CSX™
CYBERSECURITY NEXUS

State of Cybersecurity 2018

Part 2: Threat Landscape and Defense Techniques

Abstract

State of Cybersecurity 2018 reports the results of the annual ISACA global *State of Cybersecurity Survey*, conducted in October 2017. Overall results confirm that cybersecurity remains dynamic and turbulent as the field continues to mature. Cyberattacks remain a constant threat to enterprises; therefore, building a team of experts to defend against these attacks is of high priority to enterprise executives.

To equip you with a comprehensive understanding of the cybersecurity industry through the lens of those who define it—the managers and practitioners—ISACA is presenting a series of white papers that focus on individual survey topics. This report is the second in the *State of Cybersecurity 2018* series. It highlights trends in the threat landscape, focusing on the evolution of threats—notably adversary tradecraft and motivations—and the adaptations made by enterprises to combat them.

ISACA®

Table of Contents

Executive Summary

Cybersecurity, as a discipline, is at a potential inflection point. Attacks continue to increase; just this year, numerous large-scale and high-profile breaches dominated the headlines. From Equifax® to Orbitz®, millions of individuals' data were stolen by cybercriminals. As the frequency of attacks increase, the threat landscape also continues to evolve. New attack techniques, such as fileless malware, continue to gain in prominence, and new attack methods, such as Meltdown and Spectre, continue to be discovered. Meanwhile, enterprises continue to struggle with development of a skilled security team.

This year's global *State of Cybersecurity Survey* examines these issues in detail. In part one of the series, ISACA presented findings related to staffing, workforce development, budgeting and organization of security teams. In this second report, ISACA examines survey results regarding the threat landscape, types of threats that enterprises encounter, representative defense mechanisms and their success in the field.

The threat landscape is rapidly becoming much more problematic than has been the case historically. Not only are enterprises witnessing an increase in the number of attacks, but these attacks continue to evolve. Survey results indicate that a plurality of attacks are financially motivated. Accordingly, techniques employed by attackers tend to reflect this fiscal incentive, and respondents suggest that the trend will continue, at least for the short term. Survey results are not all discouraging for enterprise security teams, however; enterprises have become better equipped at planning for, responding to and mitigating certain categories of attack (e.g., ransomware), likely in response to large-scale and highly disruptive ransomware campaigns like WannaCry and NotPetya. Defenders are adopting their own set of technological advances to combat threats. New technologies, such as artificial intelligence, promise to add detection and response capability; new strategies, including defense and threat intelligence, help practitioners understand and disrupt adversary campaigns.

Key Findings

Following are the key findings that relate to the threat landscape and defense techniques:

- **Cyberattacks are increasing, but the methods employed remain relatively static.** The number of attacks is rising, and practitioners indicate that the upward trend will continue throughout the near-to-intermediate term. Despite the increase in overall numbers of attacks, however, techniques employed by attackers remain relatively constant. Some methods of attack (e.g., phishing) show a slight increase relative to other categories of attacks.
- **Motivation remains monetary, and ransomware countermeasures are nearing ubiquity.** Most attacks are still monetary in nature; they are perpetrated by cybercriminals rather than state actors or politically motivated actors. Enterprises have shifted strongly in favor of better preparation for ransomware relative to last year.
- **Ransomware is being displaced, most likely by cryptocurrency mining.** Ransomware is decreasing as enterprises defend against it more effectively. Alternate strategies, such as cryptocurrency mining, demonstrate effectiveness and better (although different) economic characteristics. This may be, in large part, underpinned by unwillingness to pay the ransom among potential victims.
- **Threat intelligence is prevalent—active defense is less familiar but effective.** Most enterprises employ some threat intelligence capability, often staffed in-house. Active defense strategies, although not understood universally among practitioners or employed in enterprises, demonstrate a high level of success when implemented.

This report describes each of these findings in more detail.

Survey Methodology

ISACA sent the survey in late 2017 to a global population of cybersecurity professionals who hold ISACA's Certified Information Security Manager® (CISM®) and/or Cybersecurity Nexus Practitioner™ (CSX Practitioner™) designations and individuals in information security positions. A total of 2,366 individuals participated in the survey and their responses are included in the results.[1]

Survey data were collected anonymously through SurveyMonkey®. Results reveal positive and negative findings about the current state of cybersecurity. The survey, which uses multiple-choice and Likert-scale formats, is organized into four major sections:

Cyberattacks are increasing, but the methods employed remain relatively static.

Motivation remains monetary, and ransomware countermeasures are nearing ubiquity.

Ransomware is being displaced, most likely by cryptocurrency mining.

Threat intelligence is prevalent—active defense is less familiar but effective.

Figure 1 represents norms of the sample population. While typical patterns are interesting to consider, it is also important to note some characteristics that reflect the population's diversity. Among those surveyed, respondents hailed from 17 industries (**figure 2**) and all seven major global regions (**figure 3**).

[1] Certain questions included the option to choose "Don't know" from the list of answers. Where appropriate, "Don't know" responses were removed from the calculation of findings. Result percentages are rounded to the nearest integer.

FIGURE 1—TYPICAL RESPONDENTS

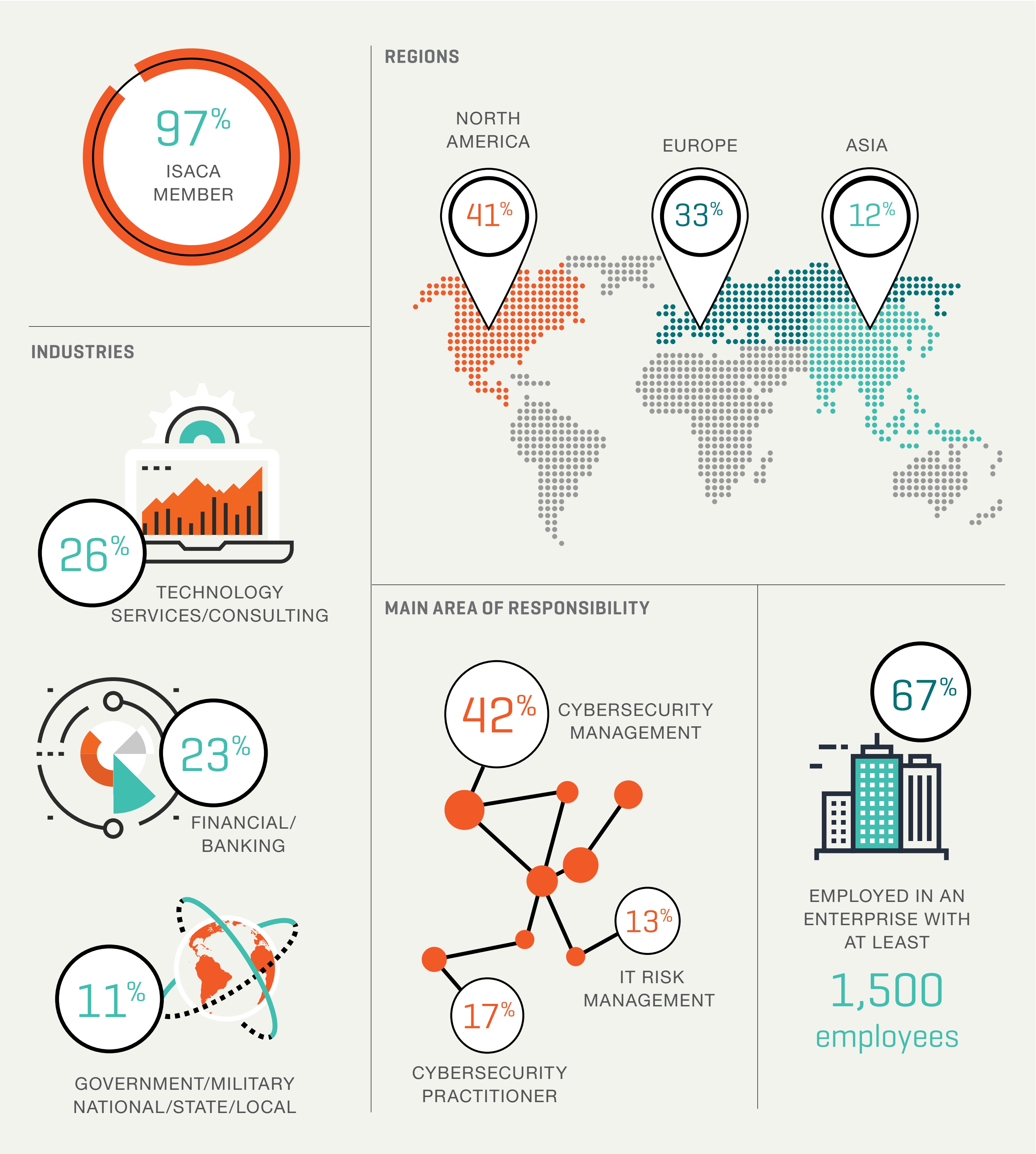


FIGURE 2—INDUSTRY SECTORS

In which of the following industries are you employed?

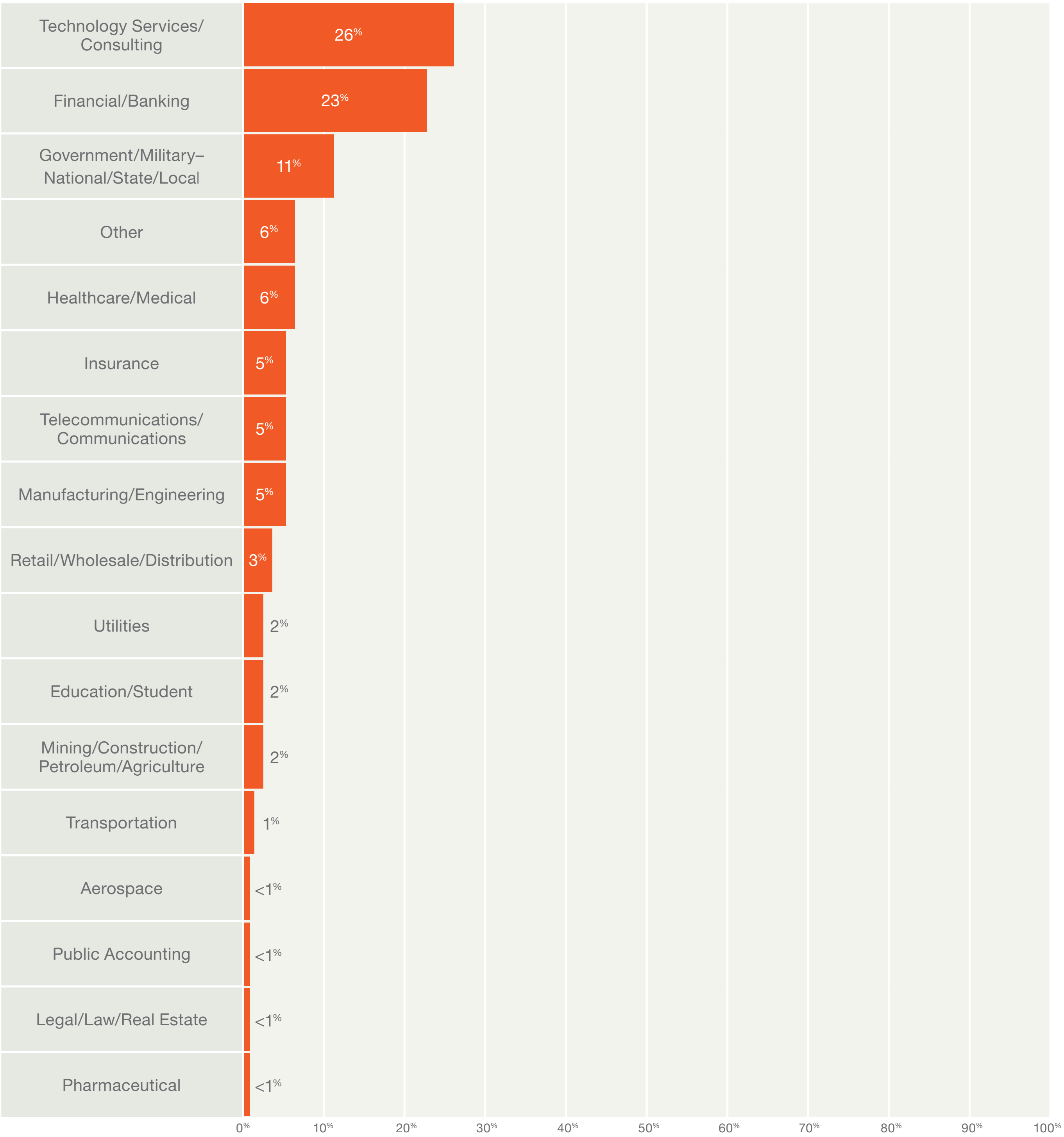
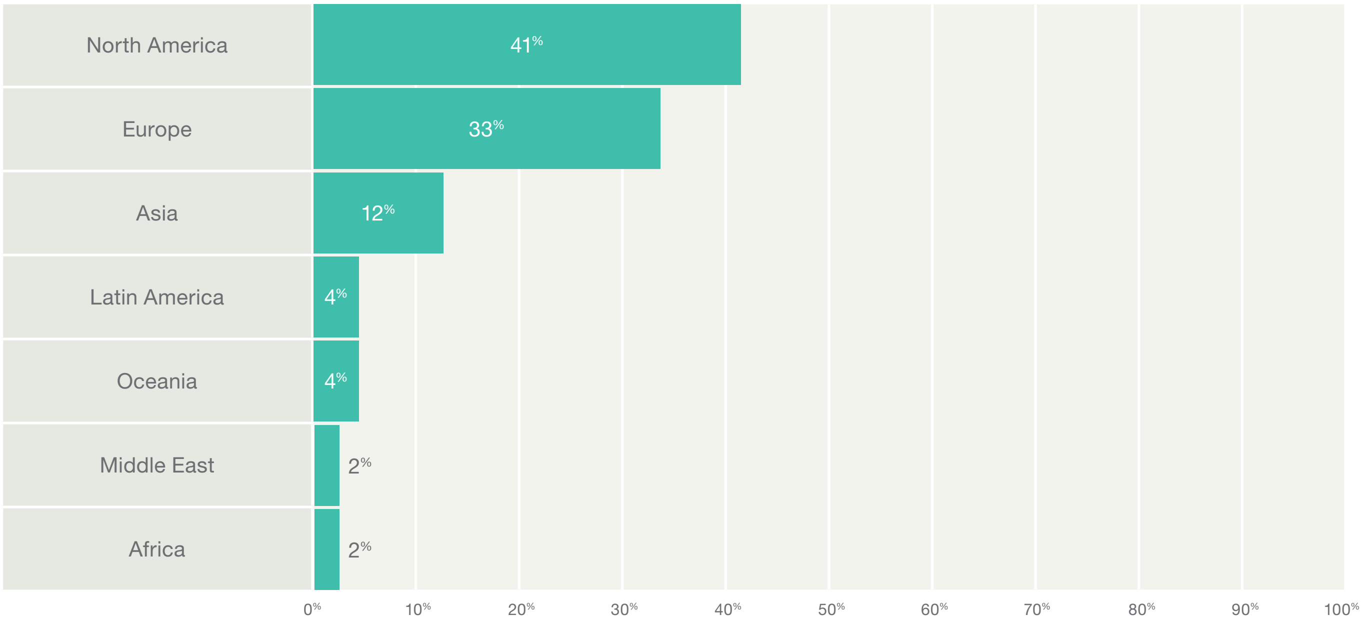


FIGURE 3—REGIONS

In which region do you reside?



Cyberattacks Are Increasing, But the Methods Employed Remain Relatively Static

Cyberattacks are on the rise again based on this year's survey. Fifty percent of respondents indicate that they are experiencing a higher volume of attacks relative to last year; 25 percent indicate that they are seeing a continuation of prior-year levels. Only six percent indicate that they are experiencing fewer attacks relative to the prior year, and 18 percent do not know if attack volume is increasing or decreasing (**figure 4**).

This increase in cyberattacks is likely to continue in 2018. Eighty percent of respondents indicate that it is either likely (38 percent) or very likely (42 percent) that their enterprises will experience a cyberattack in 2018 (**figure 5**). Note that these results are very close (in aggregate) to observations in 2017's report, where 80 percent said it was either likely (41 percent) or very likely (39 percent) that attacks will increase. The increase in the *very likely* response—three percentage points year over year—suggests a slight upward shift in the perception of attack volume.

The specific vectors of attack being observed this year shift slightly compared to last year. Phishing (40 percent), malware (37 percent) and social engineering (29 percent) were the three most commonly observed attack vectors reported by survey respondents last year. This year, the same three attack vectors occupy the top three positions again, although respondents indicate some small shifts among their relative prevalence (**figure 6**). Specifically, phishing increases slightly in prevalence, to 44 percent, while malware and social engineering remain comparable to last year's results (malware at 38 percent and social engineering at 28 percent).

FIGURE 4—CHANGE IN NUMBER OF CYBERSECURITY ATTACKS

Is your enterprise experiencing an increase or decrease in security attacks as compared to a year ago?

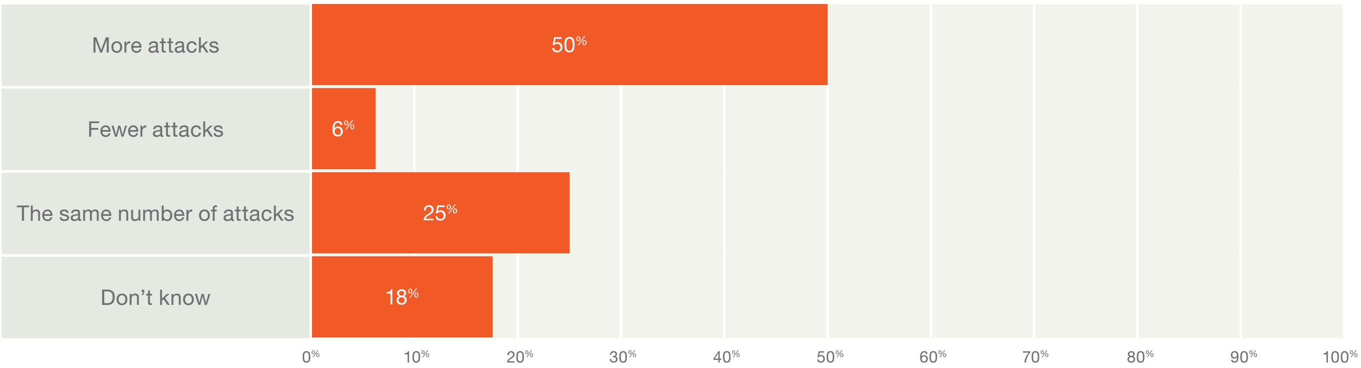


FIGURE 5—LIKELIHOOD OF CYBERATTACK IN 2018

How likely do you think it is that your enterprise will experience a cyberattack in 2018?

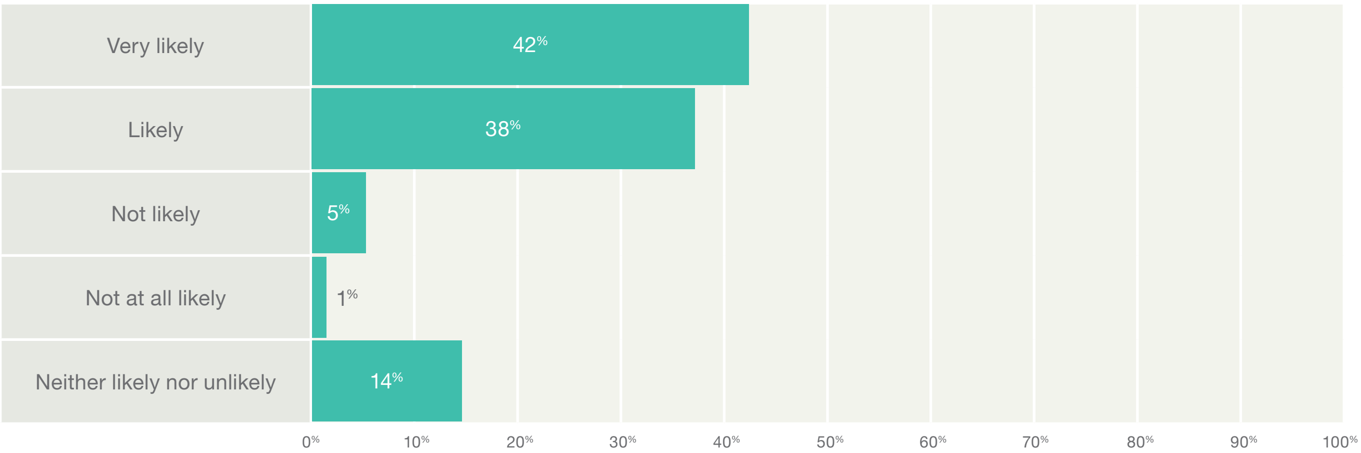
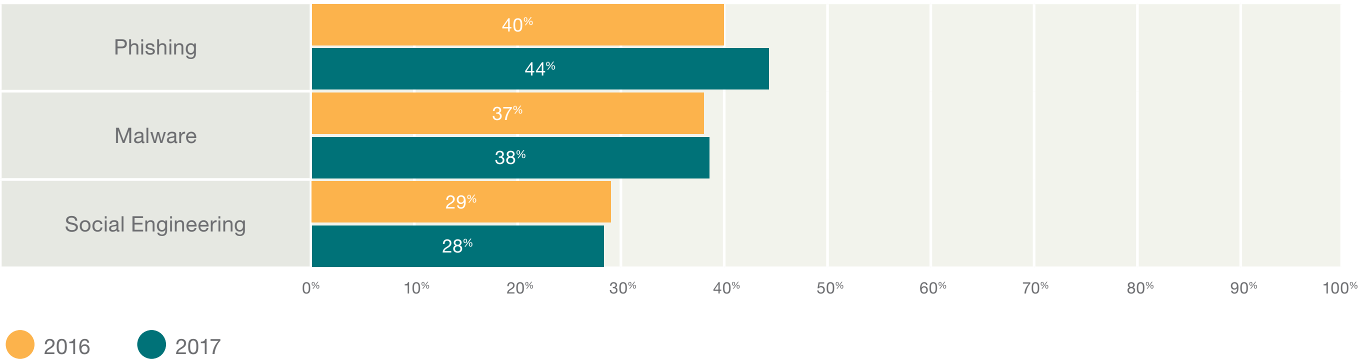


FIGURE 6—COMPARISON OF CURRENT ATTACK TYPES TO LAST YEAR'S RESULTS



In the aggregate, these results indicate continuity of attack methods in the field year over year, even though perceptions of their relative prevalence fluctuated slightly.

Implications for Enterprises

Perspectives regarding attack volume suggest subtle shifts in the experiences of respondents year over year. For example, last year, 53 percent of respondents said they saw more attacks from the prior year (three percent more than this year's results), eight percent said they saw fewer attacks (two percent more than this year's results) and 18 percent indicated that they saw about the same activity as last year (seven percent less compared to this year) (**Figure 7**). There is likewise a decrease of three percentage points among those who do not know if attacks are increasing or decreasing year over year, from last year to this year (from 21 percent to 18 percent).

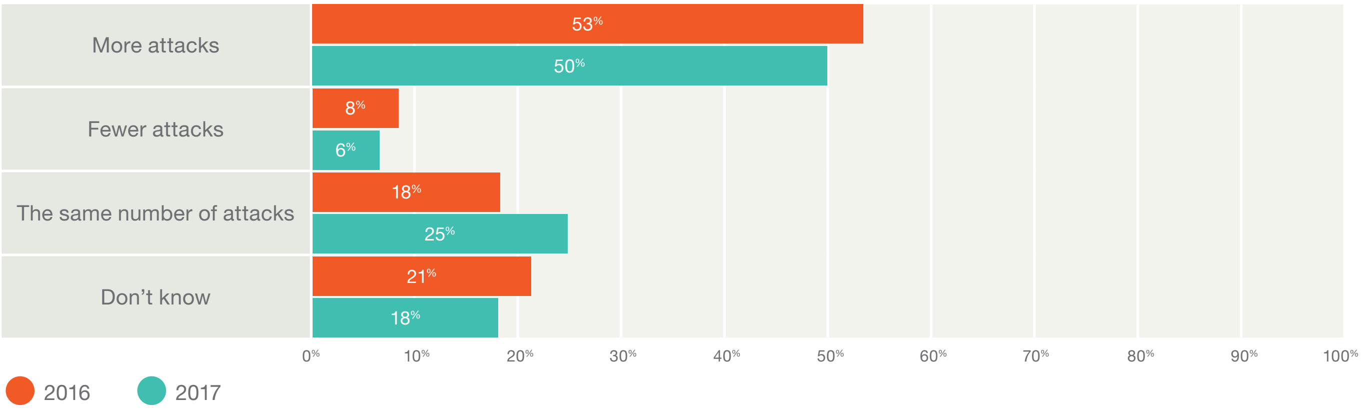
Shifting perspectives of attack volume could reflect a reduction in the overall *rate* of attack increase, i.e., attacks are still increasing but at a reduced rate from last year. A somewhat more plausible account of this shifting perspective is that attacks, while increasing in the aggregate, are increasing *disproportionately* for a subset of the total population relative to others. This, in turn, can reflect more precise and frequent (or recurrent) targeting by attackers who aim specifically at certain groups within the overall population based on some combination of factors. Some enterprises may be attacked more often—and others less often—based on their industry, susceptibility to attack, perceived value to attackers or other factors.

If certain enterprises may be targeted disproportionately, it stands to reason that *all enterprises* will benefit from a systematic and thorough understanding of attackers' motivations, tradecraft, and an enterprise's overall risk level. In short, threat intelligence and information sharing may be improving enterprises' defenses. Enterprises in industries that experience a rise in attack volume may want to leverage information-sharing resources, including, for example, Information Sharing and Analysis Centers (ISACs) or peer-networking opportunities, to gather information about attacks and attackers.

Key enterprise takeaways:

- **Attacks are likely to increase in the short-to-intermediate term. For those enterprises that are already struggling to find and retain the right personnel for security teams, this increase represents an area of potential risk. Enterprises may want to budget and staff security preparedness efforts accordingly.**
- **Automation—to the degree that it can help offset constraints or limitations in security staff—has additive value relative to strategies based on manual resources, given the increasing attack volume. Enterprises may want to consider automation-driven strategies for detection where possible and encourage automated strategies to support recovery and response efforts.**
- **Attack vectors have changed only minimally in relative frequency despite increased attack rate overall. Existing control types are still valid and useful (assuming they adapt to address evolution in the types of existing attack). Enterprises that underinvested in security controls around the most frequent attacks (phishing, malware and social engineering) may want to reallocate investment in line with the frequency of these attack vectors.**

FIGURE 7—COMPARISON OF CHANGE IN NUMBER OF CYBERATTACKS TO LAST YEAR'S RESULTS



Motivation Remains Monetary, and Ransomware Countermeasures Are Nearing Ubiquity

The primary motivation for attacks is again monetary this year. A plurality of threat actors, as reported by survey respondents, are cybercriminals. Cybercriminals represent 33 percent of those responsible for the attacks (**figure 8**). Other threat actor types include hackers (23 percent), nonmalicious insiders (14 percent), malicious insiders (11 percent), nation states (nine percent) and hacktivists (six percent).

Last year, respondents were asked what motivations would likely inspire this year's attacks. Fifty percent of last year's survey respondents forecasted that a primary motivation would be financial gain. Taken together, responses regarding threat actors and motivations across the two most recent surveys suggest that financial gain continues as a primary motivator for attackers.

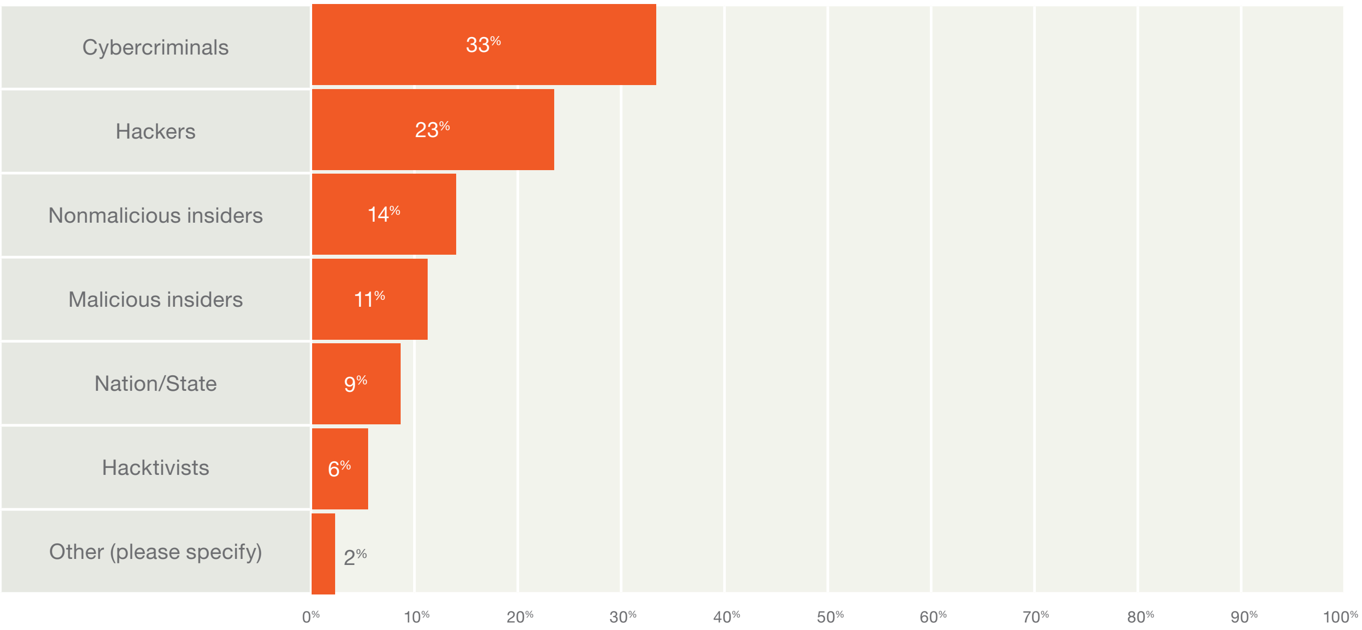
Considering the financial incentive, one might expect ransomware to be a preferred method of attack; the fundamental purpose of ransomware, after all, is to convert a victim's computing resources into financial gain by holding the resources hostage in exchange for payment. One might expect ransomware to proliferate, given all the following reasons:

- Attacks on the whole are increasing
- Malware is a top vector
- Financial gain is the primary motive

If the primary motivation is financial, one would expect an increase in ransomware overall given the increased volume

FIGURE 8—THREAT ACTORS

If your enterprise was exploited during 2017, which of the following threat actors were to blame? Select all that apply.



of attacks; however, this year's results show a drop-off in ransomware. Last year, 62 percent of survey respondents indicated that their enterprises experienced a ransomware attack; this year, the number dropped to 45 percent. This striking decrease appears to contradict the finding that attackers' primary motivation is financial.

One possible explanation for the drop-off is increased preparedness by potential victims. For example, most respondents (86 percent) indicate that their enterprises have a strategy in place to prevent or reduce the odds of occurrence for ransomware. Most (78 percent) also indicate that their enterprises have a formal process to deal with ransomware. Anti-ransomware strategies, such as employee awareness training, are also widely deployed, while 94 percent of enterprises train or advise employees about phishing and/or malware (including ransomware).

These results represent an overall increase in preparedness relative to last year, when only 53 percent of respondent enterprises had a formal process to deal with it. This is perhaps not unexpected given that this change occurred during the same period in which several high-profile ransomware events (WannaCry attack and NotPetya) occurred.

Another potential reason for the decrease in the prevalence of ransomware is victims' resistance to paying ransoms. In this year's survey, almost all respondents (92 percent) indicate that they do not believe that their enterprises will pay the ransom. Most respondents (96 percent) say that their enterprises do not maintain a supply of cryptocurrency for ransomware payments. Thus, increased preparedness (exemplified in defined policy, training/awareness and specific strategies for mitigation), coupled with a low willingness on the part of victims to make payment, undermines the efficacy of ransomware to generate financial return for an attacker.

Implications for Enterprises

From a due-diligence point of view, enterprises that have not yet implemented ransomware preparation measures (e.g., governing policy and awareness training) can be at a disadvantage if an attack occurs. Implementation of ransomware preparedness strategies on a large scale has become industry standard; enterprises that have not implemented the standard may find it challenging to assert that they followed due diligence should a regulator (or any adversely affected party) question why the enterprise failed to implement measures when so many others did.

Therefore, enterprises that have yet to implement these methods may want to rethink the decision and document their decision-making process, including documentation of their risk analysis supporting this decision. There can be valid reasons to choose not to implement specific anti-ransomware controls or processes (for example, if mitigation is included under the umbrella of a broader control or process), but documenting the analysis and decision making ahead of time can position the enterprise to sustain scrutiny after a security event.

Key enterprise takeaways:

- **Ransomware prevention and response measures, although still important and necessary, may drop off somewhat in criticality as ransomware becomes a less-preferred avenue of attack. Over the intermediate-to-long term, this may cause enterprises to deprioritize ransomware preparedness relative to other attack strategies.**
- **Enterprises lacking mechanisms to identify, respond to and mitigate ransomware attacks may be in a weaker position relative to peers because ransomware processes, procedures and tools are industry standard. Enterprises that have not implemented prevention strategies for ransomware may find it increasingly compelling to do so because of the emerging industry consensus.**

Displacement of Ransomware

The decrease in the occurrence of ransomware year over year—although perhaps expected, given the level of preparedness and pervasiveness of controls, procedures and mechanisms to combat it—is nevertheless noteworthy. It not only indicates the effectiveness of organizational preparedness, but also suggests that enterprises should prepare for future changes in the threat environment.

The drop-off in ransomware implies that attackers are shifting to alternate strategies with a better return on attacker investment. If the economics of ransomware indicated that it remains the most efficient path for attackers to convert victims' resources to cash, then ransomware would continue to be the preferred method of attack. Declining ransomware attacks imply that ransomware is not the most effective strategy, and, assuming a constant or increasing number of attacks, it stands to reason that other methods are likely to rise in prevalence, including cryptocurrency mining malware.

Cryptocurrency mining malware is similar in purpose to ransomware (i.e., as a mechanism to generate financial return by compromising a victim's machine). However, instead of attempting to extort a ransom from a victim, cryptocurrency mining malware contributes CPU cycles to a cryptocurrency ecosystem (i.e., mining).

Implications for Enterprises

The difference between ransomware and cryptocurrency mining malware is primarily the payload deployed upon infection, because cryptocurrency mining malware propagate in the same or similar ways to ransomware. Cryptocurrency mining malware have operational advantages over ransomware, provided that cryptocurrency prices stay at a level where mining is sufficiently profitable. This malware can operate without direct access to the filesystem (i.e., fileless malware), are harder to detect, and thus may operate for longer durations without being detected.

As the prices of cryptocurrencies increase, the economics of cryptocurrency mining malware becomes better for the attacker. Likewise, the ability of mining malware to remain undetected and operate for some time prior to detection means a potentially better economic return for the financially motivated adversary. This does not imply that ransomware is likely to go away; a ransomware approach has advantages in situations where time is constrained. For example, an attacker with limited time to complete a campaign can probably more rapidly, although less efficiently, extract value from victims using a ransomware campaign relative to other strategies.

Key enterprise takeaways:

- **Cryptocurrency mining malware may rise in prevalence relative to ransomware attacks in the short-to-intermediate term. Because cryptocurrency mining malware can operate and generate value for an attacker without access to a victim's host filesystem, the method of detection employed by the enterprise may require adjustments.**
- **Enterprises may want to investigate the degree to which existing controls (e.g., antimalware tools and products) operate in a fileless malware context. As ransomware is potentially displaced by other strategies that do not require filesystem access, new controls may need to be deployed or adjustments may need to be made to the operation of existing controls (e.g., enabling behavioral anomaly detection or heuristic-based antimalware scanning).**

Threat Intelligence is Prevalent—Active Defense is Less Familiar but Effective

Many enterprises realize that a solid understanding of the threat landscape correlates directly to better preparedness. For example, an enterprise that understands the motivation, techniques and tactics of an attacker can use that information to inform its understanding of its risk, better tailor its controls, adapt processes, etc.

The number of enterprises that maintain a threat-intelligence capability validates this understanding. Somewhat surprisingly, most enterprises use an in-house capability to accomplish this task. Fifty-eight percent of survey respondents indicate that they use an in-house capability to maintain situational awareness and knowledge of threats, while 37 percent indicate that they use an external provider for this task (**figure 9**).

This year's survey further explores practitioners' familiarity with active defense strategies and their effectiveness when used. Active defense involves the use of defensive techniques to deny resources to an adversary, including, for example, a honeypot or sinkhole that occupies an attacker's time. Active defense requires attackers to invest time in decoys instead of realizing the goal (or goals) of their campaign.

This year's survey asks questions about familiarity with—and implementation of—active defense strategies. Sixty-two percent of respondents are at least moderately familiar with active defense strategies, and 39 percent are not at all familiar or only slightly familiar with active defense strategies (**figure 10**). Although respondents are (as a whole) familiar with active defense strategies, only a slight majority (53 percent) are actually using them (**figure 11**).

The level of efficacy relative to implementation is particularly interesting. Of those who employed active defense strategies, a full 87 percent indicate that they were successful, compared to 13 percent who indicate that they were not successful. The survey results indicate that, although not widely implemented, active defense measures are highly effective.

One may question why the implementation percentage for active defense strategies is not higher. A few barriers to implementation can be responsible for this disparity (**figure 12**). Availability of resources is the biggest barrier cited by survey respondents. Forty-three percent of survey respondents cite skill and/or resource limitations as a primary concern, while 37 percent cite budget as a constraint. Thirty-four percent cite legal implications as a primary concern, and 30 percent cite technical implications.

FIGURE 9—INTELLIGENCE CAPABILITY FOR SECURITY THREATS AND SITUATIONAL AWARENESS

Does your security organization maintain (or contract) an intelligence capability for security threats and situational awareness? If so, is it maintained in-house or acquired through a service, subscription or other external supplier?

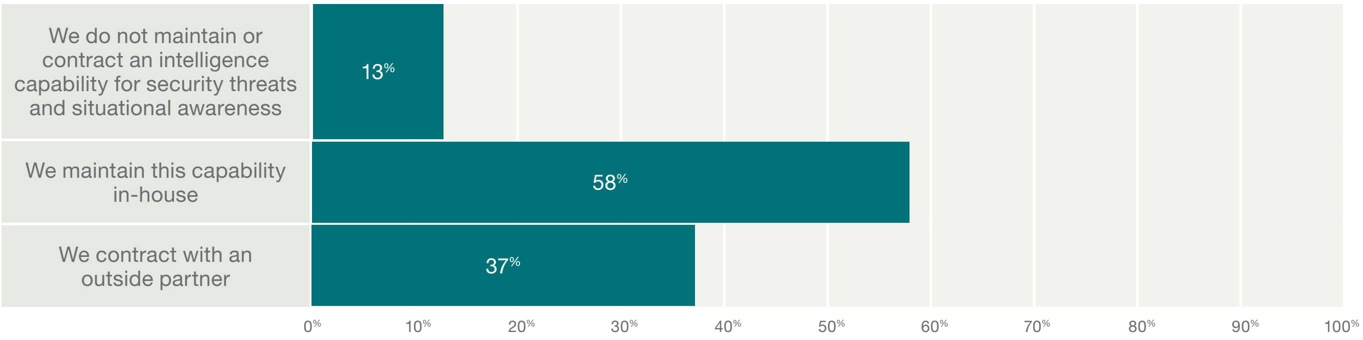


FIGURE 10—FAMILIARITY WITH ACTIVE DEFENSE

How familiar are you with the term “Active Defense” as it pertains to cybercrime prevention by enterprises?

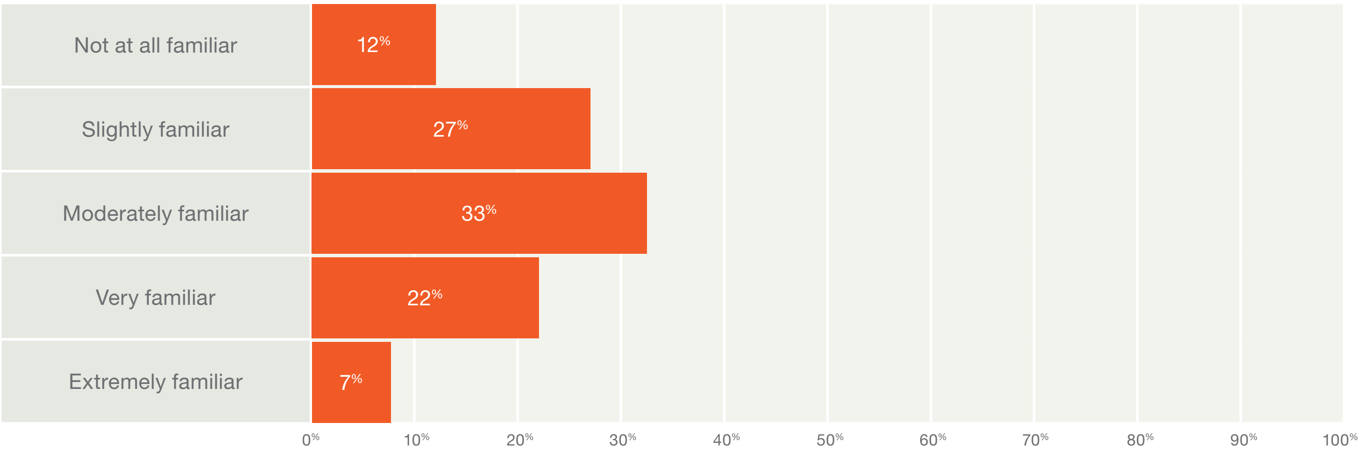


FIGURE 11—EMPLOYING ACTIVE DEFENSE TECHNIQUES

Does your organization employ “Active Defense” techniques?

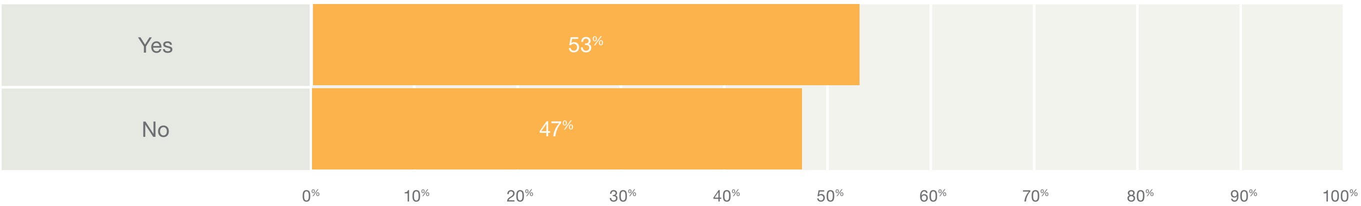
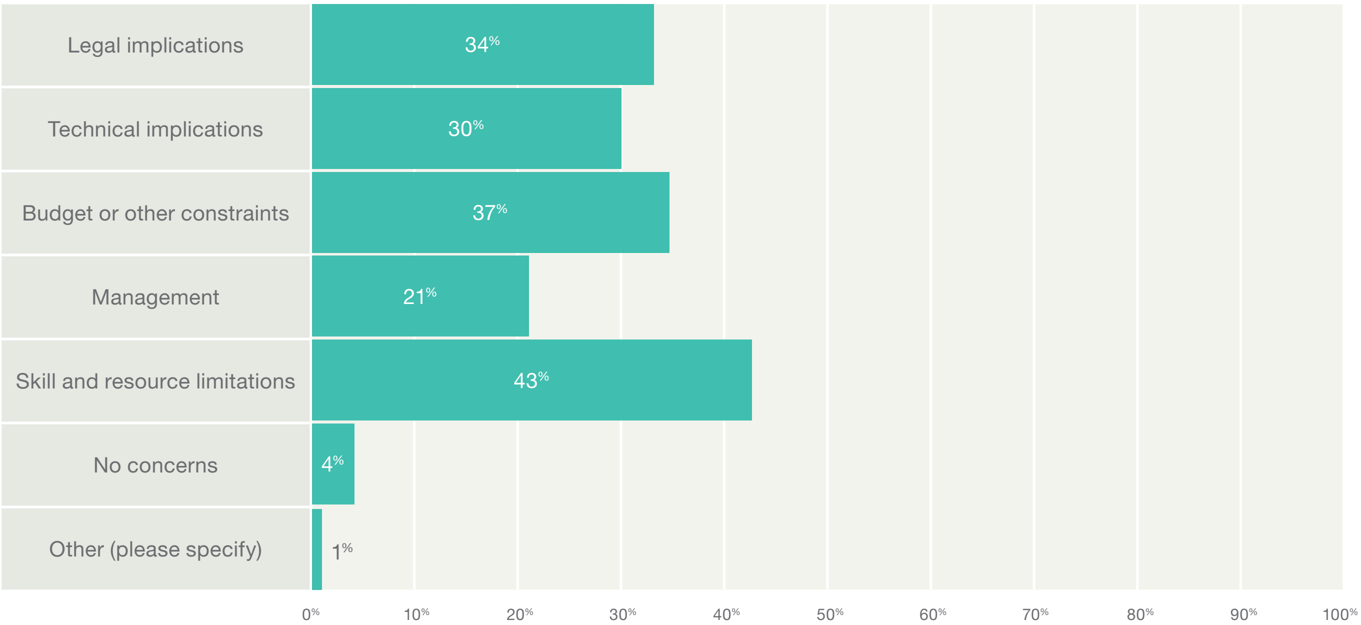


FIGURE 12—PRIMARY CONCERNS WITH ACTIVE DEFENSE

What are your primary concerns, if any, with “Active Defense” techniques? Select all that apply.



Implications for Enterprises

Although these concerns are appropriate and important for enterprises to consider carefully before adopting active defense strategies, the high level of success associated with these controls could indicate a fruitful area for security teams to explore as the threat landscape continues to become more turbulent and as attacks increase. For enterprises that have not implemented active defense strategies, the survey data suggest that now is an opportune time to incorporate the techniques into enterprise risk management as a potential mitigation strategy.

The survey data imply that several capabilities are necessary to implement active defense strategies successfully. First, responses regarding resource constraints suggest that additional skills (particularly technical skills) and additional budget are required to implement the techniques; some level of preparation, skills development and available budget are all required to lay the groundwork for active defense. Responses regarding legal considerations are also important to consider, particularly as some of the tools supporting active defense techniques can be operated in either a lawful or unlawful way (depending on the tool, jurisdiction and method of use). Additional groundwork involving legal counsel (internal or external) may be required in advance of adopting active defense techniques.

Key enterprise takeaways:

- **Active defense strategies, despite a few implementation barriers and concerns, are highly effective when implemented. Enterprises that are unfamiliar with or are unsure about employing these strategies may experience a high level of success upon implementation.**
- **Given the high level of efficacy, security teams may want to investigate strategies to overcome existing obstacles to deployment. For example, teams may focus on obtaining budget and/or skills to implement active defense; practitioners may also investigate possible legal constraints with legal counsel, etc.**
- **At a minimum, security teams may want to educate themselves on active defense strategies: what they are, how they operate and where they could best be deployed in their enterprises.**

Conclusion

As most security practitioners probably already suspect, the ISACA global *State of Cybersecurity Survey* results affirm that attacks are becoming more prevalent, attackers are adapting and evolving the methods they employ, and enterprises are shifting their defense strategies in response. Attacks continue to increase in volume—perhaps even in a targeted way, as some enterprises may be seeing attacks increase at a faster rate than other enterprises.

Attacks continue to be financially motivated and, as such, the economics underlying the mode of attack impact directly the methods employed by attackers in their selection of tradecraft. Attack vectors remain constant, and adaptations align with underlying motivations—not only on behalf of attackers, but also on the part of potential victims. For example, the ubiquity of ransomware defenses, coupled with the general unwillingness of enterprises to pay ransoms, appears to have precipitated a steep decline in ransomware relative to prior years.

Survey responses reveal interesting areas of opportunity within the threat space. For example, active defense strategies, where implemented, tend to be successful. Although some notable barriers exist, the number of respondents reporting success with active defense suggests that it may be worth investing in—and laying the groundwork for—this approach.

Acknowledgments

ISACA would like to recognize:

ISACA Board of Directors

Robert Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CGEIT, CRISC
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Certified Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

Robert E Stroud
ISACA Board Chair, 2014-2015
CRISC, CGEIT
XebiaLabs, Inc., USA

Marios Damianides, Governance Committee Chair
CISA, CISM
Ernst & Young, USA

Matt Loeb
CGEIT, CAE, FASAE
Chief Executive Officer, ISACA, USA

About ISACA

Nearing its 50th year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Technology powers today's world and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of itshalf-million engaged professionals in information and cyber security, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 217 chapters and offices in both the United States and China.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2018: Threat Landscape and Defense Techniques* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Web: www.isaca.org

Provide feedback:
www.isaca.org/state-of-cybersecurity-2018

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkd.in/ISACAOfficial

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/