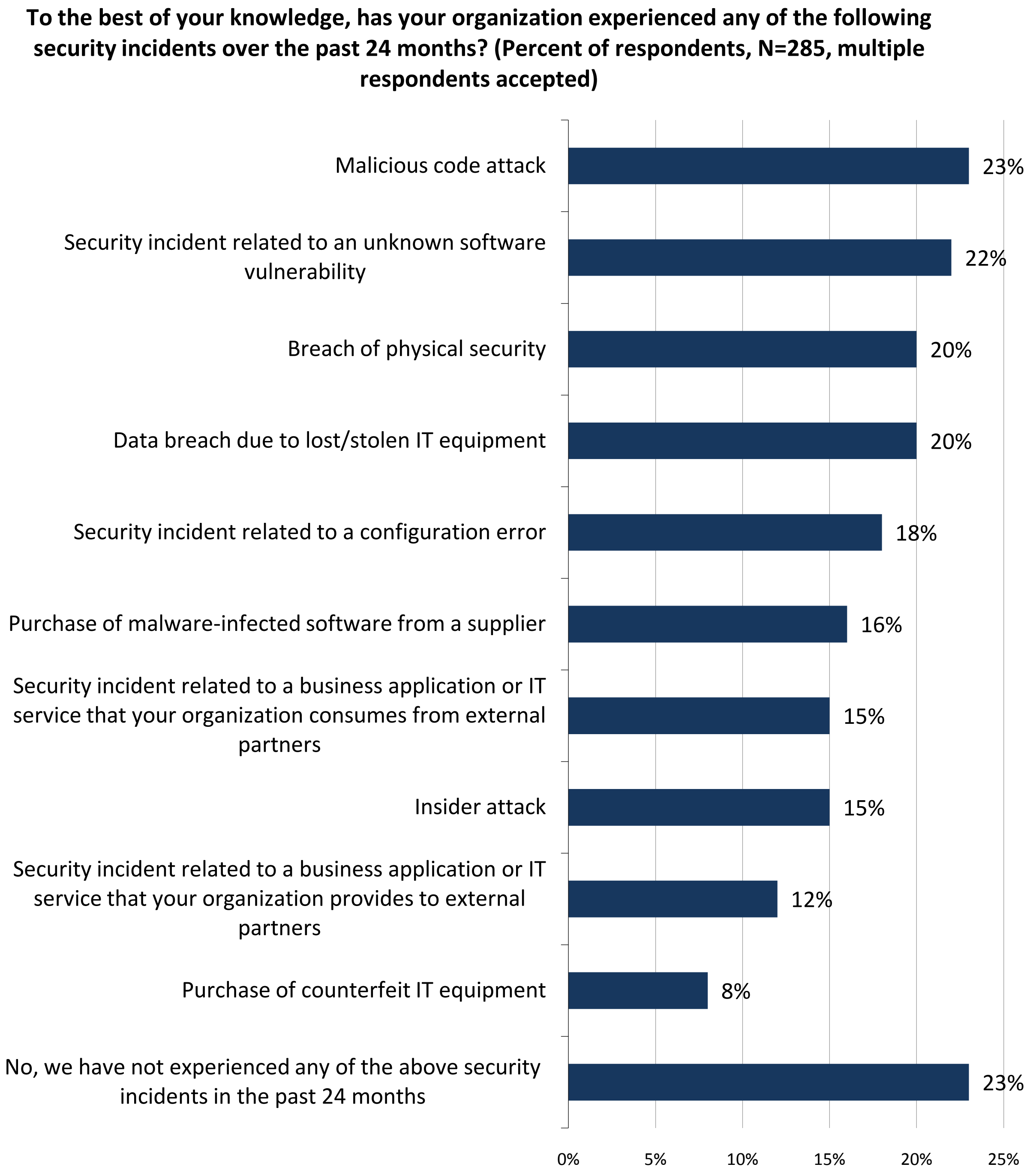
How would you rate your organization's security policies, procedures and technology safeguards in their ability to address the current threat landscape? (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

Critical infrastructure organizations have experienced numerous types of security incidents over the past two years including malicious code attacks, security incidents related to unknown software vulnerabilities, and breaches of physical security (see Figure 5).

Figure 5. Security Incidents Organizations Have Experienced Over Past 24 Months

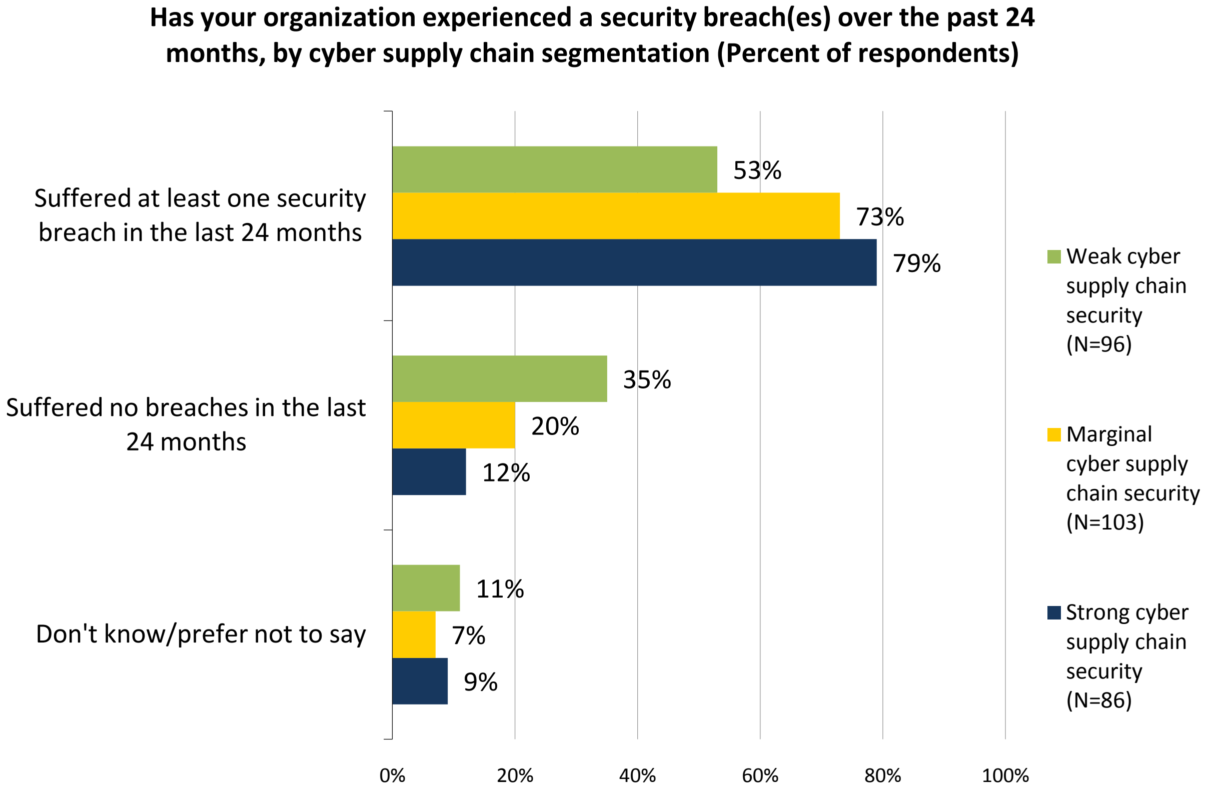


Source: Enterprise Strategy Group, 2010.

In aggregate, 68% of the critical infrastructure organizations surveyed suffered at least one security event over the past 24 months. Upon further analysis, the data also shows a counterintuitive correlation between security expertise and security breaches—organizations with advanced cyber security processes and controls were the ones that suffered the highest number of breaches. For example, 79% of respondents working at CIKR organizations with "strong" cyber supply chain security reported at least one security breach over the past 24 months (note: 24%

reported more than three security breaches). Organizations with “moderate” and “weak” cyber supply chain security reported a much smaller number of breaches (see Figure 6).

Figure 6. Security Incidents Experienced Over Past 24 Months, by Cyber Supply Chain Security Segmentation



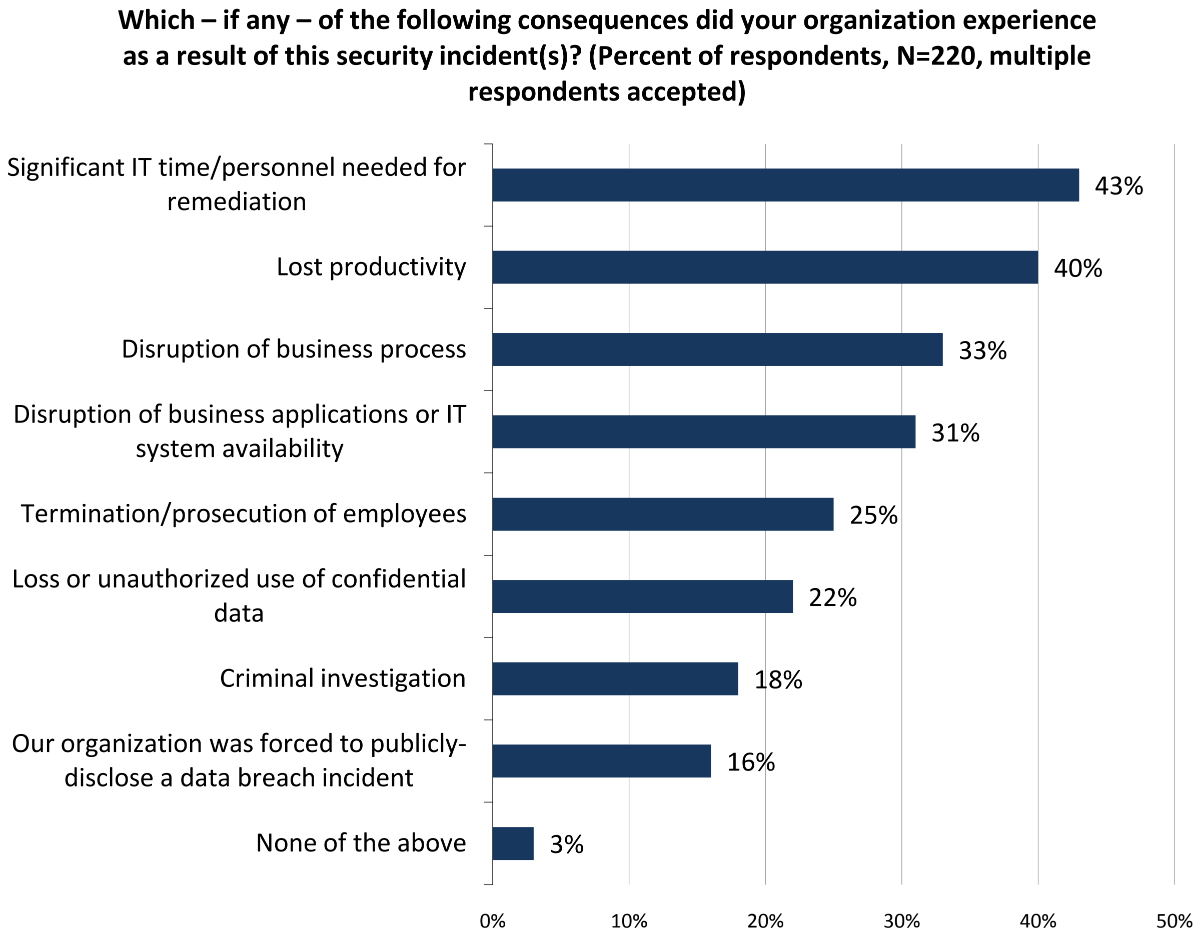
Source: Enterprise Strategy Group, 2010.

How can this data be explained? ESG believes that highly secure CIKR organizations may be detecting, reporting, and remediating security attacks. Less secure firms may face similar security attacks but lack the right security skills and controls to know what to look for and where to look. These firms may be unaware that critical IT systems have already been compromised.

Security Breaches Cause System and Service Interruptions

Security breaches can have costly ramifications. Survey respondents claimed that responding to security breaches consumes IT time and resources and lead to lost productivity. Other consequences are more ominous for critical industry organizations. One-third of respondents said that security breaches led to "disruption of business processes," while 31% pointed to "disruption of business applications or IT systems availability" (see Figure 7).

Figure 7. Consequences Experienced as a Result of Security Incident(s)



Source: Enterprise Strategy Group, 2010.

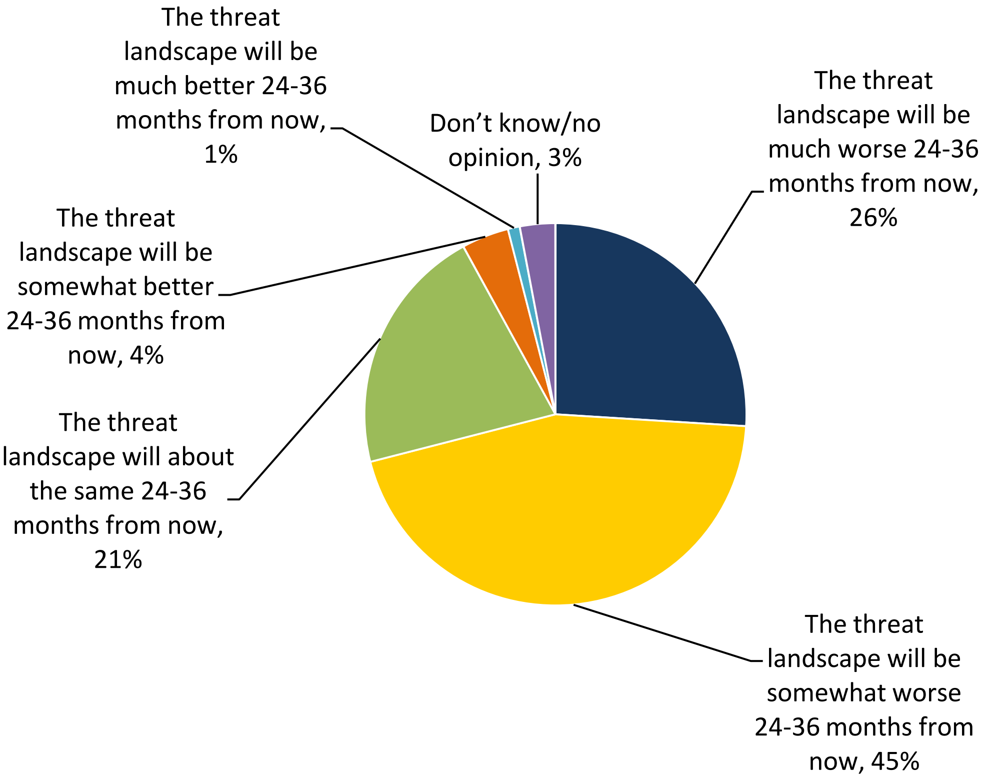
These ramifications could be extremely disruptive. For example, 41% of financial services and 40% of telecommunications firms surveyed said that a security incident resulted in "disruption of business applications or IT system availability." This could disrupt ATM transactions or 911 systems. Additionally, 42% of process manufacturing companies claimed that security incidents led to the "disruption of a business process." This could impact the food supply if a security attack cuts a food processor off from its suppliers.

This data demonstrates that cyber security incidents are already routinely disrupting CIKR organizations' business operations. Random and individual security events tend to go unnoticed, but, in aggregate, they should be seen as a cause for concern. Given this pattern of isolated security incidents and their ramifications, a much larger targeted attack could lead to systemic damages.

How will security threats progress in the future? Two-thirds of respondents believe that the threat landscape will grow more dangerous over the next two years. It is also telling that one-fourth of organizations believe that the threat landscape will grow "much worse" (see Figure 8).

Figure 8. Prediction of Cyber Security Threat Landscape 24-26 Months From Now

Compared to today, what is your prediction for the cyber security threat landscape 24-36 months from now? (Percent of respondents, N=285)

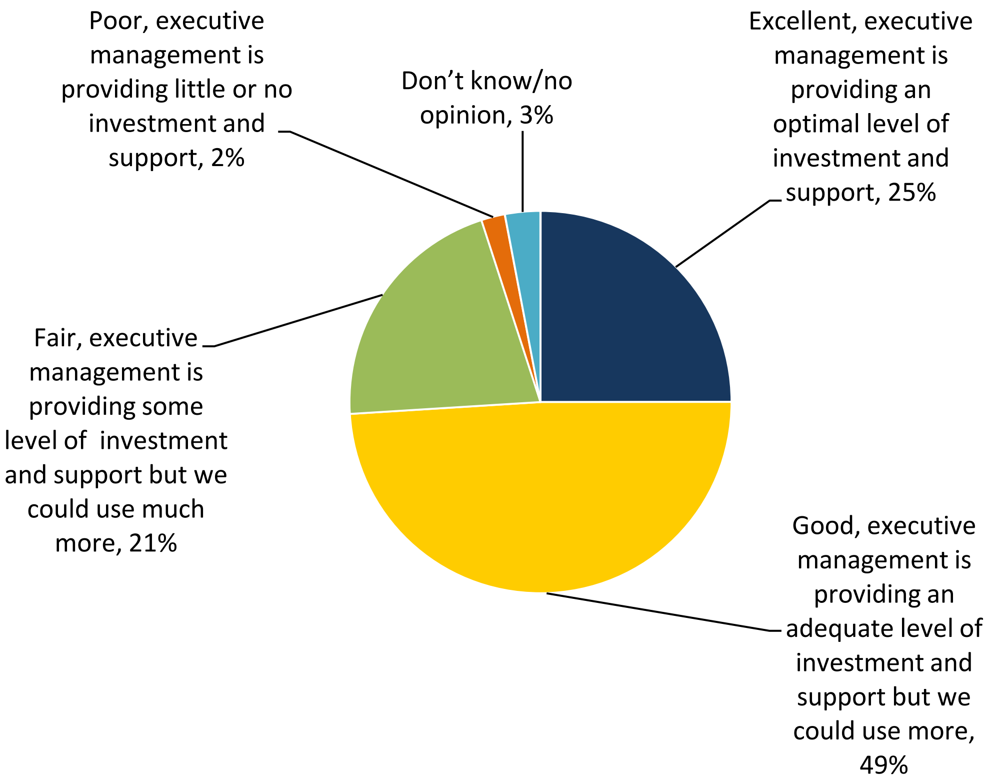


Source: Enterprise Strategy Group, 2010.

Over time, an increasing threat landscape will certainly exacerbate business risk and may even impact national security. One would think that CIKR organization executives would recognize this risk and address it with the appropriate level of cyber security investment and resources. Unfortunately, ESG found that this is not always the case: only 25% of respondents rated their executive management “excellent” in terms of cyber security investment and support. Nearly as many respondents (23%) said that executive management investment and support for cyber security initiatives was either “fair” or “poor” (see Figure 9).

Figure 9. Rating of Organizations' Executive Management Team

In your opinion, how would you rate your organization's executive management team on its willingness to invest in and support cyber security initiatives? (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

ESG Data Insight

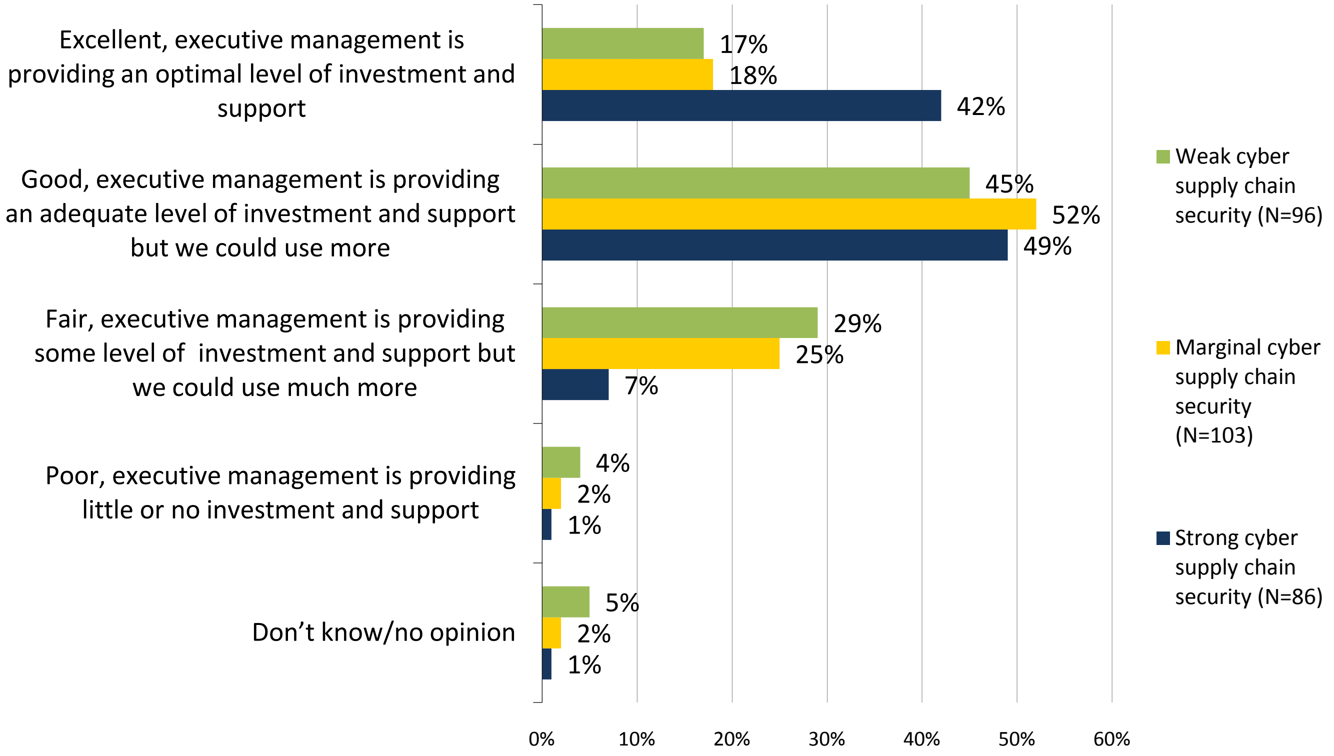
Thirty-eight percent of respondents working at telecommunications companies rated executive management's support for cyber security initiatives as "fair" or "poor."

Executive management support for cyber security seems to be a function of overall security maturity. Critical infrastructure organizations with "strong" cyber supply chain security were far more likely to give executive management a rating of "excellent" than those with "moderate" or "weak" cyber supply chain security. The alternative is true as well: only 8% of CIKR organizations with "strong" cyber supply chain security rated their executive management's support for cyber security as "fair" or "poor" (see Figure 10).

ESG interprets this data analysis as good news. CIKR organizations that emphasize cyber security awareness and education are getting the most support from executive management. Federal cyber security programs may have a similar impact by bolstering cyber security awareness and education with executives at less advanced CIKR organizations.

Figure 10. Executive Management Team Support for Cyber Security, by Cyber Supply Chain Security Segmentation

In your opinion, how would you rate your organization's executive management team on its willingness to invest in and support cyber security initiatives? (Percent of respondents)



Source: Enterprise Strategy Group, 2010.

Clearly, critical infrastructure organizations face frequent and increasingly sophisticated cyber attacks in a threat landscape that is only growing incrementally worse over time. The data does suggest that security begets security; organizations that are under attack tend to understand what they are up against, are in good shape today, and have executive support for future cyber security needs. The danger, however, is that a large number of organizations don't understand the threat landscape and seem to be missing some security incidents when they happen. These organizations are ill-prepared and aren't convincing executive management that they need help.

Cyber Supply Chain Security

Cyber security protection begins with a solid foundation: CIKR organizations must know what IT assets they have and how they are configured. Network nodes should be "hardened" before they are deployed on production networks. Access to all IT systems must adhere to the principle of "least privilege." IT administration must follow "separation of duties." Networks must be scanned regularly and software patches applied rapidly. All security controls must be monitored constantly.

Unfortunately, the data presented above indicates the need for basic improvement in order to establish a baseline of sound cyber security practices across all CIKR organizations. Once internal strong security is in place, CIKR organizations should proceed toward continuous improvement by implementing cyber supply chain security programs. 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.*

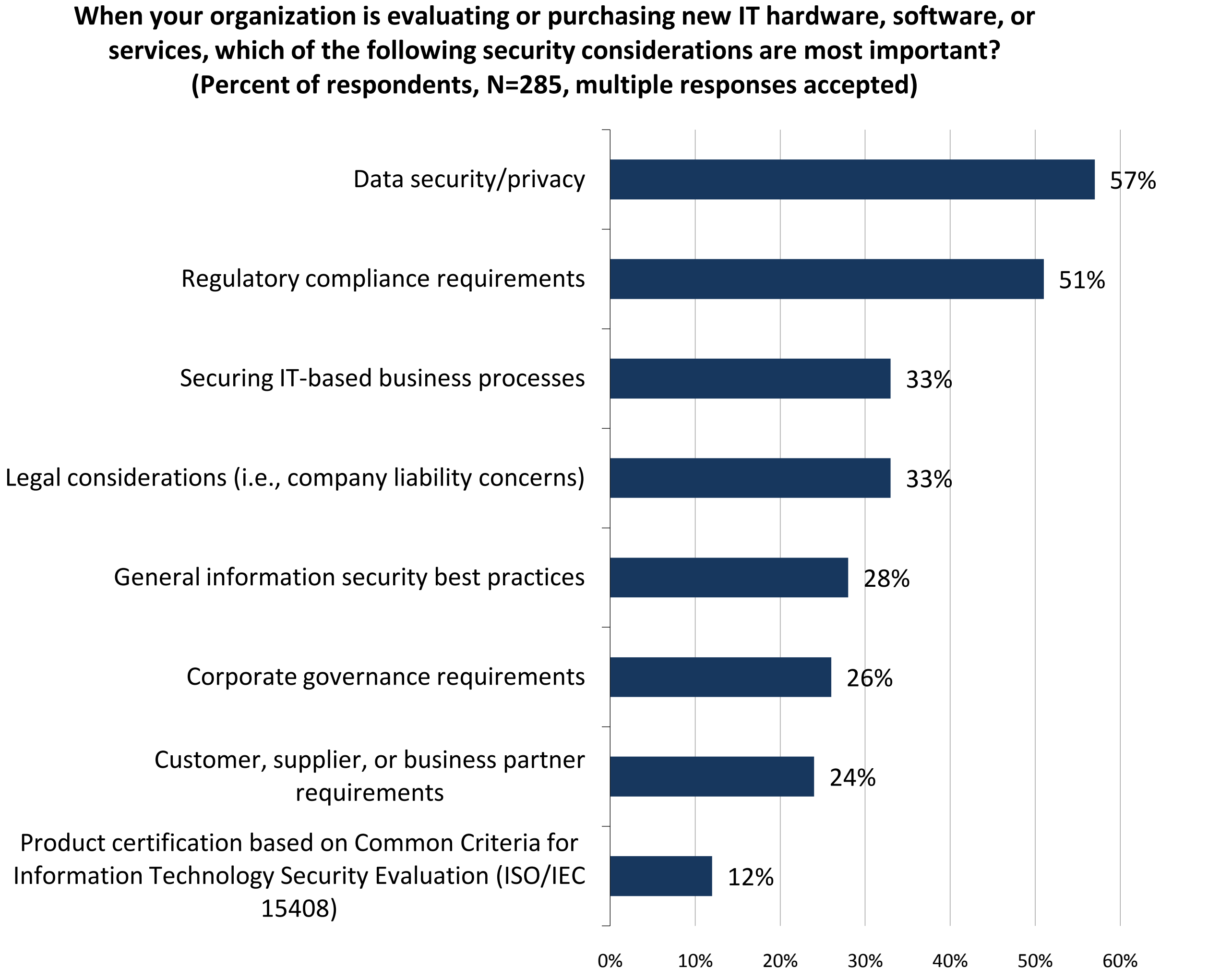
In simpler terms, CISOs (Chief Information Security Officers) should equate cyber supply chain with all the internal and external technologies, IT professionals, and end- users that touch their organizations' IT systems. With this definition established, this report will now explore cyber supply chain security in three specific areas:

1. The relationship between CIKR organizations and their IT vendors (i.e., hardware, software, and services suppliers as well as system integrators, channel partners, and distributors).
2. The security of internally-developed software.
3. Cyber security processes and controls in instances where CIKR organizations are either providing IT access to third parties (i.e., suppliers, customers, business partners), or consuming IT access from third parties (note: throughout this report, this is often referred to as "external IT").

Cyber Supply Chain Security and IT Procurement

Over the past few years, CIOs have demanded stronger security functionality from IT hardware and software products. What is behind this growing emphasis on security? Survey respondents working at critical infrastructure organizations claim that their most important security considerations when evaluating IT equipment are "data security/privacy" (57%) and "regulatory compliance requirements" (51%) (see Figure 11).

Figure 11. Security Considerations When Purchasing New IT-Related Products/Services



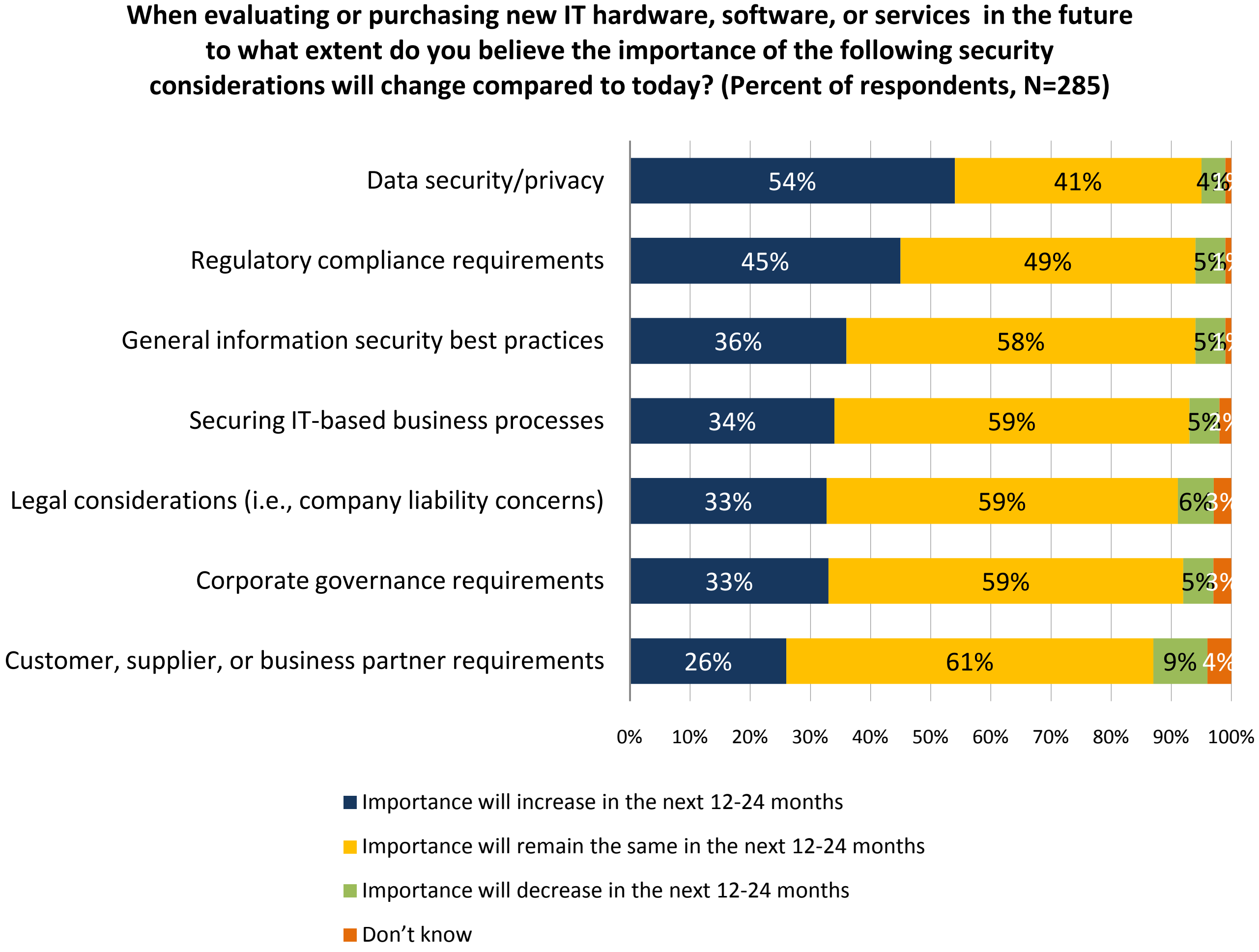
Source: Enterprise Strategy Group, 2010.

ESG believes this data represents real progress. Over the past few years, regulations like FISMA, HIPAA/HITECH, and PCI DSS have had an impact as they forced CIKR organizations to deploy and monitor basic security controls. Furthermore, regulatory compliance, combined with visible data breaches at organizations like Heartland Payment Systems, TJX, and the National Archives and Records Administration, has forced organizations to bolster sensitive data security.

While compliance and data security are now important considerations in the IT procurement process, the data also indicates that critical infrastructure organizations are less likely to think about other types of security risks. For example, Figure 11 shows that only one-third of organizations consider the requirements for securing IT-based business processes that may open network access to vulnerable mobile workers or unmanaged third party systems. The data also illustrates the limited implementation of cyber supply chain security—only 24% of organizations base their IT procurement considerations on external security requirements from customers, suppliers, or business partners, indicating that many critical infrastructure industries could do even more to “police themselves.”

While respondents believe that all of these considerations will become more important in the future, there will still be a somewhat myopic focus emphasizing data security and compliance alone. Fewer CIKR organizations take into account more comprehensive security considerations like securing IT-based business processes, corporate governance, or the security requirements of customers, suppliers, or business partners (see Figure 12).

Figure 12. How Security Considerations' Importance Will Change When Purchasing New IT-Related Products/Services



Source: Enterprise Strategy Group, 2010.

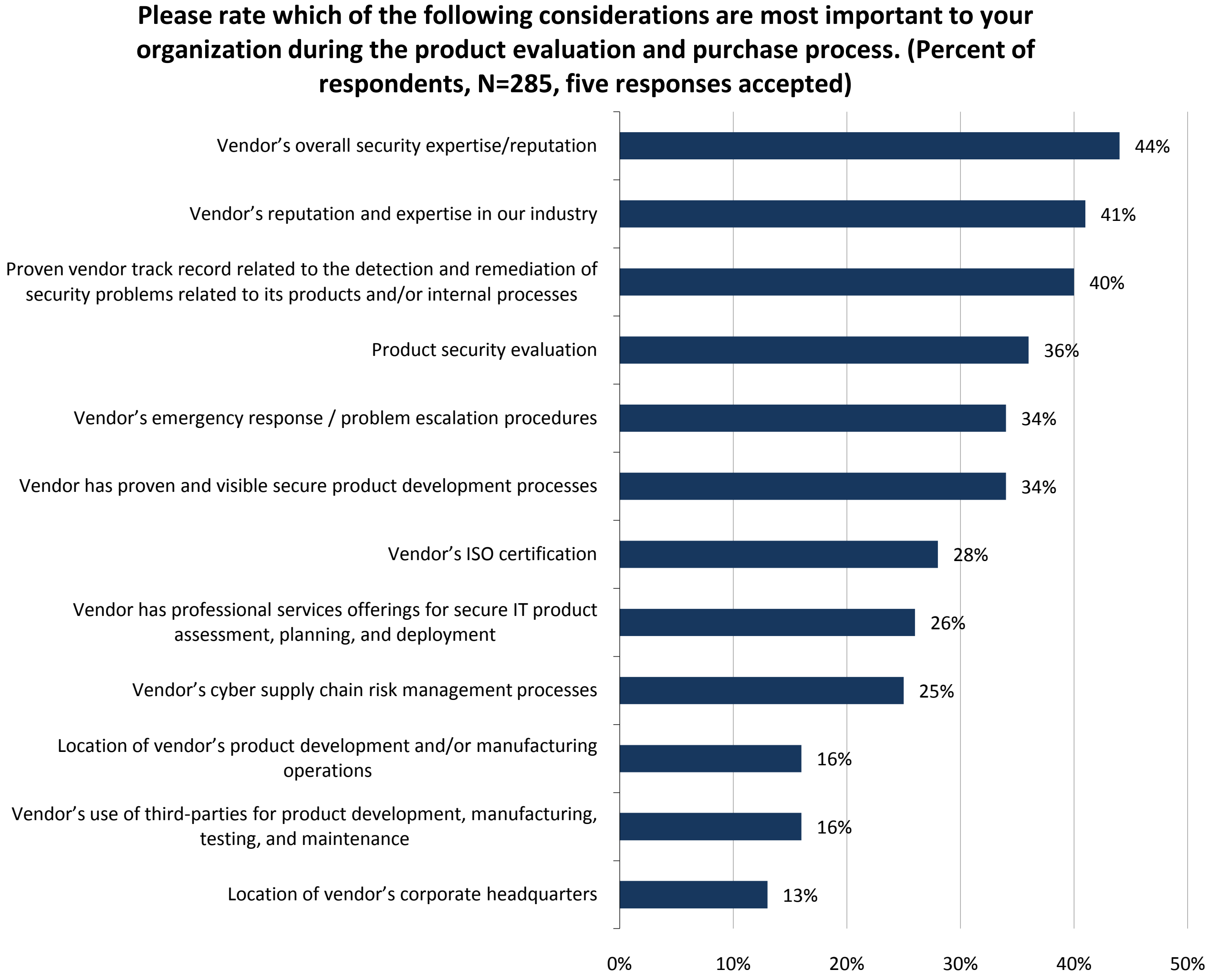
Cyber Supply Chain Security and IT Vendors

Clearly, critical infrastructure organizations' concerns about data privacy/security and regulatory compliance have led to a greater emphasis on security within the IT procurement process. With these concerns in mind, what types of cyber security attributes do CIKR organizations expect from their vendors? Survey respondents point to their vendors' "overall security expertise/reputation," their "reputation and expertise in our industry," and a "proven track record related to detection and remediation of security problems" (see Figure 13).

While ESG believes them to be a good start, these are rather basic considerations. A vendor's security reputation could be based upon effective marketing communications rather than strong security processes, procedures, and product development. Detecting and remediating security issues is a historical metric which may be rooted in security shortcomings—a vendor producing poorly-written code may become proficient with security bulletins and updates while it continues to deliver insecure products.

ESG notes that far fewer critical infrastructure organizations are performing in-depth vendor security due diligence than one might expect. It is startling to see that only 36% of the organizations surveyed believe that actual product security evaluations are "most important considerations." Most CIKR organizations are also eschewing cyber supply chain security best practices; only 34% say that their vendors' secure product development methodologies are amongst their "most important considerations" while 25% rate their vendors' cyber supply chain risk management processes as most important.

Figure 13. Most Important Considerations During Product Evaluation and Purchase Process



Source: Enterprise Strategy Group, 2010.

As previously mentioned, cyber supply chain security extends internal security processes, procedures, and controls directly to IT vendors. If an IT asset like a server or router comes from the factory with malicious firmware or poorly written software, it will immediately make any CIKR organization more vulnerable to a security attack as soon as it is deployed on the network.

To address these types of risks, cyber supply chain security best practices dictate that organizations dig into the security processes, procedures, and technology safeguards used by their IT vendors and suppliers. This is ideally accomplished via proactive and thorough IT vendor audits of software providers, hardware manufacturers, professional services vendors that install and customize IT systems, and VARs/distributors that may ultimately deliver IT gear.

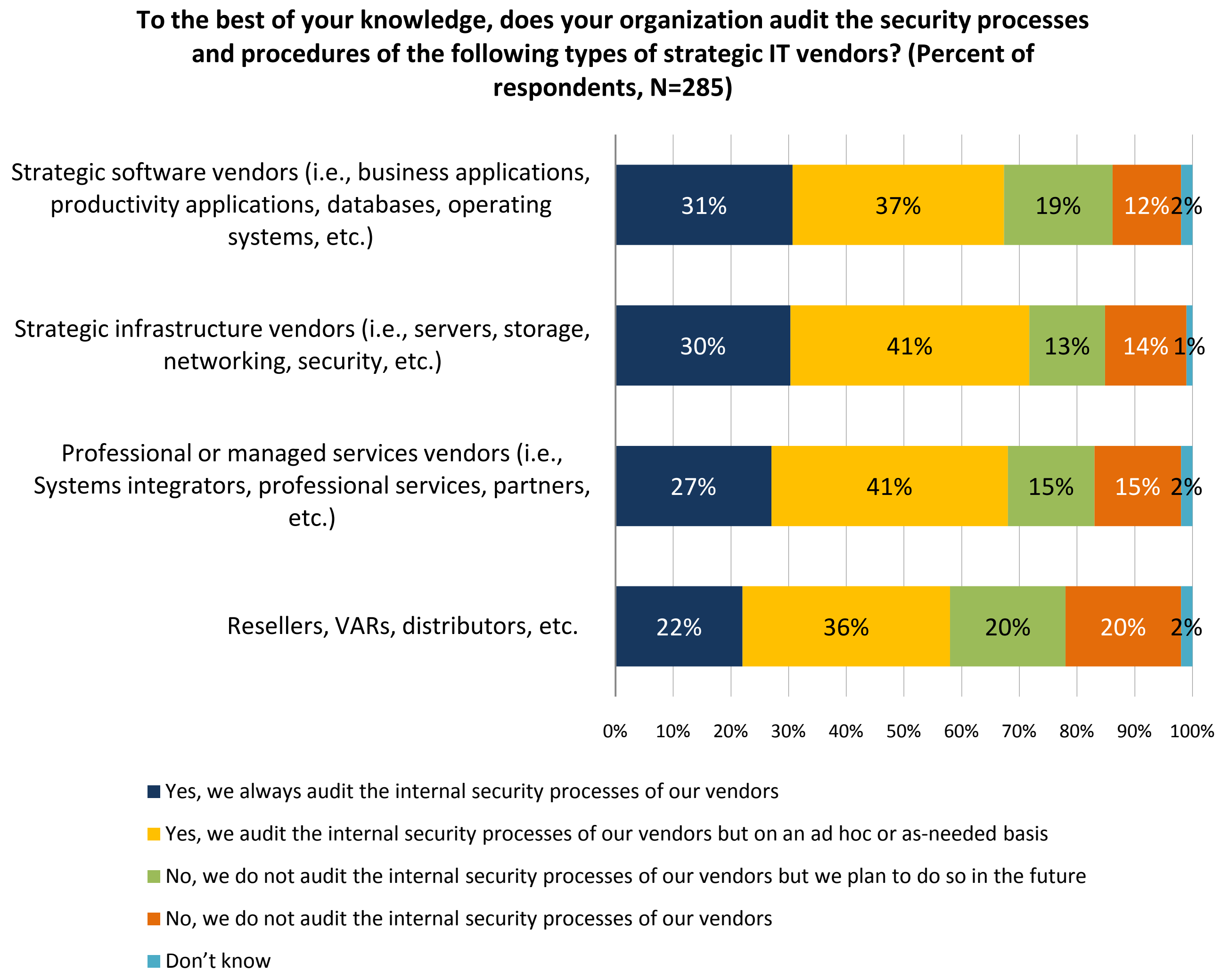
ESG Data Insight

Security-conscious organizations are more likely to conduct security audits on IT vendors. For example, 43% of critical infrastructure organizations obligated to comply with more than three regulations always conduct security audits of their strategic software vendors. This compares to 31% of the general survey population.

The ESG research data indicates both good and bad news in this area. The good news is that most critical infrastructure organizations participating in this survey do audit the processes and procedures of their strategic software vendors, strategic infrastructure vendors, professional/managed services vendors, and resellers/VARs/distributors (see Figure 14). The bad news is that less than one-third of these CIKR organizations say that they "always" audit vendor processes and procedures. Instead, most audits are done on an "as-needed" or "ad hoc" basis.

It is also clear from the data that most organizations are more methodical with strategic software and infrastructure vendor security audits than they are with professional services firms or others in the chain of distribution (i.e., resellers, VARs, distributors). This represents a real vulnerability where IT systems or equipment can be compromised in transit or as they are added to a production network. There is evidence suggesting that the Stuxnet worm was first introduced into Siemens control systems in this very way—through an infected USB drive that was mistakenly or maliciously used to install software on an existing control system. Clearly, professional services organizations and IT distributors could be malicious agents and should not get a cyber security "free pass."

Figure 14. Auditing of Security Processes and Procedures of Strategic IT Vendors

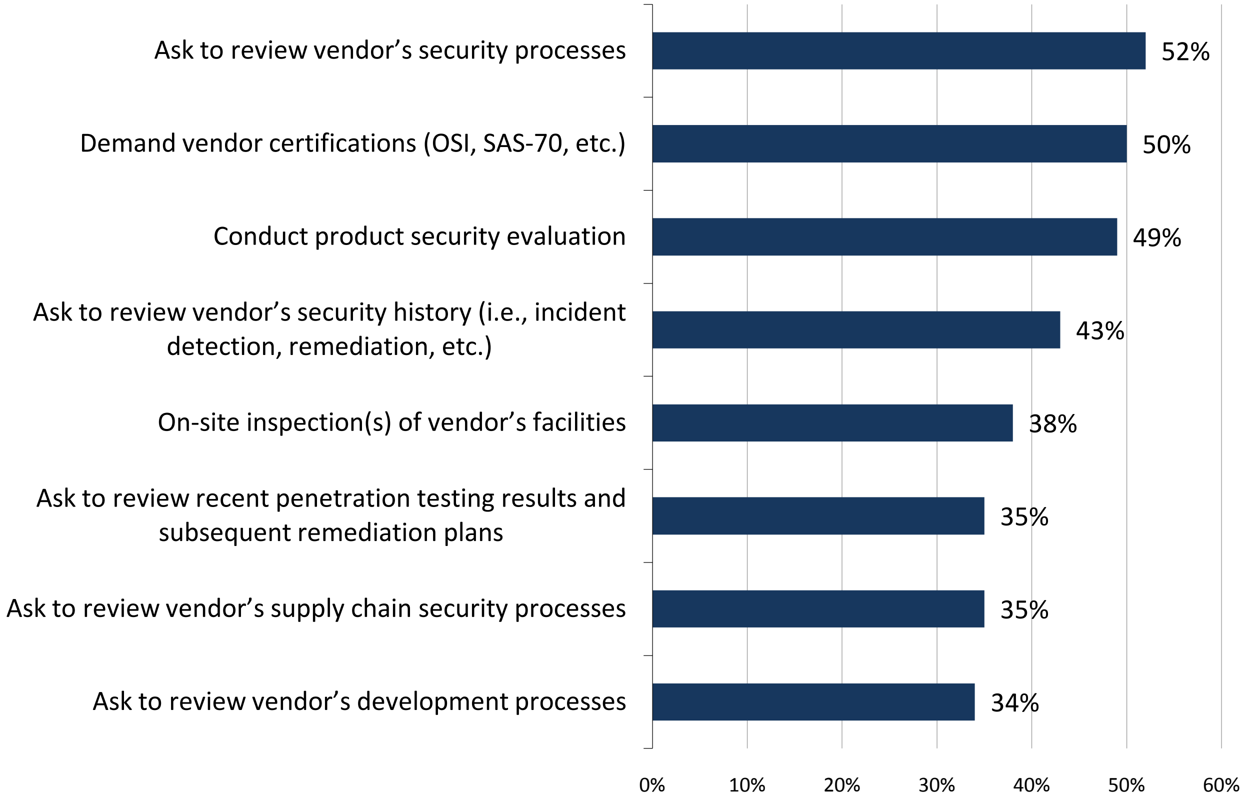


Source: Enterprise Strategy Group, 2010.

When respondent organizations do conduct vendor audits, they most often look at their vendors' security processes, demand vendor certifications, or conduct product security evaluations. Fewer go further and audit vendor facilities, cyber supply chain security processes, or product development methodologies (see Figure 15).

Figure 15. Mechanisms Used to Conduct Vendor Security Audits

You have indicated that your organization conducts audits of its IT vendors' security processes. Which of the following mechanisms does your organization use to conduct these vendor audits? (Percent of respondents, N=234, multiple responses accepted)

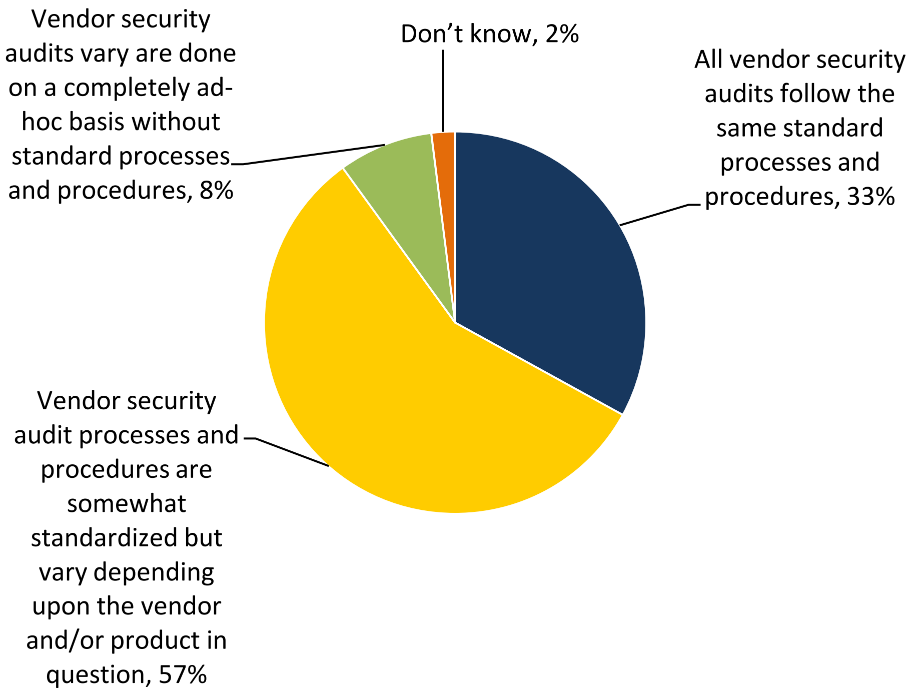


Source: Enterprise Strategy Group, 2010.

As previously noted, ESG Research found that most IT vendor audits are done on an ad hoc or as-needed basis. This means that some vendors go through security audits while others may be passed over. The data points to an additional problem around the consistency of audit procedures: one one-third of the CIKR organizations said that "all vendor audits follow the same processes and procedures" (see Figure 16). While one IT vendor may go through a highly detailed audit process, another may be given a high-level assessment, increasing the likelihood that security vulnerabilities are overlooked.

Figure 16. Current IT Vendor Security Audit Process

Which of the following statements best reflects your current IT vendor security audit process? (Percent of respondents, N=234)



Source: Enterprise Strategy Group, 2010.

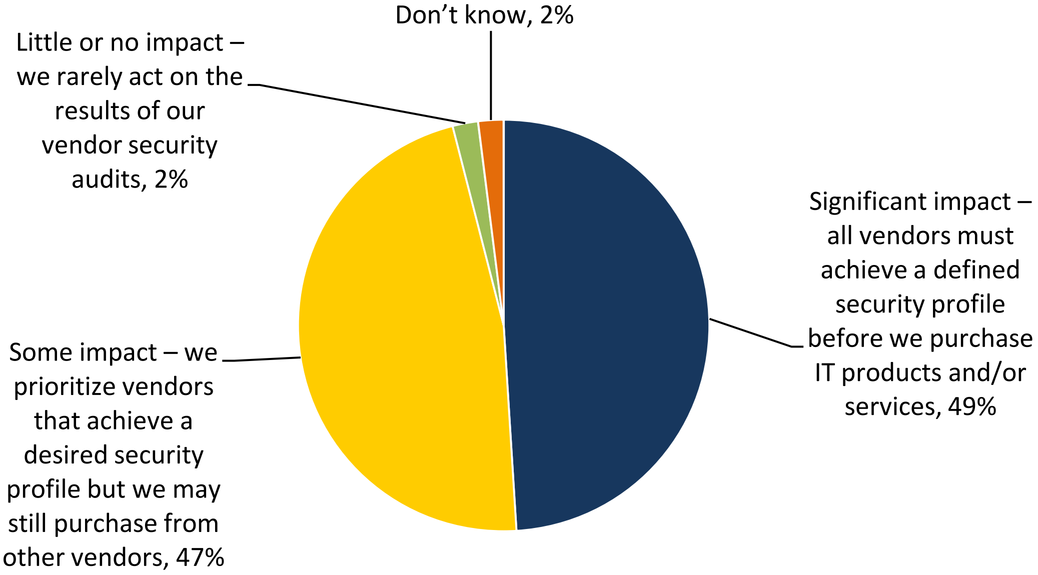
The critical infrastructure organizations surveyed by ESG perform semi-structured security audits of some IT vendors, mostly on an ad hoc or as-needed basis. What is the ultimate value of these audits? The data indicates a bifurcated population: nearly half of respondents said that vendor audits have "significant impact" on their organization's ultimate IT purchasing decisions whereby vendors are required to achieve a "passing grade" in order to sell that organization their IT products and services. The other half of the population placed less value on vendor security audits. In these cases, a "passing grade" gives vendors some level of priority, but CIKR organizations may still purchase products and services from vendors with "failing grades" or from those that haven't been audited at all (see Figure 17). In these cases, IT vendor security audits may be little more than a formality. In other words, performing IT vendor security audits may be seen as process requirement rather than a real security assessment used to select secure hardware and software to bolster overall cyber security. This type of "check box" mentality is counterproductive and extremely wasteful.

ESG Data Insight

Sixty-five percent of critical infrastructure organizations obligated to comply with more than three regulations said that vendor security audits had a "significant impact" on their procurement decisions. This compares to 49% of the general survey population.

Figure 17. How Results of Security Audits Impact Purchasing Decisions

How do the results of your IT vendor security audits ultimately impact your organization's purchasing decisions? (Percent of respondents, N=234)



Source: Enterprise Strategy Group, 2010.

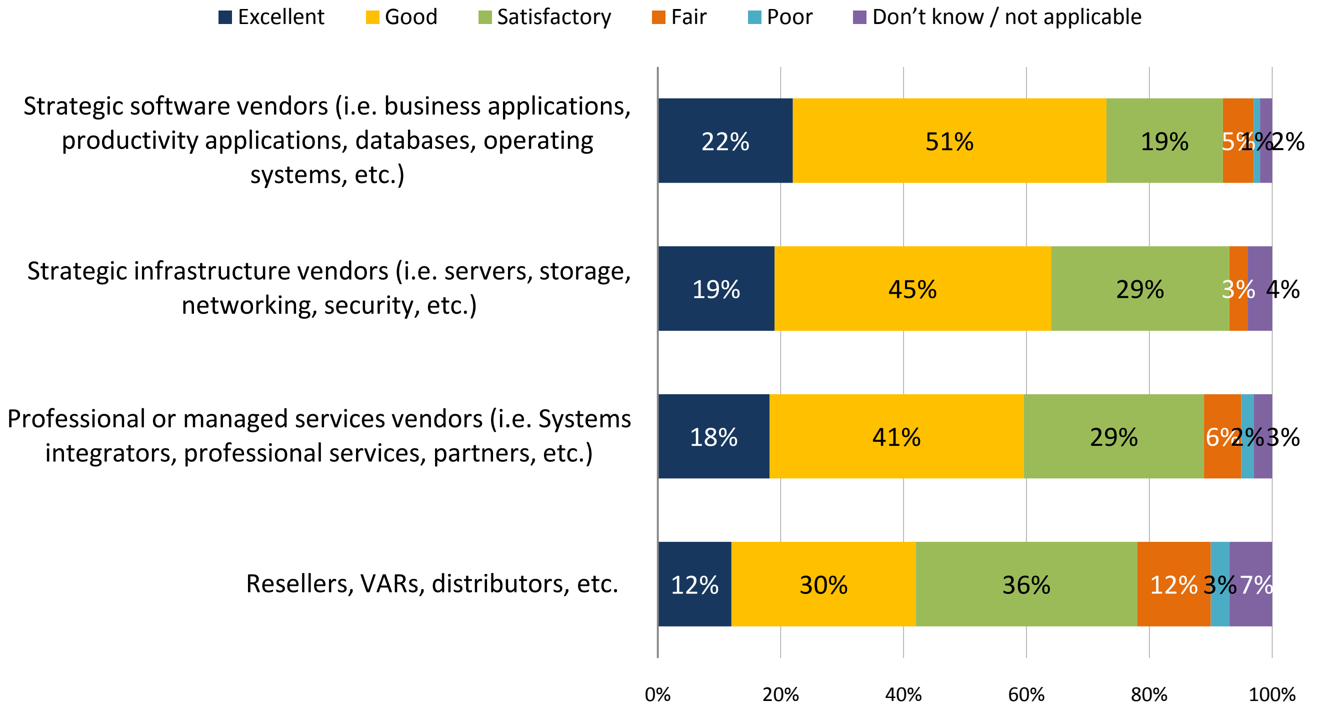
When asked to rate their vendors' commitment to and communications about their internal security processes and procedures, few respondents gave their vendors a rating of "excellent." In fact, a higher percentage of organizations rated their IT vendors' security as "satisfactory," "fair," or "poor" (see Figure 18).

Why are security perceptions so low? ESG believes that it may be a function of due diligence—CIKR organizations that carefully scrutinize their IT vendors' security are the most likely to rate their vendors' commitment to and communication about their internal security processes and procedures as "excellent." For example, 35% of CIKR organizations with "strong" cyber supply chain security rated their strategic software vendors' commitment to and communication about their internal security processes and procedures as "excellent." In comparison, only 10% of CIKR organizations with "weak" cyber supply chain security rated their strategic software vendors' commitment to and communication about their internal security processes and procedures as "excellent." It is likely that those with "strong" cyber supply chain security are asking more questions, demanding cogent answers, and eschewing IT vendors that can't or won't cooperate. CIKR organizations with "marginal" or "weak" cyber supply chain security are probably not asking as many questions or demanding as many responses. Without concrete data, impressions about IT vendors' security are based upon superficial information and assumptions rather than facts.

Note also that professional services firms and distributors get lower marks than strategic software or infrastructure vendors. This could represent a cyber security threat vector that is open for easy exploitation. This should not be dismissed as a low risk: There is evidence to suggest that the recent Stuxnet worm was introduced into control systems by professional service technicians using compromised USB flash drives.

Figure 18. Rating of IT Vendors' Commitment to and Communications About Internal Security Processes/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, N=285)

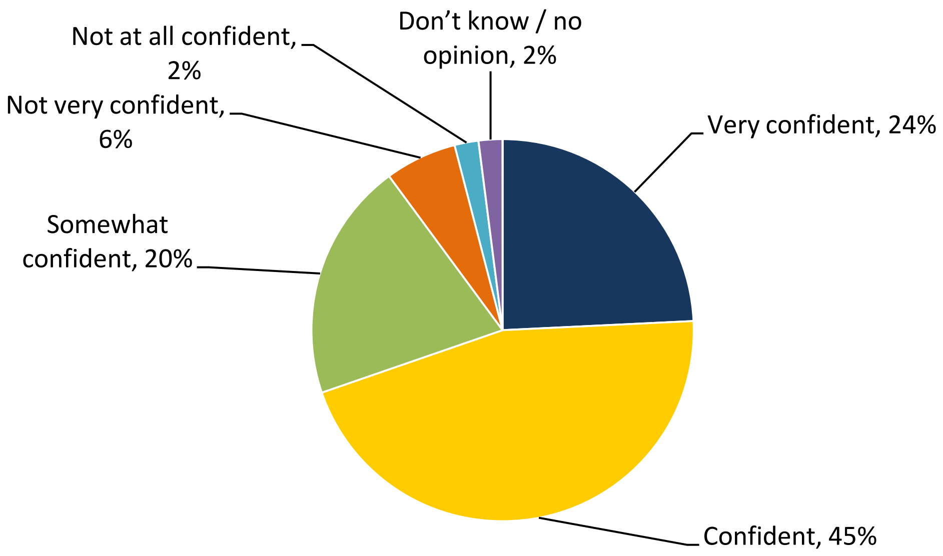


Source: Enterprise Strategy Group, 2010.

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 cyber crime or even state-sponsored cyber espionage. Given these realities, one would think that CIKR organizations would carefully trace the origins of the IT products purchased and used by their firm. ESG's data suggests that many firms aren't so sure about the geographic lineage of their IT assets—only one-fourth 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 (see Figure 19).

Figure 19. Confidence Level Related to Knowledge of Where IT Hardware and Software Products Were Developed

In your opinion, how confident are you that your organization knows where the IT hardware and software products it purchases were physically developed and/or manufactured (i.e., country of origin)? (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

In summary, ESG's research finds that many CIKR organizations are not performing an adequate amount of security due diligence with IT vendors. To close loopholes and minimize the risk of a cyber supply chain attack, vendor audit best practices would have to include the following three steps:

1. Organization "always" audits the internal security processes of strategic software vendors
2. Organization uses a standard audit process for all vendor audits
3. Organization has a policy whereby the results of IT vendor security audits have a "significant" impact on IT procurement decisions

When ESG assessed CIKR organizations through this series of IT audit steps, the results were extremely distressing. For example, only 10% of the total survey population adhered to all three best practice steps when auditing the security of their strategic software vendors (see Table 1). Since strategic software vendors are audited most often, it is safe to assume that less than 10% of the total survey population follows these best practices when auditing the security of IT infrastructure, professional services, and distributors.

Table 1. Incidence of Best Practices for IT Vendor Security Audits

Best Practice Step	Percentage of Total Survey Population
1. Organization "always" audits the internal security processes of strategic software vendors	31%
2. Organization "always" audits the internal security processes of strategic software vendors AND 3. Organization uses a standard audit process for all vendor audits	13%
4. Organization "always" audits the internal security processes of strategic software vendors AND 5. Organization uses a standard audit process for all vendor audits AND 6. Organization has a policy whereby the results of IT vendor security audits have a “significant” impact on IT procurement decisions	10%

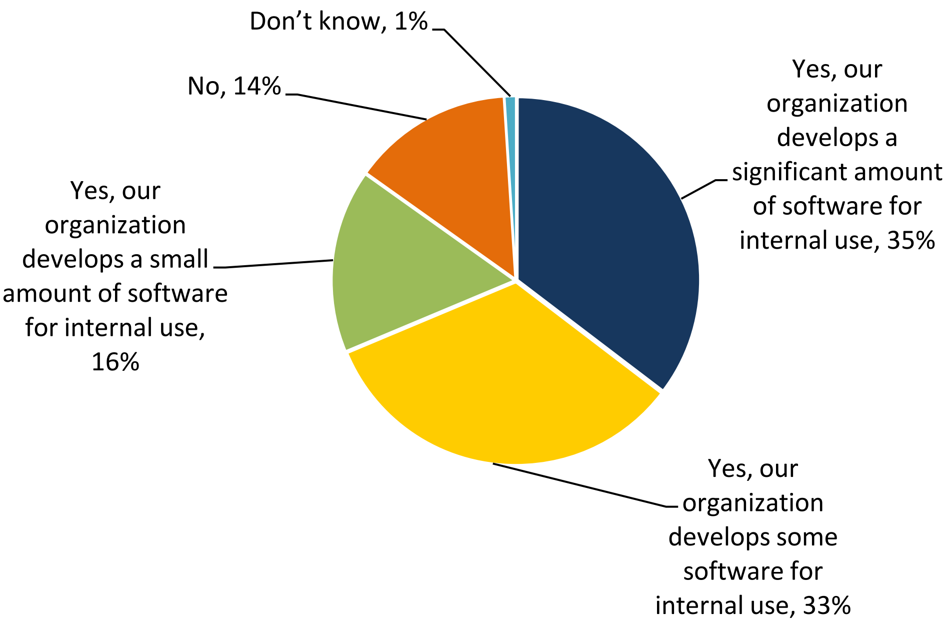
Cyber Supply Chain Security and Software Assurance

Software assurance is another key tenet of cyber supply chain security as it addresses the risks associated with a cyber security 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 35% of the CIKR organizations surveyed develop a "significant" amount of software for internal use while another 49% of organizations develop at least some software for internal use (see Figure 20).

Figure 20. Software Development Activities

Does your organization write its own software in order to develop custom business applications for its own internal use? (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

Once dismissed as a minor concern, software assurance has become increasingly important over the past few years. For example, the U.S. Department of Defense recognized the need for secure software development and established a software assurance program in 2003.

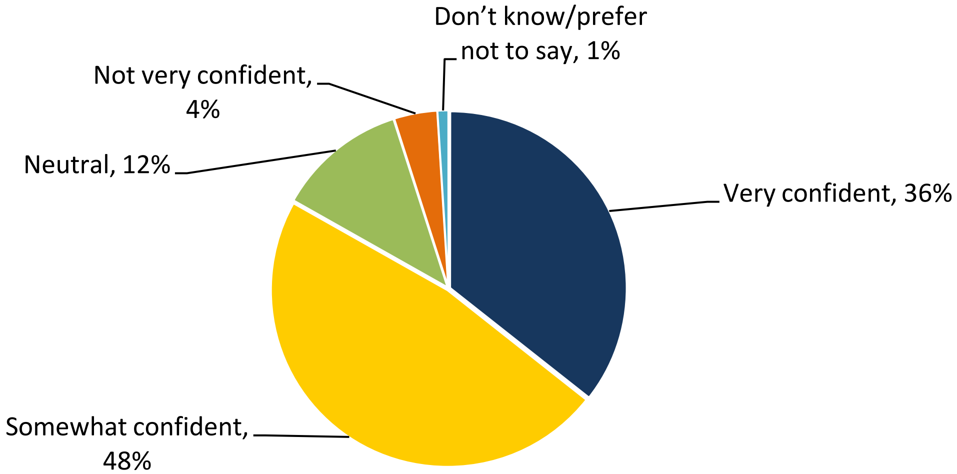
Why the focus of software assurance? Industry experts believe that approximately 70% of all cyber security attacks now target applications (primarily web applications) rather than operating systems or networks. This attack pattern is no accident since many web applications are fraught with software vulnerabilities. According to the IBM X-Force Trend and Risk Report (2008):

> *"Web applications in general have become the Achilles Heel of Corporate IT Security. Nearly 55% of vulnerability disclosures in 2008 affect web applications, and this number does not include custom-developed web applications (only off-the-shelf packages). Seventy-four percent of all Web application vulnerabilities disclosed in 2008 had no available patch to fix them by the end of 2008."*

Since 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: 36% of respondents say that they are "very confident" in the security of their organization's internally-developed software, but nearly half say they are "somewhat confident" and another 12% claim to be neutral—i.e., neither confident or not confident (see Figure 21).

Figure 21. Confidence Level in the 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=242)



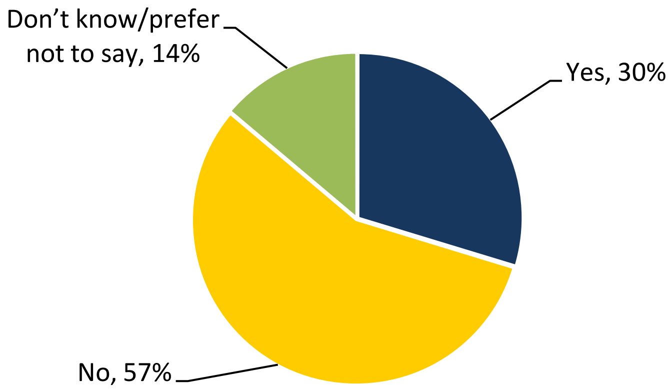
Source: Enterprise Strategy Group, 2010.

The responses captured in Figure 21 are based on opinion alone. 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. Alarmingly, 30% said "yes" (see Figure 22).

ESG also wanted to know the rate of security incidents related to compromised internally-developed software as it related to the 35% of critical infrastructure organizations that develop a "significant amount of software for internally use." Unfortunately, this population is even more vulnerable to attack—43% of CIKR organizations that develop a significant amount of software experienced a security incident directly related to the compromise of internally-developed software. In comparison, 27% of CIKR organizations that develop some software for internal use and 6% of critical infrastructure organizations that develop a small amount of software for internal use have experienced a security incident directly related to the compromised of internally-developed software. Evidently, custom CIKR software represents an attractive target for malicious insiders and external cyber criminals.

Figure 22. Security Incidents Related to Homegrown 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=242)

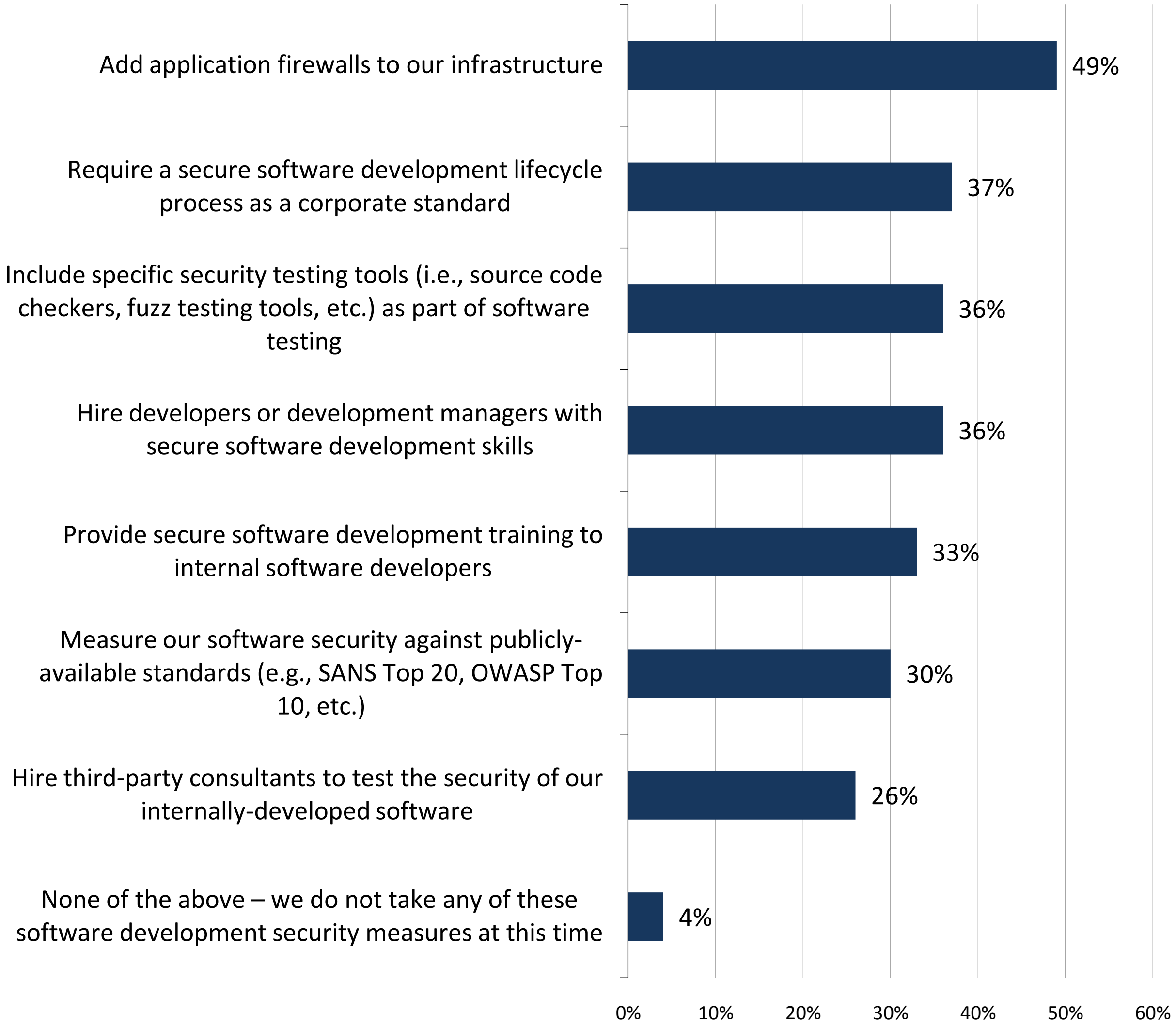


Source: Enterprise Strategy Group, 2010.

Rather than ignore the risks associated with insecure software development, the critical infrastructure organizations surveyed are instituting various software assurance countermeasures. The most popular of these is also the easiest—nearly half of the organizations surveyed have deployed application firewalls as security check points. These devices examine traffic, detect application attacks, and block them from accessing applications. Application firewalls are a logical first step as they can immediately address risk (see Figure 23).

Figure 23. Security Activities as Part of 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=242, multiple respondents accepted)

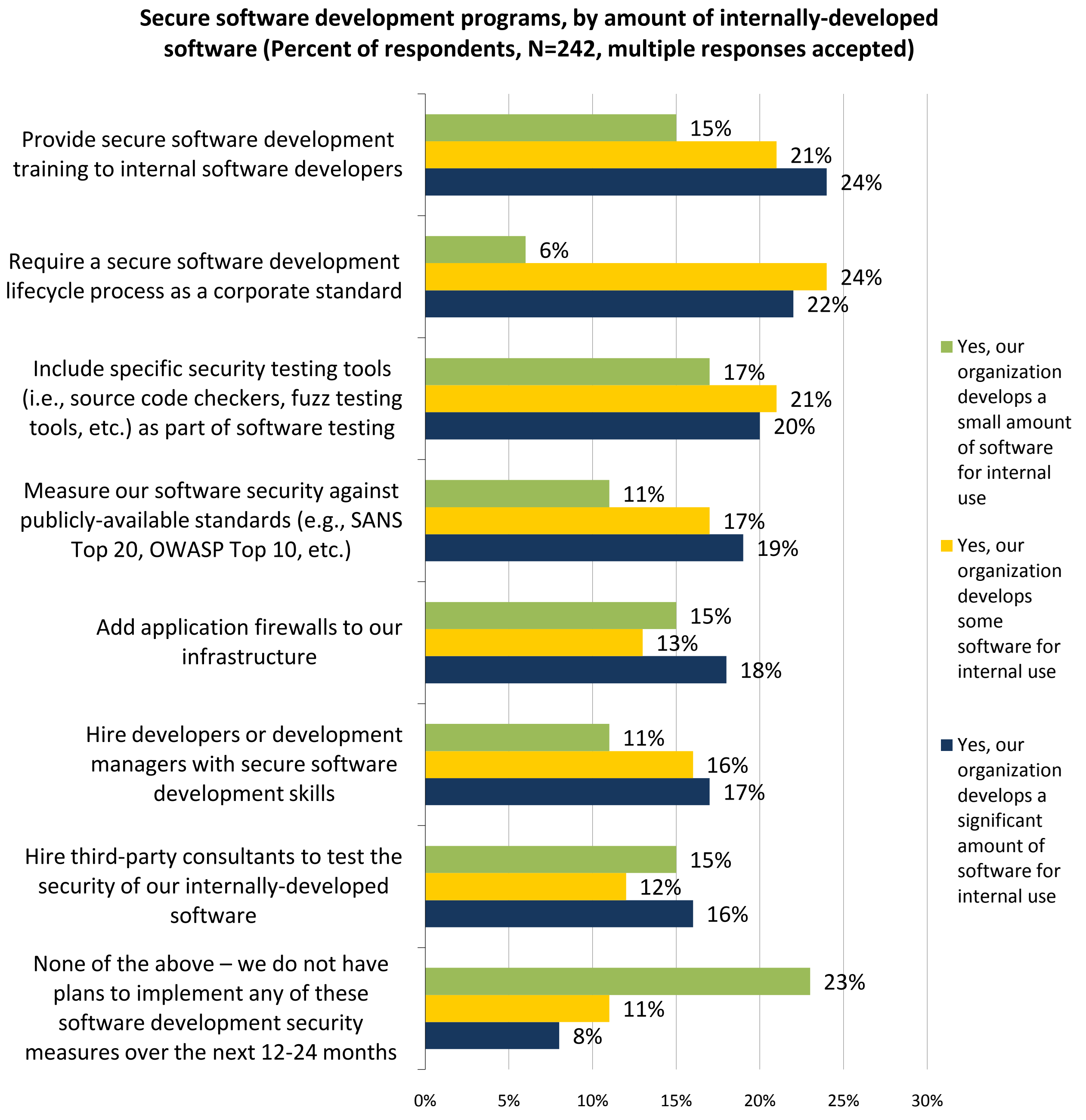


Source: Enterprise Strategy Group, 2010.

When it comes to embracing other secure software development processes, however, critical infrastructure organizations surveyed aren't as proactive: 37% "require a secure software development lifecycle," 36% "include specific security testing tools," and 36% "hire developers or development managers with secure software development skills." In an era of abundant software vulnerabilities and sophisticated cyber attacks, CIKR organizations seem rather nonchalant about their software assurance initiatives. While some implement application firewalls, most are not addressing the root cause of software security problems: insecure software development. This should be viewed as a cause for concern.

Fortunately, critical infrastructure organizations developing a "significant" amount of software for internal use are generally the most aggressive with software assurance programs, but this still leaves others vulnerable (see Figure 24). Note that 23% of organizations that develop a "small" amount of software for internal use haven't undertaken any measures for software assurance.

Figure 24. Security Activities as Part of Software Development Process

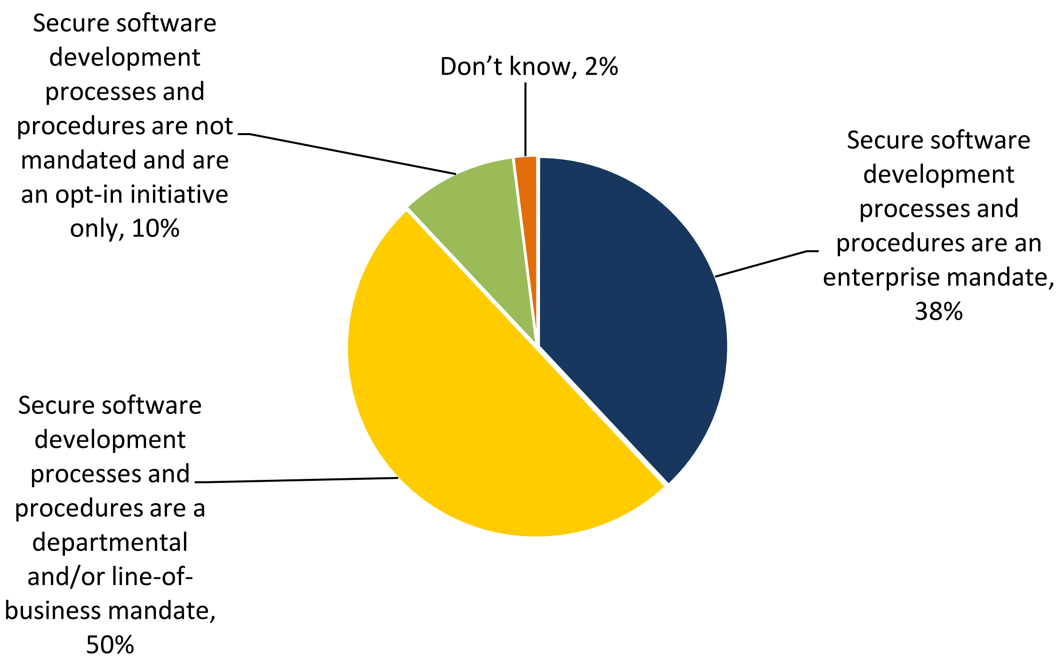


Source: Enterprise Strategy Group, 2010.

The establishment of secure software development programs is a step in the right direction, but software assurance effectiveness is a function of two factors: the number and type of programs, and how widely they are used. Half of the critical infrastructure organizations surveyed implement secure software development processes and procedures as departmental or line-of-business mandates (see Figure 25). This leaves a lot of variability where some departments institute 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 a security attack that impacts the entire enterprise.

Figure 25. Secure Software Development Initiatives

Which of the following best describes the extent of your organization's secure software development initiatives? (Percent of respondents, N=189)

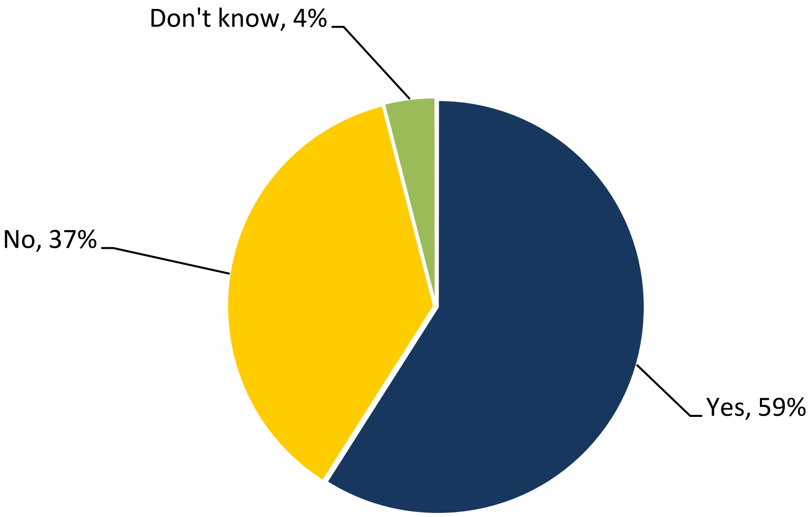


Source: Enterprise Strategy Group, 2010.

These days, secure software development extends beyond the proverbial four walls of the organization—nearly 60% of the critical infrastructure organizations surveyed currently outsources some software maintenance or development activities to third party consultants, outsourcers, or service providers (see Figure 26).

Figure 26. Software Maintenance and Development Outsourcing Frequency

Does your organization outsource any of its software maintenance or development activities to third-party consultants, outsourcers, or service providers? (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

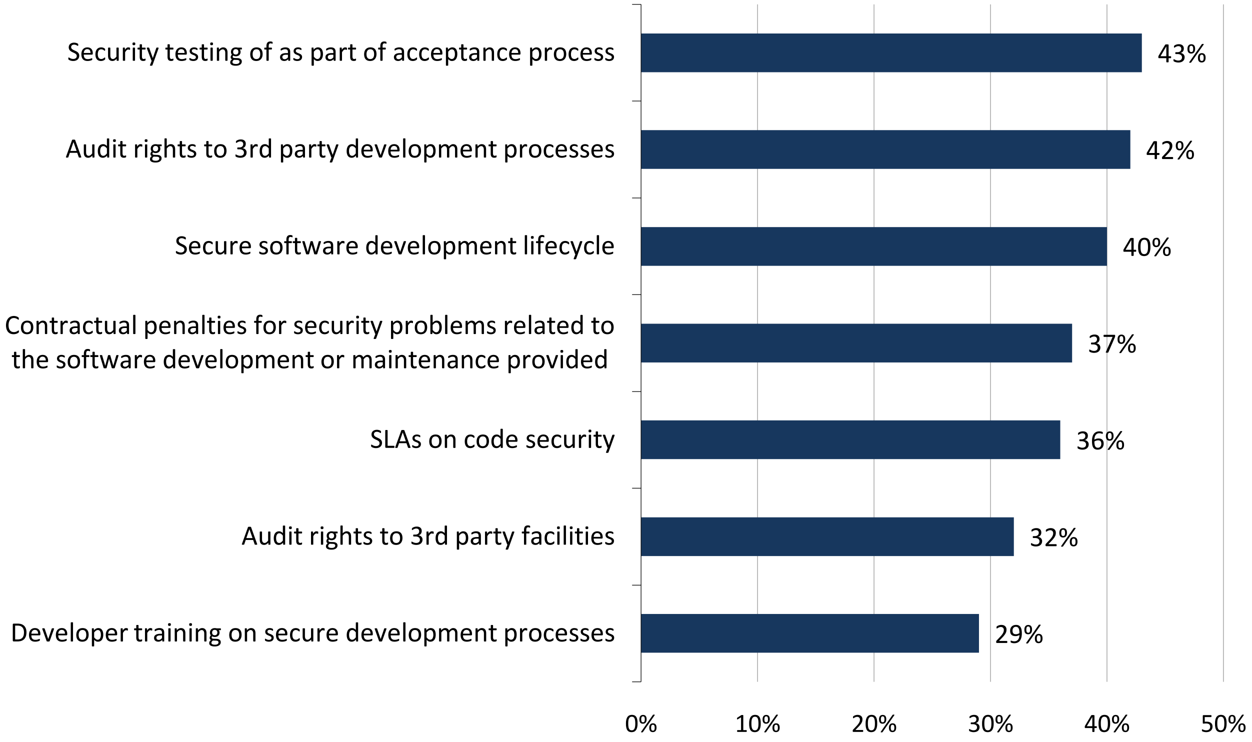
According to ESG survey respondents, software development and maintenance outsourcers are required to adhere to a laundry list of secure software development programs including security testing, security audits, and secure software development lifecycles (see Figure 27). One could make the case that many CIKR organizations place more stringent software assurance requirements on third parties than on their own internal software developers.

ESG Data Insight:

Sixty-one percent of critical infrastructure organizations with more than 20,000 employees mandate "security testing as part of acceptance process." This compares with 43% of all organizations that outsource software maintenance and development.

Figure 27. Secure Software Development Mandates for Third Party Software Maintenance and Development

Please indicate which of the following security safeguards (if any) your organization mandates as a requirement of the service provider. (Percent of respondents, N=169, multiple respondents accepted)



Source: Enterprise Strategy Group, 2010.

Software assurance best practices demand all custom software development (internal or outsourced) follow a standard secure software development lifecycle. Developers would be required to go through secure software development training and would be measured and incented on their ability to write secure code. Finally, all software would go through extensive security testing before being deployed in a production environment.

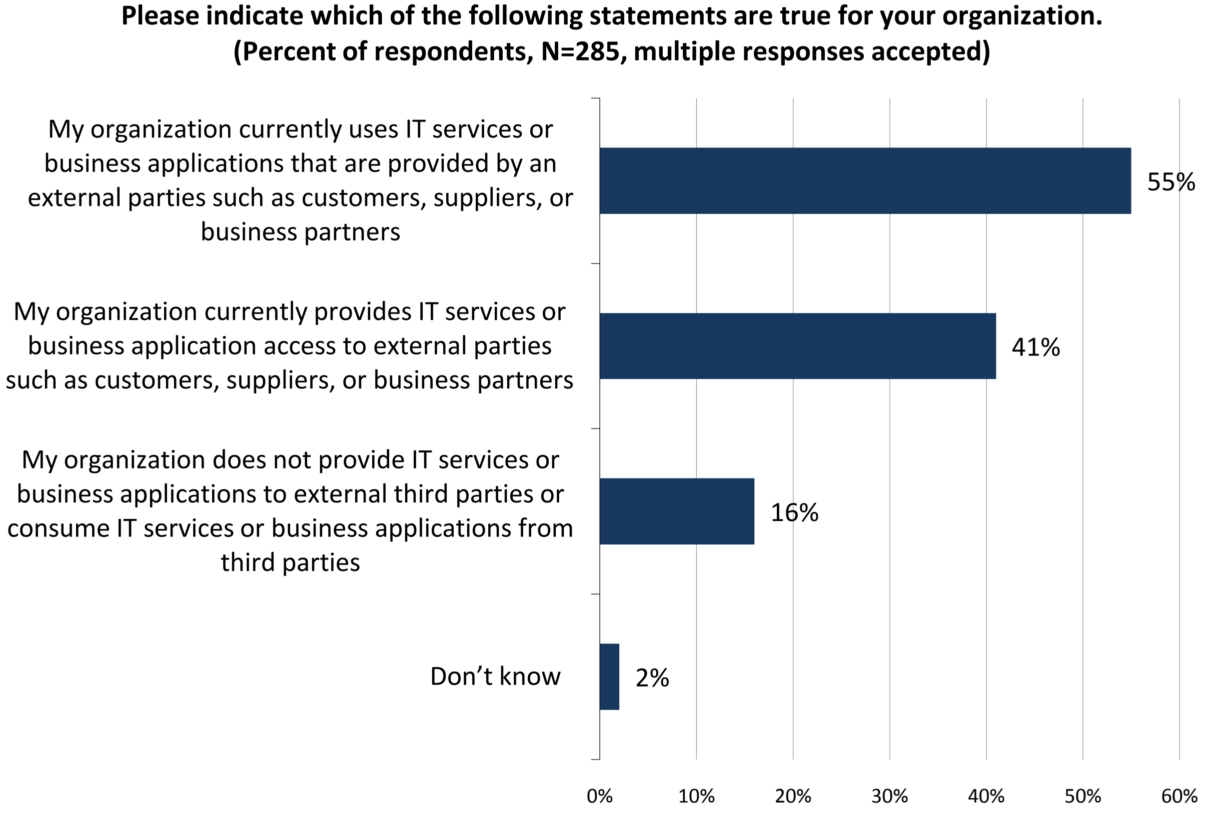
The ESG data indicates general software assurance activity, but programs appear to be randomly implemented and inconsistently enforced. This is understandable as software assurance is a fairly new discipline. Many experienced software developers were never provided with secure software development training and there are no definitive industry benchmark best practices for software assurance.

Regardless of these obstacles, however, the fact remains that insecure software makes the U.S. critical infrastructure vulnerable to attack. Addressing this risk will require critical infrastructure organizations to work more closely with federal agencies, security organizations, and IT vendors to establish and enforce standard secure software development best practices for internal and outsourced software maintenance and development. Furthermore, we saw previously that only 34% of organizations audit their IT vendors' development processes. In the future, IT vendors must be given a clear ultimatum: Establish and enforce software assurance best practices or expect to be prohibited from selling products to CIKR organizations.

Cyber Supply Chain Security and External IT

With the advent of the Internet and new types of web-friendly applications, corporate IT has become a cooperative service where enterprise organizations provide and/or consume business applications and IT services from a variety of suppliers, customers, business partners, and other external parties. This is certainly true with regard to the critical infrastructure organizations surveyed—55% of respondents say that their organization "uses IT services or business applications" provided by external parties, while 41% or organizations "provide IT services or business application access to external parties" (see Figure 28).

Figure 28. How Organizations Use IT Services



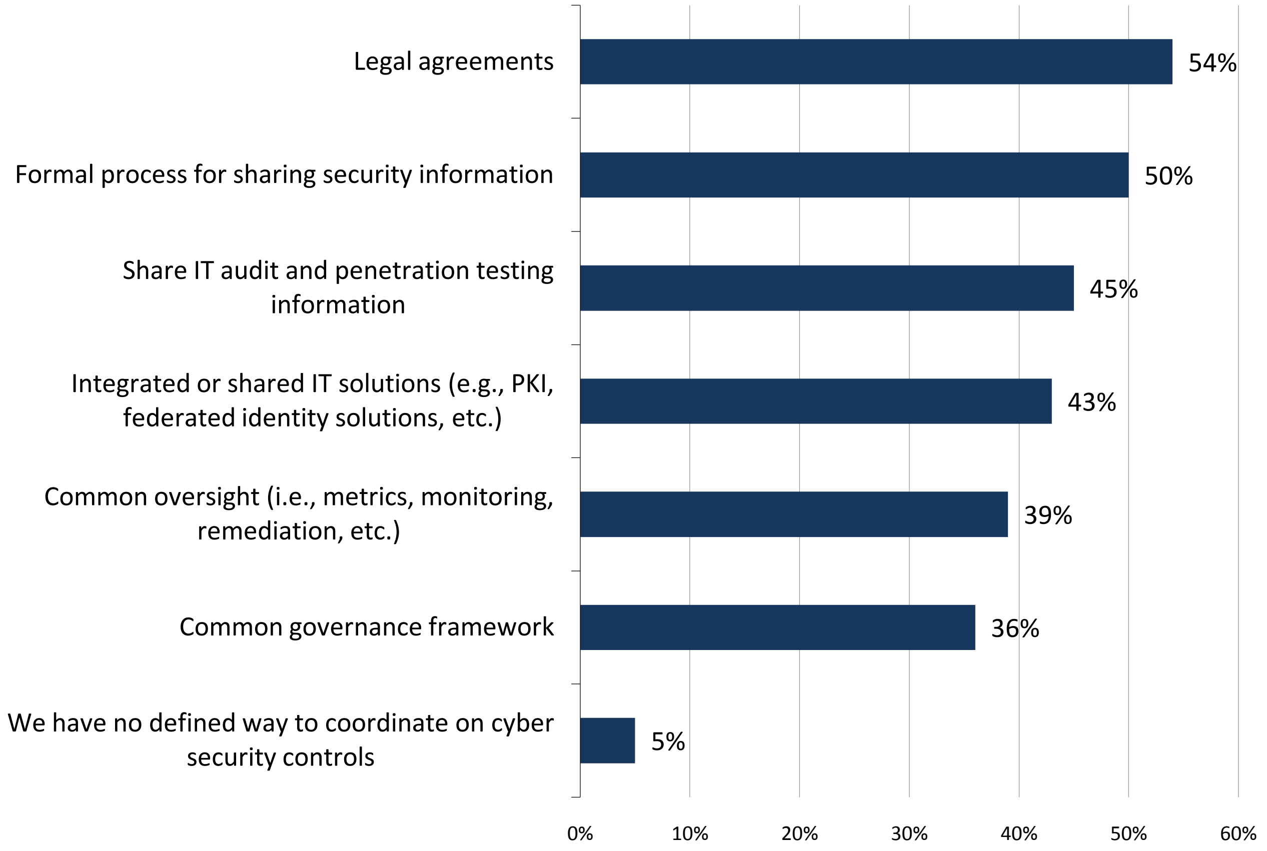
Source: Enterprise Strategy Group, 2010.

There is no question that externalizing IT helps many organizations increase productivity, improve customer satisfaction, or automate business processes. Unfortunately, these benefits come with a cost: increased cyber security risk. As the old information security adage states, "the security chain is only as strong as its weakest link." This rule applies when critical infrastructure organizations connect their IT systems with one another.

The ESG research data indicates that critical infrastructure organizations that either consume or provide external IT services are addressing this increased risk with measures such as "legal agreements, "formal processes for sharing security information," and by communicating on "IT audit and penetration testing information" with third party partners. While these safeguards are a good start, fewer organizations are implementing more cooperative and proactive controls like "common oversight" or a "common governance framework." In this case, most security arrangements fail to establish a foundation of strong security controls or tools/processes for real-time risk management (see Figure 29).

Figure 29. Security Controls Requires by Customers and Partners When Organization is Providing IT Services to External Partners

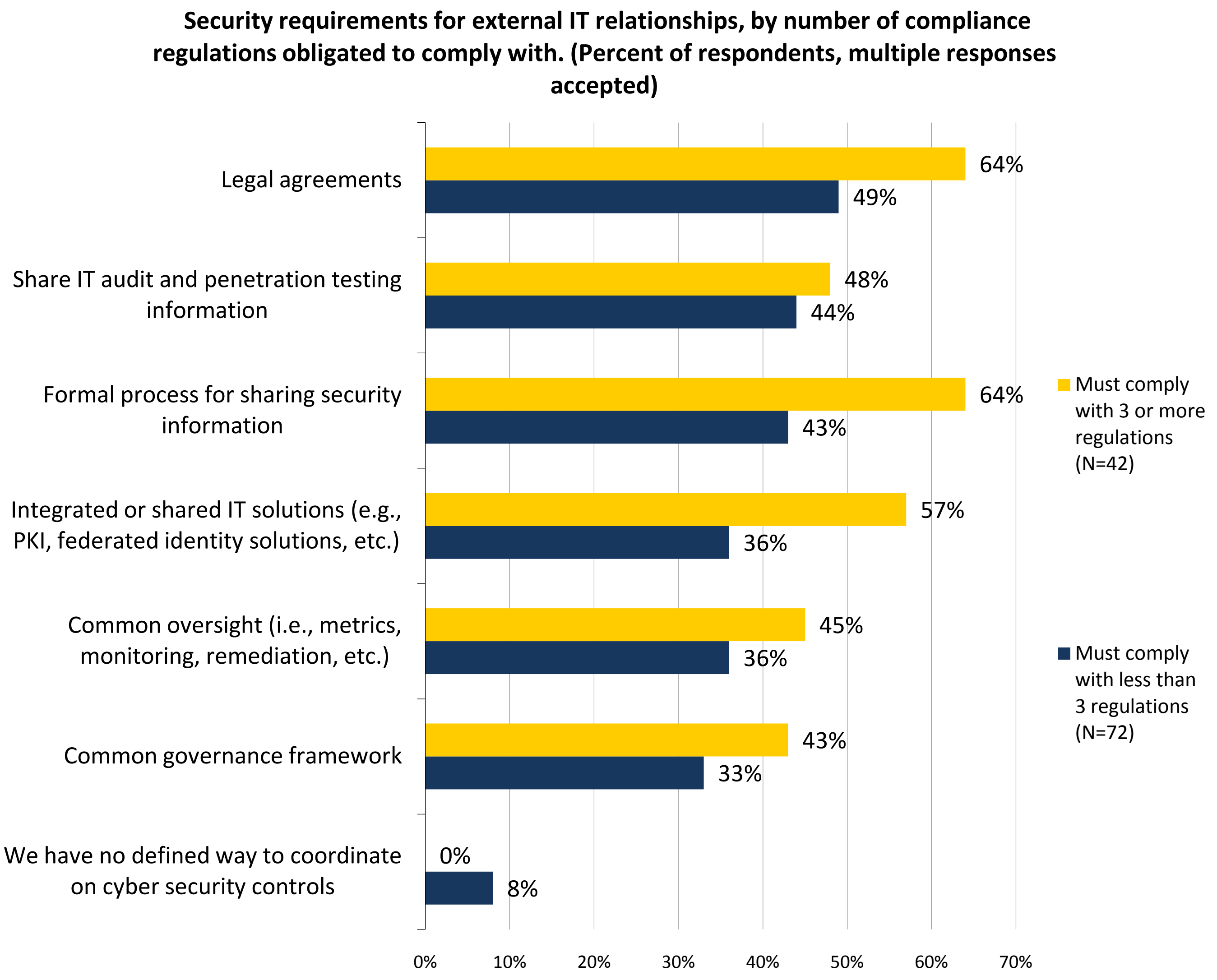
When your organization is providing IT services to external parties, which of the following security controls do your customers and partners typically require? (Percent of respondents, N=118, multiple responses accepted)



Source: Enterprise Strategy Group, 2010.

It is worth noting that critical infrastructure organizations obligated to comply with more than three government/industry regulations establish stronger cooperative security controls than less regulated firms (see Figure 30). These highly-regulated firms have lots of experience implementing security controls, monitoring activities, and working with compliance auditors. ESG's data indicates that they take this experience into external IT relationships in order to anticipate and avoid security problems from the start.

Figure 30. Security Controls Required by Customers and Partners When Organization is Providing IT Services to External Partners

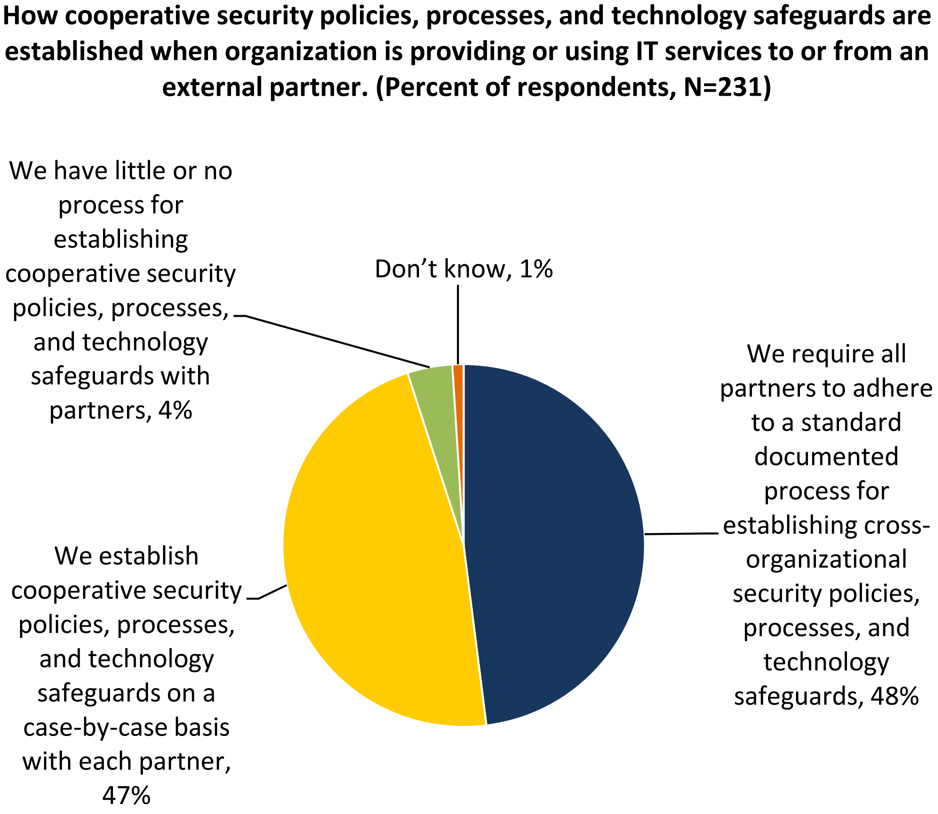

Security requirements for external IT relationships, by number of compliance regulations obligated to comply with. (Percent of respondents, multiple responses accepted)

Source: Enterprise Strategy Group, 2010.

To avoid any "weak links" in the "security chain," each and every external IT relationship should be protected with strong security policies, processes, and proactive oversight. Nearly half of the critical infrastructure organizations surveyed currently follow these best practices, requiring all partners to adhere to a standard documented process for establishing cross-organizational security. Unfortunately, the rest of the CIKR organizations surveyed are not as thorough—47% establish cooperative security on a case-by-case basis while 4% have little or no process for establishing cooperative security (see Figure 31).

Readers should note that 83% of CIKR organizations with "strong" cyber supply chain security require standard and documented cooperative security policies and safeguards with external IT partners. This compares with 35% of CIKR organizations with "marginal" cyber supply chain security and 19% of critical infrastructure firms with "weak" cyber supply chain security. Obviously, cooperative security is a fundamental cyber supply chain security best practice.

Figure 31. How Cooperative Security Policies, Procedures, and Safeguards are Established When Organization is Providing or Using IT Services From External Partner



Source: Enterprise Strategy Group, 2010.

It is worth noting that external IT relationships between business partners are rapidly increasing. This trend will only accelerate with the growth of mobile devices, web-based applications, "smart" infrastructure, and cloud computing.

Securing this increasingly complex web of connections between critical infrastructure organizations depends upon established guidelines, cooperative controls, common oversight, and real-time monitoring. A sub-set of heavily regulated organizations as well as those familiar with cyber supply chain security are headed down this path, but the majority of critical infrastructure organizations surveyed are following a more laissez faire approach that exposes them to the risks associated with "weak link" business partners.

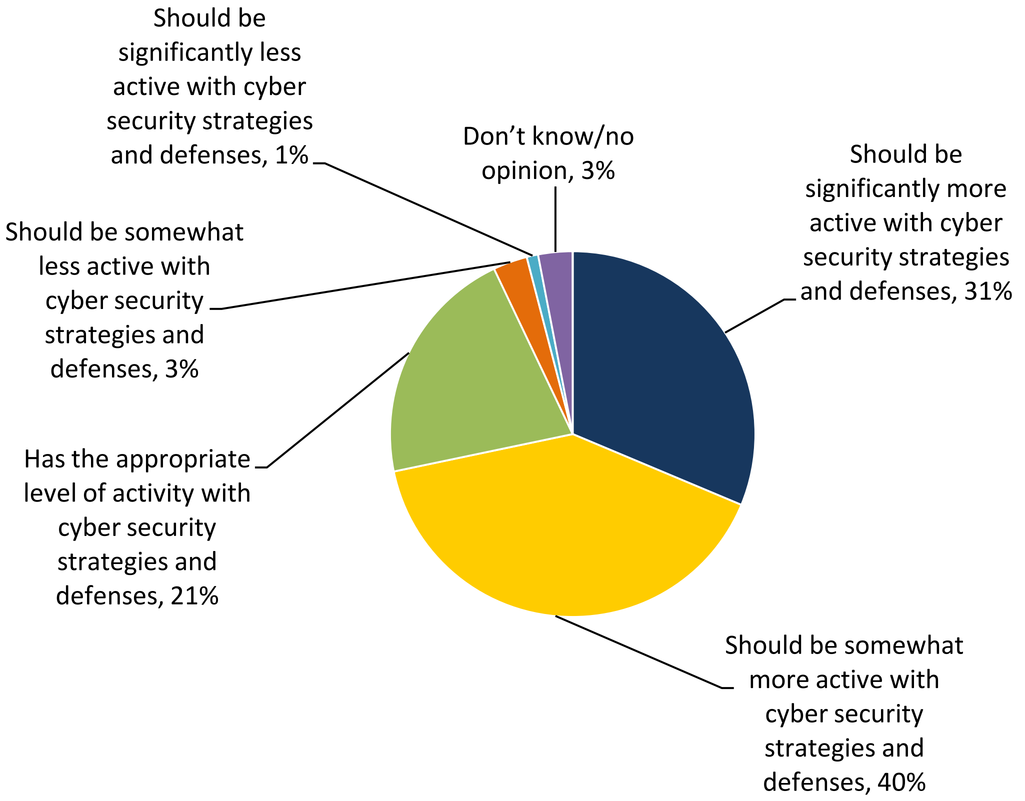
The Federal Government's Role in Cyber Security

The results of ESG's research reveal that few critical infrastructure organizations have a secure IT foundation and even fewer are proceeding toward fully securing their cyber supply chains. This alone is cause for concern, especially when most organizations believe that the information security threat landscape continues to worsen.

This begs an important question: Should the U.S. Federal Government get more involved in actively trying to improve cyber supply chain security or remain on the sidelines? Seventy-one percent of the critical infrastructure organizations surveyed believe that there needs to be more involvement from the Federal Government with nearly one-third of the overall survey population proclaiming that the government should be "significantly more active" with respect to cyber security strategies (see Figure 32). Notably, the most secure CIKR organizations are also the ones demanding more federal cyber security action. Forty-two percent of respondents working at CIKR organizations with "strong" supply chain security said that the federal government should be "significantly more active." This compares with 29% of CIKR organizations with "marginal" cyber supply chain security and 24% of critical infrastructure firms with "weak" cyber supply chain security. ESG believes that the federal government would be prudent to heed such calls for action, given that they are coming from the nation's most sophisticated and well-protected CIKR organizations.

Figure 32. Federal Government Involvement with Cyber Security Strategies and Defenses

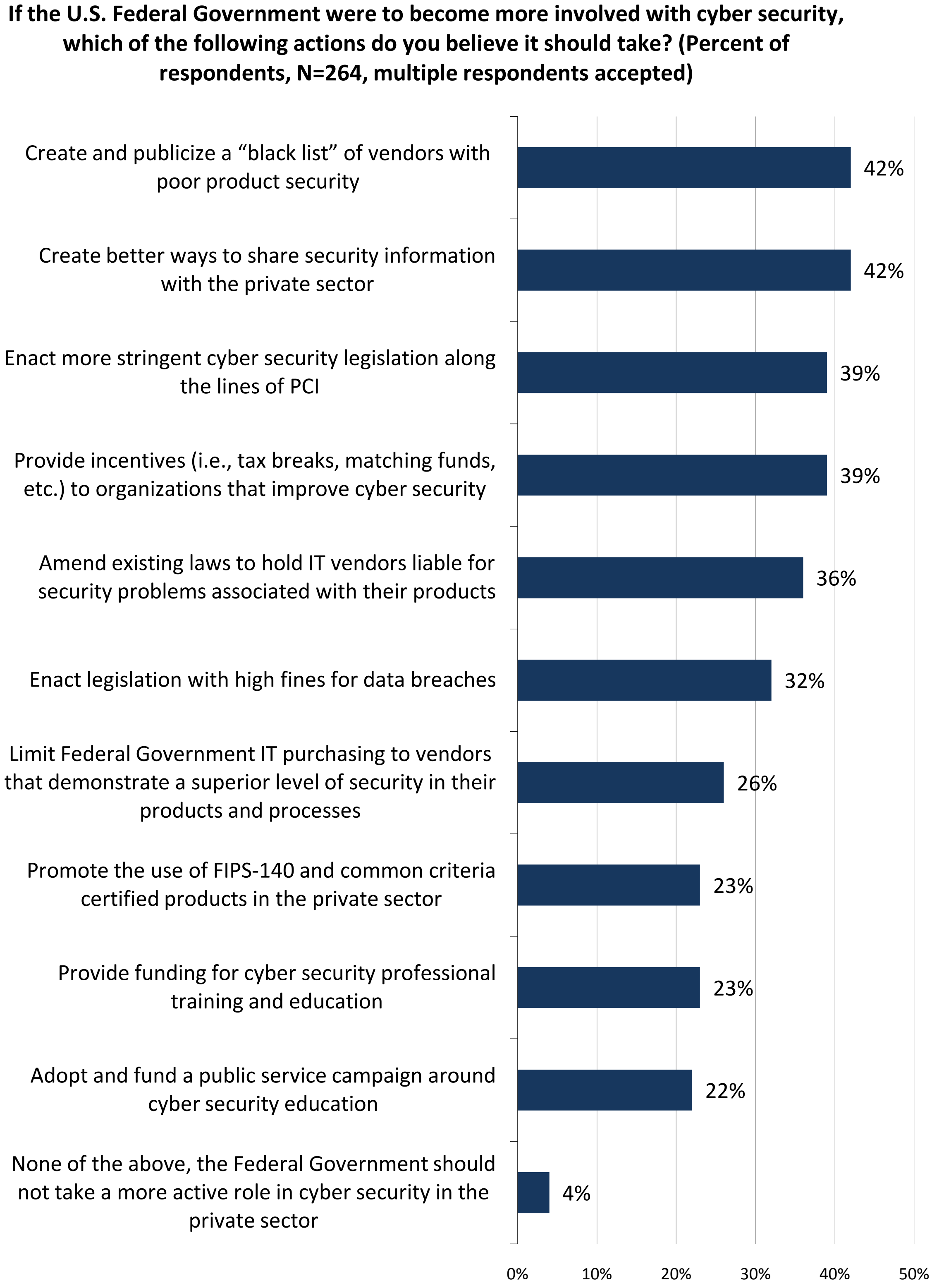
Please complete the following statement by selecting one of the responses below.
In my opinion, the U.S. Federal Government: (Percent of respondents, N=285)



Source: Enterprise Strategy Group, 2010.

Just what should the Federal Government do? ESG provided respondents with a number of potential options. The most popular responses suggest that the Federal Government "create a black list of vendors with poor product security," " create better ways to share security information with the private sector," "enact more stringent cyber security legislation along the lines of PCI," and provide various types of incentives to increase security investment at critical infrastructure organizations (see Figure 33).

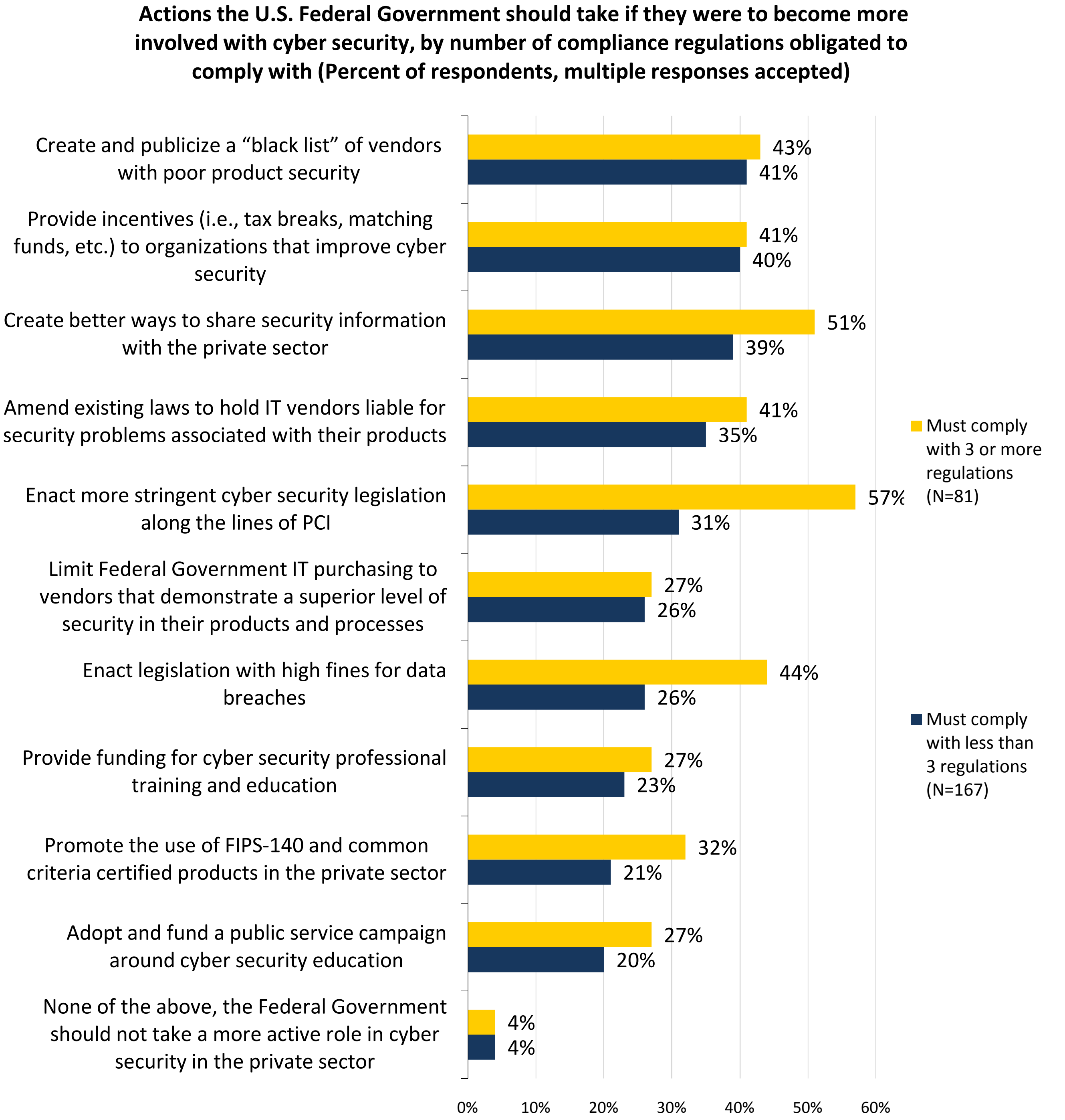
Figure 33. Actions the Federal Government Should Take with Respect to Cyber Security



Source: Enterprise Strategy Group, 2010.

It is worthwhile to look at how critical infrastructure organizations obligated to comply with more than three industry/government regulations responded to this question. This heavily-regulated sub-set of the survey population was consistently more advanced in cyber security and had ample experience with the strengths and weaknesses of regulations. It is interesting, then, that these highly-regulated organizations called for the government to "enact more stringent security legislation along the lines of PCI," and "enact legislation with high fines for data breaches" (see Figure 34).

Figure 34. Actions the Federal Government Should Take with Respect to Cyber Security



Source: Enterprise Strategy Group, 2010.

Research Implications

This research survey uncovered a pattern of security weaknesses at CIKR organizations which come in two distinct areas:

1. Basic security weaknesses (i.e., problems with day-to-day security policies, processes, and security technology safeguards).
2. Limitations in understanding or addressing cyber supply chain risks.

These problems are directly related—addressing cyber supply chain risks must be built on top of a strong security foundation.

Based upon the research data presented herein, ESG offers the following recommendations for CIKR organizations, IT technology vendors, and the U.S. Federal Government.

For Critical Infrastructure Organizations

ESG believes that approximately 65% to 75% of the CIKR organizations surveyed are not prepared for the current threat landscape, let alone future security challenges or cyber supply chain security best practices. To move forward, these firms must address existing vulnerabilities while moving toward a more comprehensive enterprise security model. ESG recommends that CIKR organizations:

- **Align enterprise security with real-time risk management.** Reading between the lines of the data, ESG sees a familiar pattern where CIKR organizations may be too focused on regulatory compliance rather than monitoring and addressing real-time cyber security risks. Rather than maintain this regulatory compliance "check box" mentality, ESG believes that firms should follow the Federal Government's FISMA 2.0 lead by continuously monitoring the security of their networks. To move in this direction, ESG suggests that CIKR organizations take a hard look at the Consensus Audit Guidelines (CAG), a focused security model made up of 20 critical security controls. CAG was developed by John Gilligan (previously CIO of the US Department of Energy and the US Air Force) under the auspices of the Center for Strategic and International Studies. Members of the Consortium include NSA, US Cert, DOD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DOD Cyber Crime Center, and others. Think of CAG as a set of security control priorities for blocking well known types of attacks and addressing common vulnerabilities. CAG is also designed for real-time security monitoring and operational efficiency. CAG's simplicity, focus, and real-time risk management design are a good fit for CIKR organizations with fundamental security issues, limited security skills, and incomplete resources.

- **Improve knowledge and communication about the cyber security landscape.** The research presents cyber security knowledge gaps in many areas. Many CIKR organizations surveyed didn't understand or weren't following cyber supply chain security best practices in areas such as IT vendor audits, software assurance, or external IT security. As a result, many security programs seem haphazard at best. To bridge this gap, ESG believes that continuing security education is a critical requirement so that CISOs understand emerging threats AND new ideas around security controls and best practices. This knowledge must also propagate around the organization to CIOs, risk managers, and corporate executives, not just security professionals. As Sun Tzu stated in *The Art of War*, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

- **Make immediate and long-term changes around software assurance**. ESG's data indicates that about half of all large and small CIKR organizations have implemented application firewalls. This is a good first step to protect vulnerable web applications from attack, but it doesn't address the root cause: poorly-written, insecure software. Most developers have no clue how to write secure code. It is worth noting here that until the last few years, secure software development was universally ignored—even at universities with the best computer science programs in the world. To address this weakness, all software developers should be required to review publicly-available software assurance resources like the SANS Institute's top

25 software errors. Beyond this, developers should be incented to attend more formal secure software development training. CIKR organizations should also add specific security-oriented test suites and tools ASAP. Finally, all firms that develop software should establish a Secure Development Lifecycle along the lines of Microsoft's SDL. SDL is not an "all or nothing" program; rather, it can be implemented in a phased approach which Microsoft calls, "crawl, walk, run." Again, this can help resource-constrained critical infrastructure organizations gain short- and long-term benefits.

- **Formalize external IT security.** Over the next few years, new technologies like mobile IP devices, "smart planet" applications (i.e., smart grids, smart appliances, IP-connected cars, etc.), Web 2.0 applications, and cloud computing will blur the lines between internal and external IT systems and end-users. The problem, however, is that security vulnerabilities driven by these trends greatly exacerbate the risk of a cyber attack on the U.S. critical infrastructure. This scenario was demonstrated during the recent Cyber Shockwave exercises where cell phone vulnerabilities were used to disrupt global telecommunications networks, Internet access, and the U.S. electric power grid. It is disturbing to see that so many CIKR organizations are enjoying the benefits of external IT while minimizing the risks. While cyber supply chain security remains a work-in-progress, CISOs should do all they can to solidify external IT security. This means instituting standard contracts, governance frameworks, security controls, and cooperative oversight for all external IT services—regardless of whether the organizations is the IT provider or consumer. Anyone involved in external IT security should begin this effort with a thorough review of the SAIC/University of MD paper, *Building a Cyber Supply Chain Reference Model.*
- **Fully integrate security into IT procurement.** Processes and procedures governing IT vendor security audits lack consistency and utility. Furthermore, many CIKR organizations simply base purchasing decisions on their vendors' security reputations or historical data. This backward-looking approach can't help CIOs determine if new IT products may introduce systemic risk into their business operations. As mentioned, best practices for IT vendor security audits should include the following steps:
    - Audit all strategic IT vendors (including service providers and distributors)
    - Follow a standard audit process for all vendors
    - Implement a corporate policy where IT vendor security audit results have a significant impact for all procurement decisions

It is important for CIKR organizations to understand the truth about the IT industry. Many companies continue to minimize security best practices and secure product design in favor of higher profit margins and time-to-market advantages. This behavior will continue until customers demand security excellence from IT vendors. To alter the IT vendor security status quo, critical infrastructure organizations must push back on IT vendors without exception. Vendors that fail IT security audits must be presented with a stern ultimatum: Fix these issues in a reasonable timeframe or sell your products elsewhere.

For the IT Industry

The entire IT industry, including product companies, service providers, outsourcers, distributors, and investors, must realize that strong security processes and practices will become a CIKR requirement sooner rather than later. IT industry organizations that have already embraced security best practices have a market advantage that will lead to increasing CIKR sales over the next few years. To prepare for this security transition, the entire IT industry must:

- **Understand what's coming.** Within the next 2-3 years, most CIKR and other enterprise organizations will conduct in-depth security audits and base procurement decisions upon the audit results. This will likely progress to the point of real-time data exchange between CIKR organizations and strategic partners. IT industry organizations must realize that the way to address these changes is by investing in strong security policies, procedures, and product development—not marketing programs or sales gimmicks.

- **Push back on suppliers, service providers, and distributors.** Large IT vendors like Cisco, Dell, EMC, HP, IBM, Microsoft, and Oracle have to enforce more security muscle on their suppliers, partners, and distributors. Hardware manufacturers must institute supply chain security with best practices like the NSA Trusted Access Program. This means auditing and monitoring suppliers and then sharing this information with key CIKR customers. Furthermore, IT vendors must make sure that security becomes a part of their services and distribution strategy. Systems integrators must understand and communicate security risks and controls for technology components as well as integrated solutions. Distributors, resellers, and VARs must document and take responsibility for any product modifications made to IT hardware and software while in their chain of custody.

- **Pay particular attention to control systems.** As the Aurora vulnerability and Stuxnet worm demonstrate, critical industrial equipment is a vulnerable attractive target. Addressing this vulnerability should be an IT industry focus encompassing any network, server, or software application that passes packets or interacts with SCADA systems. Think in terms of behavior anomaly detection, intrusion detection/prevention systems, trusted software components, and real-time monitoring for all critical control systems.

- **VCs should add security to their set of startup requirements.** The Sand Hill Road crowd of venture capitalists must also recognize the security sea change approaching and make sure that technology startups include security as part of their business plans. To capitalize on the burgeoning security focus, VCs should partner with security-smart investors in the Beltway or VC firms like In-Q-Tel with direct ties to the defense or intelligence community.

- **Work with other vendors to establish acceptable best practice standards.** When Section 253 of Senate Bill S.3480 proposed changes to Federal Acquisition Regulation (FAR) for supply chain risk management, it caused panic in the IT vendor community as evidenced by a letter to Senators Collins and Lieberman from Cisco, IBM, and Oracle. The companies were concerned that new IT vendor security requirements could add undue cost to their businesses and preclude the Federal Government from buying cutting edge technologies. The Senators quickly responded with a public response to address Cisco, IBM, and Oracle's "concerns" and "misconceptions." This exchange demonstrates that cyber supply chain security remains extremely complex and confusing. What determines acceptable vendor security? How will competing vendors be measured on their security? Will certain vendor security requirements be necessities while others simply preferred? How long will vendors have to comply with new requirements? It is in the IT industry's best interest to work cooperatively and come up with industry best practices as soon as possible. Agreement on this issue should be worked out at leading IT vendors' corporate headquarters, not simply delegated to Washington industry groups like TechAmerica.

- **Teach customers how to fish.** Many other technology industry leaders have already established internal cyber supply chain security best practices but haven't shared the lessons learned or best practices with CIKR organizations. There is a business opportunity here for them to do so.

- **Communicate openly, honestly, and often.** Tech industry marketing is often used to simplify complex technology or sell a utopian vision of the future. This is antithetical to what's needed for cyber security. Henceforth, the technology industry must be prepared to talk about security in more holistic and candid terms. This includes vendor security efforts, risks, and security controls associated with new technologies and how IT companies and products contribute to systemic security. Savvy firms with strong security should use this communication to gain market advantage. Others should be prepared to respond with honesty, not spin. Remember that in the near future, strong security will become an IT industry litmus test at CIKR organizations.

For the U.S. Federal Government

Cyber security recommendations for the federal government are eloquently presented in the aforementioned CSIS report, *Securing Cyberspace for the 44th Presidency*. Based upon its security and IT industry experience as well as the data analyzed for this research project, ESG adds to this list with the following recommendations for the U.S. Federal Government:

- **Use the ESG data as input for the "Assessment" phase.** The National Infrastructure Protection Plan released in 2009 shows a risk management framework (Figure S-2, pg. 4) where the first three steps are "set goals and objectives," "identify assets and systems," and "assess risks." ESG's data points to problems in each area. For example, many CIKR organizations have not set a goal to lower the risk associated with poor IT vendor security. The majority of critical infrastructure organizations aren't assessing the risks associated with external IT relationships. Many firms may not be identifying homegrown software as a critical asset or system. The ESG report recognizes a few basic problems that should be noted and addressed by DHS and other federal agencies as soon as possible.

- **Aggregate efforts.** ESG is aware of at least ten cyber security bills making their way through the U.S. Congress and Senate. In some ways, this should be expected as cyber security falls into a multitude of legislative domains, but all of this activity can't help but result in redundant efforts, legal complexity, and gridlock. Senate Majority Leader Harry Reid (D, NV) is urging Congress to aggregate bills in order to pass cyber security legislation this year, but with the November elections looming, this is unlikely. Given the security weaknesses uncovered in this report, ESG believes it is imperative that Congress recognize the urgency required here. It is best to pass legislation and then fix regulatory issues/loopholes in the future rather than delay actions further.

- **Work with, but not for, the technology industry.** While ESG urges the technology industry to embrace security best practices, many firms will view security investments in relation to profitability rather than national security. Washington must send a respectful message that myopic financially-focused behavior by IT vendors will no longer be tolerated. Yes, politicians need to balance security and business objectives, but it is important to remember that the technology industry has had 10+ years to address security weaknesses. Leading firms that have done so already should reap benefits of new sales and ROI on their security investments. Others should not be able to delay inevitable security requirements.

- **Balance carrots and sticks.** As Figure 34 illustrates, CIKR organizations understand the need for more stringent cyber security legislation, but need help to get there. Federal programs that promote cyber security education and provide incentives (i.e., tax credits, government-sponsored loans, etc.) will go a long way to encourage resource-constrained CIKR organizations to participate—perhaps a cyber security equivalent of the Health Information Technology for Economic and Clinical Health Act (HITECH) which offered federal incentives, grants, and loans to stimulate investment in technologies for Electronic Health Records (EHR). Along with these incentives, HITECH also strengthened HIPAA security requirements and imposed a long-term financial penalty for medical organizations that do not convert to EHR by 2015. Based upon ESG research, this type of carrot and stick program would be a good fit for improving CIKR security.

- **Promote federal standards, experience, and knowledge**. There is a tremendous amount of cyber security work happening within the Federal Government. Unfortunately, the private sector has little or no knowledge about these efforts. The Federal Government must do a better job of self-promotion. For example, NIST could work with private information security organizations to promote the NIST 800 series of best practices or work with endpoint security software vendors to encourage more widespread use of the Secure Content Automation Protocol (SCAP).

- **Streamline the certification process.** Vendors are right to complain that Washington has too many overlapping standards and certifications, especially within DoD. These must be consolidated into a single set of standards that apply across all civilian, military, and intelligence agencies. Standards can certainly be tiered where federal security standard level 1 applies to civilian agencies while NSA relationships are contingent upon level 4 certification. Finally, it is time to work with international partners to modernize Common Criteria certification as it is simply too costly and time consuming for the modern cycle of technology innovation.

Research Methodology

To gather data for this report, ESG conducted a comprehensive online survey of senior IT and business professionals from U.S. private- and public-sector organizations in August 2010. Target organizations were restricted only to those in industries categorized by the U.S. Department of Homeland Security (DHS) as Critical Infrastructure and Key Resources (CIKR). To qualify for this survey, individual respondents were required to be senior IT or business managers personally responsible for or familiar with their organization's information security policies and procedures, especially with respect to the procurement of IT products and services. Respondents who did not have a high degree of responsibility or familiarity with information security policies and procedures were disqualified. 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 285 IT and business 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

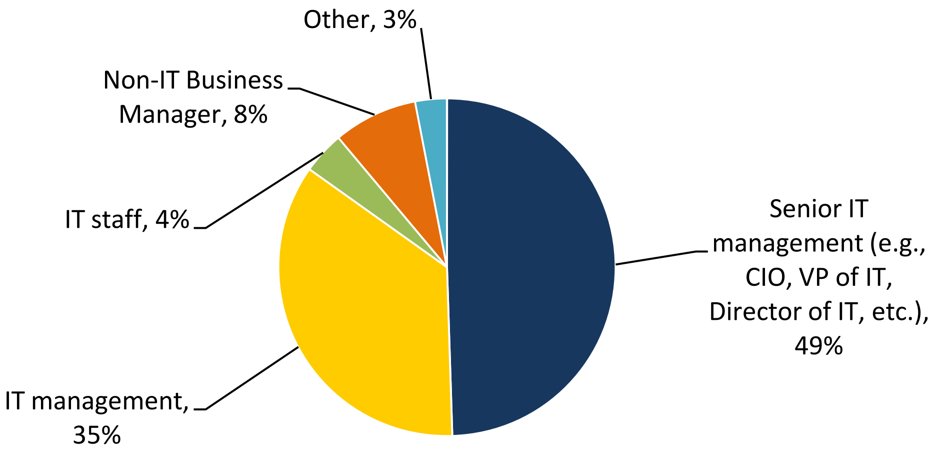
The data presented in this report is based on a survey of 285 qualified respondents. The figures below detail the demographics of this respondent base.

Respondents by Job Responsibility

Respondents' current job responsibility is shown in Figure 35.

Figure 35. Survey Respondents by Job Responsibility

Which of the following best describes your current responsibility within your organization? (Percent of respondents, N=285)



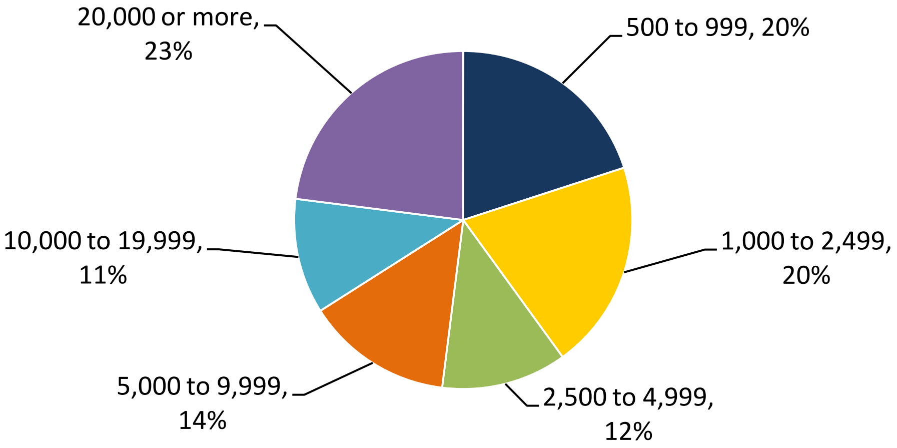
Source: Enterprise Strategy Group, 2010.

Respondents by Number of Employees

The number of employees in respondents' organizations is shown in Figure 36.

Figure 36. Survey Respondents by Number of Employees

How many total employees does your organization have worldwide? (Percent of employees, N=285)

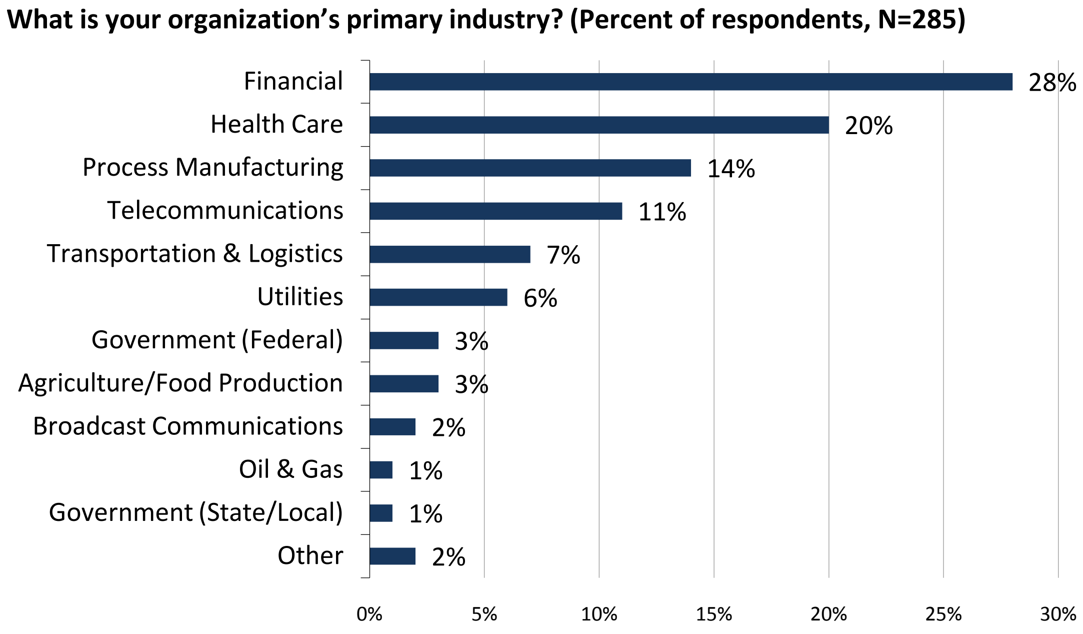


Source: Enterprise Strategy Group, 2010.

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 Figure 37.

Figure 37. Survey Respondents by Industry

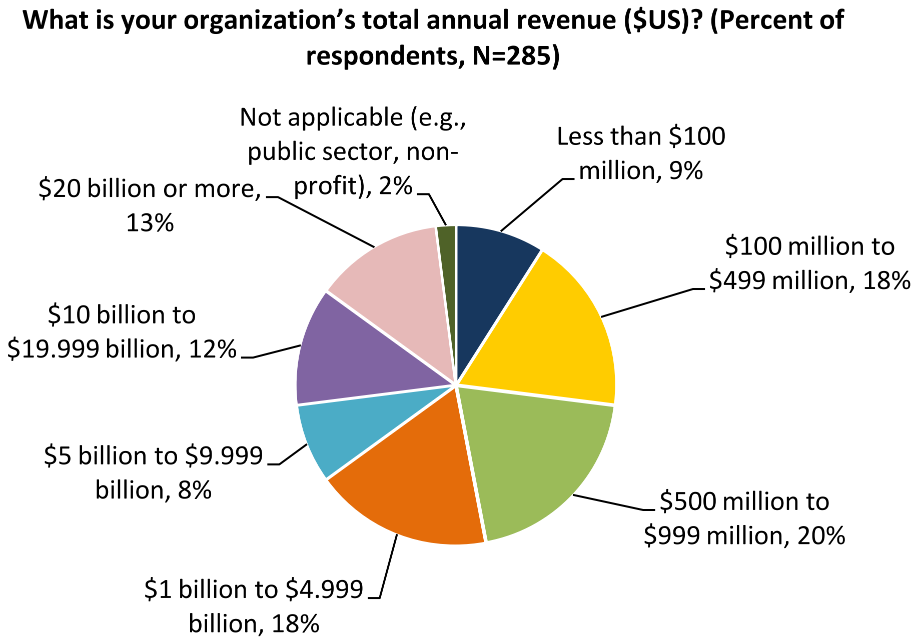


Source: Enterprise Strategy Group, 2010.

Respondents by Annual Revenue

Respondent organizations' annual revenue is shown in Figure 38.

Figure 38. Survey Respondents by Annual Revenue

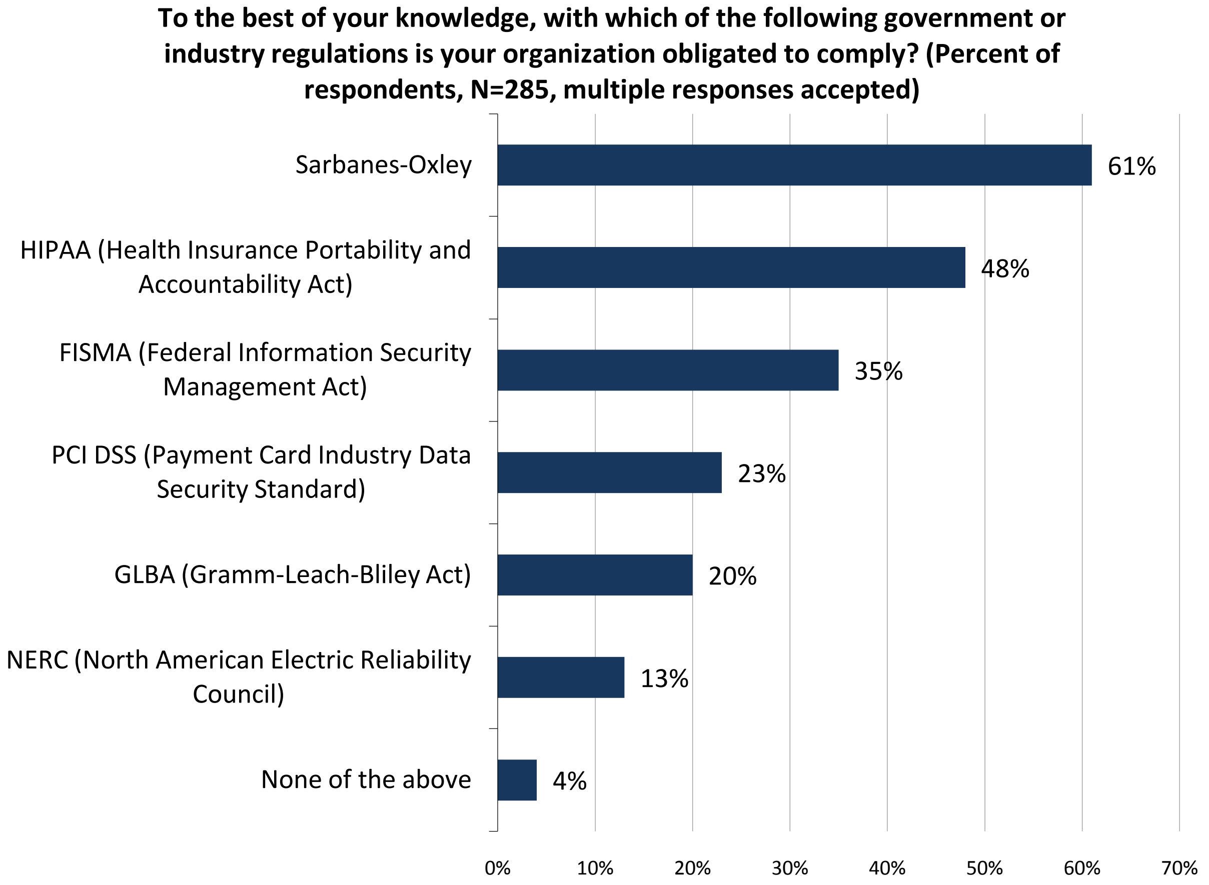


Source: Enterprise Strategy Group, 2010.

Respondents by Compliance Requirements

The government or industry regulations respondent organizations are required to comply with are shown in Figure 39.

Figure 39. Survey Respondents Compliance Regulations



Source: Enterprise Strategy Group, 2010.

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

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