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

ESG Research Insight Report

Top-of-mind Threats and Their Impact on Endpoint Security Decisions

By Doug Cahill, ESG Senior Analyst; and Jack Poller, ESG Analyst

October 2017

This ESG Study was commissioned by Cylance
and is distributed under license from ESG.

Contents

Executive Summary

In the first half of 2017, Cylance commissioned Enterprise Strategy Group (ESG) to conduct a survey of 300 IT and information security professionals representing large midmarket (500 to 999 employees, 12%) and enterprise-class (more than 1,000 employees, 88%) organizations. Survey respondents were located in the United States (43%), Japan (21%), United Kingdom (13%), France (12%), and Germany (11%).

The survey included representation from multiple industry verticals, including manufacturing (21%), information technology (18%), financial services (13%), communications and media (11%), retail/wholesale (7%), business services (7%), health care (6%), government (5%), and others (13%). All respondents were involved in the purchase process for their organization's endpoint security products and services and knowledgeable about their organization's endpoint security policies, processes, and safeguards.

Based upon the data collected as part of this research project, ESG concludes:

- **Cybercriminals, phishing, and unknown malware get top billing**. While cybersecurity professionals continue to face a wide gamut of threat types perpetrated by cybercriminals, hacktivists, nation-states, and insiders using many different vectors, the combination of cybercriminals using phishing to introduce malware as a means to penetrate their organization is top of mind. Cybercriminals are especially top of mind with 90% of research participants stating they are either very concerned or concerned about the threat posed by this type of bad actor.

- **Ransomware repeats**. Ransomware attacks have been broad-based, infecting an appreciable population of endpoints. Many organizations experience a recurrence of ransomware incidents with 22% saying the same ransomware re-infected the same endpoints, and 38% noting that the same ransomware had infected other endpoints. Such recurrence of ransomware incidents exposes endpoint security efforts and remediation steps as insufficient.

- **Endpoint infections affect operations**. Operational outcomes from infected endpoints are more common than data loss or financial impacts. Thirty-two percent of participating organizations suffered business interruption, 31% experienced a loss of employee production, and 28% cited delays to other IT projects while devoting time and effort to incident remediation. Reimaging is the method of choice, with nearly a third of organizations reimaging 100 or more endpoints per month, another indicator of inadequate endpoint security.

- **Machine learning is a strategic feature**. Organizations realize they can gain increases in efficiency and efficacy by incorporating machine learning technology into their endpoint security solutions to improve their defense-in-depth strategy. In fact, 47% of respondents indicated that their organization has already deployed machine learning technology for endpoint security either extensively or on a limited basis.

The Threat Landscape

The threat landscape continues to evolve as bad actors focus their energy on developing sophisticated, targeted attacks. While attacks perpetrated by cybercriminals via phishing methods that introduce unknown malware are top of mind, organizations express concern about the diverse spectrum of the threat landscape. Old vectors (e.g., removable storage and drive-by downloads), new methods (e.g., "store and forward" via cloud apps), and new threat types (e.g., multi-stage) are also cause for pause with cybersecurity professionals.

Cybercriminals Pose the Greatest Concern

The widespread publicity devoted to major criminal cyber-attacks in the last few years has demonstrated that no organization is immune. Targets have included health care providers, governments, major websites, banks, retailers, and other organizations across many industries. In addition to attack types such as key stroke loggers that steal user credentials, cybercriminals perpetrated an onslaught of ransomware attacks in 2016 and 2017. The most publicly reported ransomware attack, known as WannaCry, is reported to have affected more than 230,000 endpoints across more than 150 countries, including FedEx and the National Health Service of the UK. A common thread across the landscape is the vulnerability of endpoint systems.

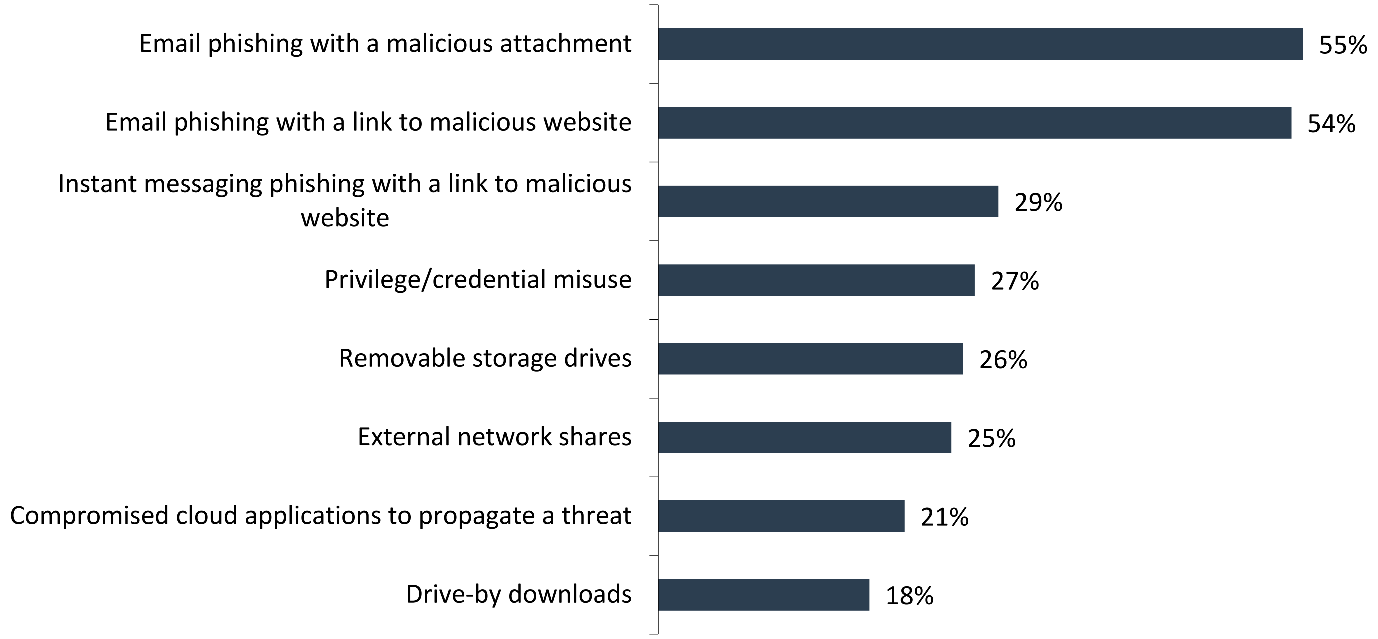
Awareness about cybercriminal activity has risen to the point that 90% of survey respondents indicate that they are concerned about the threat posed by cybercriminals. Likewise, with broad media coverage devoted to North Korean involvement in the WannaCry/Petya/NotPetya ransomware attacks and alleged Russian involvement in political-related hacking, 82% are concerned about nation-state cyberespionage. An almost equal number of respondents also expressed concern about threats posed by hacktivists and insiders, both external actors gaining access to insider credentials as well as malicious insiders.

Email Phishing Has Been the Primary Attack Vector and Presents the Greatest Concern

Phishing has proven to be a very successful attack method for cybercriminals via which threats such as ransomware are all too often introduced. And as is true with legitimate business models, cybercriminals tend to stick with what is tried and true, until their return on investment diminishes. Thus, although actors use a variety of methods to perpetrate attacks against an organization, more than half of respondents report that email phishing, either with a malicious attachment or a link to a malicious website, has been the primary attack vector (see Figure 1) employed against their organization in the last two years. Reflecting the increasing importance of instant messaging (IM) and mobile devices in the workplace, the next most frequent attack vector has been IM phishing, according to 29% of respondents.

Figure 1. Attack Vectors Experienced in the Past Two Years

To the best of your knowledge, have any of the following attack vectors and methods been used against your organization in the past two years (regardless of if those attacks led to one or more systems being compromised or disrupted)? (Percent of respondents, N=300, multiple responses accepted)



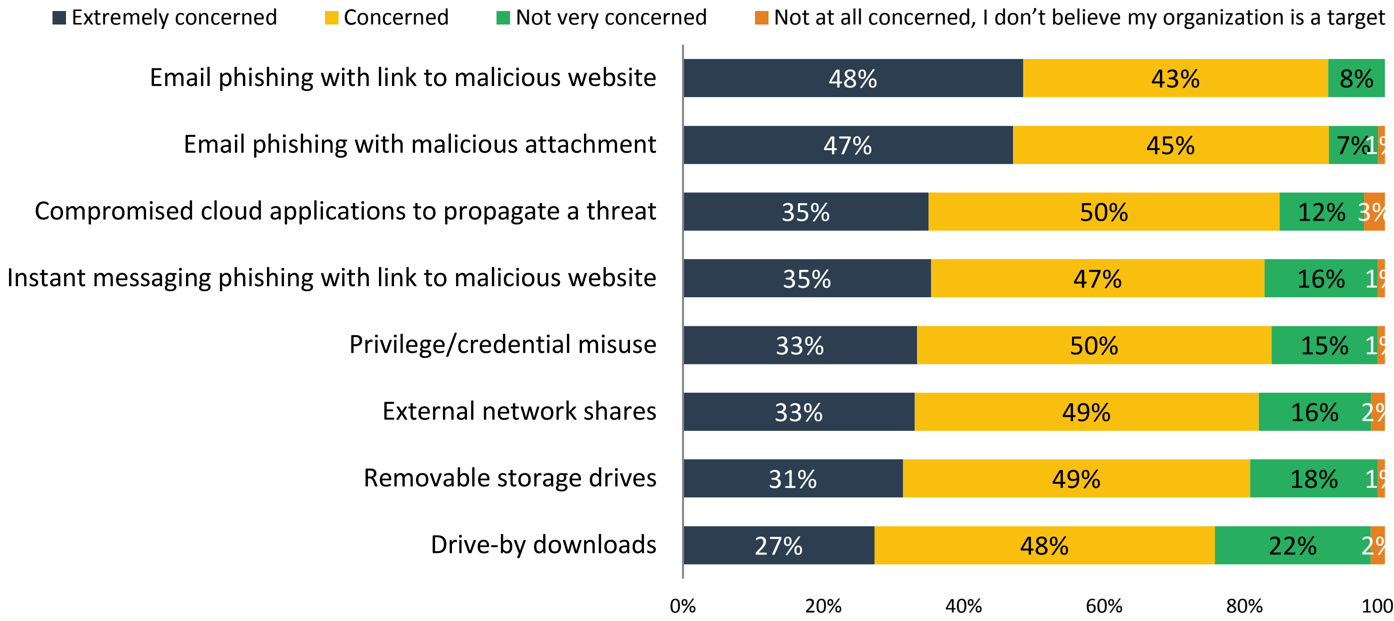
Source: Enterprise Strategy Group, 2017

It is not surprising, then, that looking forward, 91% of cybersecurity professionals express the greatest concern over the threat posed by email phishing (see Figure 2).

While only 21% of respondents indicate that they have experienced attacks using compromised cloud applications to propagate a threat, 85% of respondents are concerned that they will be attacked in this manner in the future. This reflects the increasing relevance of cloud apps and the familiarity of employees with cloud app notifications. For example, employees have become conditioned to receiving email, from colleagues, business partners, friends, and others, notifying them of new files in enterprise file sync and share (EFSS) apps such as Dropbox and Google Drive. Bad actors trade on this conditioning, using email or IM phishing to induce downloads of malicious files, often a component of a multi-stage attack.

Figure 2. Attack Vectors of Concern in the Future

Bad actors employ different vectors and methods to deliver threats such as malware with respect to "how they get in." Please indicate your level of concern with each of the following methods that could be used to attack your organization? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2017

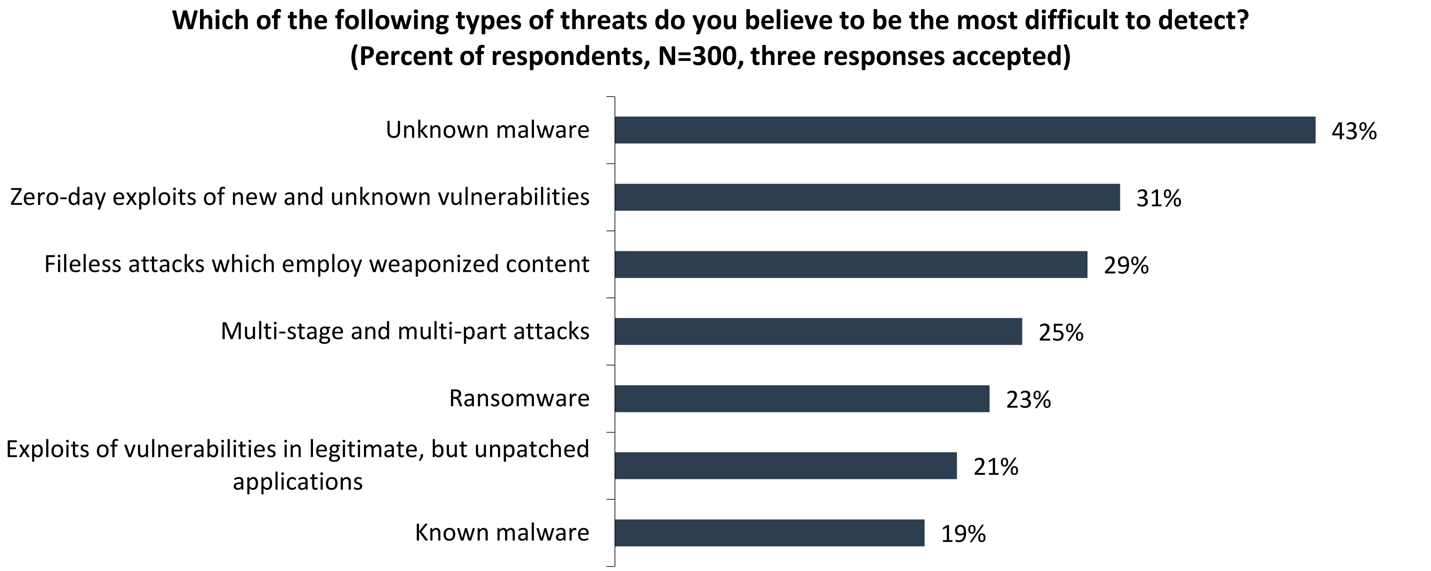
Known Malware Is Most Prevalent While Unknown Malware Is the Primary Concern

As ransomware continues to receive significant public attention, organizations experience the gamut of threat types. Sophisticated malicious actors are now employing a variety of anti-security, anti-sandbox, and anti-analyst evasion techniques that make their activities look benign and their software look innocent to hide from traditional signature-based endpoint security systems. In addition to writing new, advanced malware, some with such detection evasion capabilities, adversaries employ polymorphic malware and reuse commodity malware, leading to research results that reflect a difference in what has been experienced versus what is of concern.

There's a dichotomy between the perception of threat risk and the reality of that threat behavior in the wild. For instance, known malware was the most frequent threat type experienced in the past two years, according to 35% of survey respondents, but only 27% perceive it as posing the greatest risk to their organization's endpoints. Conversely, unknown malware was most frequently experienced by 29% of respondents, yet many more (44%) believe that unknown malware represents the greatest risk to their organization's endpoints.

The higher level of concern versus experience with new and unknown malware is rooted in the perception of the associated risks: 44% of survey respondents believe that unknown malware is the most difficult to detect (see Figure 3).

Figure 3. Types of Threats that Are Most Difficult to Detect



Source: Enterprise Strategy Group, 2017

Ransomware Attacks Are Prevalent, Recurring, and Operationally Impactful

While the most common forms of ransomware encrypt files and interrupt the course of business, some extortionists threaten to release corporate data to the public. Most recently, cybercriminals extorted HBO, threatening to release new episodes of *Game of Thrones*. This type of public exposure is not only a financial risk, but also can present an unrecoverable risk to an organization's reputation.

Another dichotomy exists between organizations' experience with ransomware, their perception of relative detection difficulty, and the associated risk. While one quarter of respondents said ransomware was the most frequent threat type experienced in the past two years, and 23% said it was the most difficult threat to detect, 38% said that ransomware posed the greatest risk to their organization's endpoints, with the scope of ransomware attacks and their recurrence contributing factors.

> ...nearly half of the respondents noted that their organization had been the victim of a ransomware attack in the last year....

At 46%, nearly half of the respondents noted that their organization had been the victim of a ransomware attack in the last year and more than half of those (56%) reported more than 5% of their organization's endpoints were infected. It is noteworthy that only 12% of affected organizations paid the ransom. But the remediation step of choice, restoring impacted data from a backup, which is employed by over half (53%) of the respondents, appears to be ineffective given the recurrence of the same ransomware. Nearly a quarter of research participants whose organizations have been recent ransomware victims stated that they experienced a recurrence of the same ransomware on the same endpoints and 38% experienced the same ransomware but on different endpoints.

The other common remediation step, reimaging, used by 41% of organizations infected by ransomware, appears to have become a standard operating procedure and another indicator of how such attacks adversely impact business operations.

Compromised Endpoints Disrupt Productivity and Operations

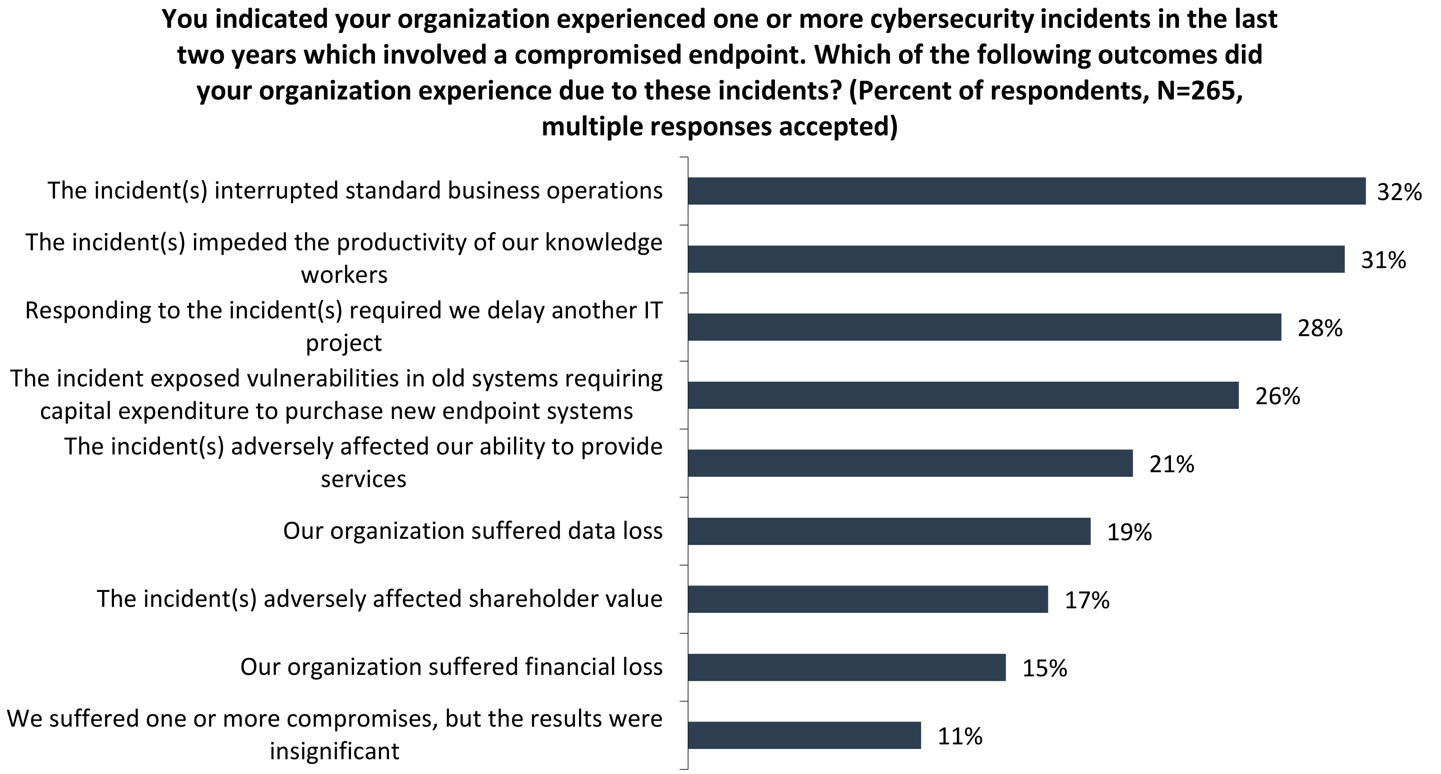
During the time it takes IT to remediate infections, employees lose access to their endpoints, interrupting the employees' ability to conduct business. Ransomware infections not only impact productivity, but by holding critical data hostage, ransomware can also impair or halt business services until the data is recovered, either via restoring from backups or by succumbing to the extortion. Damages from ransomware extend far beyond loss of the data itself, and in extreme cases such as health care providers, ransomware can delay or even prevent providing patient care.

Many organizations still have an installed base of older, down-rev systems that are more susceptible to ransomware attacks. These organizations must make capital and operational investments to upgrade and update their endpoints. For regulated industries, including those using regulated devices, updating or upgrading is more complex and time-consuming, requiring validation efforts and sometimes regulatory agency approval.

Incident response and remediation efforts such as incident investigation, data restoration, system reimaging, or engagement with third-party services, takes time, effort, and often funding, especially when paying a ransom. These efforts interrupt IT staff and can delay other IT projects.

It follows then that the four most commonly cited impacts of compromised endpoints were operational in nature (see Figure 4), including interrupting standard business operations (32%), impeding the productivity of knowledge workers (31%), incident response delaying other IT projects (28%), and incidents exposing vulnerabilities in older systems and requiring capital expenditures for replacement systems (26%).

Figure 4. Impact of Compromised Endpoints



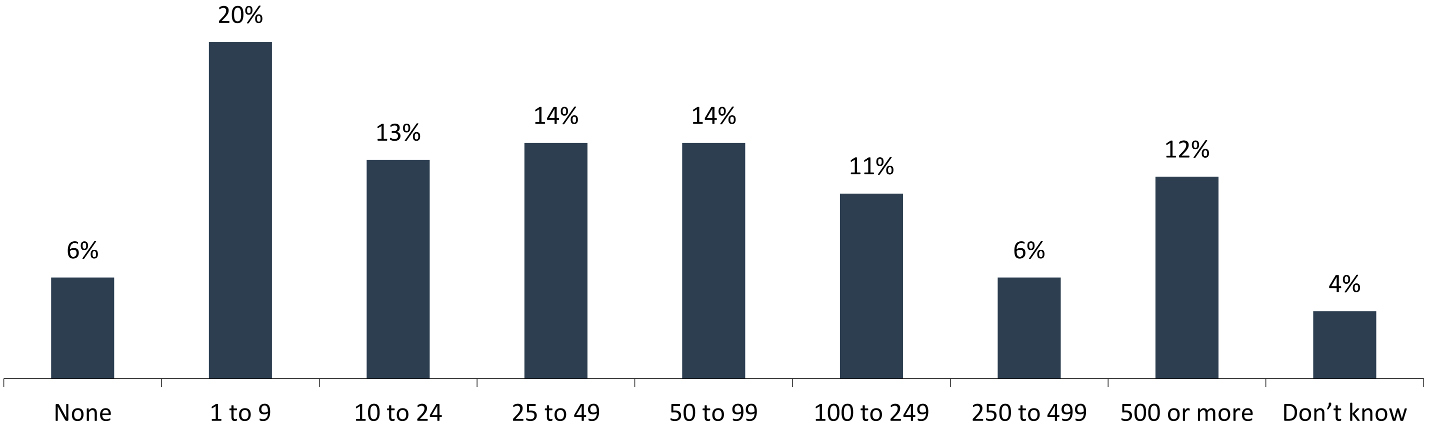
Source: Enterprise Strategy Group, 2017

Investigating a compromised endpoint to discover and remove malicious or altered files from infected endpoints takes time and effort, and carries with it the risk that a bad file might be missed, leaving the endpoint in a compromised state. Or a file critical to the operation of the system might be inadvertently deleted, rendering the endpoint unreliable or inoperative. Rather than taking those risks, many organizations take the expedient action of remediation by reimaging from a golden master.

With many infections, this becomes a "rinse and repeat" strategy (see Figure 5). Twenty-nine percent of respondents said their organization reimages 100 or more systems every month, and 12% said their organization reimages more than 500 systems per month. It takes a dedicated team of IT professionals to reimage hundreds of endpoints each month, and the volume of infections hints at inadequacies in endpoint security controls.

Figure 5. Extent of Reimaging as Remediation for Infections

On average, how many endpoint computers does your organization reimage per month to remediate these infections? (Percent of respondents, N=265)



Source: Enterprise Strategy Group, 2017

Machine Learning Is a Strategic Technology to Prevent Future Infections

Organizations have taken both tactical and strategic steps to prevent future incidents as they look to leverage their existing investments in cybersecurity tools and staff and put new technologies in play.

Tactical actions taken by research participants include:

- Training. As noted previously, email phishing has been the primary vector for attacks, and is the primary expected vector in the near future. Organizations can reduce phishing response rates and raise security awareness by training employees to recognize spoofed emails and texts, and to practice good hygiene, such as checking URLs before clicking links. Training repetition, phishing simulations, and red teams, where an independent group attempts to induce bad employee behavior, can reinforce initial cybersecurity training, and 35% of organizations that have suffered a security incident are instituting additional end-user training.

- Updating and upgrading AV solutions. One-third of respondents who have had a security incident in the last two years said they are upgrading and updating to the latest release of their existing antivirus software, and 28% are starting to utilize additional controls available in their AV suite. Even though upgrades can potentially block more infections, organizations are often slow to update because it takes time and pulls staff away from other critical tasks. Another time-consuming task is tuning the AV suite to meet the specific needs of the organization. Deciding which options and additional controls to enable may require specialist training and testing before widespread implementation, during which time the organization may be exposed to greater risk.

- **Updating, upgrading, and patching endpoints.** Many attacks, including the WannaCry ransomware, achieve success by exploiting known vulnerabilities in the endpoint operating system. Often those security holes have already been identified and closed, and the fix is available as a patch or in a new release. Some organizations may avoid routine patching, believing that the risk of the patch causing a problem with the endpoint is greater than the security risk of leaving a known bug exploitable. The risk, interruption, and cost of upgrading to a new operating system release is even greater than with patching, so organizations often delay such upgrades, sometime for years after they become available. Upgrades and patches may also be gated by software compatibility. But there is a correlation between having experienced an infection and organizations' stated intentions to patch more often, with one-third of organizations that have experienced cybersecurity incidents indicating that they have decided to increase the frequency with which they update and patch their endpoint operating systems.

- **Penetration testing.** Thirty percent of organizations that have been attacked have conducted penetration testing. An independent group without prior knowledge of the existing cybersecurity infrastructure can approach penetrating the organization using the mindset of a determined malicious hacker. The goal is to expose weaknesses and vulnerabilities that may be overlooked by those with a financial, political, or emotional stake in the outcome. Once identified, the organization can apply quick fixes or look at strategic solutions to their specific issues.

One of the strategic solutions being pursued by research participants who have had an incident is to purchase and deploy "next-generation" AV (NGAV) controls that employ machine learning (ML) for threat detection. ML provides the ability to evaluate large volumes of data, including attributes of binary executables. The deployment of ML-based NGAV products is well underway, with 47% of organizations having already deployed such solutions extensively or on a limited basis, and another 47% noting they are either currently engaged in a project to deploy this technology or are planning on or interested in doing so.

Machine Learning Has Both Efficacy and Efficiency Benefits

Big data, descriptive analytics, diagnostic analytics, behavioral analytics, prescriptive analytics, predictive analytics, expert systems, neural networks, machine learning, deep learning, supervised learning, unsupervised learning—these are techniques and technologies in the broad and complex field of artificial intelligence. These terms are also used, and abused, by cybersecurity vendors in an effort to gain attention in a crowded marketspace.

Cybersecurity professionals are learning to see beyond the hype and develop an understanding of the benefits of machine learning applied to endpoint security. These professionals are deploying machine learning technology for endpoint security to obtain these benefits, including:

- **Increased efficacy**. Machine learning systems create detection algorithms using attributes of known good and bad executables as a baseline from which such detection algorithms can determine the probability that a new binary is good or bad. Whereas traditional signature-based AV systems rely on a database of known good or bad files, ML systems apply their algorithms to identify malicious attributes in otherwise innocuous files, detecting obfuscated and new and previously unknown malware. As noted earlier, unknown malware is perceived to be the hardest threat to detect, and one-third of respondents said that ML technology can detect new and unknown malware before they execute. Thirty-two percent said that ML can detect new and unknown malware that evades other endpoint security technologies.

- **Increased efficiency**. Cybersecurity vendors perform the heavy lifting in machine learning: gathering large bodies of good applications and known malware, developing and training behavior models, and creating detection algorithms. Once deployed in an endpoint, the algorithms are applied to render "good" or "bad" verdicts. On the endpoint, ML-based NGAV products hold the promise of making efficient use of system resources and research respondents agree, with 28% of those who are deploying or evaluating ML-based endpoint security systems sharing that they are doing so because they have a smaller CPU and memory footprint. In addition to the value of reducing the use of system resources, 27% of respondents recognize that they gain management efficiency by eliminating the need for frequently updating the AV signature database, and 25% understand that ML systems can help protect air-gapped systems (those not connected to the Internet).

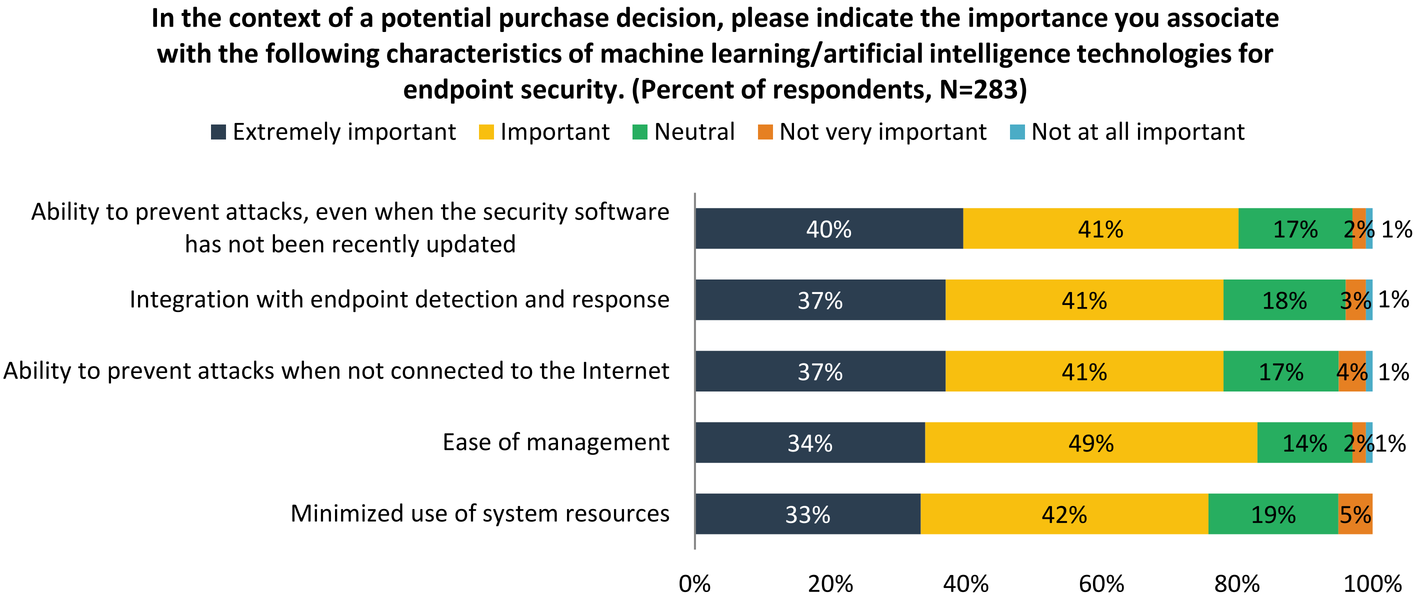
- **Increased staff productivity**. Using machine learning to detect and prevent infections from unknown malware reduces the number of incidents that must be investigated and remediated by the cybersecurity team. ML can also help cybersecurity professionals to identify repeated and effective incident response processes and patterns. This in turn can enable automation of incident triage, containment, mitigation, and remediation tasks, and free up valuable resources for other critical tasks. This is especially important in light of the global cybersecurity skills gap. Prior ESG research revealed that 45% of organizations claim to have a problematic shortage of cybersecurity skills—the biggest skills gap of all types of IT skills.[1] Organizations understand that they can't hire their way out of the skills shortage, and 25% are deploying machine learning endpoint security solutions to maximize the productivity of their existing staff.

Machine Learning Is a Core Component of Defense-in-depth Strategies

The benefits of machine learning are so compelling that only 3% of organizations expressed no interest in or plans to deploy ML-based solutions. In aggregate, almost half (47%) of respondents have already deployed ML technology for their endpoint security, and another 23% are engaged in pilot projects.

The characteristics of machine learning that organizations consider important to their purchasing decision correlated closely with the perceived benefits (see Figure 6).

Figure 6. Purchasing Criteria for ML-based Endpoint Security



Source: Enterprise Strategy Group, 2017

Thirty-seven percent of respondents said integrating machine learning with endpoint detection and response was a very important purchasing criterion, and 31% said that adding ML as a component of their defense-in-depth strategy was their primary motivation for deploying or investigating machine learning.

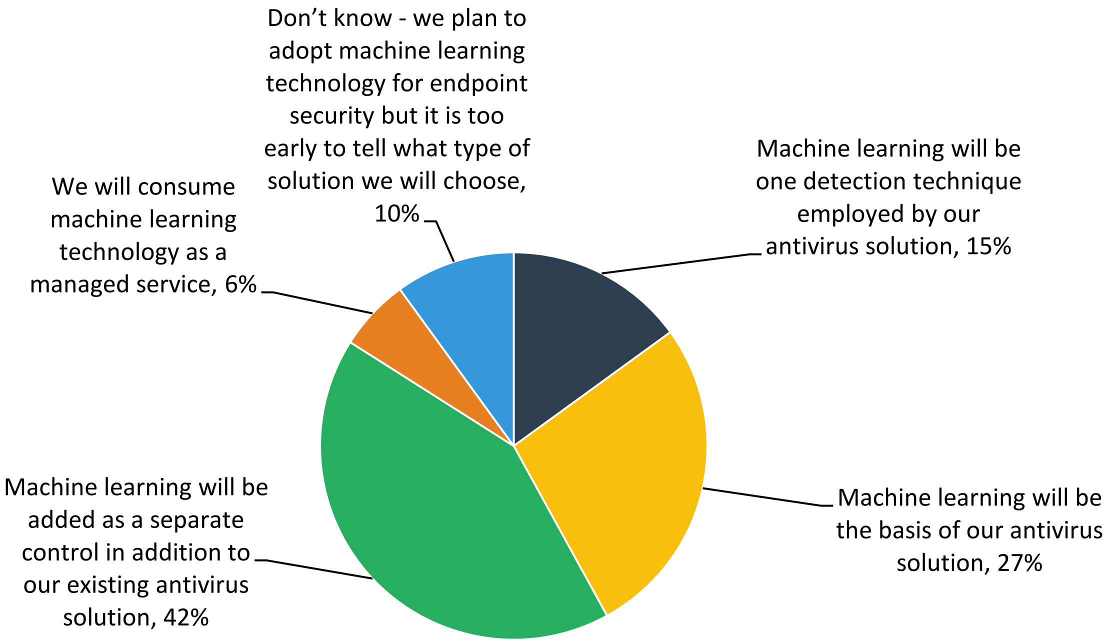
[1] Source: ESG Brief, *2017 Cybersecurity Spending Trends*, March 2017.

Cybersecurity professionals recognize that, even with the benefits that can be obtained by applying machine learning to endpoint security, they are often employed in addition to other endpoint detection, prevention, and response tools.

Of the organizations planning to adopt or deploying machine learning today, just over one-quarter (27%) expect ML to be the basis for their antivirus solution (see Figure 7). Defense-in-depth strategies are much more prevalent, with 42% expecting ML to be added as a separate control, and 15% expecting ML to be just one of many techniques used by their AV solution.

Figure 7. Machine Learning and Endpoint Security Strategy

You indicated you plan to adopt, or have interest in adopting, machine learning for endpoint security. Two years from now, how do you expect your organization will ultimately run/operate machine learning technology for endpoint security? (Percent of respondents, N=142)



Source: Enterprise Strategy Group, 2017

The Bigger Truth

While the threat landscape continues to evolve, the tried and true continues to reign supreme. Organizations are most concerned about cybercriminals, phishing, and unknown malware. This combination of bad actor, method, and threat type disrupt end-user and IT productivity. Remediation by reimaging has turned into a “rinse and repeat” cycle, especially as the result of ransomware infections, with some organizations reimaging hundreds of machines per month, only to be re-infected, often with the same ransomware, exposing weaknesses in their endpoint cybersecurity strategy.

The first levers organizations pull immediately post-incident are generally centered on that which is in their immediate control: influencing user behavior with additional training, identifying weaknesses via red team and pen testing exercises, and updating and upgrading endpoint operating systems and AV solutions. But cybersecurity professionals also seek more strategic solutions and understand the efficacy and efficiency gains they can realize with machine learning. As such, machine-learning-based antivirus is becoming an increasingly important feature of a defense-in-depth endpoint security strategy.

Appendix: Research Methodology and Respondent Demographics

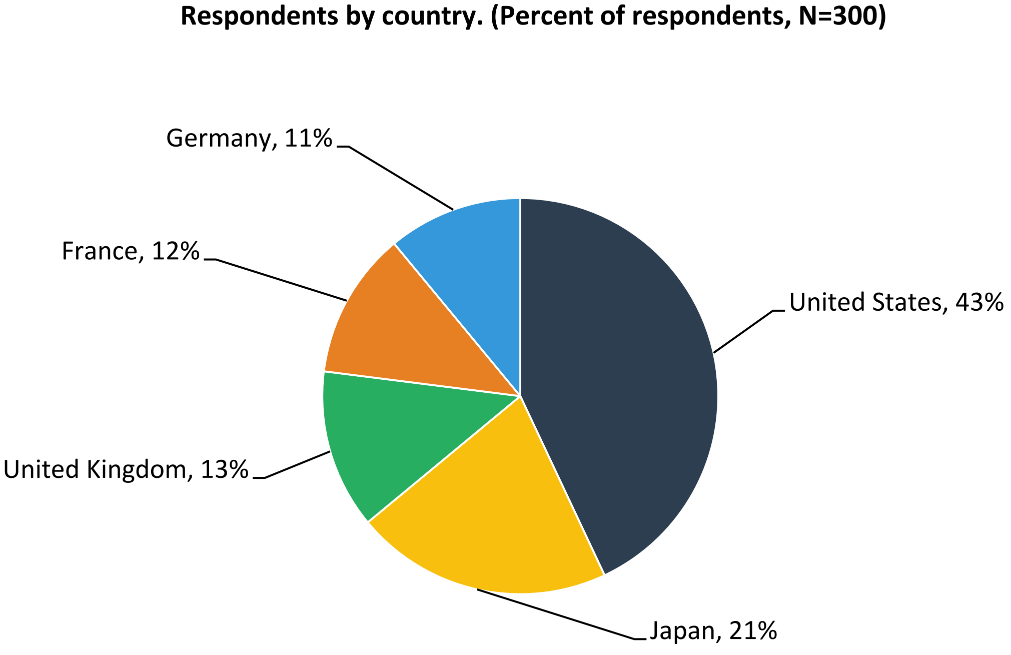
To gather the quantitative data for this report, ESG conducted a comprehensive online survey of security decision makers from private- and public-sector organizations in the United States, United Kingdom, France, Germany, and Japan between June 26, 2017 and July 20, 2017. To qualify for this survey, respondents were required to have reported a high level of knowledge of the policies, processes, or technical safeguards in place to secure their organization's endpoint devices. Additionally, all respondents must have reported material involvement in the purchase process for endpoint security products and services. Moreover, all respondents must have been employed at organizations with at least 500 employees. 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 several criteria) for data integrity, a final sample of 300 respondents remained.

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

Figures 8-12 detail the demographics of the respondent base from the quantitative survey, including respondents' current role in the organization, respondent organizations' size, and primary industry.

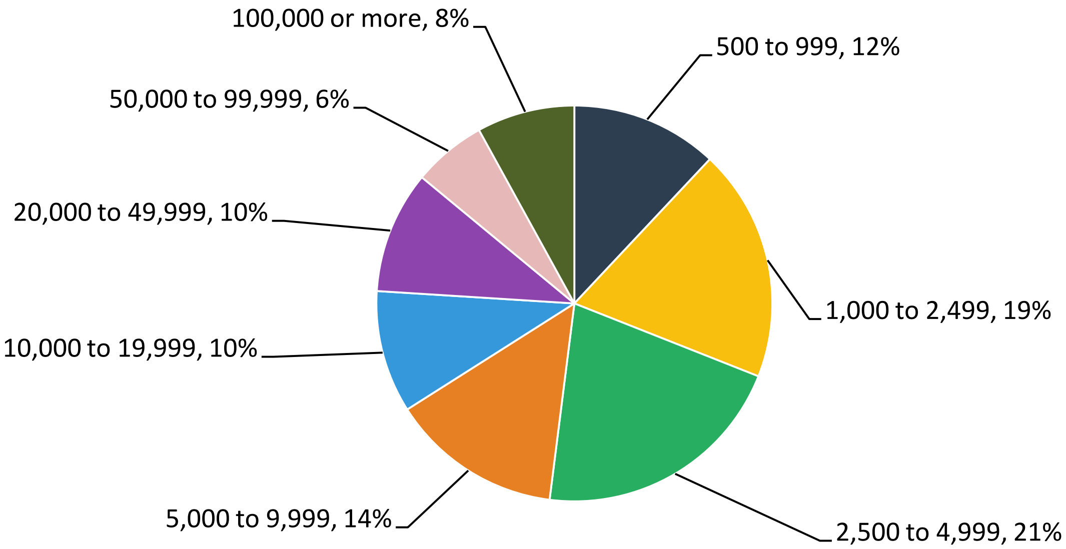
Figure 8. Survey Respondents, by Geographic Location



Source: Enterprise Strategy Group, 2017

Figure 9. Survey Respondents, by Number of Employees

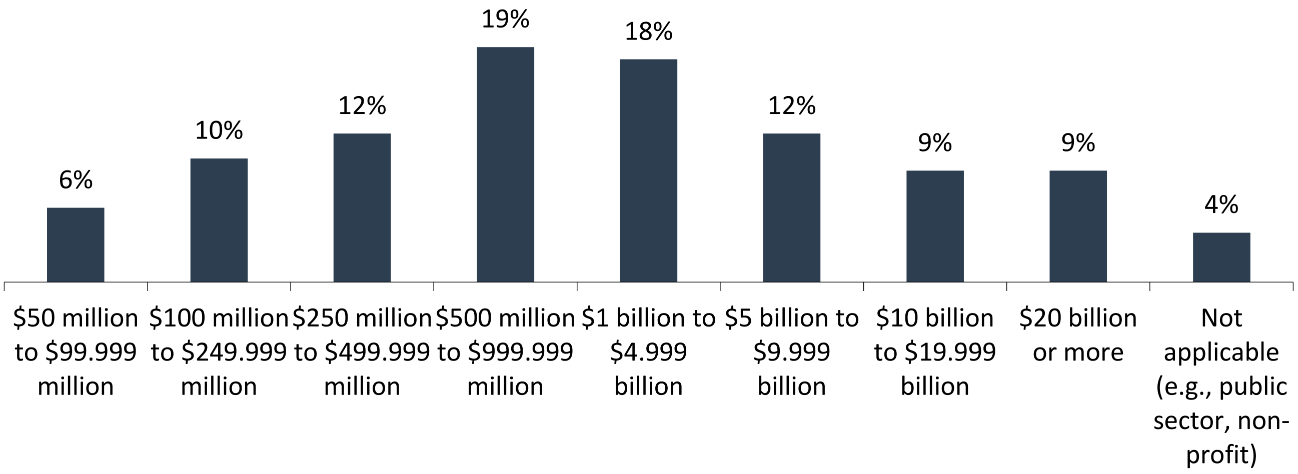
How many total employees does your organization have worldwide? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2017

Figure 10. Survey Respondents, by Organizations' Annual Revenue

What is your organization's total annual revenue ($US)? (Percent of respondents, N=300)



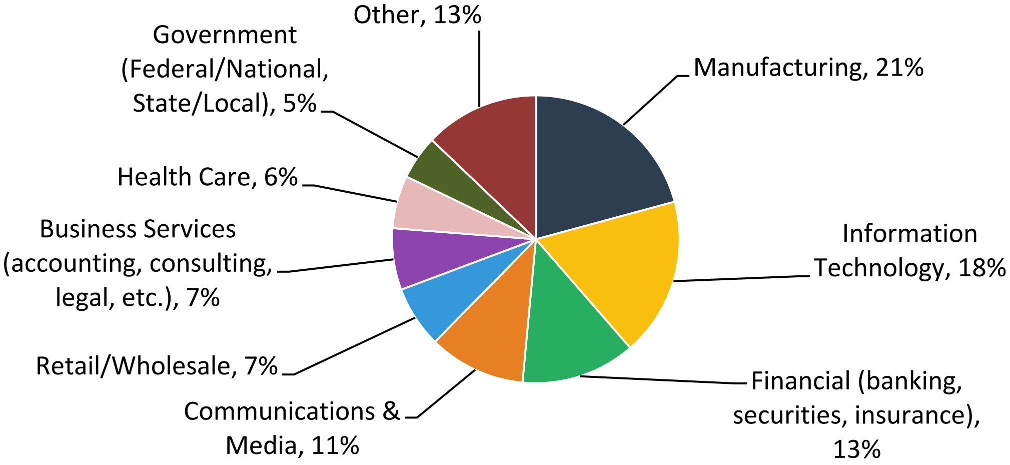
Source: Enterprise Strategy Group, 2017

Respondents by Industry

Respondents were asked to identify their organization's primary industry. In total, ESG received completed, qualified responses from individuals in 20 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 11.

Figure 11. Survey Respondents, by Industry

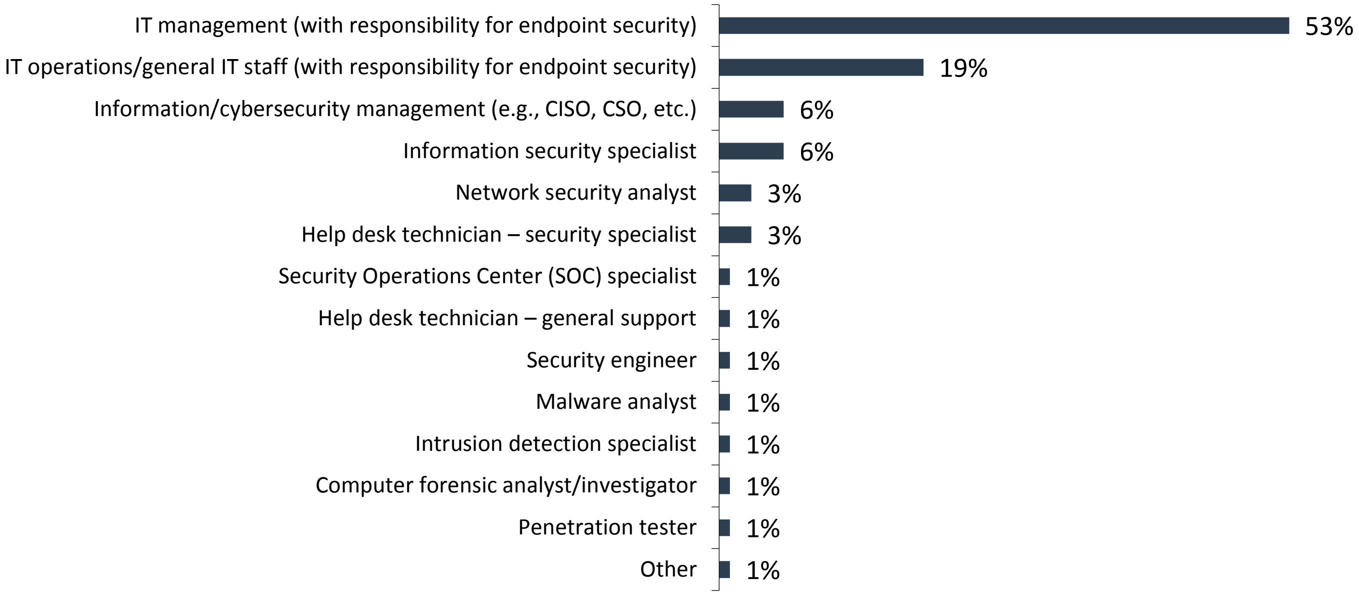
What is your organization's primary industry? (Percent of respondents, N=300)



Source: Enterprise Strategy Group, 2017

Figure 12. Survey Respondents, by Role

Which of the following best describes your current role within your organization? (Percent of respondents, N=300, one response accepted)



Source: Enterprise Strategy Group, 2017

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.