ESG Brief

Critical Infrastructure Organizations Want More Cybersecurity Help from Washington

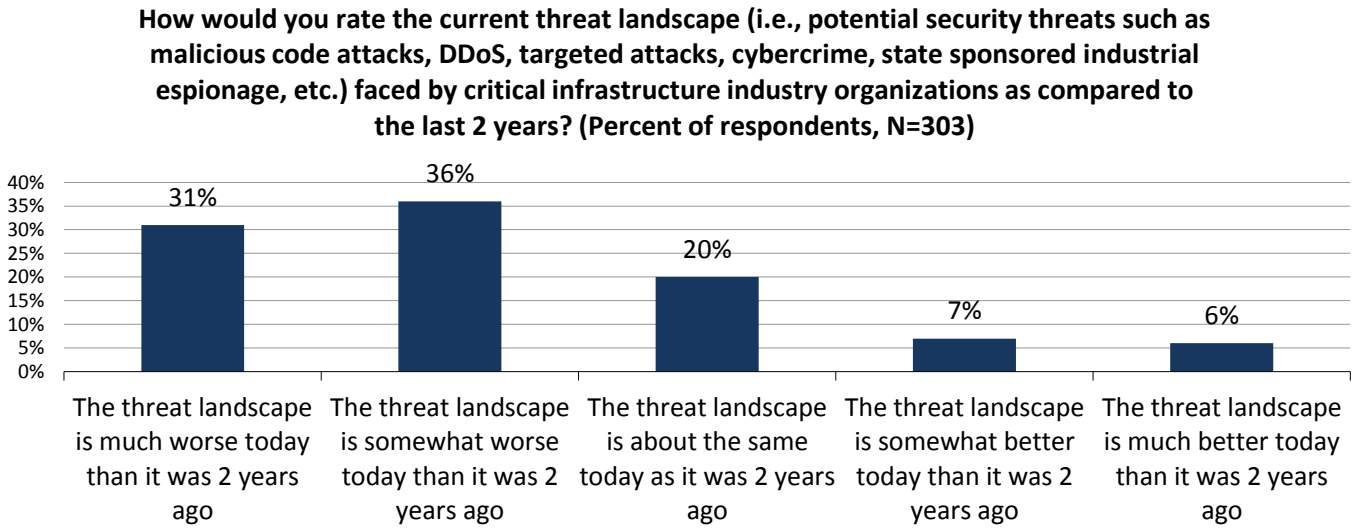
Date: March 2015 **Author:** Jon Oltsik, Senior Principal Analyst and Bill Lundell, Senior Research Analyst

Abstract: *Since the administrations of George H.W. Bush and Bill Clinton, Washington politicians have pledged to address cyber-vulnerabilities within critical infrastructure industries. Has anything changed? Not really. The research conducted by ESG and presented in this brief reveals that critical infrastructure organizations continue to experience numerous security incidents and believe that the threat landscape is only getting worse. Furthermore, security professionals working at these organizations remain unclear about the U.S. government's cybersecurity strategy. In spite of this confusion, critical infrastructure organizations believe that it's time for Washington to get more involved in cybersecurity issues and create cybersecurity programs that offer real help.*

The State of Cybersecurity at Critical Infrastructure Organizations

The Enterprise Strategy Group (ESG) recently surveyed 303 IT and information security professionals with awareness of or responsibility for cyber supply chain policies and processes and with overall knowledge of the state of cybersecurity at their organizations. Survey respondents were located in the United States and work for large midmarket (i.e., 500 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations that operate in critical infrastructure industries as designated by the U.S. Department of Homeland Security. This research project was intended to assess the state of cyber supply chain security and the overall cybersecurity status of organizations in critical infrastructure industries since these entities face constant cyber-attacks from a variety of adversaries including cyber-criminals, hacktivists, and nation states, so they have a bird's eye view of the threat landscape on a daily basis. When asked to assess this threat landscape in comparison to two years ago, nearly one-third (31%) of organizations claim that the threat landscape is *much worse* than it was two years ago while 36% believe that the threat landscape is somewhat worse than it was two years ago (see Figure 1). While not surprising, this is discouraging, as an attack on U.S. critical infrastructure could be the "cyber Pearl Harbor" predicted by numerous politicians and pundits.

Figure 1. Critical Infrastructure Organizations Believe that the Cyber-threat Landscape Is Getting Worse

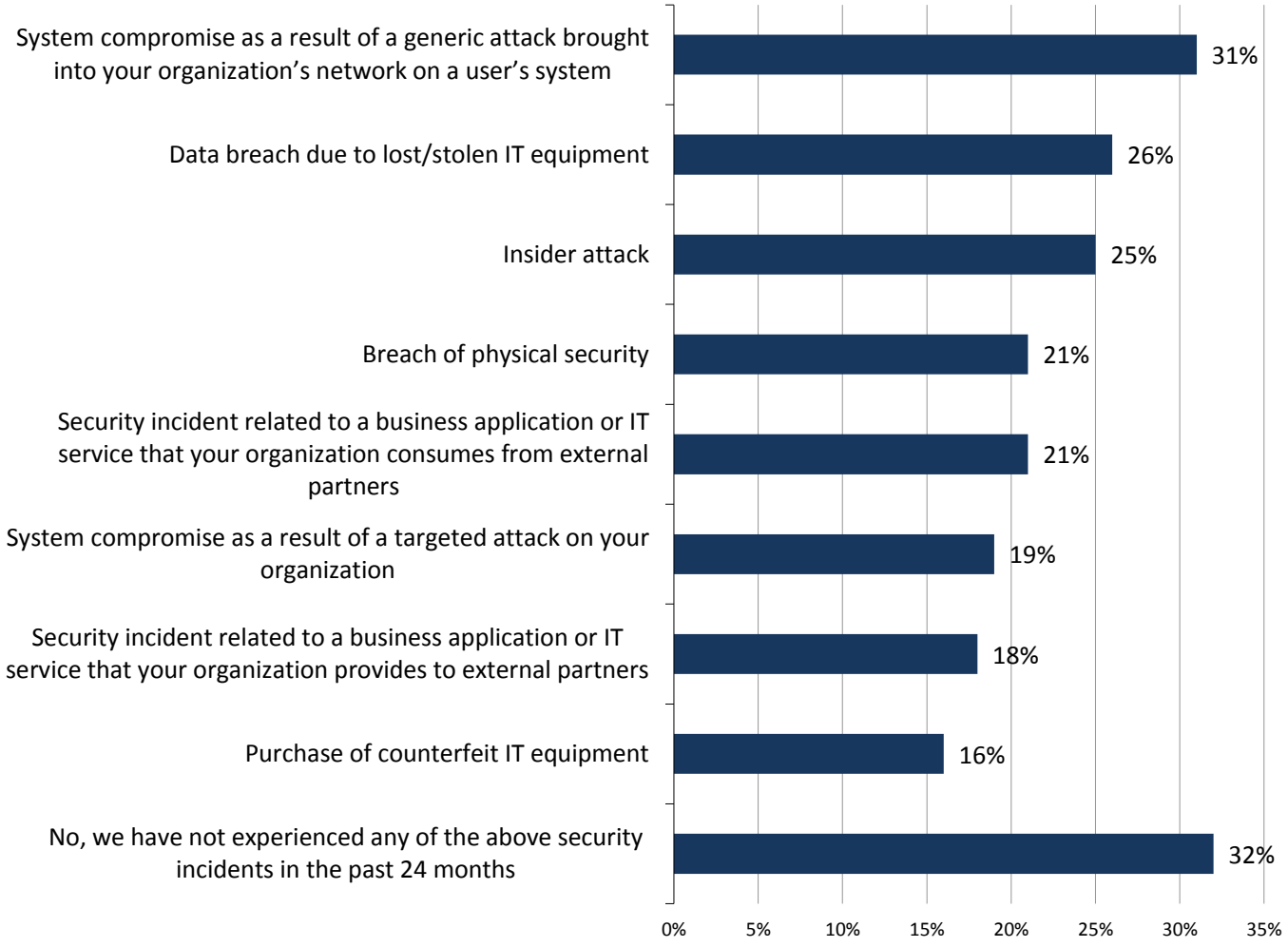


Source: Enterprise Strategy Group, 2015

Security professionals' opinions may be related to the fact that most of their organizations experienced one or several security incidents in the past 24 months. In fact, according to Figure 2, many report a wide variety of incidents including system compromises resulting from generic attacks on user systems (31%), data breaches due to lost or stolen equipment (26%), insider attacks (25%), breaches of physical security (21%), and targeted attacks (19%). The data also points to vulnerabilities in the cyber supply chain. In some cases, security incidents were related to business relationships in which several organizations open IT applications and services to one another. While these arrangements offer cost and operational benefits, they also expose each organization to threat vectors emanating from partner networks. It is also noteworthy that 16% of organizations experienced security incidents related to the purchase of counterfeit IT equipment. Clearly, this risk is still pervasive.

Figure 2. Critical Infrastructure Organizations Have Experienced a Variety of Security Incidents

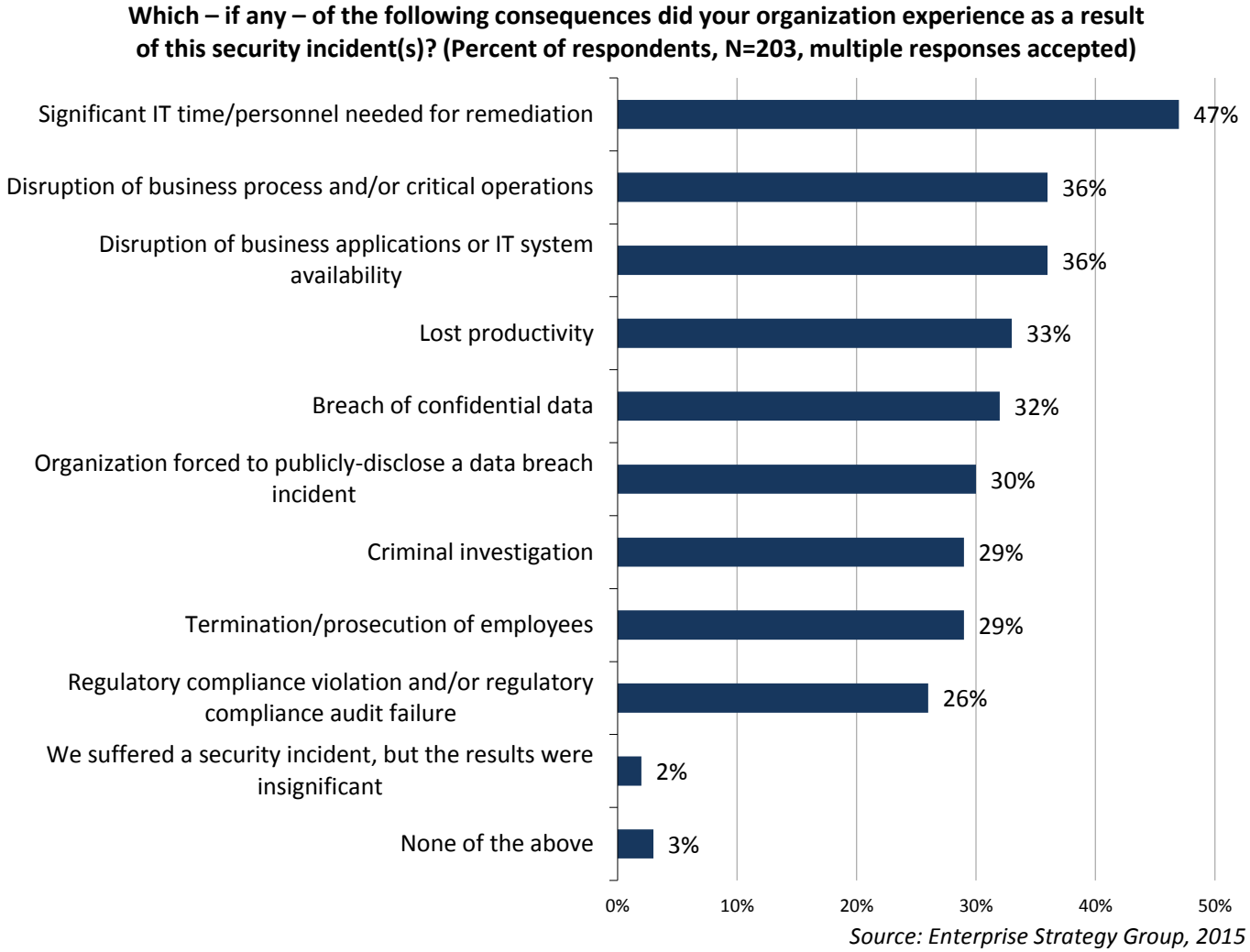
To the best of your knowledge, has your organization experienced any of the following security incidents over the past 24 months? (Percent of respondents, N=303, multiple responses accepted)



Source: Enterprise Strategy Group, 2015

Respondents were then asked to describe the consequences of these security incidents. Not surprisingly, nearly half (47%) of organizations report that security incidents require time and personnel for remediation, but many security incidents also impact the business mission—36% said that security incidents disrupted business processes and/or critical operations, 36% pointed to disruption of a business application, 33% described lost productivity, and 32% said that security incidents led to a breach of sensitive data (see Figure 3). In critical infrastructure industries like financial services, business process disruption could translate to an ATM network going offline, while the breach of a health care organization could expose the sensitive health care records of thousands of patients.

Figure 3. Consequences of Security Incidents at Critical Infrastructure Organizations



Source: Enterprise Strategy Group, 2015

Cybersecurity, Critical Infrastructure Organizations, and the U.S. Government

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

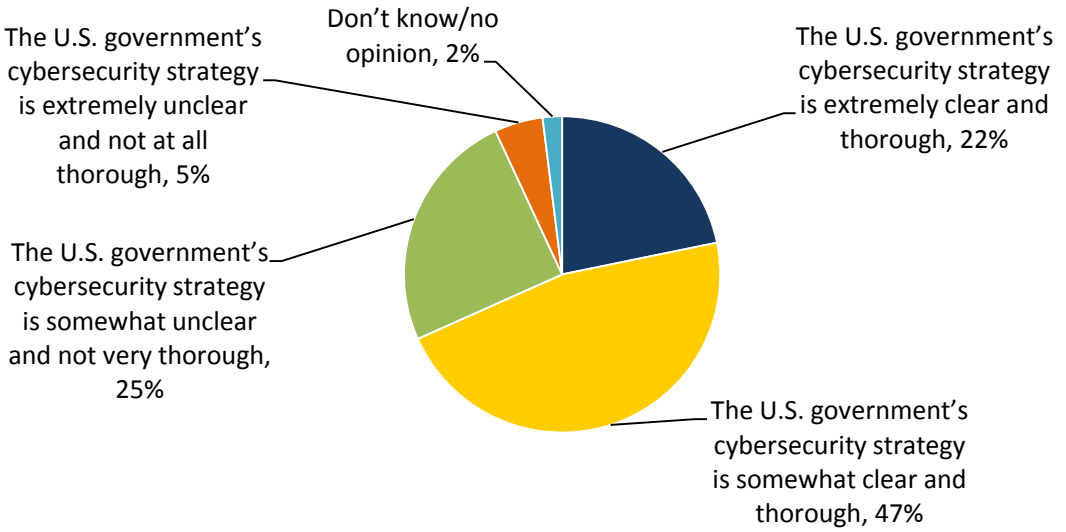
Security professionals working at critical infrastructure industries have been directly or indirectly engaged with U.S. Federal Government cybersecurity programs and initiatives through several presidential administrations. Given this lengthy timeframe, ESG wondered whether these security professionals truly understood the U.S. government's cybersecurity strategy.

According to Figure 4, the results are mixed at best. One could easily conclude that the data resembles a normal curve in which the majority of respondents believe that the U.S. government's cybersecurity strategy is somewhat clear while the rest of the survey population is distributed between those that believe that the U.S. government's cybersecurity strategy is very clear and those that say it is unclear. ESG views the results somewhat differently, however. In spite of over 20 years of U.S. Federal cybersecurity discussions, many security professionals remain uncertain about what the

government plans to do in this space. Clearly, the U.S. Federal Government needs to clarify its mission, its objectives, and its timeline with cybersecurity professionals to gain their trust and enlist their support for public/private programs.

Figure 4. Opinion about U.S. Federal Government's Cybersecurity Strategy

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

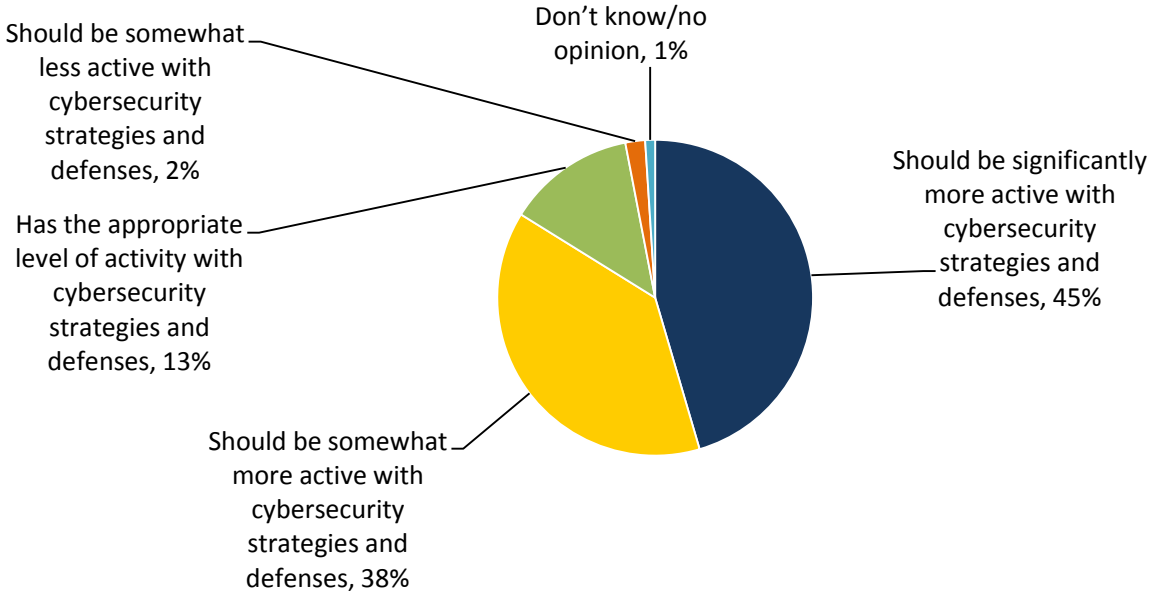


Source: Enterprise Strategy Group, 2015.

While critical infrastructure security professionals may be tentative about the Federal Government's strategy, they would also like to see Washington become more engaged. Nearly half (45%) of critical infrastructure organizations believe that the U.S. Federal Government should be *significantly* more active with cybersecurity strategies and defenses while 38% believe that the U.S. Federal Government should be somewhat more active with cybersecurity strategies and defenses (see Figure 5).

Figure 5. Critical Infrastructure Organizations Want More Cybersecurity Involvement from the U.S. Federal Government

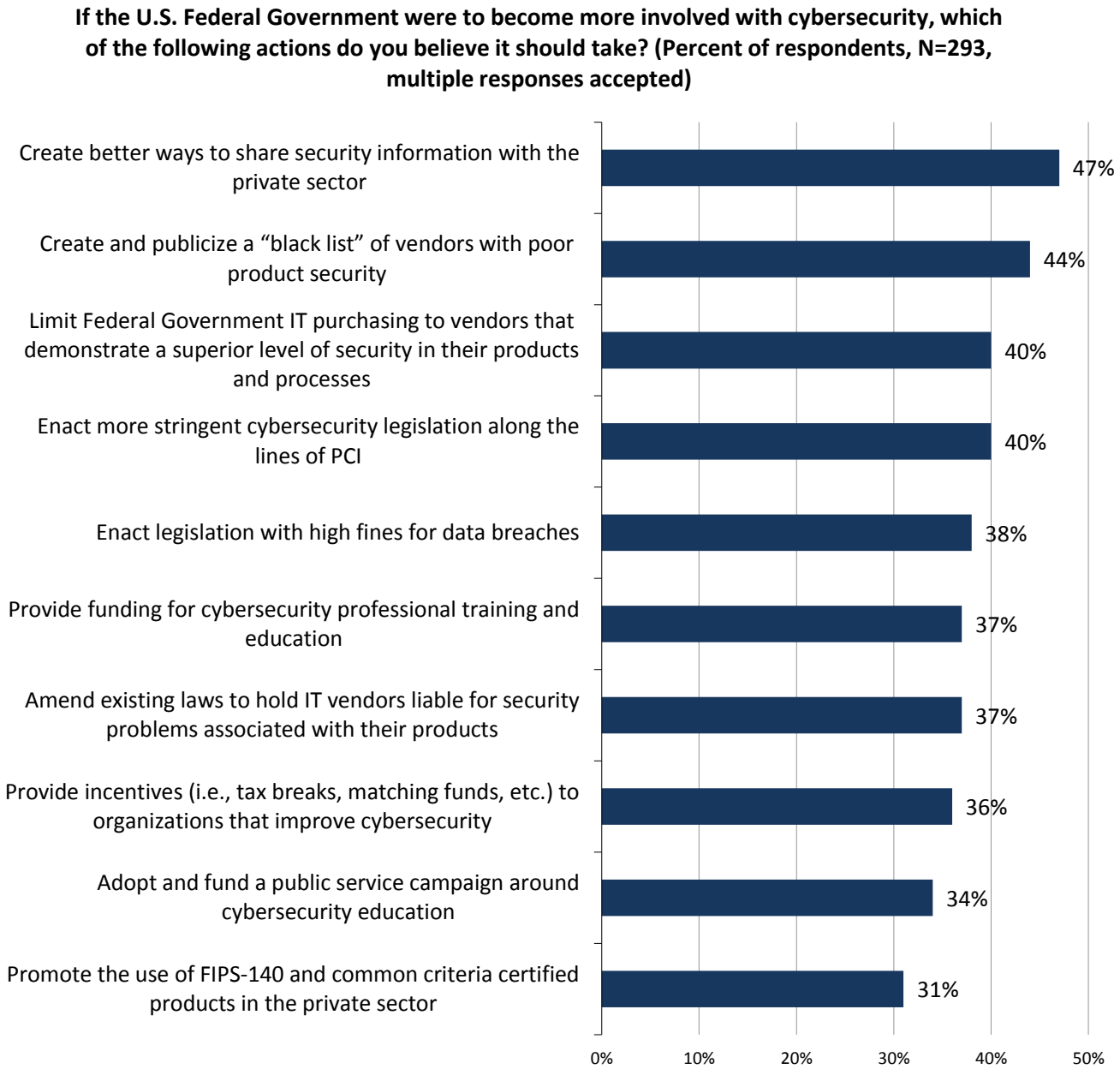
Please complete the following statement by selecting one of the responses below. In my opinion, the U.S. Federal Government: (Percent of respondents, N=303)



Source: Enterprise Strategy Group, 2015.

Finally, ESG asked the entire survey population of security professionals what types of cybersecurity actions the U.S. government should take. Nearly half (47%) believe that Washington should create better ways to share security information with the private sector. This aligns well with President Obama's executive order urging companies to share cybersecurity threat information with the Federal Government and one another. Cybersecurity professionals have numerous other suggestions as well. Some of these could be considered government cybersecurity enticements. For example, 37% suggest more funding for cybersecurity education programs while 36% would like more incentives like tax breaks or matching funds for organizations that invest in cybersecurity. Alternatively, many cybersecurity professionals recommend more punitive or legislative measures—44% believe that the Federal Government should create a "black list" of vendors with poor product security (i.e., the cybersecurity equivalent of a scarlet letter), 40% say that the Federal Government should limit its IT purchasing to vendors that display a superior level of security, and 40% endorse more stringent regulations like PCI DSS or the institution of laws with higher fines for data breaches (see Figure 6).

Figure 6. Critical Infrastructure Organizations Suggestions for U.S. Government Cybersecurity Actions



Source: Enterprise Strategy Group, 2015.

The Bigger Truth

The research in this brief presents a clear and compelling picture:

1. Critical infrastructure organizations are under cyber-attack and they believe that things are getting worse.
2. The security incidents experienced by critical infrastructure organizations vary widely, disrupt business operations, and carry high costs.
3. Security professionals working at critical infrastructure organizations remain unclear about the U.S. government's cybersecurity strategy. Nevertheless, this key constituency believes that Washington should be more active with its cybersecurity strategy and programs.

ESG believes this brief should send a cogent and concise message to Washington. The U.S. Federal Government must engage with critical infrastructure security professionals, improve its communication by articulating a logical cybersecurity strategy, express a clear mission statement that includes success metrics, and find ways to provide help sooner rather than later. Of course it's unrealistic to expect Draconian cybersecurity policies and regulations from Washington, but it's apparent that cybersecurity professionals would like to see the U.S. Federal Government use its visibility, influence, and purchasing power to produce cybersecurity "carrots" and "sticks." In other words, Washington should be willing to reward IT vendors and critical infrastructure organizations that meet strong cybersecurity metrics and punish those that cannot adhere to this type of standard.

In 2009, President Obama stated, "…it's now clear that cyber threats are one of the most serious economic and national security challenges we face as a nation." On the other side of the political spectrum, a recent press release on cybersecurity legislation from Senator John McCain (R-AZ) stated, "Every day we delay moving forward with this legislation, our nation grows more vulnerable, our privacy and security are increasingly at-risk, and our adversaries are further emboldened." These declarations from political adversaries seem to point to bipartisan support for greater cybersecurity participation from Washington. Based upon the research presented in this brief, this type of commitment would be welcome with open arms by organizations within critical infrastructure industries.