State of Cybersecurity 2020

Part 2: Threat Landscape and Security Practices

ABSTRACT

State of Cybersecurity 2020 reports the results of the annual ISACA® global *State of Cybersecurity Survey*, conducted in the fourth quarter of 2019. This Part 2 survey report focuses on the threat landscape, the measures security professionals employ to keep their enterprises safe, and key trends and themes in the practice of security. This year's data confirms trends from prior years and considers responses to several new survey questions regarding critical innovations, including AI-enabled security tools. While some findings were anticipated—including an expectation of increased cyberattacks—others provide new insights related to the security impact of organizational structure, staffing and hiring challenges.

CONTENTS

Introduction

To say that the world has changed dramatically in 2020 is not hyperbole. In just a few months, the COVID-19 pandemic transformed the world with stay-at-home orders, travel restrictions, product shortages, social distancing and remote work. Technology has assumed a new importance in the global response to the pandemic. While people are sheltering in place, technology enables communication and collaboration among employees and across enterprises at a time when employees cannot work together physically. In the security field, it was always common to say that business runs on technology—now, the world cannot run without it: Technology is undeniably the *sine qua non* of the global response to pandemic.

Practitioners accountable for keeping enterprises secure are adapting: They are flexible, and innovate quickly, as enterprises acclimate to new ways of doing business, to new challenges and to the unknown. Remote workers, once often the exception, are now the rule—at least for the interim. Constrained by operational challenges (for example, when staff are unavailable due to family care or illness), security efforts can falter. Many IT organizations face increasing budgetary uncertainty. Cybercriminals, exploiting fear and tragedy, develop new strategies to steal and disrupt.

In this environment, data and information are critical, including data about cybersecurity performance—what does and does not work, how and where improvements can be made, and what peers are doing in their enterprises. Insights like these help enterprises understand how their efforts compare to those of other organizations, while information about the threat landscape helps enterprises prepare for future cyberattacks. While some of the immediate challenges resulting from COVID-19 may resolve after the immediate crisis is over, lessons learned and changes in the way business is conducted may last well into the future.

In this environment, data and information are critical, including data about cybersecurity performance—what does and does not work, how and where improvements can be made, and what peers are doing in their enterprises.

This report, Part 2 of ISACA's global *State of Cybersecurity Survey* results, focuses on the threat landscape, the measures security professionals employ to keep their organizations safe, and key trends and themes in the practice of security.

Executive Summary

This report focuses on the threat landscape, reviews security trends and themes, and considers responses to new survey questions in emerging areas—including the application of AI-enabled security tools. Key findings are highlighted below.

- **Attacks are increasing, but leveling continues.** Similar to previous years, attacks continue to increase. However, last year's data suggested a slight downturn, or leveling, in the rate of attacks compared with prior years. This year, that trend continues. While more attacks continue to be observed by a plurality of respondents, that plurality itself is decreasing year over year—thus, the *rate* at which attacks increase continues to decline over time. This finding may indicate that attacks are nearing a saturation point, or may reflect broader shifts in technology adoption.
- **Security functions are scattered within IT operations.** For the first time, ISACA asked about security functions performed by the IT operations team. Responses suggest that IT operations teams perform many diverse security functions. Given the emergence of DevOps and DevSecOps practices in many organizations, cybersecurity team staff shortages, and the increased awareness of the importance of good cyberhygiene across many enterprises, it is not surprising that many security functions, including incident response, and maintaining, updating, or implementing security tools and systems, are performed by IT operations.
- **Cybercrime remains underreported.** Sixty-two percent of professionals believe that enterprises are failing to report cybercrimes, even in situations where they have a legal or contractual obligation to do so. This trend, highlighted in last year's report, continues unabated—professionals still indicate that they believe firms are underreporting cybercrime. Practitioners—particularly those in regulated industries and in jurisdictions where financial or other penalties can result from failure to report—should take particular notice of this finding.
- **Lack of staff and oversight impacts operational performance.** The number of respondents reporting that they are significantly understaffed fell by seven percentage points from last year; however, the vast majority of organizations (62 percent) remain understaffed. While Part 1 of *State of Cybersecurity 2020* highlights the impact of this condition on the job market, this report delves deeper into the related operational consequences. Specifically, challenges in acquiring and retaining staff track directly with an observed decline in security readiness. Understaffed security teams—along with those challenged in acquiring new staff—are significantly more likely to have experienced more cyberattacks. Oversight of the security function and reporting structure also correlate

with security performance (as measured by outcome).

- **AI solutions may increase visibility, though adoption lags.** Organizations that use machine learning and/or artificial intelligence solutions appear to have increased visibility into attacks. Despite this correlation, AI-based strategies have yet to see broad adoption. Although it may be early in the adoption curve, the outlook is promising based on these positive signs.
- **Ransomware returns as a primary post-exploitation monetization strategy.** Ransomware surpasses cryptocurrency mining as the primary monetization strategy post-exploitation. This change likely reflects a combination of factors, including cryptocurrency prices, fileless malware and living-off-the-land (LotL) strategies,[1] and increasing use of cloud resources. For practitioners, this finding can influence preparedness strategies, and it is a useful data point for determining how to prioritize detection techniques.

Survey Methodology

In the final quarter of 2019, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold ISACA's Certified Information Security Manager® (CISM®) certification or have information security job titles. Survey data were collected anonymously via SurveyMonkey®. A total of 2,051 respondents completed the survey, and their responses are included in the results.[2]

The survey presented respondents with multiple-choice and Likert scale-format questions organized into six major sections:

- Hiring and skills
- Diversity
- Security operations
- Cybersecurity budgets
- Cyberattacks and threats
- Organizational cybersecurity and governance

The survey's target population consists of individuals who have cybersecurity job responsibilities. Of the 2,051 respondents, 913 indicate that their primary professional area of responsibility is cybersecurity. **Figure 1** captures key demographic norms across a diverse set of survey respondents.

Respondents represent over 17 industries and hail from 102 countries (**figure 2**).

[1] Living-off-the-Land (LotL) techniques use what already exists in an environment to exploit points of entry in IT systems. See Schwartz, S.A.; "Why 'living off the land' has become a preferred method of cybercrime," 20 February 2019, https://www.ciodive.com/news/why-living-off-the-land-has-become-a-preferred-method-of-cybercrime/548767/.

[2] 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

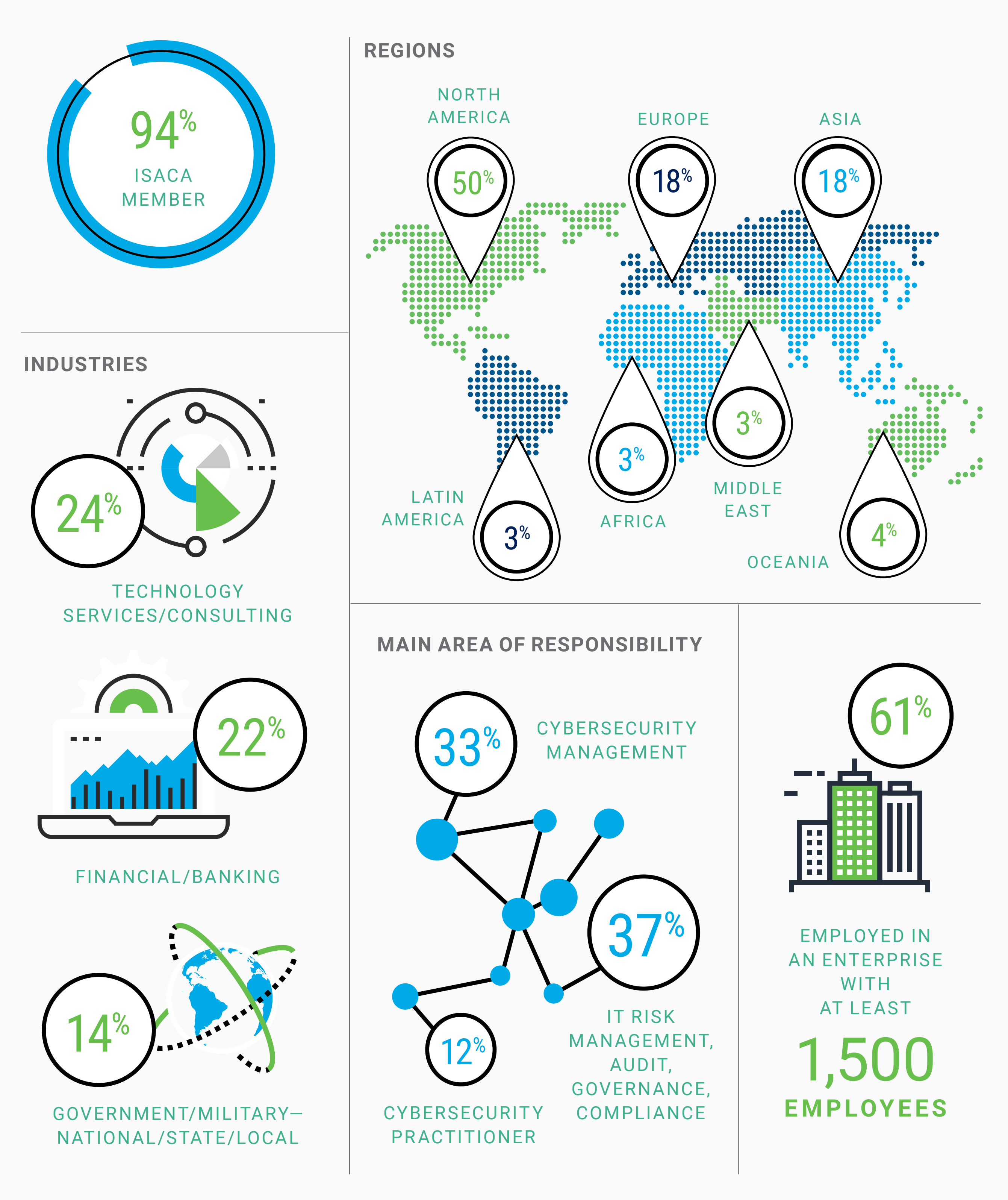
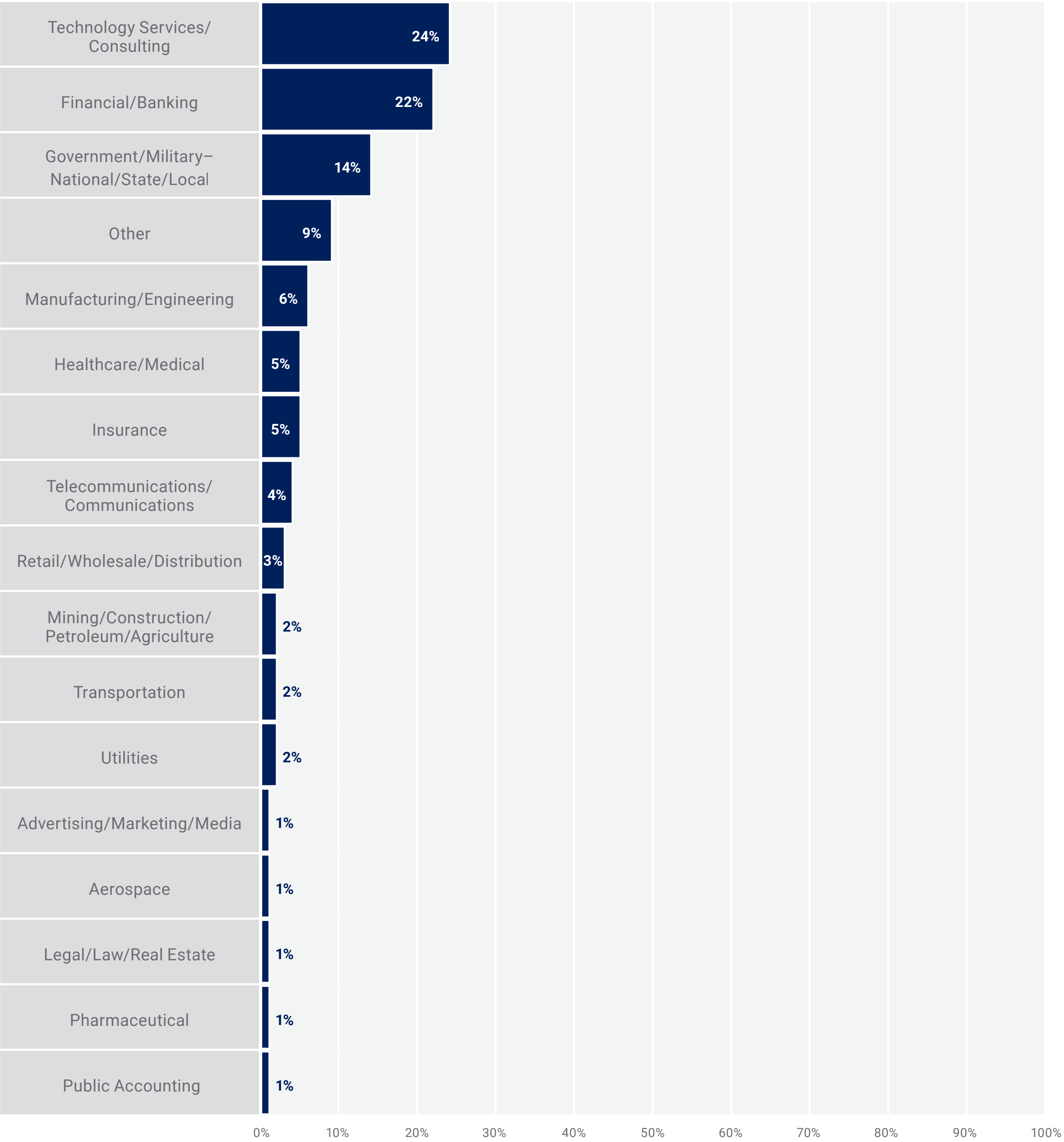


FIGURE 2—INDUSTRY SECTORS

Indicate your organization's primary industry.



Attacks Are Increasing, but Leveling Continues

As in previous years, attacks are increasing. Thirty-two percent of respondents report an increase in the number of attacks relative to a year ago. Twenty-four percent of respondents cite the same number of attacks, while six percent cite a decrease in attacks (**figure 3**).

Compared with last year, there is perhaps some good news buried in this otherwise dismal data point. Specifically, in the previous year's data, just over 39 percent[3] of respondents indicated that they had observed more attacks than the prior year (a plurality of respondents, itself down from prior years). Last year's report hypothesized that the rate of attacks is leveling off somewhat (i.e., attacks increased, but the percent of respondents reporting more attacks declined year over year). The fact that only 32 percent of respondents report more attacks this year highlights the continuity of this leveling trend today and confirms the hypothesis from last year's report (**figure 4**).

The root cause of this leveling is not entirely clear from the data. One explanation is that attacks may have reached a saturation point: The volume of attacks is already so high that incentives trail off for attackers. A more likely explanation might be the increasing prevalence of external computing environments like cloud services.

Cloud Adoption

Cloud adoption continues to increase as enterprises continue to embrace software-as-a-service (SaaS) applications for critical business activities and continue to look to platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) solutions to bolster or replace internally hosted resources. As resources are moved externally, one might expect a corresponding shift in the number of attacks that directly target end-user computing environments. Attacks will still be conducted—and they may even be successful—but where those attacks are directed may shift from internally hosted devices to those hosted at cloud services providers.

As the surface area of an enterprise computing environment decreases (given, for example, that organizations are shifting to the cloud), one would expect to see a corresponding decrease in the number of visible attacks (particularly unsuccessful ones) at lower levels of the network stack, wherever operations have shifted. Due to the deliberate and purposeful abstraction of the lower levels of the network stack in a cloud context, many of those attacks may no longer be visible to the enterprise end user as they are subsumed into and handled by the cloud provider's security operations team.

ISACA's data collection for this report preceded COVID-19. The current restrictions around social distancing led many organizations to favor remote work, which shifted critical resources and business services outside the traditional perimeter. Although this trend has been steadily gaining momentum for years, the current change in business dynamics is likely to represent a comparatively seismic shift in externalization. Given this change, one could expect future data to reflect a corresponding shift in visible attacks, if the previous hypothesis is correct.

[3] Prior reports omit response choices "Don't know" and/or "Prefer not to say" in some cases. To allow year-over-year comparison, this year's report cites the raw 2019 and 2020 data with these answer choices included.

FIGURE 3—CHANGE IN NUMBER OF CYBERSECURITY ATTACKS

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

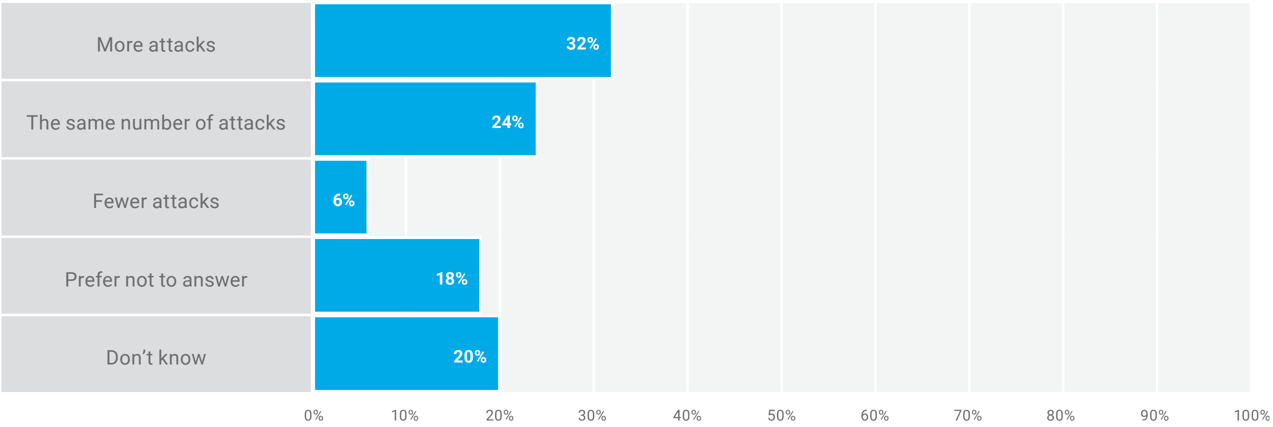
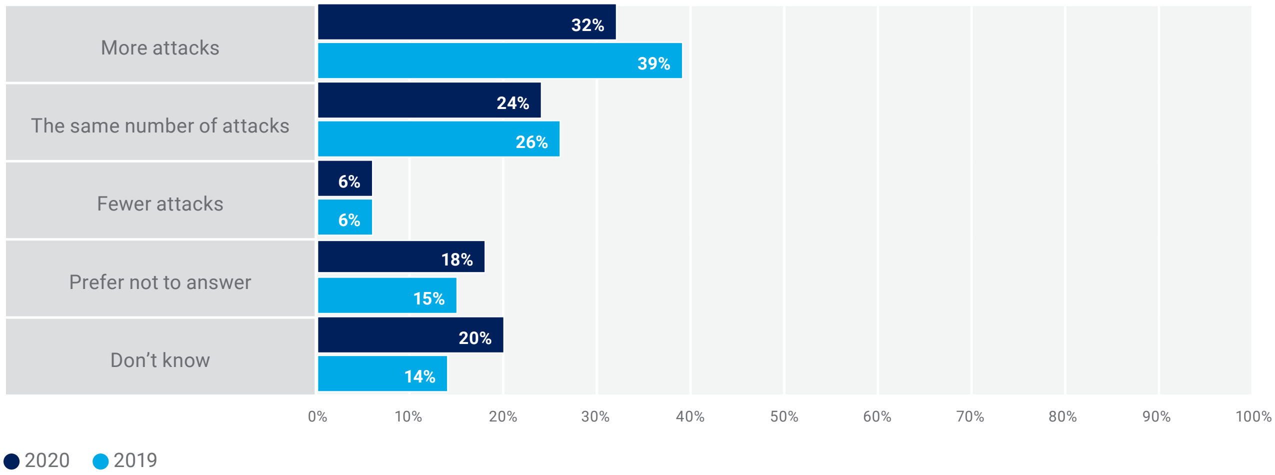


FIGURE 4—CYBERSECURITY ATTACK TRENDING

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



Threat Actors and Attack Types

To the extent that they are known, attacks continue to be of the same types that were most commonly identified in prior years. Twenty-two percent of respondents indicate that cybercriminals are to blame for exploits (down from 32 percent last year), 19 percent are attributed to hackers (23 percent in the prior year), and 11 percent to malicious insiders (13 percent in the prior year) (**figure 5**). Interestingly, insider threats were responsible for more than 20 percent of attacks (11% malicious insiders and 10% nonmalicious insiders), which also represents a downward shift from last year's 28 percent.

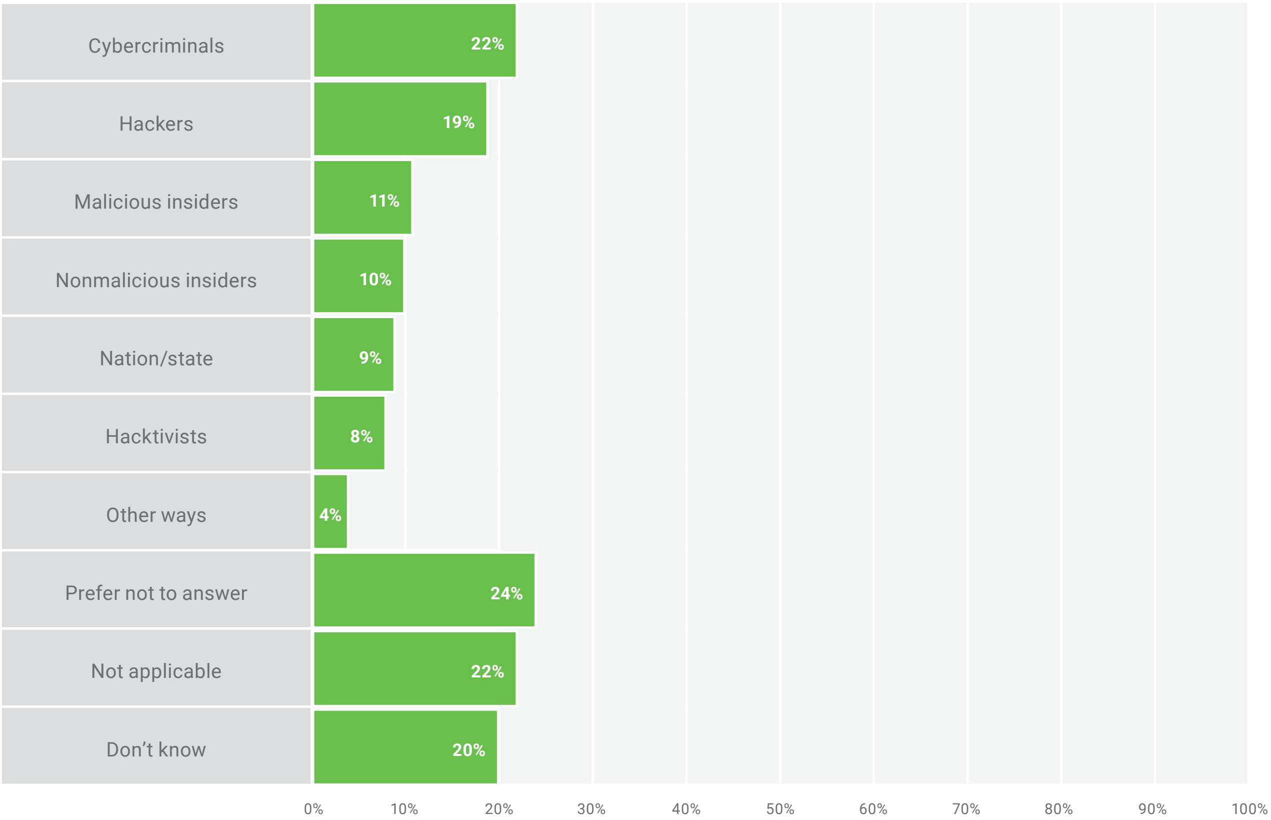
Strategies used by attackers continue to run the gamut. In the latest survey, ISACA sought more granular answers than it had in the past. Social engineering is the most popular method; 15 percent of compromised respondents report this strategy as the vehicle to entry. Advanced persistent threat (APT) is the second-most common source (at 10 percent), and ransomware and unpatched systems tied for the third-most common method (at nine percent each) (**figure 6**).

Looking forward, practitioners expect increased attacks to continue into next year. Fifty-three percent of respondents indicate that the likelihood of experiencing a cyberattack over the next year is either very likely (22 percent) or likely (31 percent). This is to be expected, given that the volume of attacks has tended to increase year over year—particularly when considering all attack types (including phishing, malware, etc.).

Although on the surface, this may seem pessimistic, the numbers this year represent an improvement from last year. Last year, 79 percent of respondents indicated some degree of likelihood that they will be attacked.[4] This optimism is reflected as well in the level

FIGURE 5—THREAT ACTORS

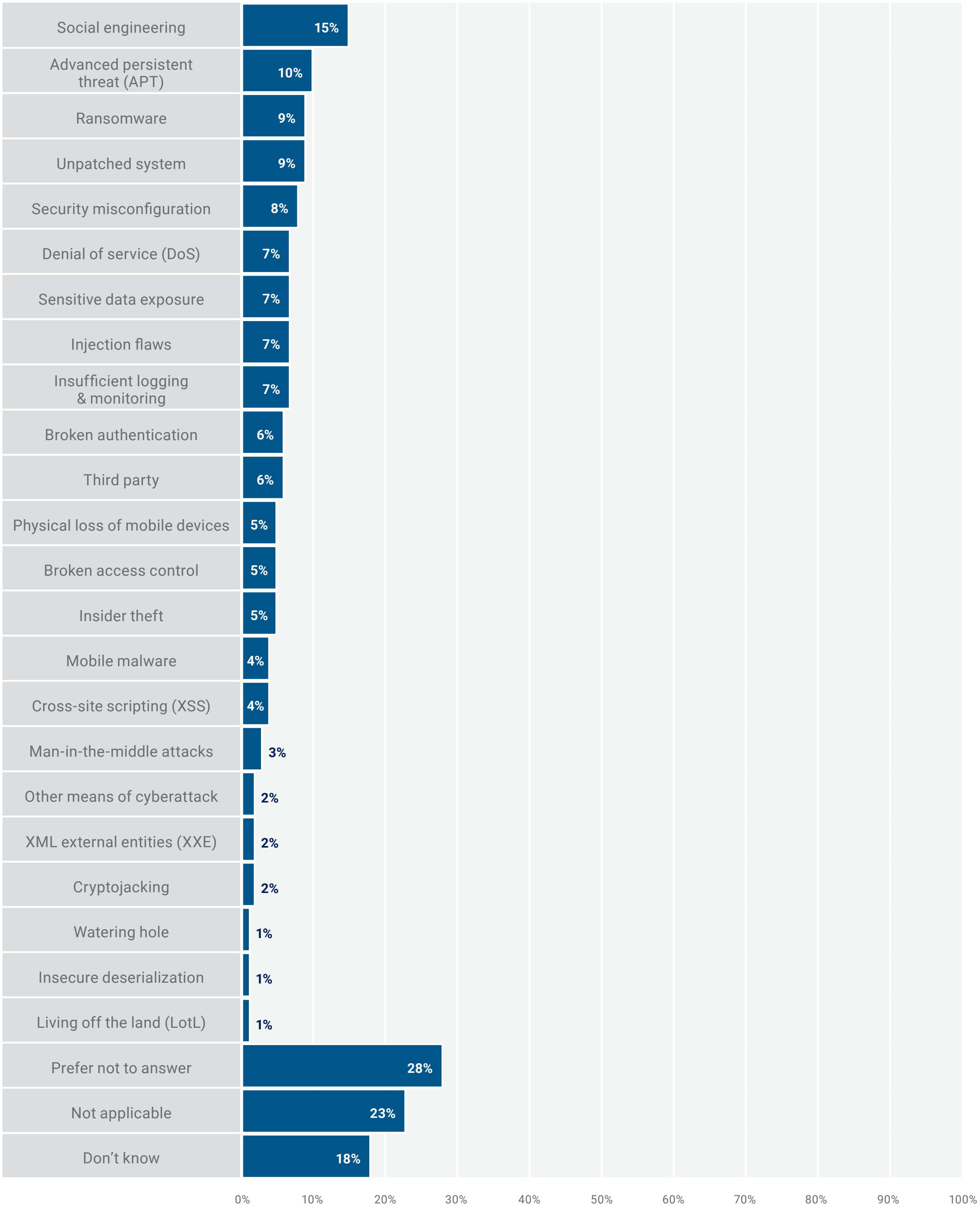
If your organization was exploited this year, which of the following threat actors were to blame? Select all that apply.



[4] Note that ISACA posed this question differently in the 2019 survey; in the 2018 survey, it had three "likely" answer choices: "very likely," "likely" and "somewhat likely."

FIGURE 6—ATTACK TYPES

If your organization was compromised this year, which of the following attack types were used? Select all that apply.



of practitioner confidence in the ability to detect and respond to cyberthreats. Cumulatively, 74 percent of those surveyed are either completely confident (four percent), very confident (30 percent) or somewhat confident (40 percent) in their organization's capabilities. This is up slightly from last year's 71-percent confidence level.

Security Functions Are Scattered Within IT Operations

For the first time, ISACA asked about security functions being performed by the IT operations team and also inquired about frameworks in use. The data suggest that IT operations teams perform a number of diverse security functions; for example, 66 percent of respondents indicate that the IT operations team is involved in incident response and 63 percent indicate that IT operations maintain, update or implement security tools and systems (**figure 7**). This should come as no surprise given the emergence of DevOps and DevSecOps practices in many organizations. But, arguably, DevOps and DevSecOps are only a partial answer to this situation. Some of this circumstance may be driven out of necessity (i.e., IT staff do the job because of small or understaffed security teams). In fact, those respondents who indicate that their cybersecurity staff is significantly or somewhat understaffed are more likely to have security functions performed by IT operations *(***figure 8***)*.

> ...those respondents who indicate that their cybersecurity staff is significantly or somewhat understaffed are more likely to have security functions performed by IT operations.

And, while necessity may be the driver, who is better positioned to find and mitigate a network attack, or stop malware during a routine IT help desk call, than the enterprise infrastructure staff who designed it? While enterprises must promote good security practices through appropriate segregation of duties, network operations—which regularly has direct visibility into underlying traffic—can help inform incident response (and other security operations tasks) in unexpected ways.

Organizations want everyone in their purview to practice safe cyberhabits. Now IT is getting involved, and it makes sense as the next logical step in the culture of cyber being propogated. In a large enterprise, this centralization can occur in multiple ways: either through direct consolidation, relocation of the function under the broader IT umbrella, through the security operations center (SOC)—either a combined SOC or a SOC integrated into a broader network operations center (NOC)—or any number of other avenues.

For a small organization, it is less likely (though still possible) that a shift from security operations to IT represents an increase in maturity. In this case, the more likely explanation is that there simply is no security operations function—or a limited one without sufficient capacity (in staff or budgetary resources)—to support the organization. Therefore, one can expect to see security operations fall under broader IT. Since this is the first year that ISACA collected this data, further analysis must wait until a trend becomes observable (i.e., will security become more or less consolidated under IT over time?).

Strong security relies on educating the enterprise employees and stakeholders on good cyberhygiene.

FIGURE 7—IT OPERATIONS PERFORMING SECURITY FUNCTIONS

Is your IT operations team responsible for any of the following security functions? Select all that apply.

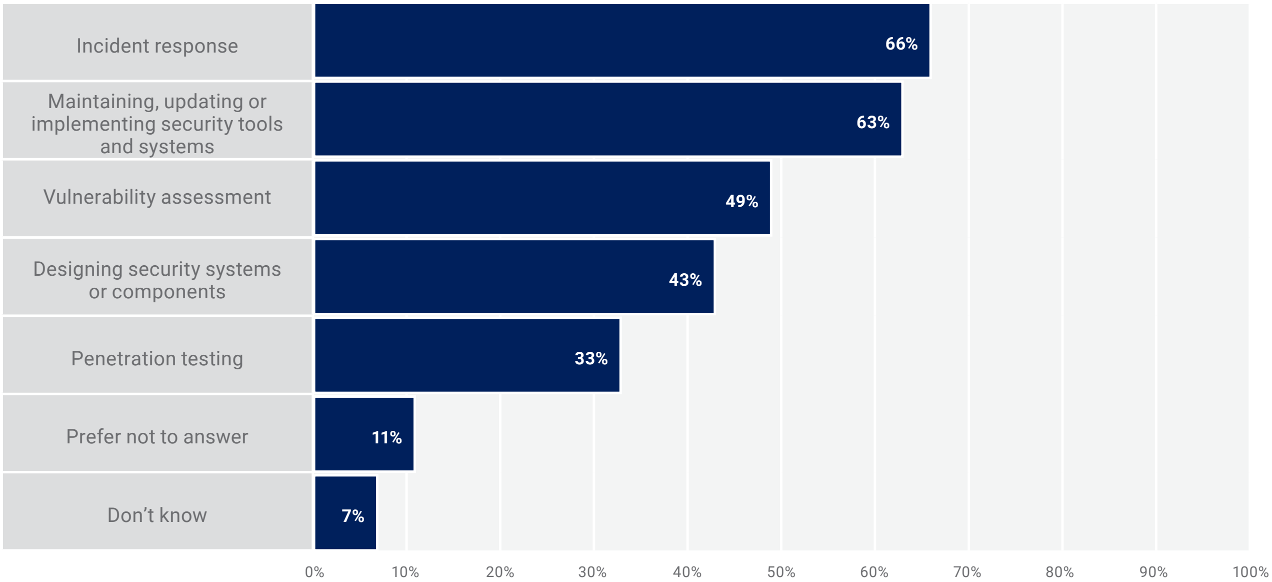
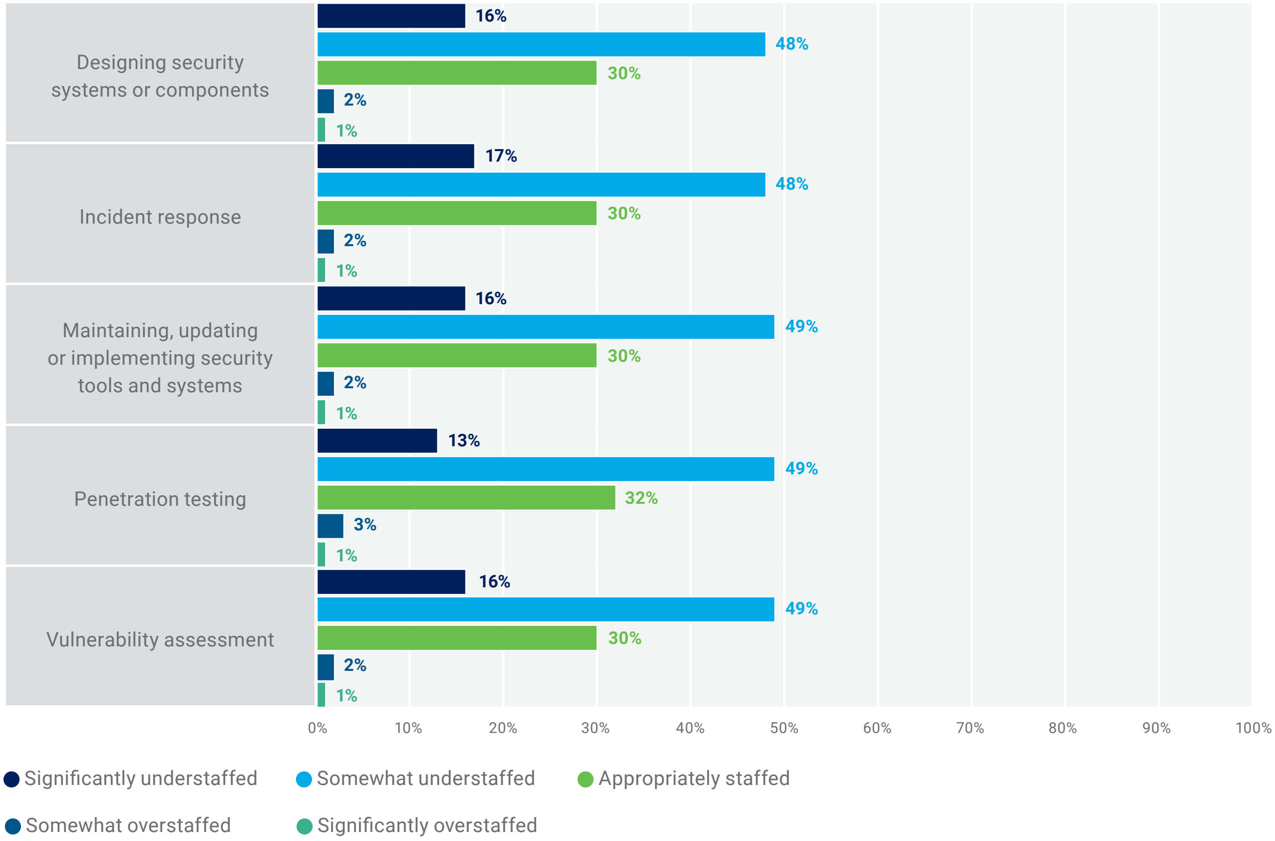


FIGURE 8—SECURITY STAFFING LEVELS RELATIVE TO TASKS PERFORMED BY IT OPERATIONS[5]



[5] The responses "I don't know," "Prefer not to answer" and "N/A" are omitted from this figure.

Cybersecurity training and awareness programs continue to have a positive impact on overall employee awareness within the enterprise. Seventy-eight percent of respondents indicate that these programs have a strong or some positive impact. Only 11 percent indicated that cybersecurity training and awareness programs have little or no positive impact on overall cybersecurity awareness within their organizations.

The most recent survey also asked about frameworks used to govern the enterprise's security functions. The US National Institute of Standards and Technology (NIST) was cited as the top framework used according to 56 percent of respondents. ISO/IEC 27000[6] was cited a close second with 53 percent indicating its use. Additionally, COBIT® and ITIL® were also referenced by 25 percent and 33 percent, respectively.

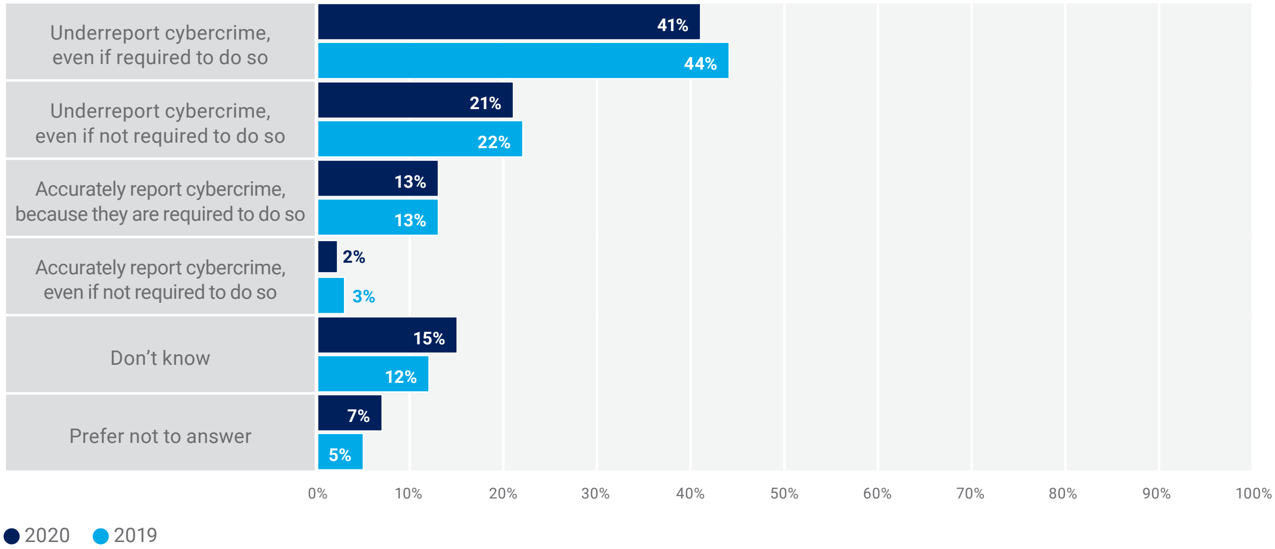
Cybercrime Remains Underreported

Last year's survey report considered the degree to which there was a perception of cybercrime underreporting, in the presence or absence of contractual or legal requirements to report. ISACA found that cybercrime, though an ongoing threat for most enterprises, was perceived to be significantly underreported. Last year, 44 percent of those surveyed believe cybercrime is underreported, even given unambiguous legal or contractual requirements to the contrary. Twenty-two percent of those surveyed believed it is underreported only in situations where there is no such requirement. Sixteen percent of respondents stated that they believe cybercrime is accurately reported.

Unfortunately, this trend has continued. This year, 41 percent of respondents indicate that they believe enterprises underreport in the presence of requirements to do so. A further 21 percent believe that enterprises underreport without such a requirement. In total, a staggering 62 percent of practitioners believe cybercrime is underreported, while 15 percent believe it is accurately reported (**figure 9**).

FIGURE 9—ENTERPRISE REPORTING OF CYBERCRIME

Do you believe that when it comes to reporting cybercrime, most organizations:



[6] International Organization for Standardization (ISO®), ISO/IEC 27000:2018, "Information technology — Security techniques — Information security management systems — Overview and vocabulary," February 2018, https://www.iso.org/standard/73906.html

These numbers are problematic for a few reasons. First, some regulations (not to mention contractual requirements) carry with them a penalty for failure to report. Based on this data, an inference can be drawn that many organizations are knowingly or unknowingly taking on regulatory risk. The fact that this phenomenon may be as widespread as it suggests that we will see more organizations incur regulatory enforcement action as a result.

Second, this perception of underreporting is concerning given how well integrated cybersecurity teams appear to be. Digging into the numbers suggests that the issues are systemic in many enterprises. Seventy percent of respondents indicated that their enterprise's cybersecurity strategy is aligned to organizational objectives. This implies a degree of coordination between nonsecurity stakeholders and the security function. Likewise, 53 percent of respondents report that the board of directors has adequately prioritized cybersecurity. It would be expected, given prioritization of cybersecurity at the board level, that the security function would therefore be integrated into enterprise governance. The fact that the perception of underreporting continues given strong coordination with other groups and implicit oversight implies a systemic—perhaps in some cases even purposeful—failure to report.

Lack of Staff and Oversight Impacts Operational Performance

This year, ISACA explored the impact of organizational factors—staffing, reporting structure and placement within the enterprise—on security outcomes. The data show that staffing correlates to outcome. Specifically, the level of staffing (understaffed, overstaffed, adequate staffing) and the ability to hire (i.e., the time it takes to fill open positions) correlate both to confidence in internal capabilities and to the number and frequency of attacks.

The results are perhaps not surprising given the expectation that well staffed organizations perform better—but, note that there are several possible explanations for why this is so. It is unclear from the data whether this points to reduced capability on the part of understaffed or slow-to-hire organizations (i.e., where the result of the reduced capability is increased susceptibility to attack) or whether the magnitude of attacks is exacerbated by lack of staff or inability to hire (i.e., where impacts and ripple effects from attacks are felt farther or more acutely). Either way, there is a demonstrable correlation between staffing and both confidence in internal capabilities and, in some cases, number of attacks.

For example, 21 percent of "significantly understaffed" respondents report that they are completely or very confident in their organization's ability to respond to threats. Thirty percent of "somewhat understaffed" respondents report they are completely or very confident in their organization's ability to respond to threats, and those who indicated their enterprise was "appropriately staffed" reflect a 50-percent confidence level.[7] In short, as levels of appropriate staff size increase, so too does confidence. Perhaps this is to be expected as it is obviously more challenging to be confident about a situation where key resources are lacking.

[7] Note that low numbers of respondents reporting overstaffing prevents useful analysis along this portion of the cross-section.

ISACA further observed that the impact extends beyond confidence into the number of attacks experienced by organizations. Enterprises that are able to fill open positions suffer fewer attacks. As timeframe to hire staff decreases, so too do numbers of attacks correspondingly decrease. Fifty-three percent of those enterprises that hired in two weeks or less had fewer or the same number of attacks compared to last year. Twenty-six percent of those from enterprises that fill open security positions in two weeks or less indicated they had experienced an increase in attacks compared to a year ago, while 30 percent from organizations taking 1 or 2 months experienced more attacks. Thirty-five percent of respondents in enterprises taking three months to hire reported an increase in attacks and 38 percent from those taking 6 months or more. The most commonly attacked group, those unable to fill open security positions, cited more attacks at a rate of 42 percent (**figure 10**).

Organizational Structure Impacts Confidence Levels

Organizational structure and placement within the organization plays a role here as well. Like last year, the most confident organizations are those in which the cybersecurity function reports to a CISO. Forty percent of respondents reporting to a CISO are either completely or very confident in their enterprise's ability to detect and respond to threats, while only 31 percent of those reporting to a CIO indicate comparable confidence (**figure 11**).

This dynamic is also reflected in other representations or perceptions—including whether a respondent believes that cybercrime is being appropriately reported. Sixty-one percent of those reporting to a CISO indicate that they think cybercrime is underreported, while 73 percent of those reporting to the CEO think that this

FIGURE 10—NUMBER OF ATTACKS RELATIVE TO HIRING ABILITY

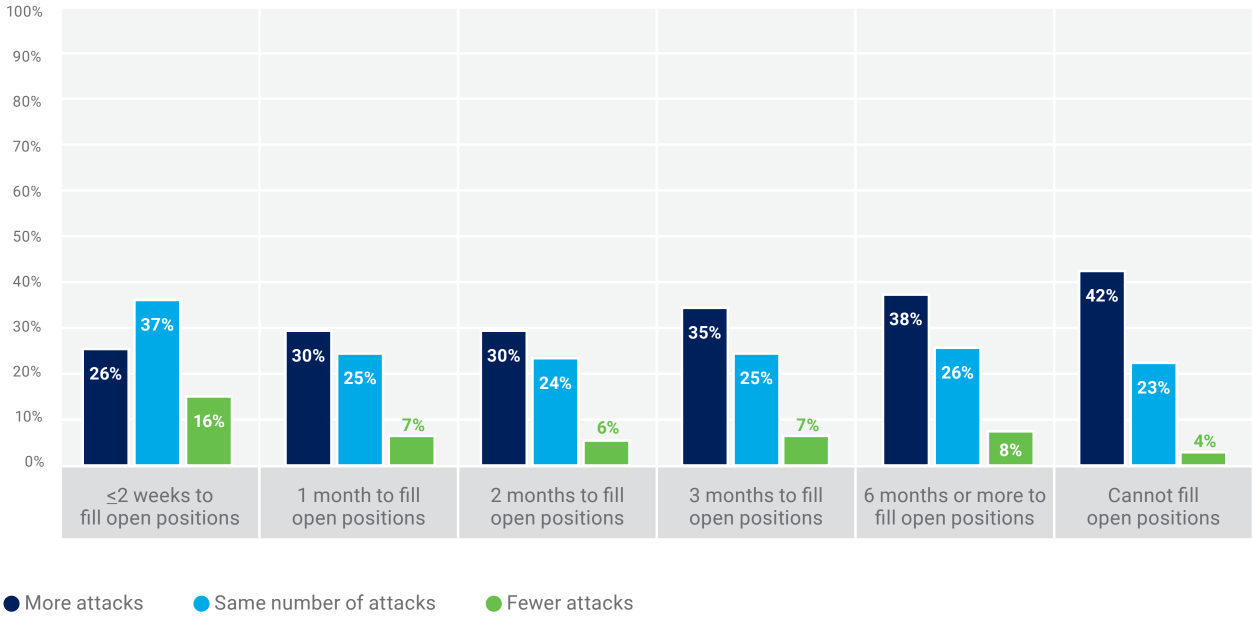
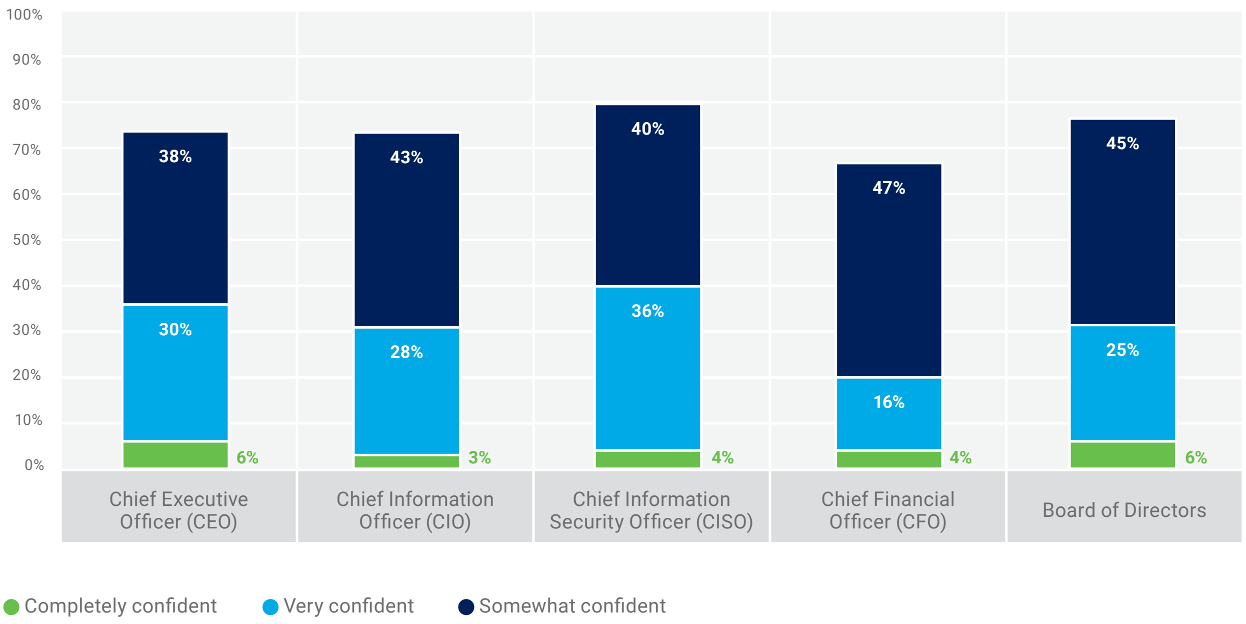


FIGURE 11—CONFIDENCE LEVEL AND REPORTING STRUCTURE



is the case. Interestingly, those respondents reporting to the CEO also indicate the lowest percentage (14 percent) of their perception that their enterprise accurately reports cybercrime.

Perhaps it is not surprising that staffing and organization play a role in performance. Possibly more surprising is that outcomes do not correlate to reporting level. Just because a security team/organization reports at a higher level in the organizational hierarchy does not ensure greater staff confidence. One explanation is that presence or absence of a CISO can be considered a barometer of organizational security commitment—the implication being, that by having a CISO, the enterprise (likely) thought about security and prioritized it.

AI Solutions May Increase Visibility, Though Adoption Lags

This year, for the first time, ISACA inquired about the use of artificial intelligence (AI) and machine learning solutions in security programs. Despite numerous products in the marketplace that provide these capabilities, adoption is still relatively low. Only 30 percent of those surveyed use these tools as a direct part of their operations capability (**figure 12**). As reported in *State of Cybersecurity 2020, Part 1*, 20 percent of respondents indicate an increased reliance on artificial intelligence or automation to help mitigate the cybersecurity skills gap.

The low number of respondents using AI is somewhat surprising, given that solution vendors increasingly incorporate machine-learning capabilities into existing solutions. It is possible that some respondents—despite the fact that they employ solutions including these capabilities—are simply unaware of these features. Even accounting for this possibility, a 30-percent adoption number is striking, indicating that AI-enabled security products are still not the industry norm.

The numbers tell a complicated but interesting story. Among respondents who report more attacks since last year, 38 percent are using AI solutions, while 44 percent are not. From this metric alone, one is tempted to conclude that use of AI security solutions reduces attacks. However, the implications are more nuanced; among those who indicate that they are experiencing fewer attacks, 34 percent are using AI, while 48 percent are not (**figure 13**). This indicates that using AI both increases responses for more attacks and fewer attacks simultaneously. How can this be true?

There are several possible explanations. Attacks can be both successful and unsuccessful. Reduction in

FIGURE 12—USE OF AI IN SECURITY OPERATIONS

Do you use artificial intelligence (such as machine learning or robot process automation [RPA]) in your security operations?

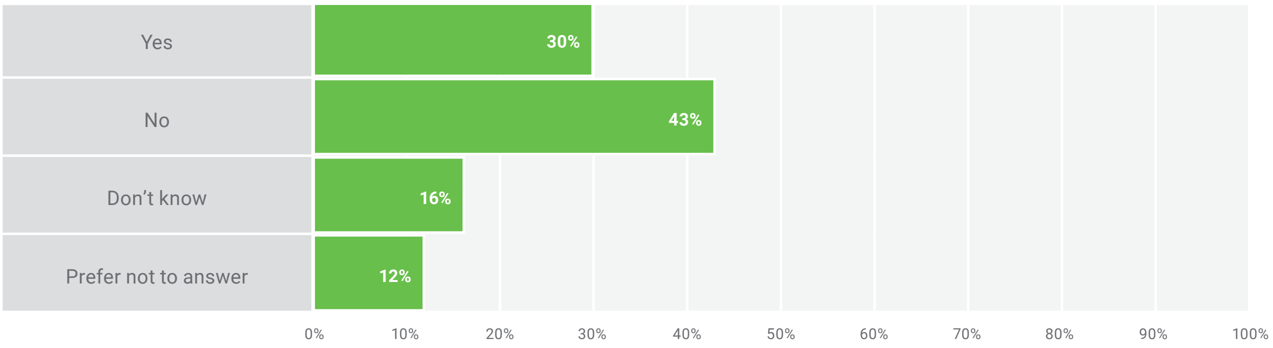
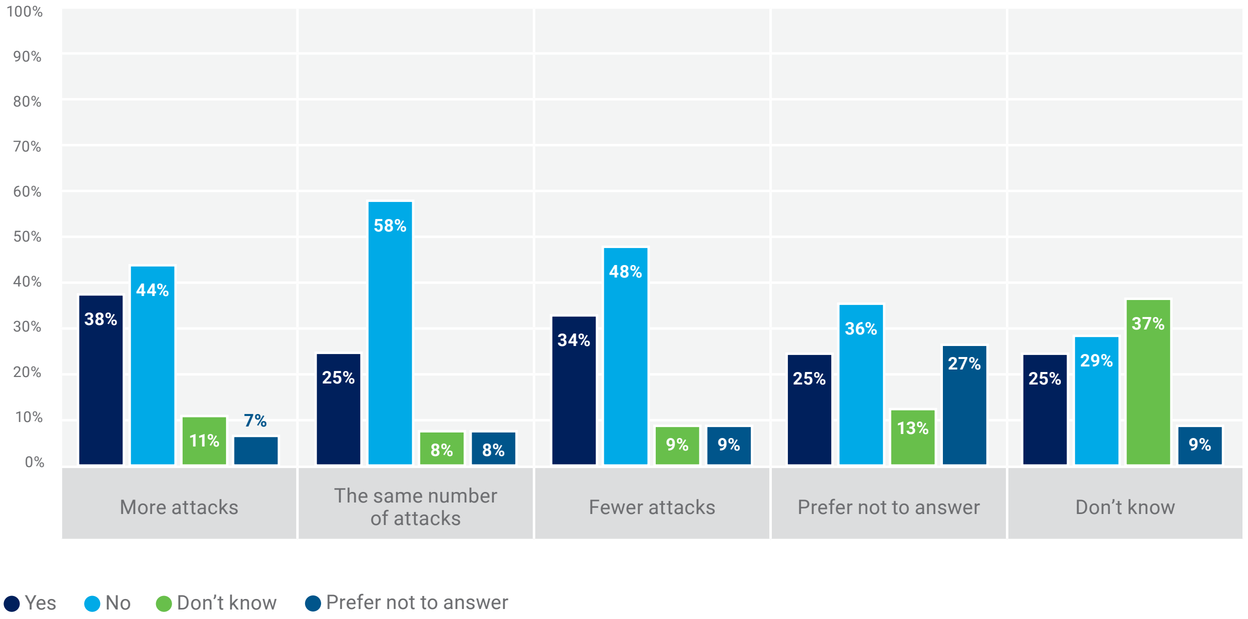


FIGURE 13—AI USE AND NUMBER OF ATTACKS

Do you use artificial intelligence in your security operation?



overall attacks can be explained by a reduction in false positives for some enterprises—and discovery of otherwise invisible attacks for others. As the false positive rate decreases, it might reduce the overall attack number in enterprises that have a legacy—and largely noisy—set of existing instrumentation. For enterprises that find previously undiscovered attacks, the attack rate will increase.

Another explanation lies in the number of respondents reporting that attacks stayed the same and those reporting that they did not know (or would not indicate) whether attacks increased. For example, among respondents who experienced the same number of attacks, 25 percent of those using AI solutions report that attack activity stayed the same, while 58 percent (33 percentage points) of those not employing AI solutions observed no change in frequency.

These data points suggest another possible explanation: increased visibility. Respondents are better able to quantify attack rate with the presence of AI tools. Seeing fewer attacks is not always the optimal outcome. Observation of more attacks can occur for a few different reasons:

- Increasing frequency of attack activity
- Increased impact (but not frequency) of attack activity
- Increased visibility into attack activity

It is possible that a respondent whose enterprise has encountered more attacks may actually be experiencing a better outcome—provided that such observations position the respondent's enterprise to take action. In this case, if the underlying dynamic in the numbers reflects increased visibility, this is a promising sign for AI-based tools.

Ransomware Returns as Primary Post-exploitation Monetization Strategy

Ransomware and cryptocurrency-mining malware again traded positions for the top mechanism of post-exploitation monetization.

Two years ago, survey results reported a shift, as cryptocurrency-mining malware surpassed ransomware as the most-reported mechanism of post-exploitation monetization. This year, nine percent of respondents suffering a security compromise report that ransomware was a component of the attacker activity, while only two percent indicate that cryptojacking (i.e., cryptocurrency-mining malware) was employed in attacks on their enterprises. Both approaches allow attackers to convert access to compromised resources into dollars. Ransomware attackers seek to leverage access to get users to pay them directly, while cryptocurrency-mining attackers seek to convert CPU time into work performed for cryptocurrency mining.

From an attacker point of view, both strategies have advantages and disadvantages. Ransomware has a quick reward, but campaigns are likely to be short-lived, because those in the security ecosystem (vendors, end users, authorities, etc.) become aware of these campaigns quickly and move to shut them down. Cryptocurrency-mining malware, by contrast, operates over a longer time period, but does so more stealthily, allowing an attacker to operate longer before being discovered.

This change in leading monetization strategy likely reflects a combination of factors—including cryptocurrency prices, fileless malware and living-off-the-land strategies,[8] and increasing use of cloud resources.

[8] *Op cit* Schwartz

Conclusion: The Road Ahead

Undoubtedly, the cybersecurity profession will change, considering recent events. The long-term impacts will likely take years to be fully realized and understood and, in the meantime, enterprises will need to live with some uncertainty. This year's *State of Cybersecurity Survey* data provide insight on how professionals can increase certainty in at least a subset of the broader landscape. The data suggest that AI-enabled tools may offer visibility benefits, that investments in resource acquisition may translate into potentially better outcomes, and that investments in cloud may have the unexpected benefit of reducing visible attacks against enterprises.

The perception of cybercrime underreporting continues to be an area of concern that ISACA will continue to monitor. Should this trend continue, the regulatory and contractual implications alone are obviously undesirable. However, underreporting signifies violations of codes of ethics required by licensure and credentialing bodies—which is disturbing, given the criticality of protecting organizational data. For organizations in regulated industries, or those that have strong contractual obligations for notification, it is worth paying attention to this unsettling dynamic.

Acknowledgments

ISACA would like to recognize:

ISACA Board of Directors

Brennan P. Baybeck, Chair
CISA, CRISC, CISM, CISSP
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rolf von Roessing, Vice-Chair
CISA, CISM, CGEIT, CISSP, FBCI
FORFA Consulting AG, Switzerland

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

Pam Nigro
CISA, CRISC, CGEIT, CRMA
Health Care Service Corporation, USA

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
AppGate Federal Group, USA

Asaf Weisberg
CISA, CRISC, CISM, CGEIT
introSight Ltd., Israel

Rob Clyde
ISACA Board Chair, 2018-2019
CISM
Board Director, Titus and Executive Chair, White Cloud Security, USA

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

Greg Grocholski
ISACA Board Chair, 2012-2013
CISA
Saudi Basic Industries Corporation, USA

David Samuelson
Chief Executive Officer, ISACA, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

Disclaimer

ISACA has designed and created *State of Cybersecurity 2020, Part 2: Threat Landscape and Security Practices* (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

Website: www.isaca.org

Provide feedback:
www.isaca.org/state-of-cybersecurity-2020

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/ISACAGlobal

Instagram:
www.instagram.com/isacanews/