ESG Research Insights Report

2017 Business Cybersecurity Trends

By Jon Oltsik, ESG Senior Principal Analyst; and Jack Poller, ESG Analyst

August 2017

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

Contents

Executive Summary

In the first half of 2017, Webroot commissioned Enterprise Strategy Group (ESG) to conduct a survey of 200 perimeter security and network influencers and decision makers with knowledge of anti-malware technologies and perimeter protection in place at their organization. The goal of this study was to share the results with Webroot technology partners to examine the challenges their business customers are facing as they take on malware and other cyber threats at network perimeters. All ESG research references and charts in this research insights report are based on this research unless otherwise noted.

Survey respondents were located in North America, and were employed at enterprise-class (1,000 or more employees, 93%) or large midmarket (500-999 employees, 7%) organizations. The survey included representation from multiple industry verticals including manufacturing (28%), finance (18%), retail and wholesale (9%), healthcare (9%), business services (8%), government (7%), IT (5%), and communications and media (5%), among others.

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

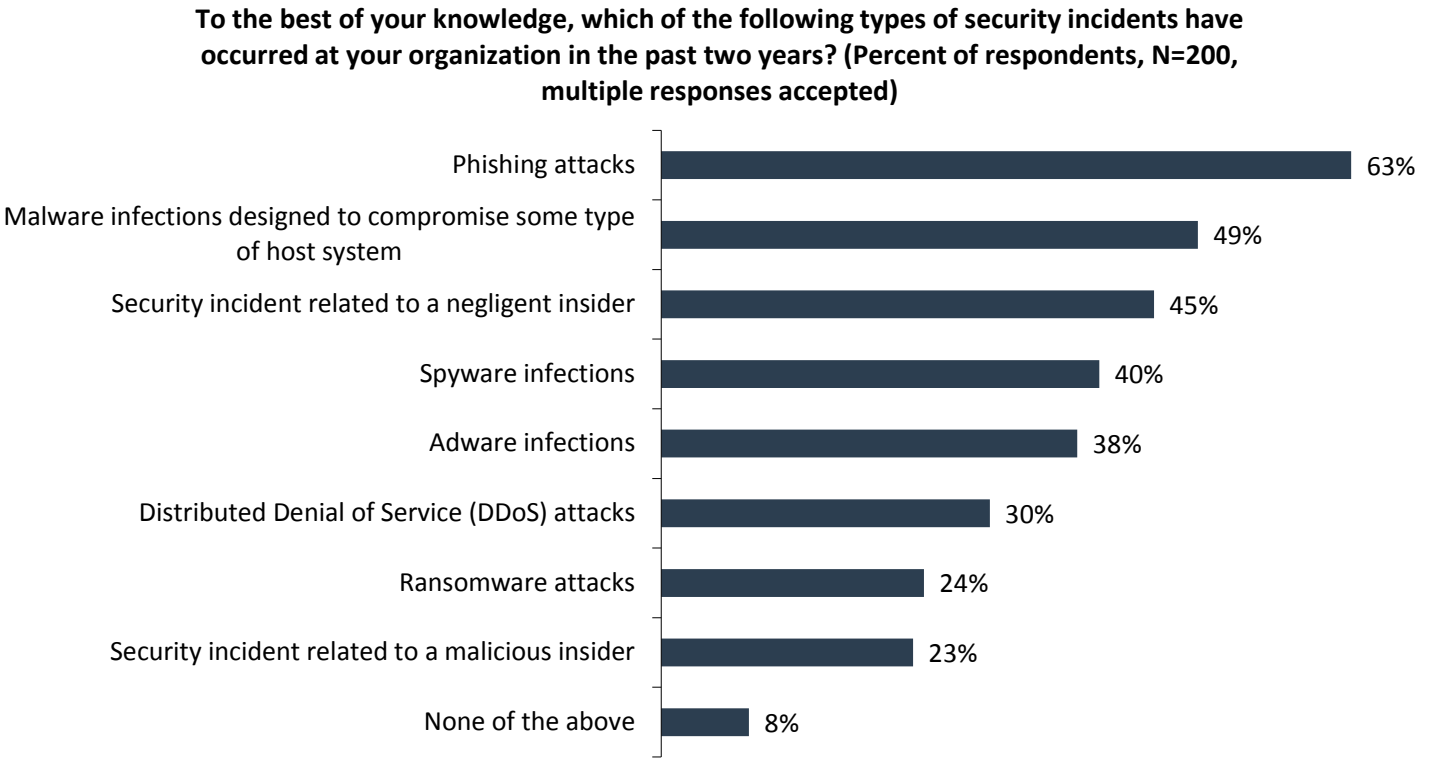
- Security remains an issue. Nine out of ten security professionals report they've had a security incident in the last two years, and 12% said they've had more than 25 breaches. These security incidents included phishing attacks, adware, spyware, malware, and ransomware, and respondents indicate they expect these types of attacks to continue in the next two years.
- Detecting malware is challenging. Cybersecurity professionals have a long list of challenges they face with malware detection and prevention. Survey respondents point to the increasing sophistication of malicious actors and the malware they create, the increased volume of attacks, and the increased use of mobile devices, which has expanded the attack surface.
- Security professionals are searching for help. Infosec pros believe that they will continue to face more of the same types of attacks. As a result, 88% are researching, evaluating, and deploying new tools to help protect their organization's assets. In light of the global cybersecurity skills shortage, organizations are turning to third parties for additional services and support, as well as investigating integrated architectures to accelerate detection and remediation and lighten the workload.

Attacks Introduced at the Network Edge Continue Unabated

Cybersecurity can be an intimidating discipline for most organizations. The threat landscape is increasingly dangerous, as malicious actors focus their energy on developing sophisticated, targeted, polymorphic attacks designed to evade traditional signature-based detection systems. Mobile- and cloud-first initiatives, digital workplace transformation, and IoT applications are increasing the size and complexity of the IT infrastructure, expanding the attack surface, and increasing the risks to the organization.

The network perimeter represents a significant entry point for successful attacks, with nearly two-thirds (63%) of respondents indicating they've suffered from phishing attacks over the past two years (see Figure 1). Other security incidents include malware, spyware, adware, and ransomware.

Figure 1. Types of Security Incidents in the Past Two Years



Source: Enterprise Strategy Group, 2017

Unfortunately, security incidents are not a one-time event. Ninety percent of respondents said that they have experienced more than one security incident in the past two years, with 41% indicating they've endured two to five incidents. Surprisingly, even with significant prevention efforts, 12% of organizations have suffered more than 25 cybersecurity incidents.

Despite ongoing investments in cybersecurity, why are so many organizations continually compromised? According to Figure 2, respondents believe a variety of issues are driving security incidents, including:

- Risky user behavior. Less than one-third (29%) of respondents say their employees aren't adequately trained and often engage in risky behavior like opening unknown email attachments or clicking on suspicious URLs. This may be a result of organizations relegating end-user cybersecurity training to a one-time event as part of new employee orientation to effectively "check the box" on meeting cybersecurity training requirements. Even with growing cybersecurity budgets, security professionals may perceive that the benefits of routine training are outweighed by the need to invest in other areas of cybersecurity.

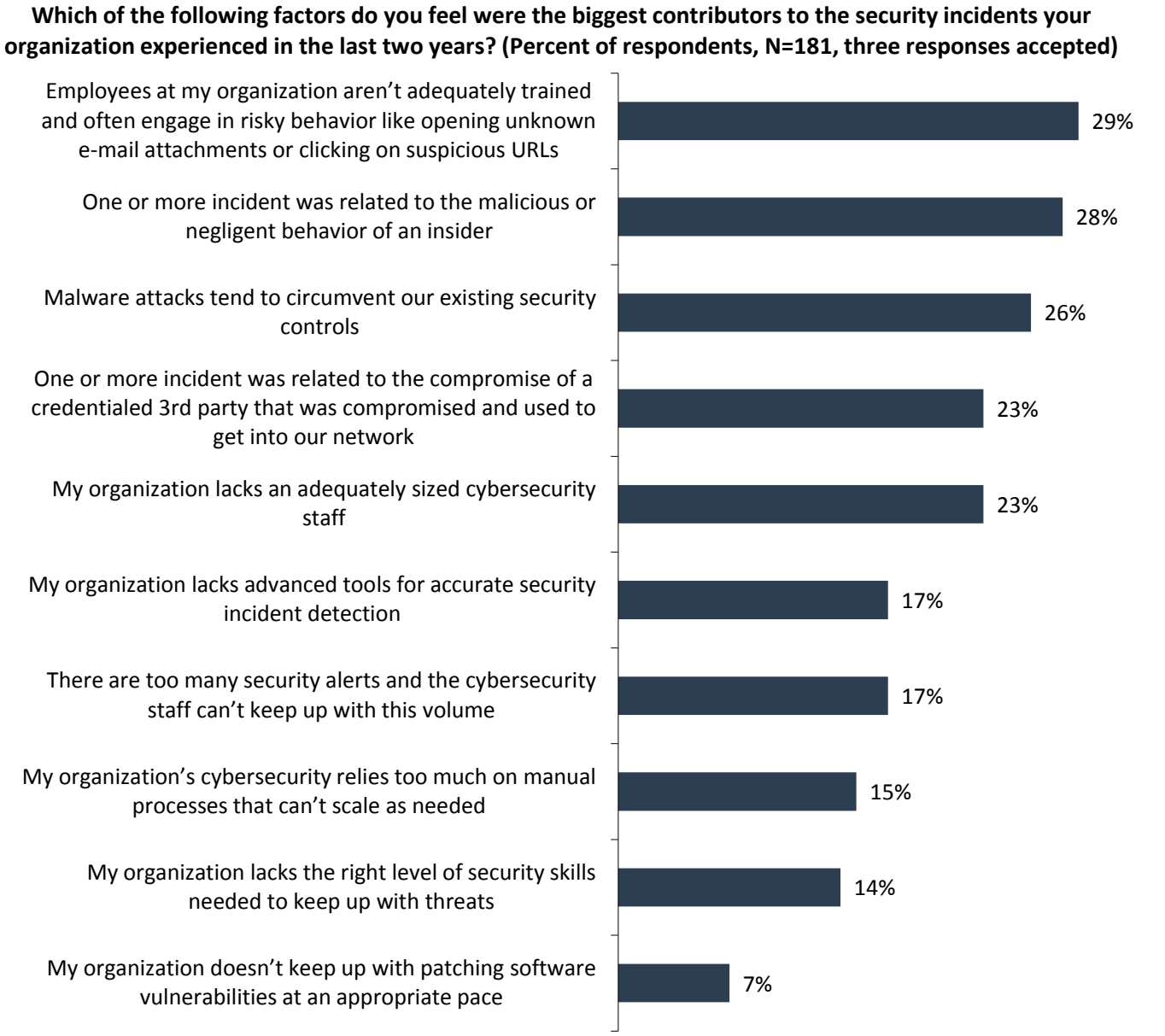
- Insider compromise. Twenty-eight percent of respondents indicate one or more of their security incidents was related to the malicious or negligent behavior of an insider. For example, users with stored WiFi connections can unknowingly and automatically connect to a bogus WiFi network created to masquerade as a coffee shop WiFi hotspot, exposing themselves to malware injection, identity theft, and data theft.

  Malicious insiders intent on causing damage may be able to bypass traditional security controls, or may share their identity with unauthorized users. Once past a perimeter security check, those with bad intent can install malware or ransomware, or exfiltrate confidential data.

- Inadequate security controls. More than one-quarter (26%) of those surveyed indicate that in the past two years, malware attacks tended to circumvent their security controls. In some cases, sophisticated cyber-adversaries develop exploits intended to bypass security controls but in many cases, organizations fail to update security controls or patch vulnerable systems, making them an easy target for malware attacks.

Modern malware and potentially unwanted applications (PUAs) tend to be polymorphic, and can be automatically generated with tools that produce large volumes of unique, single-use files. As each malicious file is delivered to a very small number of users, it may be difficult or impossible for traditional signature-based security technologies to detect and prevent infection.

Figure 2. Biggest Contributing Factors to Security Incidents



Source: Enterprise Strategy Group, 2017

It is also worth noting that 23% of respondents say the biggest contributing factor to their security incidents over the past two years is that they don't have enough cybersecurity staff, while 14% say their organization lacks the right level of

security skills to keep up with threats. These skills are in high demand and difficult to find due to the global cybersecurity skills shortage. According to ESG research from earlier this year, 45% of organizations claim to have a problematic shortage of cybersecurity skills.[1] Since there is really no end in sight for the cybersecurity skills shortage, CISOs will not be able to hire their way out of security deficiencies. To bridge this gap, organizations must invest in training and innovative, intelligent technologies designed to help increase efficacy, efficiency, and productivity.

The impact of successful attacks is often exacerbated by cybersecurity staffing deficiencies and skills limitations. This is substantiated by the fact that 44% of respondents indicated that remediation of a cybersecurity incident required significant time and IT personnel attention (see Figure 3). Successful attacks harmed organizations through lost productivity, disruption of business, breach of confidential data, damage to the company's reputation and goodwill, and other impacts.

Figure 3. Impact of Security Incidents

Source: Enterprise Strategy Group, 2017

Malware Detection Is Getting Harder

In order to detect (and remediate) malicious activities, cybersecurity staff typically gather information from an assortment of data sources including endpoint detection and response (EDR) tools, antivirus software, network security analytics dashboards, and SIEM systems. SOC personnel then contextualize, enrich, and analyze this data to piece together the timeline, scope, and impact of malicious activities. Once a true incident is detected and prioritized, cybersecurity staff

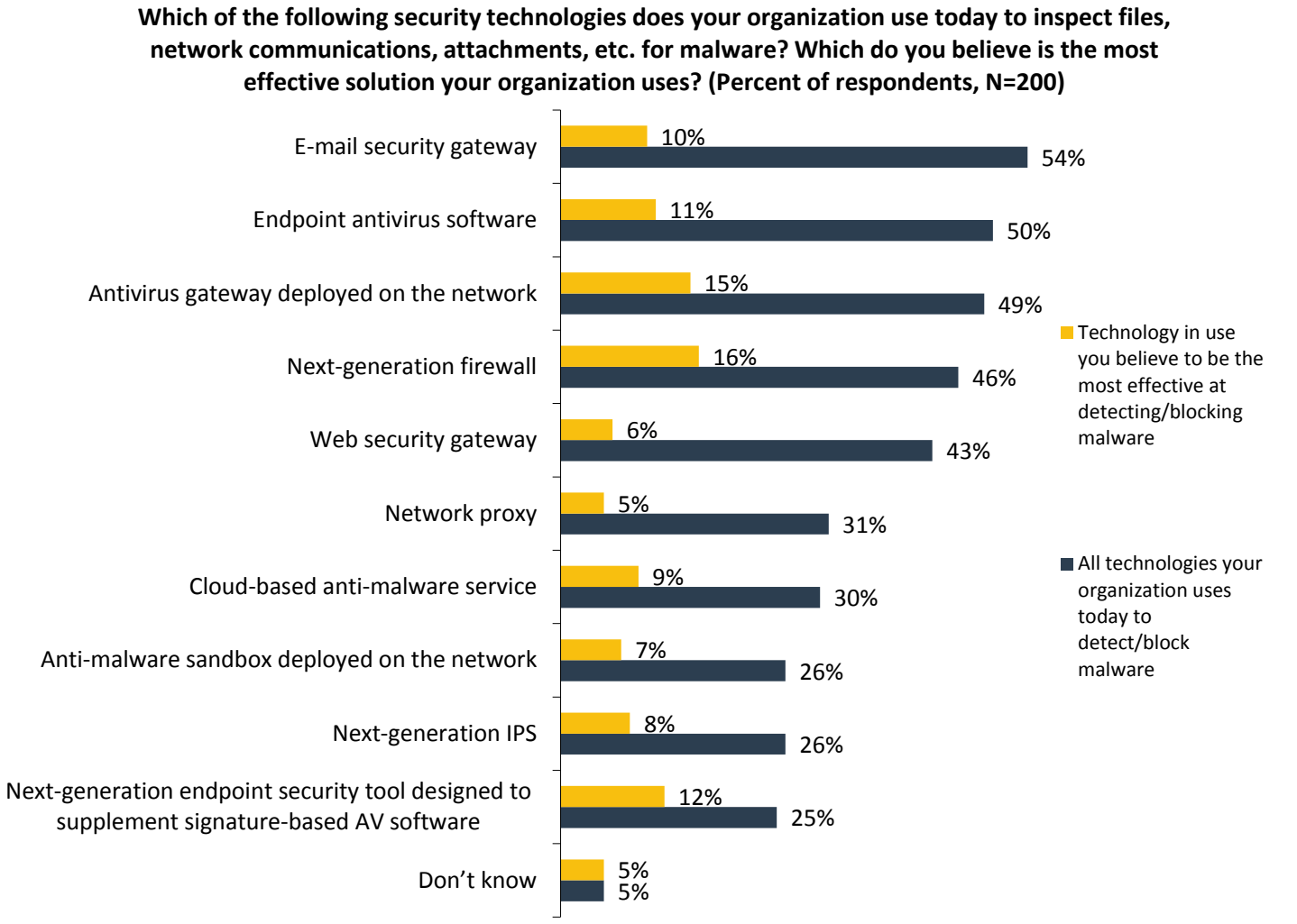
[1] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

collaborate with IT operations teams to remediate compromised or vulnerable systems to mitigate risk or minimize the impact of a security breach.

As part of the research, ESG asked respondents about the number of tools and services used in their organizations' malware detection activities. The data revealed that one-third of organizations use six to ten tools while 29% use 11 to 25 tools for malware detection. The variety of tools currently in use spanned email security gateways, endpoint antivirus software, network antivirus gateways, next-generation firewalls, and web security gateways, among others (see Figure 4).

It should be noted that while more than half (54%) of those surveyed use email security gateways, only 10% found these gateways to be their *most effective* solution to malware. IT trends like cloud computing, mobility, digital transformation, IoT, and hybrid and multi-cloud environments add to the complex mix of cybersecurity tasks involving multiple people and tools, and may be contributing to the mismatch between security technology deployment and perceived effectiveness.

Figure 4. Technologies Used for Malware Detection



Source: Enterprise Strategy Group, 2017

In aggregate, changes in the IT environment combined with a rise in sophisticated malicious actors appear to be increasing the difficulty of incident detection at many organizations, as more than half (54%) of respondents believe that incident detection has become more difficult during the past two years, identifying several likely culprits, including:

- **Malware sophistication.** Almost half (48%) of respondents said malware has become more sophisticated over the past two years. As stated earlier, polymorphic malware can be difficult to detect when employing traditional signature technology. Malware is also now designed to be short-lived, hosted on websites that only exist for a few hours, further impeding detection.

- **Targeted attacks**. Forty-six percent of those surveyed said malware attacks have become more targeted over the past two years. Like corporations, malicious actors take return on investment into account, and targeted attacks can have a better return than more broad-based attacks.

  Attackers also have specific goals in mind. Thirty-eight percent of respondents indicated that attackers intended to exfiltrate corporate data as a criminal act, 35% said attackers wanted to disrupt the business through denial of service, 23% faced hacktivists who wanted to embarrass or expose the organization, and 22% said attackers were involved in obtaining data for corporate espionage.

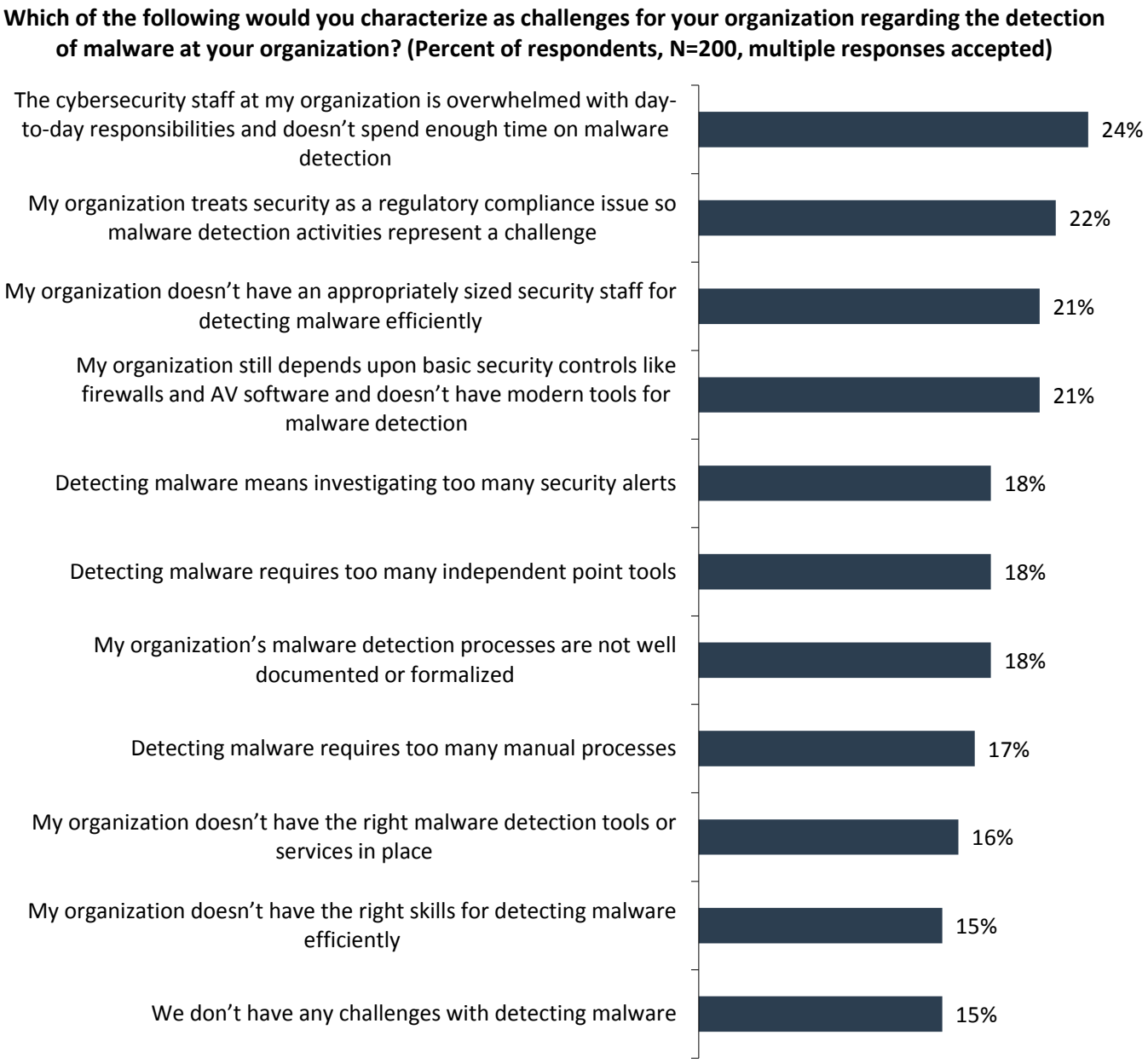
- **Increasing attack volume**. Forty-five percent of respondents said that there is a greater volume of malware today than in the past two years. This is most likely because attackers have found success with their efforts, and now attack a multitude of users, devices, application vulnerabilities, etc.

- **More mobile devices**. Almost one-third (31%) of respondents said that increasing use of mobile devices is making malware detection more difficult. Mobile devices often operate outside of the network perimeter, beyond the purview of corporate cybersecurity controls. In addition, due to their market penetration, malicious actors are now expanding beyond traditional Windows PCs, creating malware specifically for mobile device operating systems. Organizations that neglect cybersecurity controls for mobile devices expose themselves to more security incidents.

Survey respondents predict that over the next two years they will continue to face more of the same types of security incidents that they've been dealing with in the past two years. Forty-one percent of those surveyed predict they will face malware infections, 35% predict phishing attacks, and 29% predict ransomware attacks.

Cybersecurity professionals agree that there are many tasks that make malware detection challenging. According to Figure 5, many of these challenges are the result of inadequate tools and technologies, which have not kept pace with the advances in malware. Another key driver is the ongoing global cybersecurity skills shortage.

Figure 5. Challenges Associated with Malware Detection



Source: Enterprise Strategy Group, 2017

Organizations Are Searching for New Solutions

As previously noted, malicious actors have been successful using sophisticated phishing, ransomware, and malware attacks, and respondents predict that these attacks will continue in the next two years. As a result, organizations are seeking new methods to detect and prevent attacks introduced at the edge of the network.

In aggregate, 88% of those surveyed indicated that they are searching for new tools and technologies, with more than one-quarter (28%) saying they are extremely active and regularly research, evaluate, and deploy new types of security technologies. What type of solutions are these organizations evaluating?

- New technology. Forty-three percent of respondents plan to invest in new threat detection technology, and 31% plan new incident response technology investments. This may be a result of the latest developments in big data and

machine learning, which are enabling advanced analysis of ever larger data sets. Applying these techniques to cybersecurity data can enable higher accuracy, reduce false- positives, and accelerate threat detection and remediation.

- Staffing and outsourcing. Organizations need to address their existing staffing issues, and continue to look for qualified cybersecurity personnel. Thirty-four percent of respondents plan to hire additional staff, while 34% are also trying to provide additional cybersecurity training for their existing staff, and 32% plan for additional training of their security team. Nearly one-quarter (24%) of respondents expect their organization to increase activities around third-party risk management, and 13% plan to outsource cybersecurity tasks.

- Integrated environments. One-quarter (24%) of respondents plan to integrate point tools to build an integrated cybersecurity architecture, and 14% plan to automate security operations tasks. These actions typically lead to the development of security operations and analytics platform architectures (SOAPA), which aggregate and integrate an entire suite of cybersecurity tools into a software architecture across the enterprise. SOAPA solutions are designed for asynchronous cooperation so security analysts can quickly pivot across tools to find data and take action as they need to in real time, lightening the load on the security team and accelerating incident detection and response.

Cybersecurity budgets are growing correspondingly, with 83% of respondents indicating that their 2017 cybersecurity budget increased, and 89% anticipating their 2018 cybersecurity budget will be even bigger.

The Bigger Truth

Modern IT architectures are becoming more complex as organizations embrace initiatives such as mobile- and cloud-first, digital transformation, and IoT, resulting in an expanding attack surface. Simultaneously, the threat landscape is becoming more dangerous as malicious actors gain in sophistication, and are better able to hide their activities with polymorphic and targeted malware.

Organizations, however, continue to have malware-related security incidents, as shown by the research conducted by ESG. More than half (54%) of those surveyed said that malware detection is becoming more difficult. Security professionals predict that they will continue to have malware, adware, spyware, ransomware, and other security incidents in the next two years. This highlights the need for CISOs to deploy new technologies such as big data and machine learning to improve the effectiveness of threat detection. Integrating and automating threat detection into an overall security operations and analytics platform architecture (SOAPA) should be a core element of any strategic security plan, and can help improve threat detection and remediation efficiency, potentially alleviating the challenges associated with the global cybersecurity skills shortage.

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

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188