CYBERSECURITY NEXUS

# State of Cybersecurity 2019

## Part 2: Current Trends in Attacks, Awareness and Governance

## Abstract

*State of Cybersecurity 2019* reports the results of the annual ISACA® global *State of Cybersecurity Survey*, conducted in November 2018. Some findings reinforce discoveries from prior years—specifically, that the top attacks and threat actors remain largely the same. Other findings provide new insight for cybersecurity management: respondents indicate that cybersecurity departments are best served when reporting to either a chief information security officer (CISO) or chief executive officer (CEO), rather than reporting to a chief information officer (CIO). *State of Cybersecurity 2019* captures an outlook on cybersecurity from the perspective of those who define the field—cybersecurity managers and practitioners. This second of two reports focuses on current trends in cybersecurity attack vectors and response methodologies, organizational governance and program management.

# CONTENTS

# Executive Summary

This year's global *State of Cybersecurity Survey* confirms that many practitioners continue to face significant challenges—not only technically, but also organizationally and professionally—in a maturing, dynamic and sometimes turbulent field. In the *State of Cybersecurity 2019* series, ISACA interprets the latest survey results. Part 1 examines professional themes, including workforce hiring trends, retention and diversity. This white paper, the second of two, analyzes current trends in cybersecurity attack vectors, response methodologies, organizational governance and program management. ISACA research endeavors to identify the attacks that are most prevalent and determine which programs and reporting structures combat the prevailing attacks most effectively.

## Key Findings

The threat landscape looks substantially similar year over year: respondents indicate that the most prevalent attacks follow the same vectors as in prior years but anticipate that attack volume will increase in 2019. Enterprises can offset escalating intensity in the threat landscape through better governance and reporting structures that promote confidence in security across the enterprise.

The following are the key survey findings about cybersecurity attacks, awareness and governance:

- **Consistency reigns across threat actors and attack vectors.** Top threat actors and attack vectors remain largely consistent year over year. The top three threat actors include cybercriminals, hackers and nonmalicious insiders. Respondents generally expect attacks to increase quantitatively in 2019; phishing, malware and social engineering continue to top the list of prevalent attack types for a third year.
- **Expansion of attacks may be stabilizing.** While almost half of the respondents indicated that they are experiencing an increase in attacks relative to last year, a slight leveling did occur. When compared to last year, the percentage of respondents indicating that their enterprises are experiencing more attacks decreased by four percentage points, indicating that quantitative expansion of attacks may be easing somewhat. Furthermore, the percentage of respondents who indicate that they are experiencing fewer attacks compared to the prior year is up by one percentage point over last year. Albeit relatively small, this reversal underscores the interpretation that expansion in number of attacks may be leveling off.
- **Cybercrime may be significantly underreported.** Cybercrime is perceived as significantly underreported by survey respondents. Most respondents believe that cybercrime is consistently underreported, despite legal or regulatory requirements obligating enterprises to report such instances.
- **Measuring effectiveness of security awareness programs does not drive confidence in threat mitigation.** An assessment of an anti-phishing program's effectiveness increases the confidence in the program itself, but not in the enterprise's capability to combat cybersecurity threats.
- **Governance dictates confidence level.** Respondents indicate greatest confidence in a cybersecurity team's capability to detect attacks and respond effectively when the cybersecurity teams report to the chief information security officer (CISO). Of the top three reporting structures, the chief information officer (CIO) inspires the least confidence.

# Survey Methodology

In the final quarter of 2018, ISACA sent survey invitations 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. The survey data were collected anonymously via Survey Monkey®. A total of 1,576 respondents completed the survey, and their responses are included in the results.[1]

The survey, which used multiple-choice and Likert scale formats, was organized into six major sections:

- Hiring and Skills
- Diversity in Cybersecurity
- Cybersecurity Budgets
- Cyberattacks and Threats
- Cyberawareness Training Programs
- Organizational Cybersecurity and Governance

Due to the nature of the survey, the targeted population consisted of individuals who have cybersecurity job responsibilities. Of the 1,576 respondents, 1,020 indicated that their primary professional area of responsibility is cybersecurity. **Figure 1** shows additional survey-respondent demographic norms.

While acknowledging norms across the sample population, it is important to note its diversity as well. Among those surveyed, respondents hailed from over 17 different industries (**figure 2**).

# Consistency Reigns Across Threat Actors and Attack Vectors

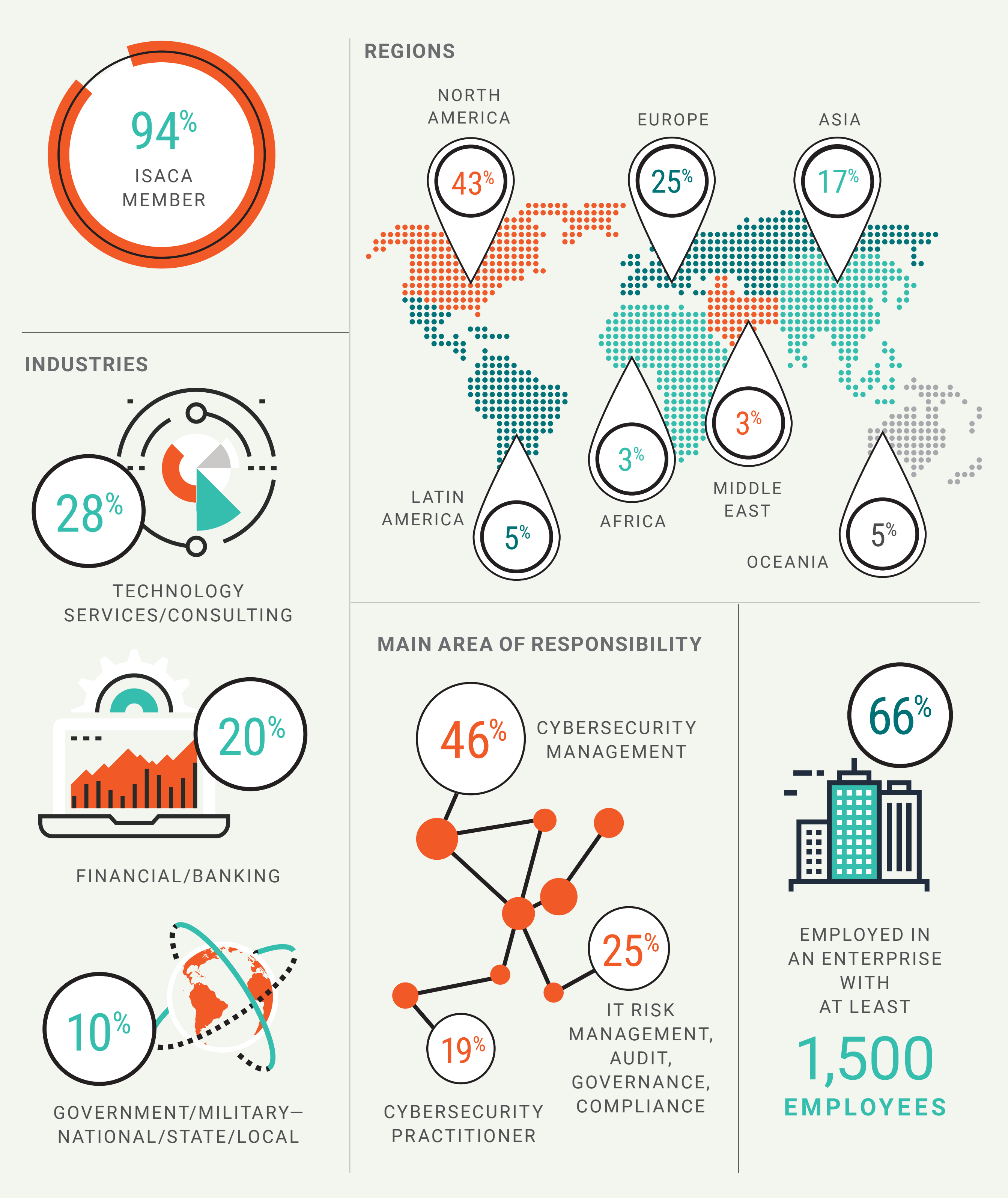
Regarding cybersecurity incidents and attacks, respondent data yield potentially encouraging, yet cautionary, insights. Overall, prevalent types of attack and threat actors remain the same for a third year running. However, additional data collected relating to cybercrime reporting shows a somewhat concerning portrait of a professional field that does not trust itself to report cybersecurity incidents to the authorities, even if a legal or regulatory statute exists that requires an enterprise to report such incidents. Although cyberattacks appear to be stabilizing in terms of emerging vectors and threat actors, underreporting of cybercrime is widely perceived to be the norm.

Top cybersecurity threat actors and their weapons of choice are almost identical to those reported in last year's results. Specifically, the top three identified threat actors this year include:

- **Cybercriminals**—32 percent (33 percent prior year)
- **Hackers**—23 percent (23 percent prior year)
- **Nonmalicious insiders**—15 percent (14 percent prior year)

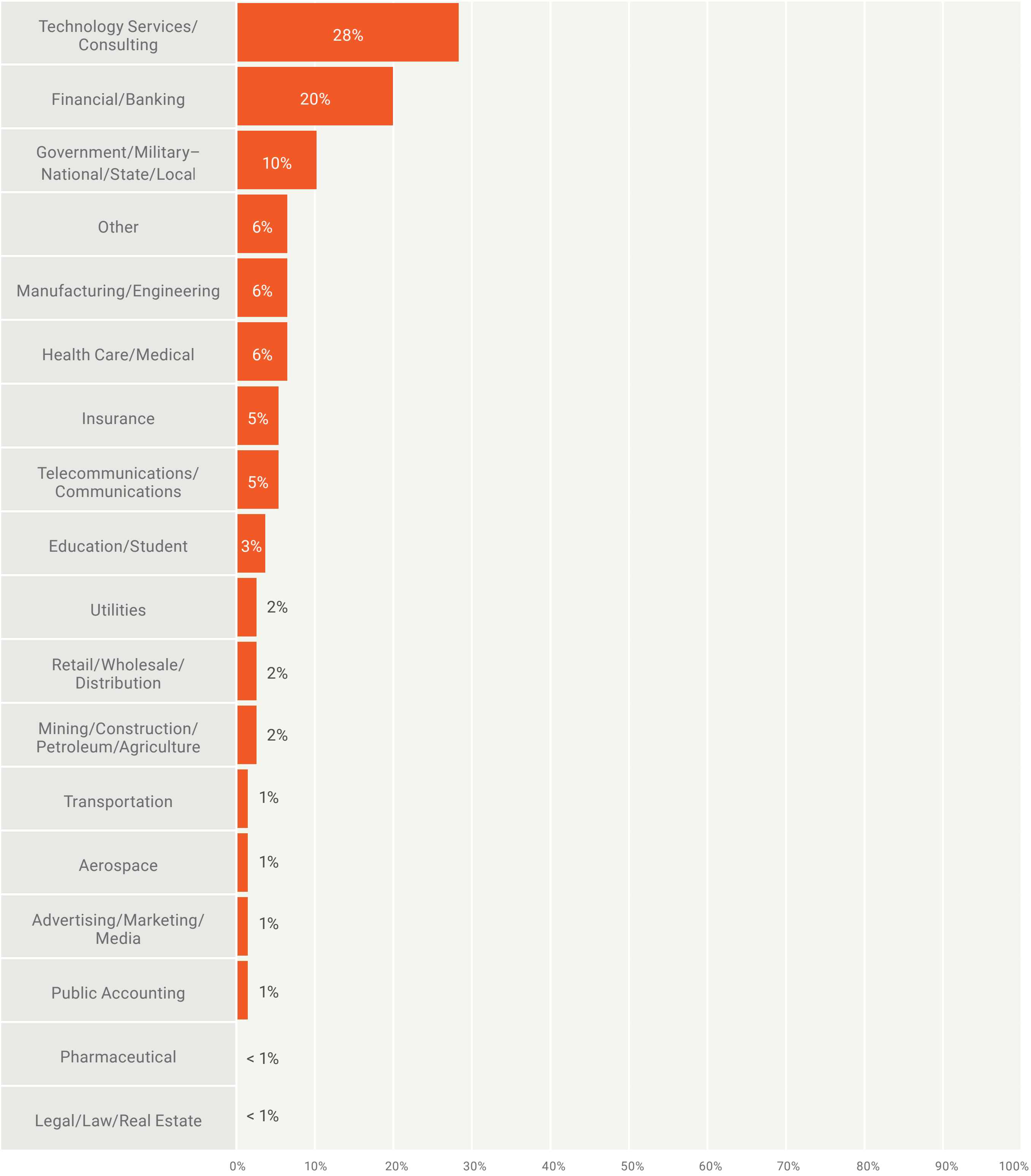
[1] Survey data were collected anonymously online. Certain questions included the option to choose "Don't know" from the list of answers. Where appropriate, "Don't know" responses were removed from the calculation of findings. Result percentages are rounded to the nearest integer.

## FIGURE 1—RESPONDENT DEMOGRAPHICS



## FIGURE 2—INDUSTRY SECTORS

In which industry are you employed?

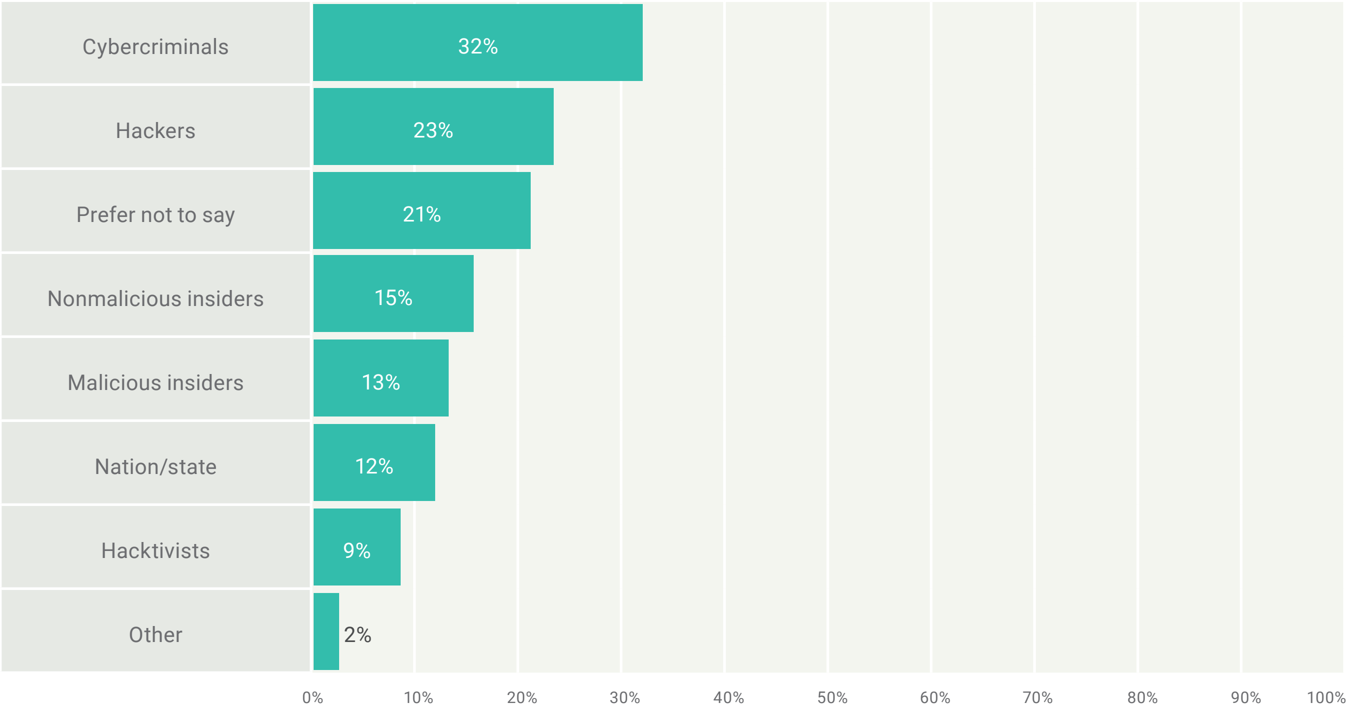


However, this year, many respondents choose to keep the identity of an attacker anonymous, with 21 percent indicating that they preferred not to disclose the identity of the attackers (**figure 3**).[2]

Phishing, malware and social engineering top the list of common attack types, just as they did in the prior two years (**figure 4**).

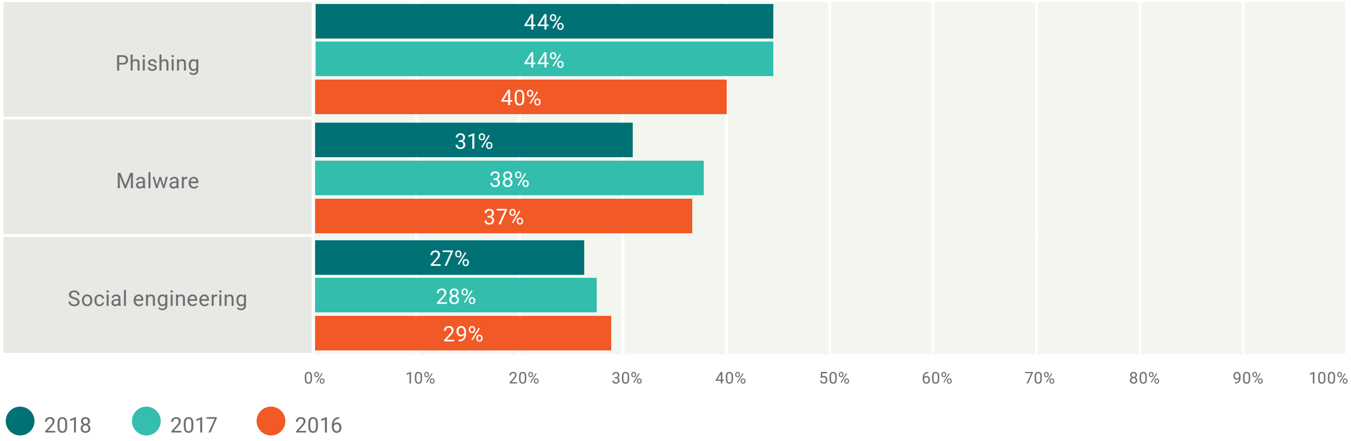
## FIGURE 3—THREAT ACTORS

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



## FIGURE 4—COMPARISON OF CURRENT ATTACK TYPES TO PRIOR YEARS

Select all that apply.



[2] The "prefer not to say" selection was not an option for this question in prior-year surveys.

- **Phishing** remains the most prevalent (reported by 44 percent of respondents)
- **Malware** is a distant second (reported by 31 percent of respondents)
- **Social engineering** is the third most-common attack type (reported by 27 percent of respondents)

The percentage of respondents reporting phishing attacks remains consistent with last year's result (also 44 percent), but those respondents reporting malware attacks decreases seven percentage points this year, and those respondents reporting social engineering attacks decreases one percentage point. However, taken overall, these changes are largely negligible.

Considering the relatively unchanged nature of prevalent cyberattackers and exploitation tools that they use year over year, a trend emerges that helps to establish a profile of personas and their associated capabilities. These personas can aid incident responders' consideration of potential exploitation scenarios. Based on the data from the last three years, if an attack occurs against a system of responsibility, an incident responder can reasonably assume that a higher-than-average probability exists that the incident is due to either a phishing exploitation, a malware implementation or social engineering. Additionally, the responder can assume that a higher-than-average probability exists that the incident is the result of actions undertaken by either a cybercriminal, a hacker, or a nonmalicious insider within the organization.

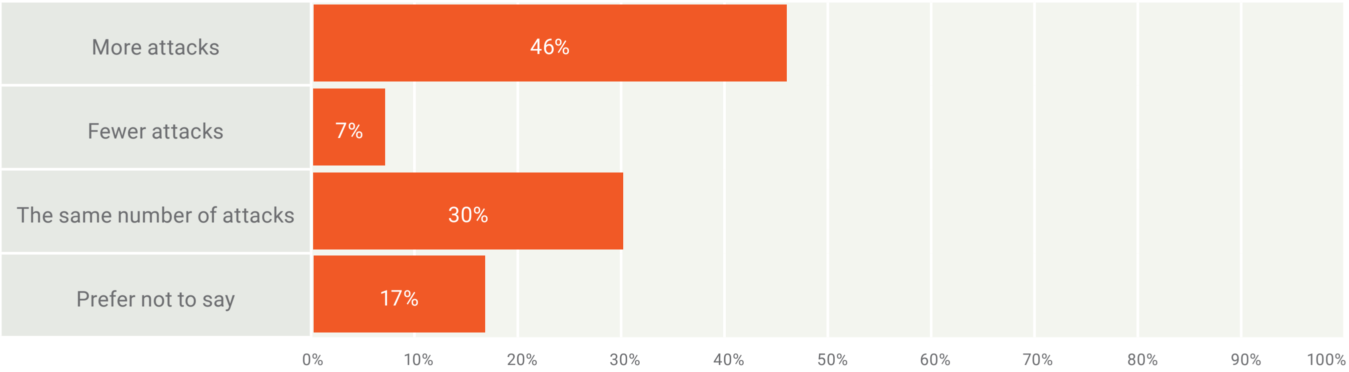
# Expansion of Attacks May Be Stabilizing

For the latest survey year, 46 percent of respondents indicate that their enterprises are experiencing an increase in attacks relative to last year; however, when compared to last year's results, a slight leveling did occur (**figure 5**). Year over year, the percentage of respondents indicating that they experienced more attacks decreased by four percentage points (46 percent this year vs. 50 percent the prior year). Additionally, results indicate a one-percentage-point increase in the percentage of respondents reporting fewer attacks over the prior year (seven percent this year vs. six percent the prior year). Although these findings should not justify any enterprise's reduction in cyberdefense, the results provide a bit of encouragement for those actively battling attackers.

In 2018, a smaller percentage of responding cybersecurity professionals reported that their

**FIGURE 5—CHANGE IN NUMBER OF CYBERSECURITY ATTACKS**

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



enterprises are very likely to experience an attack in 2019 (**figure 6**): the percentage is down, from 42 percent last year to 34 percent this year, representing an eight-percentage-point decrease. Likewise, a smaller percentage of respondents believed that an attack was likely, down from 38 percent to 26 percent, year over year, representing a 12-percentage-point decrease.

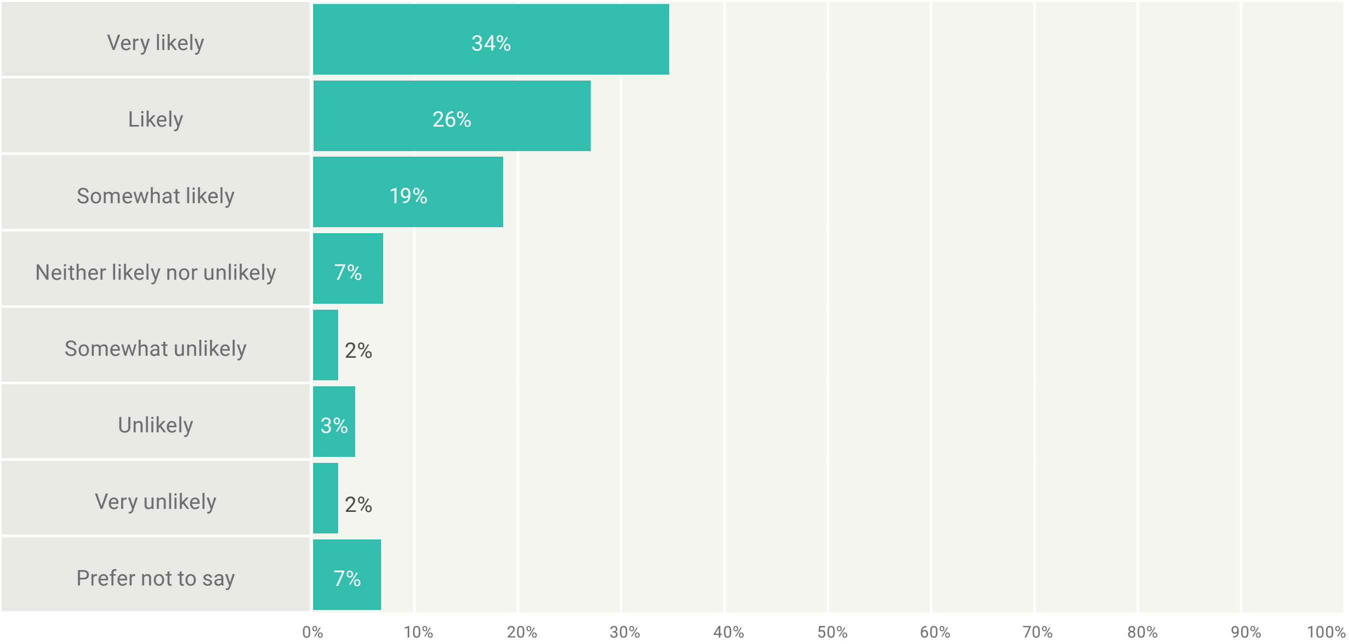
These results may indicate a stabilizing trend in attack volume; however, it is critically important that respondents' current-year perceptions in 2018 and expectations for 2019 do not lead enterprises to conclude that the threat of cyberattacks is diminishing. Overall, 46 percent of 2018 respondents indicate that they experienced more attacks year over year; and likewise, 60 percent of respondents indicate that it is either likely (26 percent) or very likely (34 percent) that their enterprises will experience a cyberattack in 2019.

## Intraorganizational Intelligence Provides Moderate Levels of Confidence

When considering the potential stabilization of cyberattack volume on enterprises, it is important to consider the mechanisms and capabilities that may compromise organizational threat intelligence and response. Survey results indicate that cybersecurity intelligence capability

### FIGURE 6—LIKELIHOOD OF CYBERATTACK IN 2019

How likely is it that your enterprise will experience a cyberattack next year?

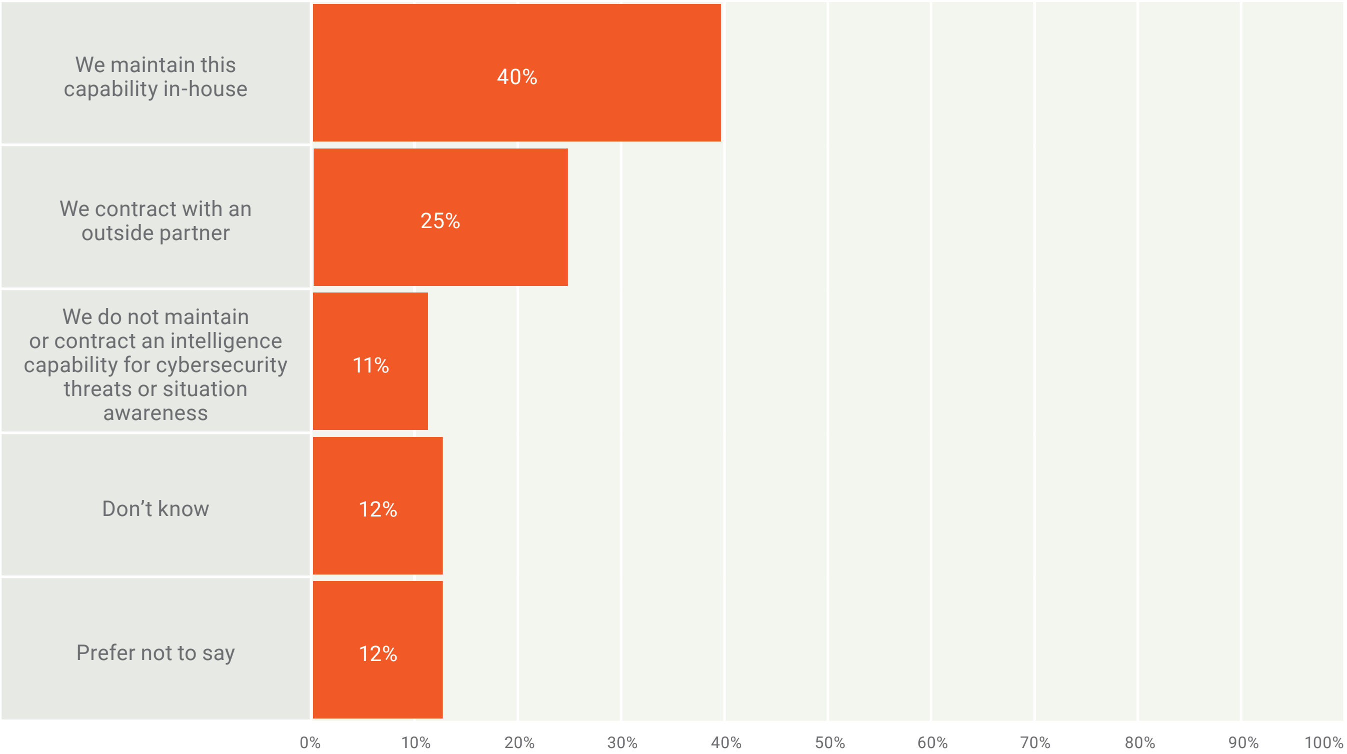


"In spite of the fact that the number of breaches has stabilized, the severity and impact of those breaches has increased immensely. Cybersecurity can suffer from a siloed and static approach. Most teams are missing the attacks that significantly impact organizations because they do not have the size or expertise to keep up with the attackers and their existing security tools and processes are segregated and seldom work in tandem, leaving the teams staring at multiple consoles and drowning in alerts and incidents."

**RENJU VARGHESE**, FELLOW & CHIEF ARCHITECT, CYBERSECURITY & GRC, HCL TECHNOLOGIES

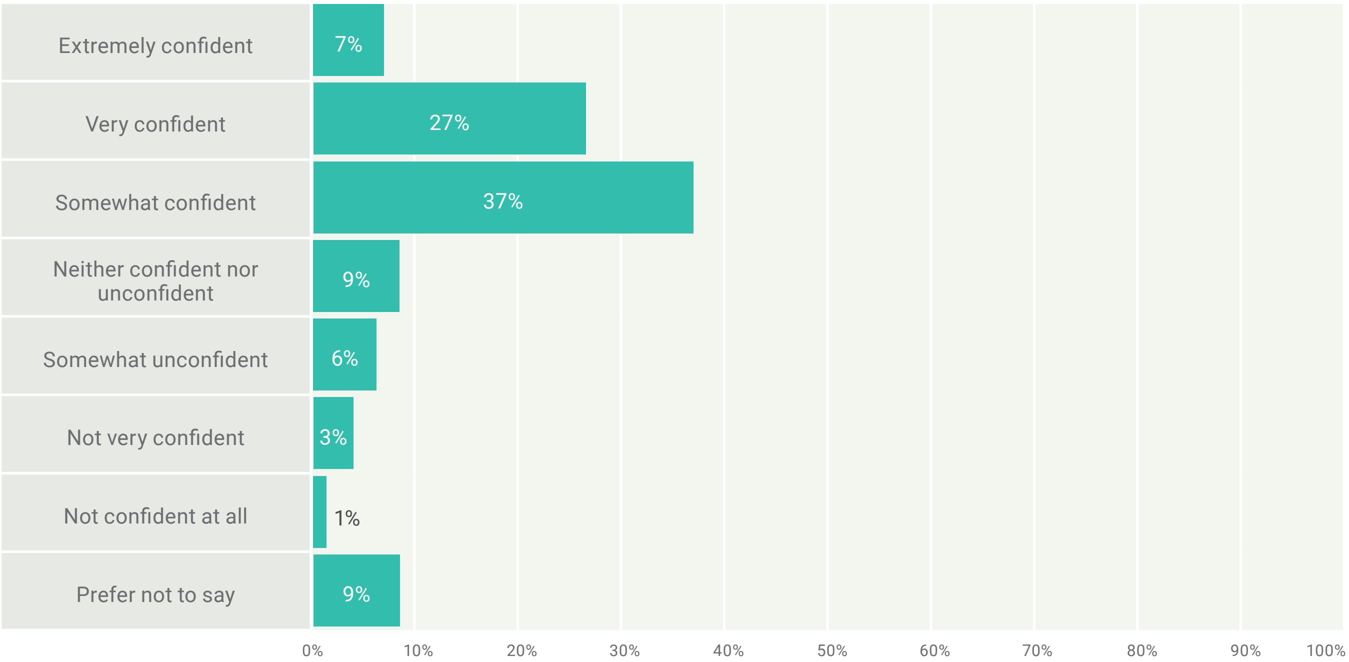
## FIGURE 7—INTELLIGENCE CAPABILITY FOR SECURITY THREATS AND SITUATIONAL AWARENESS

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



## FIGURE 8—CONFIDENCE IN CYBERTEAMS

How confident are you in your enterprise's cybersecurity team's ability to detect and respond to cyberthreats?



is most commonly maintained in-house: 40 percent of respondents indicate that their capability is internal to the enterprise (**figure 7**). Over 70 percent of respondents indicate that they feel at least somewhat confident in their enterprise cybersecurity team's ability to detect and respond to cyberthreats (**figure 8**).

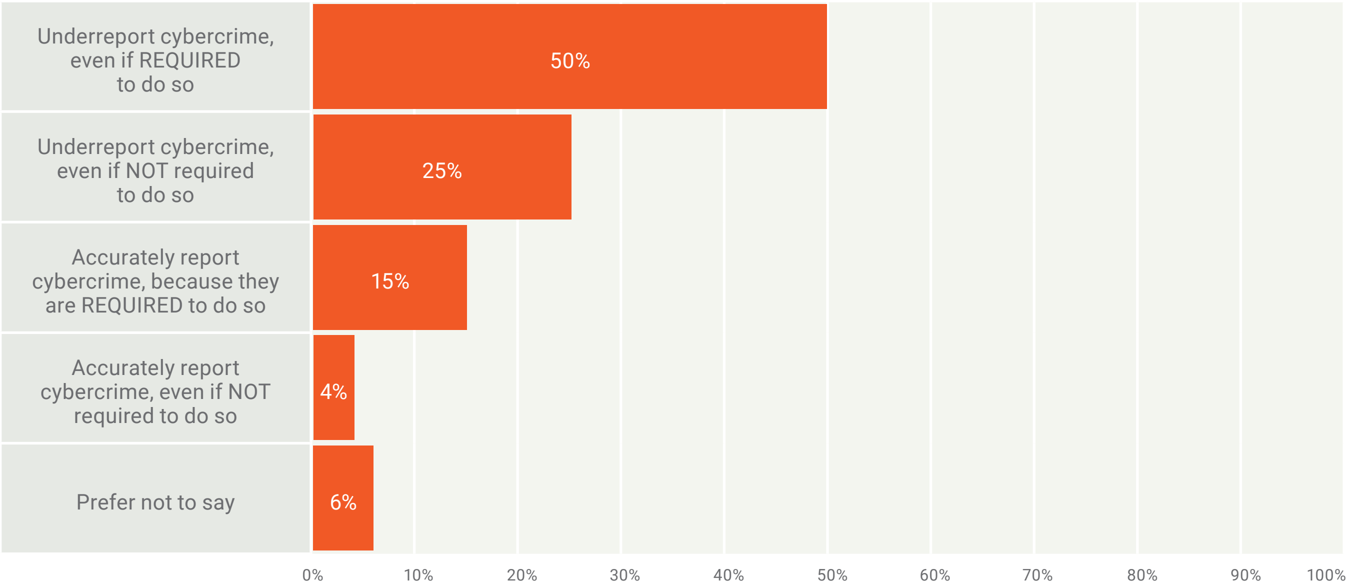
# Cybercrime May Be Significantly Underreported

Although the survey responses shown previously in **figure 7** and **figure 8** appear encouraging when taken at face value, other data points suggest potential cracks in the veneer of confidence. The majority of respondents (75 percent) indicate their belief that the actual instances of cybercrime are intentionally suppressed. If this level of underreporting does in fact reflect reality—acknowledging that the survey asks respondents to reflect on their *belief* in this regard—many cybercrime statistics presented by governments and businesses would have to be treated skeptically by comparison. Indeed, 50 percent of respondents believe that most cybercrime is underreported, even if enterprises *are legally required to report incidents* (**figure 9**).

Grappling with the true impact of cyberattacks and cybercrime proves a slippery wrestle. Even in light of a (potentially) stabilizing trend in attack volume and relative confidence in enterprise threat response capabilities, respondents share an apparent cynicism regarding cybercrime and reporting. The high percentage of respondent skepticism regarding cybercrime reporting substantially may offset the optimism indicated by any leveling of cybersecurity attack volume and consistency of threat actors and exploitation techniques. Enterprises need to consider that many cybercrime incidents may go unreported—despite legal and regulatory requirements to report—and address any propensity to not report these incidents.

**FIGURE 9—ENTERPRISE REPORTING OF CYBERCRIME**

Do you believe that when it comes to reporting cybercrime, most enterprises...



# Measuring Effectiveness of Security Awareness Programs Does not Drive Confidence in Threat Mitigation

While the number of cyberattacks may have slightly leveled off, malware, social engineering and phishing continue to be the primary vectors of compromise year over year. Analysis of this survey result may lead some cybersecurity professionals to question whether cybersecurity awareness is sufficient within their enterprises. This year's survey yields interesting discoveries regarding the implementation and management of cybersecurity awareness programs. Not surprisingly, most enterprises promote awareness through internal training programs, without external input, and report cybersecurity information and awareness data to executives through the chief information security officer (CISO) or chief information officer (CIO).

## Internal Efforts Predominate in Cybersecurity Awareness

One of the most common methods of raising cybersecurity awareness within an enterprise is awareness training. Given that phishing remains the number one vulnerability exploited by miscreants, understanding the scope of anti-phishing training within an enterprise proves to be a helpful and revealing datapoint.[3] Most respondents indicate that their enterprises use more than one mechanism to combat phishing, including employee training programs, online training programs, email newsletters, phishing simulations or some combination of the four, to combat phishing threats (**figure 10**).

While application of cybersecurity awareness programs is important, measuring the effectiveness of awareness programs is also key to building organizational resilience. Therefore, enterprises want to know whether their application of protective mechanisms are effective.[4] Because phishing attacks continue to be the primary method through which attackers gain access, the ISACA survey asked respondents to report levels of confidence in their enterprises' ability to assess effectiveness of phishing awareness programs. More often than not, respondents report confidence in their enterprise's ability to assess the program effectiveness accurately; 39 percent of respondents indicate that they are at least somewhat confident in their enterprise's assessment abilities, and 45 percent of respondents indicate that they are very confident or completely confident (**figure 11**).

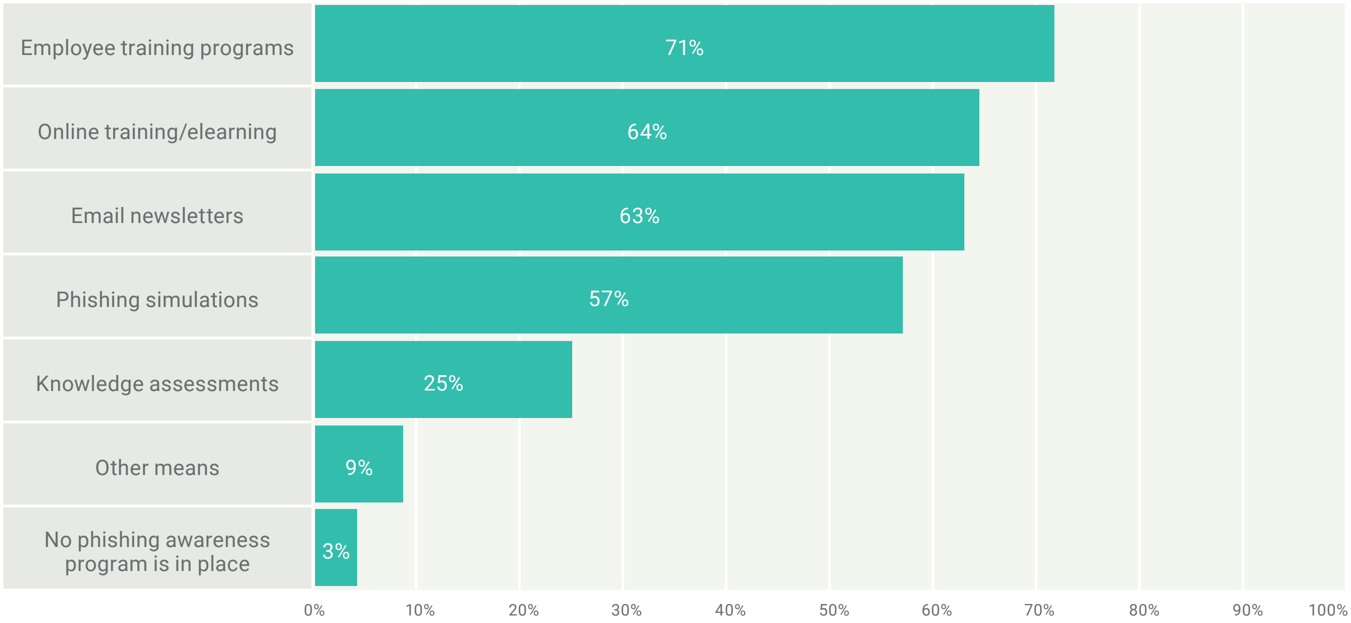
The confidence level increases substantially for respondents who indicate that their enterprises measure and regularly report the effectiveness of phishing awareness programs: 58 percent of respondents whose enterprises regularly report the effectiveness of phishing awareness programs indicate that they feel very confident or completely confident in program effectiveness—a 13-percentage-point increase over those respondents whose enterprises do not regularly measure the effectiveness. Although regular assessment and reporting of phishing awareness programs increases confidence in their effectiveness, it does not affect perceptions of cybersecurity team response capabilities: curiously, assessment of a cybersecurity awareness program's

[3] See also ISACA, *Phishing Defense and Governance: How to Improve User Awareness, Enhance Controls and Build Process Maturity*, USA, 2019, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Phishing-Defense-And-Governance.aspx.

[4] See also ISACA, *Improving Security Awareness Using Marketing Techniques*, USA, 2019, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/improving-security-awareness-using-marketing-techniques.aspx.

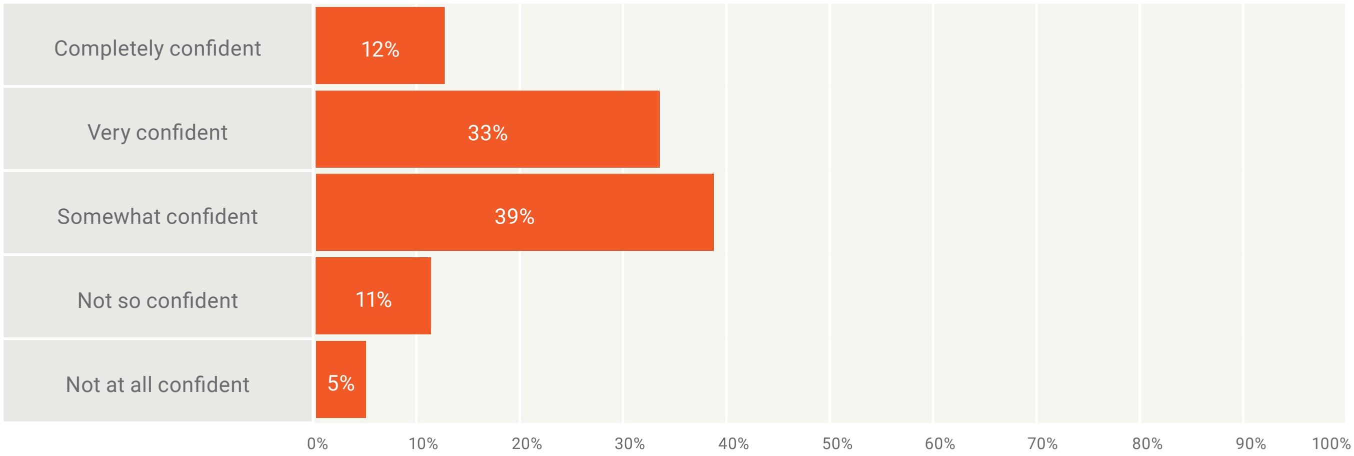
### FIGURE 10—METHODS USED TO PROMOTE PHISHING AWARENESS

Which, if any, of the following are used by your enterprise to promote phishing awareness and mitigate phishing threats? Select all that apply.



### FIGURE 11—ACCURATELY ASSESSING THE EFFECTIVENESS OF PHISHING AWARENESS PROGRAMS

How confident are you in your enterprise's ability to accurately assess the effectiveness of your phishing awareness program?



effectiveness increases confidence in the awareness program itself, but not in the cybersecurity organization's designated capability to combat cybersecurity threats.

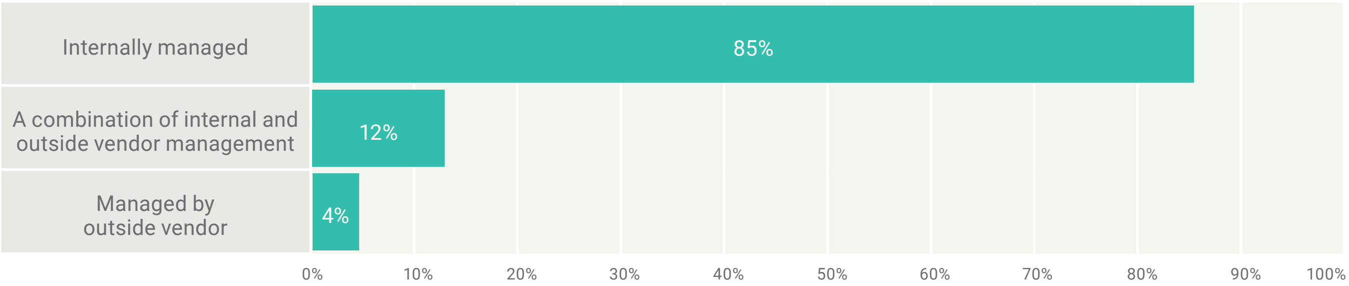
## Vendor Awareness Programs vs. Home-Grown Programs

Security awareness program development is critical to effective implementation. Like firewalls and other security tools, awareness programs can harm more than help if they are poorly developed, improperly configured or badly implemented. Therefore, understanding how awareness programs are developed and managed is paramount to effective implementation. When asked who developed the security awareness programs currently in place within their enterprises, respondents are split between in-house programs (38 percent) and a combination of in-house and vendor-developed programs (also 38 percent); a minority of respondents indicate development solely by an outside vendor (25 percent). No matter the origin of development, however, the vast majority of security awareness programs currently in place are managed by internal personnel: 85 percent of respondents indicate that their security awareness programs are internally managed (**figure 12**).

Interestingly, enterprises that manage their cybersecurity awareness programs internally are also more likely to manage their cybersecurity intelligence programs internally and are more confident in their cybersecurity team's ability to detect and respond to cyberthreats.

FIGURE 12—SECURITY AWARENESS PROGRAM MANAGEMENT

Who manages the security awareness program for your enterprise today?



# Governance Dictates Confidence Level

Discussions in cybersecurity today often revolve around the particular reporting structure of the cybersecurity organization within an enterprise. Most cybersecurity organizations ultimately report to the chief-officer level—which can include a range of possible officers (**figure 13**). The top three executives to whom cybersecurity organizations reports include the CISO (43 percent of respondents), the CIO (27 percent) and the CEO (13 percent). These organizational structures are consistent with those reported last year, except for a slight increase in reporting to the CEO, which rose one percentage point.

Survey results suggest that the particular executive to whom cybersecurity reports can affect perceived confidence in the team's ability to detect and respond to cyberthreats. Despite superficial uniformity, year over year, regarding reporting structure, this year's survey results clearly establish that enterprises in which the cybersecurity team reports to the CISO have the highest level of respondent confidence in the team's ability to detect and respond to threats:

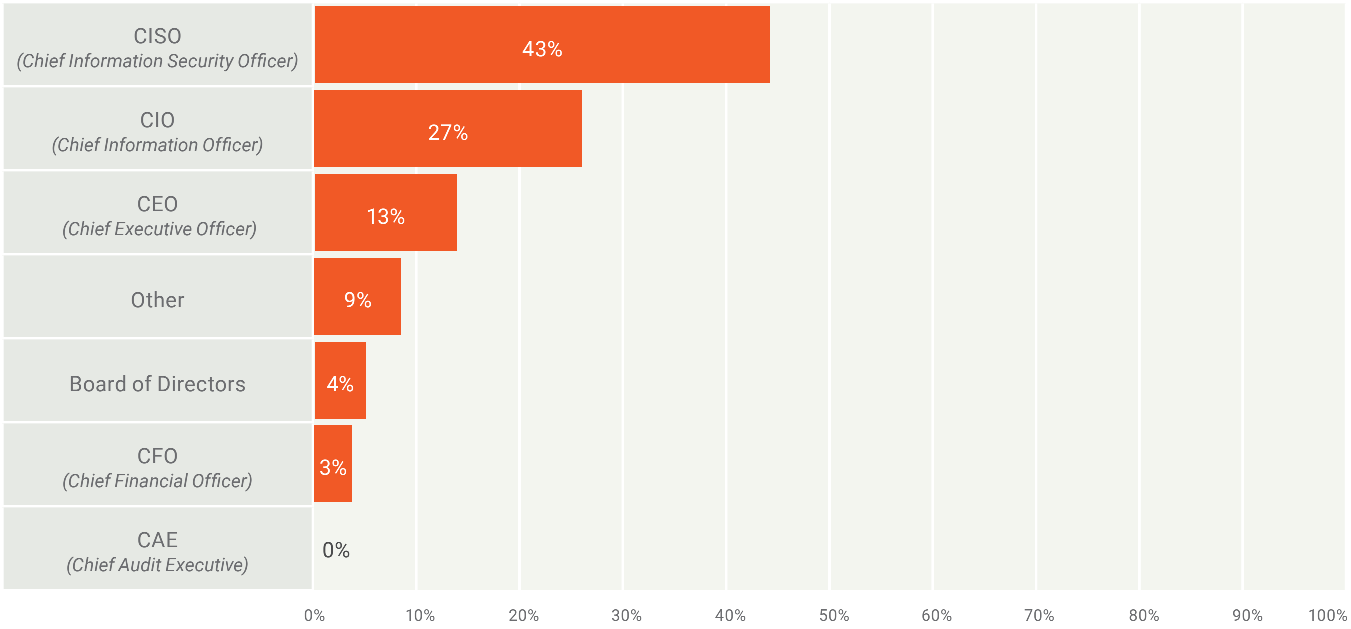
- **CISO reporting path**—Seventy-nine percent of respondents in enterprises whose cybersecurity team reports to the CISO indicate that they are at least somewhat confident in their cybersecurity team's abilities to detect and respond to threats.
- **CEO reporting path**—Seventy-four percent of respondents in enterprises whose cybersecurity team reports to the CEO indicate that they are at least somewhat confident in the cybersecurity team's threat detection and mitigation abilities, even though only 13 percent of survey respondents report to the CEO.
- **CIO reporting path**—Sixty-eight percent of respondents in enterprises whose cybersecurity team reports to the CIO indicate that they are at least somewhat confident in their cybersecurity team's abilities to detect and respond to threats.

Analysis of this data provides powerful insight to the current debate about IT governance of cybersecurity. According to the data, there is an 11-percentage-point differentiation in confidence levels of cybersecurity teams—with those reporting to a CISO garnering a higher confidence level than those reporting to a CIO. Yet, over a quarter of enterprises structure themselves so that cybersecurity teams report to the CIO.

The data seem to corroborate—even, perhaps, to quantify—the confusion that many enterprises experience when they structure cybersecurity with information technology. Although these fields are adjacent, they are not synonymous. Managing and implementing information technology is substantially different than securing and protecting it. A CIO's main goal is enabling information flow, and, in this reporting structure, cybersecurity may fall to a secondary consideration. This mentality can lead to disaster in the long term and—per analysis of the data—leads to lack of confidence in an enterprise's cyberreadiness in the short-to-medium term. In fact, a higher percentage of respondents are confident in cybersecurity reporting to the CEO than to the CIO.

## FIGURE 13—ORGANIZATIONAL REPORTING STRUCTURE FOR CYBERSECURITY

To whom does cybersecurity report in your enterprise?



# Conclusion: Stabilization and Consolidation

ISACA survey results show that in terms of threats and threat actors, 2018 was a year of stabilization and reflection for threats and threat actors. Analysis of attack trends shows very similar results when compared to prior years. For example, threat actors and attack vectors have remained largely the same. However, cause for celebration is far from given as faith in cyberattack reporting appears concerningly low. Additionally, like prior years, attack frequency is expected to increase. *State of Cybersecurity 2019, Part 1*, published earlier this year, highlighted the difficulty of hiring qualified cybersecurity professionals. Considering the state of the workforce relative to the current threat landscape in which they operate, as denoted in this Part 2 report, enterprises should continue to exercise caution, to optimize cybersecurity intelligence, maintain workforce readiness and ensure operational responsiveness.

Executives may consider examining cybersecurity program implementation and management in terms of governance structure, given that confidence in cybersecurity teams' abilities to detect and respond to attacks is clearly tied to their reporting structure, with the CISO instilling the most confidence. Additionally, in-house management of a cybersecurity awareness program may prove more effective than external management. Finally, regardless of management, all programs should be assessed to determine (and maintain) their effectiveness and efficiency.

# Acknowledgments

ISACA would like to recognize:

## Lead Developer

**T. Frank Downs**
CEH, CEI, ECSA, LPT
ISACA, USA

## Expert Reviewers

**Dustin Brewer**
CSXP, CEH, CHFI, CSIS
ISACA, USA

**Marie Gilbert**
ISACA, USA

**Karen Heslop, J.D.**
ISACA, USA

## ISACA Board of Directors

**Rob 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, CRISC, COBIT 5 Foundation, GRCP
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 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

**David Samuelson**
Chief Executive Officer, ISACA, USA

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

## About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, 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 220 chapters worldwide and offices in both the United States and China.

## About HCL

HCL Technologies (HCL) is a leading global technology company that helps global enterprises reimagine and transform their businesses through digital technology. HCL operates in 44 countries and had consolidated revenues of US $8.4 billion for the 12 months ending 31 December 2018. HCL provides an integrated portfolio of services informed by its Mode 1-2-3 growth strategy. Mode 1 encompasses core services in the areas of applications, infrastructure, business processes outsourcing (BPO) and engineering, research and development services, leveraging DRYiCE™ Autonomics to transform clients' business and IT landscape, making them lean and agile. Mode 2 focuses on experience-centric, outcome-oriented, integrated offerings of Digital and Analytics, IoT WoRKS™, Cloud Native Services, and Cybersecurity and GRC services to drive business outcomes and enable enterprise digitization. Mode 3 strategy is ecosystem-driven, creating innovative IP-partnerships to build product and platform business. HCL leverages its global network of integrated co-innovation labs to provide holistic multiservice delivery in key industry verticals including financial services, manufacturing, telecommunications, media, publishing, entertainment, retail and consumer packaged goods, life sciences and healthcare, oil and gas, energy and utilities, travel, transportation and logistics, and government. With 132,328 professionals from diverse nationalities, HCL creates real value for customers by taking "Relationships Beyond the Contract." For more information, please visit www.hcltech.com.

## Disclaimer

ISACA has designed and created *State of Cybersecurity 2019, Part 2: Current Trends in Attacks, Awareness and Governance* (the "Work") primarily as an educational resource for IT audit 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, IT audit professionals should apply their own professional judgments to the specific circumstances presented by the 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-2019

**Participate in the ISACA Online Forums:**
https://engage.isaca.org/onlineforums

**Twitter**:
www.twitter.com/ISACANews

**LinkedIn:**
www.linkedin.com/company/isaca

**Facebook:**
www.facebook.com/ISACAHQ

**Instagram:**
www.instagram.com/isacanews

CyberSecurity & GRC Services
*by HCL Technologies*

HCL

# Inspiring business confidence through **Dynamic Cybersecurity**

## Our services portfolio

- Strategy & architecture
- Transformation & Integration
- Managed Security Services

## Solutions domains

- Infrastructure & Cloud security
- Application security
- Governance Risk & Compliance
- Identity & Access Management
- Business Continuity / Disaster Recovery
- Data Security & Privacy
- Security of Things

**21+** Years of Experience | **6** CyberSecurity Fusion Centers | **350+** Client Relationships | **40+** Global Delivery Centers