ISACA | HCL

State of Cybersecurity 2021

Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity

Security

CONTENTS

ABSTRACT

State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity reports the results of the annual ISACA® global *State of Cybersecurity Survey,* conducted in the fourth quarter of 2020. Part 2 focuses on the threat landscape, the impact of the COVID-19 pandemic on security programs and the challenges of assessing cybersecurity maturity. The survey findings reinforce past reporting and, in certain instances, mirror prior-year data, despite new challenges that enterprises face amidst the ongoing global pandemic and opportunistic threat actors.

Executive Summary

Now in its seventh year, the ISACA® global *State of Cybersecurity Survey* continues to identify current challenges and trends in the cybersecurity field. *State of Cybersecurity 2021, Part 1*[1] analyzes the survey results regarding cybersecurity workforce development and resourcing. In Part 2, ISACA examines the survey results pertaining to security operations, cyberthreats and cybersecurity maturity.

After a three-year trend of a slowing rate in new attacks, the percentage of enterprises experiencing more cyberattacks than the previous year reversed course and attacks increased, reaching a level not seen since 2018.

The survey findings are largely consistent with the findings from prior years, including the continued impact that insufficient staffing levels to combat cyberthreats have on operations. Following are the key survey findings about security operations, cyberthreats and cybersecurity maturity:

- After a three-year trend of a slowing rate in new attacks, the percentage of enterprises experiencing more cyberattacks than the previous year reversed course and attacks increased, reaching a level not seen since 2018.
- Respondent confidence in the ability of their cybersecurity teams to detect and respond to cyberthreats remains high at 77 percent—a three-percentage-point increase from 2020 survey data. Similarly, 32 percent of respondents believe that their cybersecurity training and awareness programs have a strong positive impact on overall cybersecurity awareness, up from 28 percent last year.
- Respondent data largely show that the global pandemic i s not deterring planned work for the reporting period. Forty-four percent of respondents say that threat actors are not taking advantage of the pandemic to disrupt organizational activities, and 43 percent note that their enterprises are not increasing their security technology spending due to the pandemic.
- The colocation of work into formal network operations centers (NOCs) and security operations centers (SOCs) drives integrated response capabilities. ISACA sought insights about the amount of security-related work being handled by IT operations. The top three security functions being handled by IT operations are incident response (66 percent); maintaining, updating or implementing security tools and systems (65 percent); and vulnerability assessments (53 percent).
- Top cyberattack concerns and sources of exploitation nearly mirror findings from a year ago, except that insider threats—both malicious (10 percent) and nonmalicious (8 percent)—continue their steady decline from 28 percent in 2019 and 21 percent in 2020.
- New to this year's ISACA survey report are insights gleaned from survey respondents about cybersecurity maturity assessment. Sixty-five percent of enterprises assess their cybermaturity. Those that perform these assessments are more likely to have appropriately staffed security teams and are more likely to report appropriately funded cybersecurity budgets. Respondents with a pulse on security program measurement and maturity are more than two times more confident in the ability of their enterprise to detect and respond to cyberattacks.

Respondents with a pulse on security program measurement and maturity are more than two times more confident in the ability of their enterprise to detect and respond to cyberattacks.

The number of responses to this year's survey increased 44 percent over last year and exceeds all prior participation,[2] which, coupled with a decrease in those selecting the "Prefer not to answer" option for multiple questions, increases the confidence level in the conclusions drawn in this report.

[1] ISACA, *State of Cybersecurity 2021, Part 1: Global Update on Workforce Efforts, Resources and Budgets*, USA, 2021, www.isaca.org/bookstore/bookstore-wht_papers-digital/whpsc211

[2] The 2020 State of Cybersecurity Survey received 2,051 responses, compared with 3,659 responses to the 2021 survey.

Survey Methodology

In the final quarter of 2020, ISACA sent online survey invitations to a global population of cybersecurity professionals who hold the ISACA Certified Information Security Manager® (CISM®) certification or have registered information security job titles. The survey data were collected anonymously via SurveyMonkey. A total of 3,659 respondents completed the survey in its entirety, and their responses are included in the results.[3]

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

- Hiring and skills
- Security operations
- Cybersecurity budgets
- Cyberattacks and threats
- Organizational governance and risk management

The survey target population is individuals who have cybersecurity job responsibilities. Of the 3,659 respondents, 1,721 indicate that cybersecurity is their primary professional area of responsibility. **Figure 1** shows demographic information about the respondents, who hail from more than 120 countries. **Figure 2** further illustrates the breadth of survey input, showing that respondents represent more than 17 industries.

[3] 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, consistent with prior-year survey reports. Result percentages are rounded to the nearest integer.

FIGURE 1: Respondent Demographics

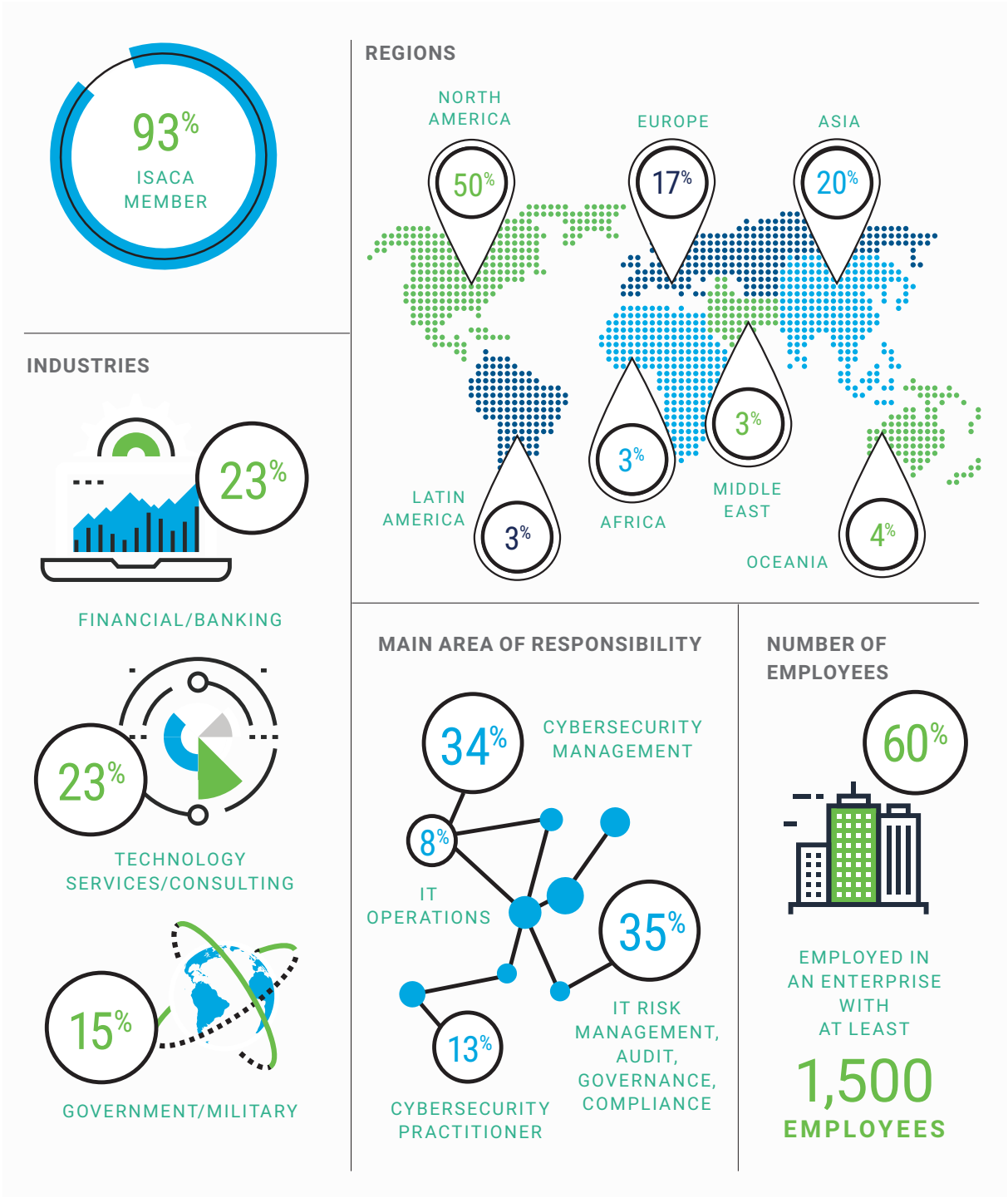
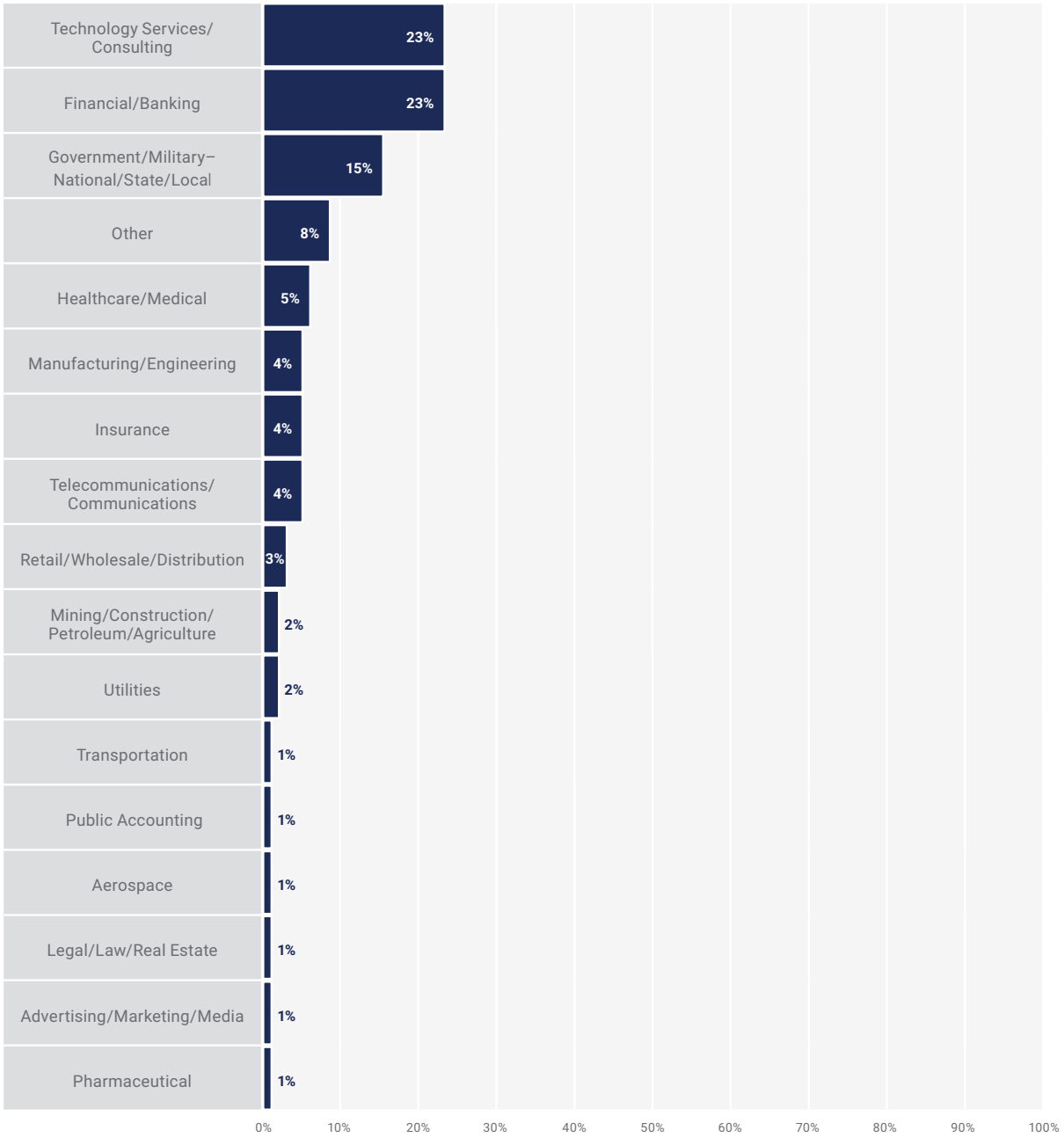


FIGURE 2: Industries Represented

Please indicate your organization's primary industry.



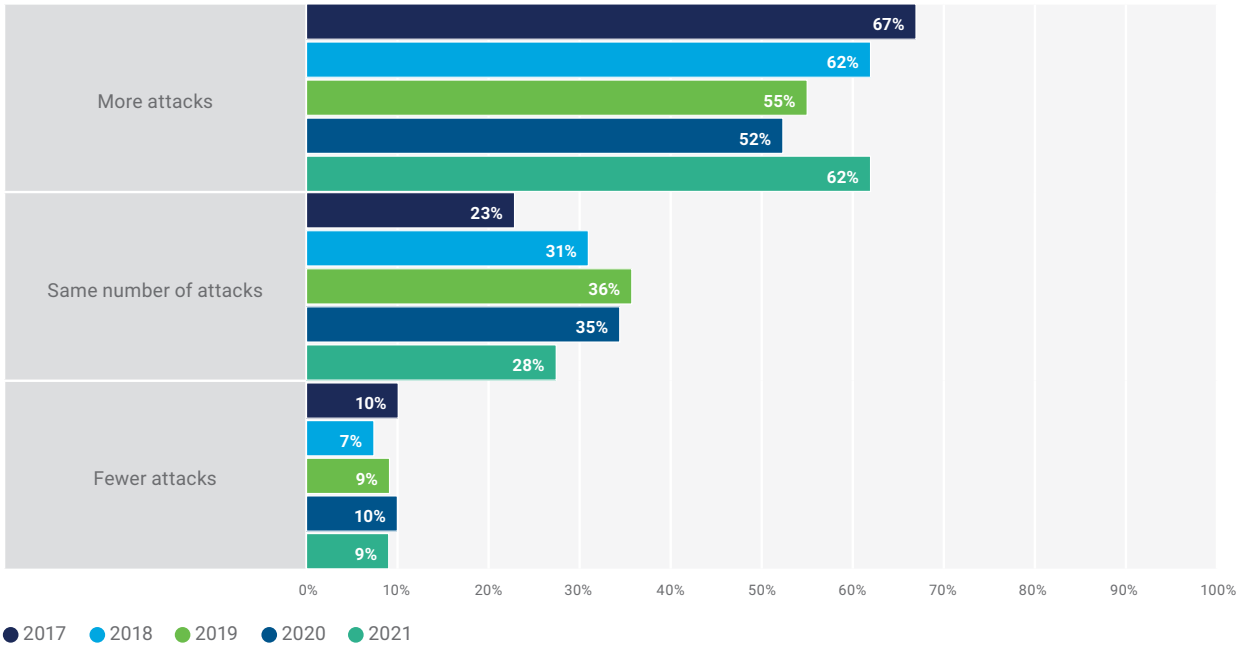
Rate of Increase in Cyberattacks Jumps After Slowing in Recent Years

After a three-year trend of a slowing rate in new attacks, the percentage of enterprises experiencing more cyberattacks than the previous year reversed course and attacks increased, reaching a level not seen since 2018. **Figure 3** compares five years of cyberattack reporting.

This year, 35 percent of respondents report that their enterprises are experiencing more cyberattacks (**figure 4**), which is three percentage points higher than last year. Of note, those who prefer not to answer decreased by two percentage points from the previous year; therefore, although the current threat landscape surely supports any hypothesis that enterprises are being attacked more, it is also plausible that respondents are simply more comfortable with generalized data sharing. Also of interest is that 44 percent of respondents say that threat actors did not take advantage of the pandemic to disrupt organizational activities (**figure 5**).

This year, 35 percent of respondents report that their enterprises are experiencing more cyberattacks, which is three percentage points higher than last year.

FIGURE 3: Five-Year Comparison of Cybersecurity Attack Reporting[4]



[4] The responses "Don't know" and "Prefer not to answer " are omitted from this figure.

FIGURE 4: Change in Number of Cybersecurity Attacks

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

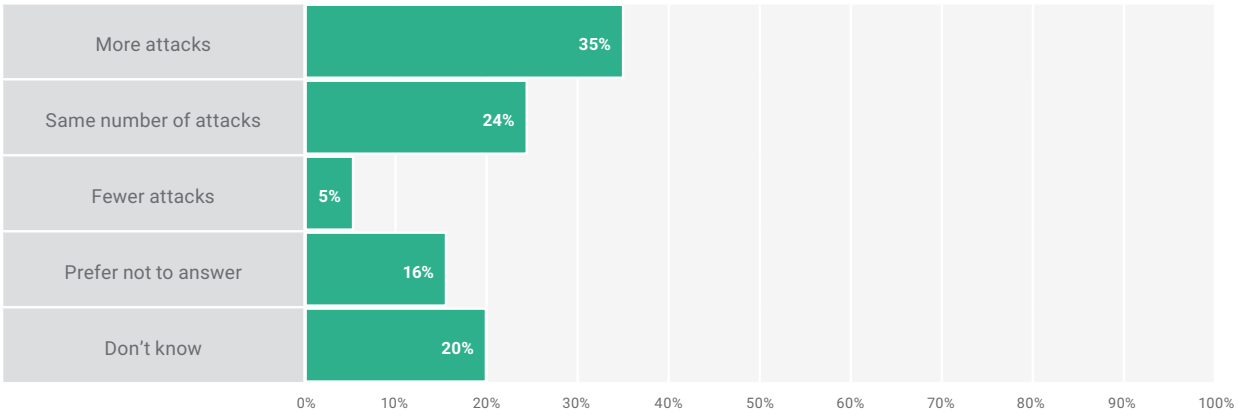
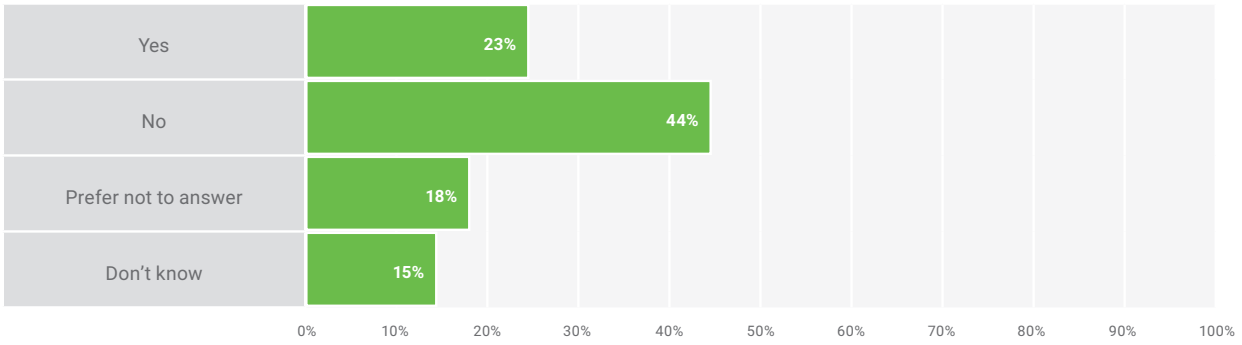


FIGURE 5: Opportunistic Disruption

Did threat actors take advantage of the COVID-19 pandemic to disrupt your organization's activities?



Confidence and Awareness Improve

Respondents' confidence in the ability of their cybersecurity teams to detect and respond to cyberthreats remains high at 77 percent—a three-percentage point increase from 2020 survey data (**figure 6**). Similarly, enterprises see an improvement in cybersecurity training and awareness programs, with 32 percent of respondents believing that their programs have a strong positive impact on overall cybersecurity awareness, up from 28 percent last year (**figure 7**).

FIGURE 6: Organizational Confidence for 2020 and 2021

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

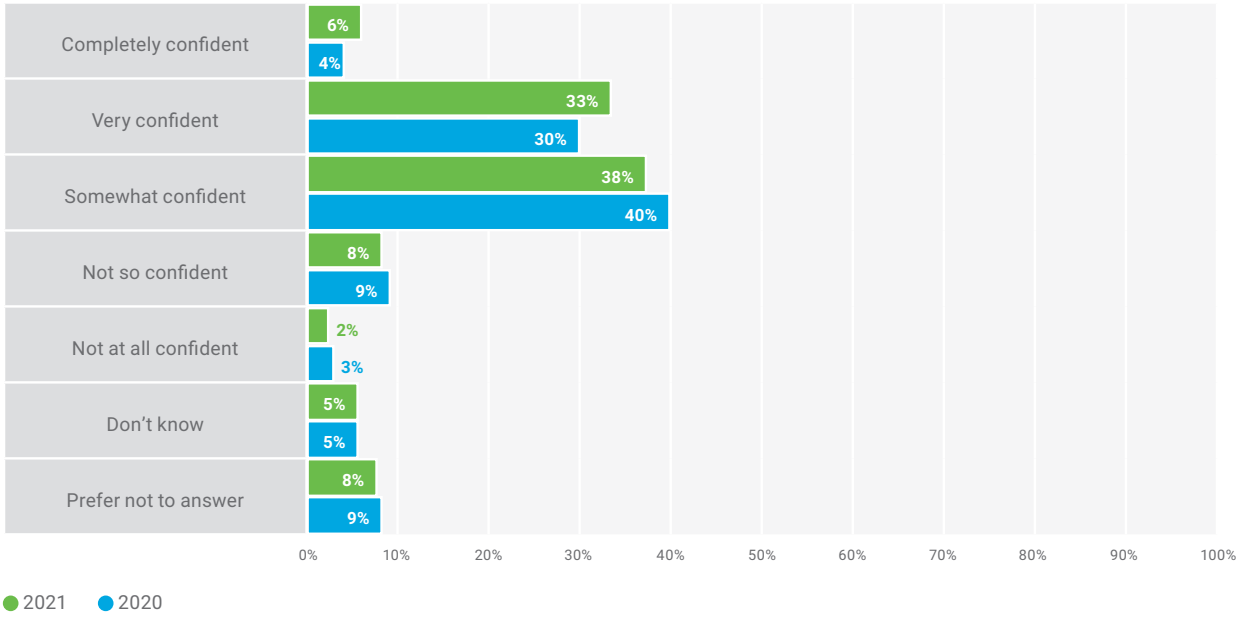
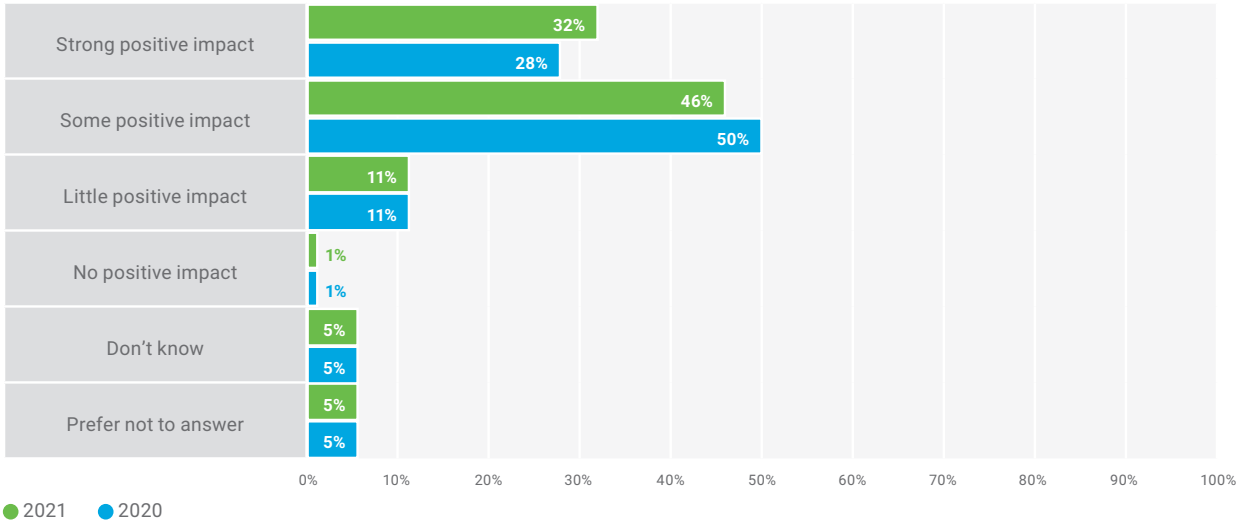


FIGURE 7: Cybersecurity Awareness Program Impact for 2020 and 2021

What impact, if any, do you feel that cybersecurity training and awareness programs have had on overall employee cybersecurity awareness in your organization?



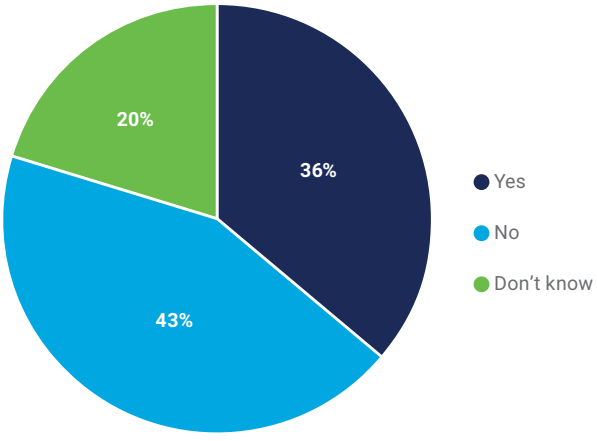
Perseverance Rises Amid Pandemic

State of Cybersecurity 2021, Part 1 reports that, despite being understaffed and overworked, the cybersecurity workforce quickly pivoted during the COVID-19 pandemic and enabled enterprises to continue operations with a wholly or mostly remote workforce.

Notwithstanding the adversity experienced by so many enterprises around the globe, respondent data largely show that the global pandemic is not deterring planned work for the reporting period. Forty-four percent of respondents (**figure 5**) say that threat actors are not taking advantage of the pandemic to disrupt organizational activities, and 43 percent note that their enterprises are not increasing their security technology spending due to the pandemic (**figure 8**).

FIGURE 8: Spending on Security Technology

Has your organization increased its spending specifically on new security technology initiatives during the COVID-19 pandemic?



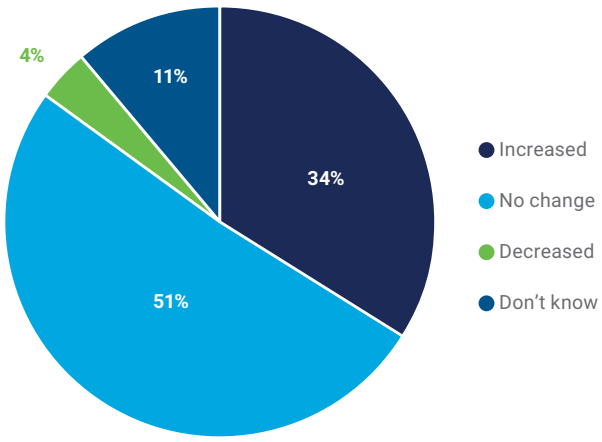
When asked about the impact of COVID-19 on cloud migration in their enterprises (**figure 9**), 51 percent of respondents report that the pandemic has had no effect on cloud migration.

The prevalence of remote work throughout the pandemic appears to be motivating strategic changes that are better suited for a highly mobile workforce. More than one in three enterprises adopted either a Secure Access Service Edge (SASE) model[5] or Zero Trust[6] security strategy as a cybersecurity approach (**figure 10**) because of the pandemic.

The prevalence of remote work throughout the pandemic appears to be motivating strategic changes that are better suited for a highly mobile workforce.

FIGURE 9: Cloud Migration

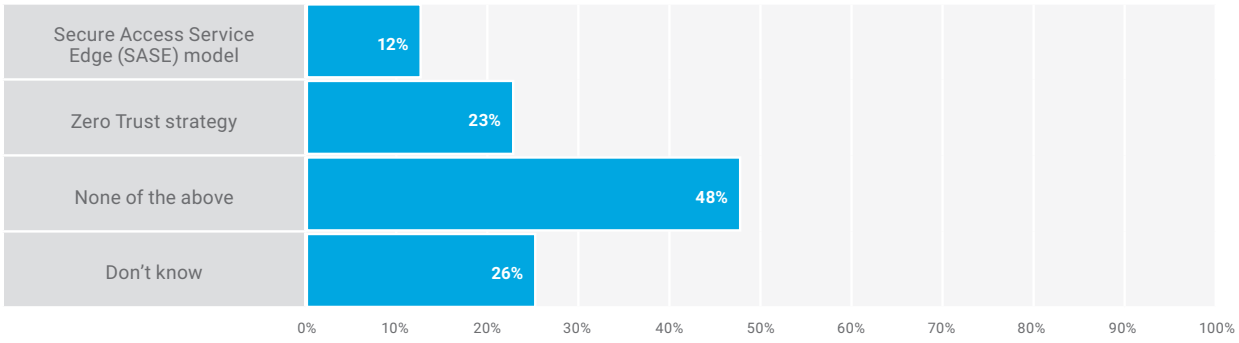
What impact, if any, has the COVID-19 pandemic had on cloud migration within your organization?



[5] The Secure Access Service Edge (SASE) model can help organizations ensure secure access from any device location, a feature that is especially important in the context of existing remote working arrangements during the COVID-19 pandemic.
[6] The Zero Trust security model states that anything outside or inside of the network cannot be trusted—and that every device or individual trying to access network resources must be authenticated.

FIGURE 10: Pandemic's Impact on Cybersecurity Approach

As a result of the COVID-19 pandemic, has your organization adopted any of the following? Select all that apply.



Threat Actors, Attacks Change Little

Top cyberattack concerns are identical to last year (**figure 11**): enterprise reputation (78 percent); data breaches concerns (69 percent); supply-chain disruptions (49 percent).

The reported sources of exploitation nearly mirror the findings from a year ago (**figure 12**). Twenty-three percent of respondents report that cybercriminals are responsible for exploitation (up from 22 percent last year), 17 percent of exploits stem from hackers (down two percentage points from the prior year), and 10 percent of respondents attribute exploits to malicious insiders (down one percentage point from last year).

Of interest, insider threats—both malicious (10 percent) and nonmalicious (8 percent)—continue their steady decline, from 28 percent in 2019 and 21 percent in 2020.

FIGURE 11: Cyberattack Concerns

What are your top concerns related to a cyberattack on your organization? Select all that apply.

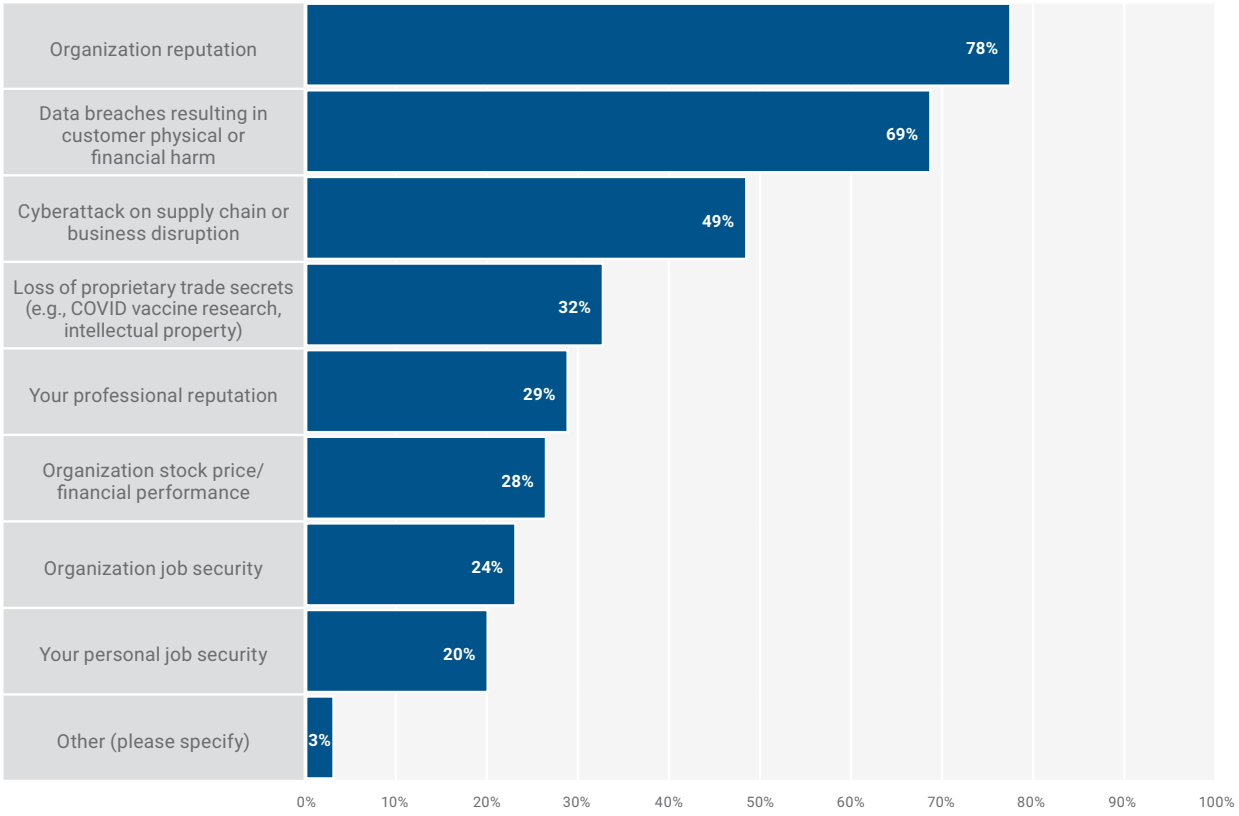
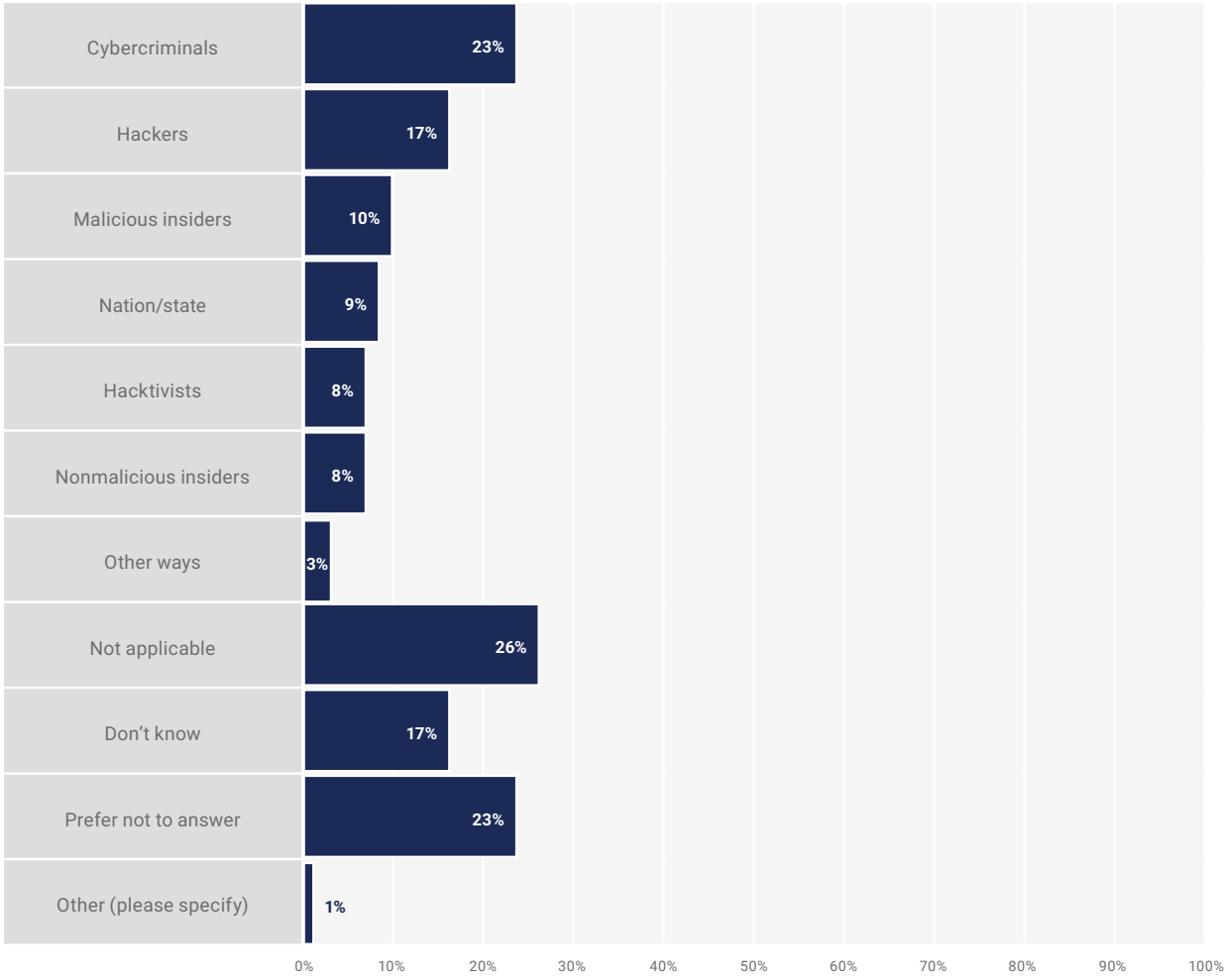


FIGURE 12: Threat Actors

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

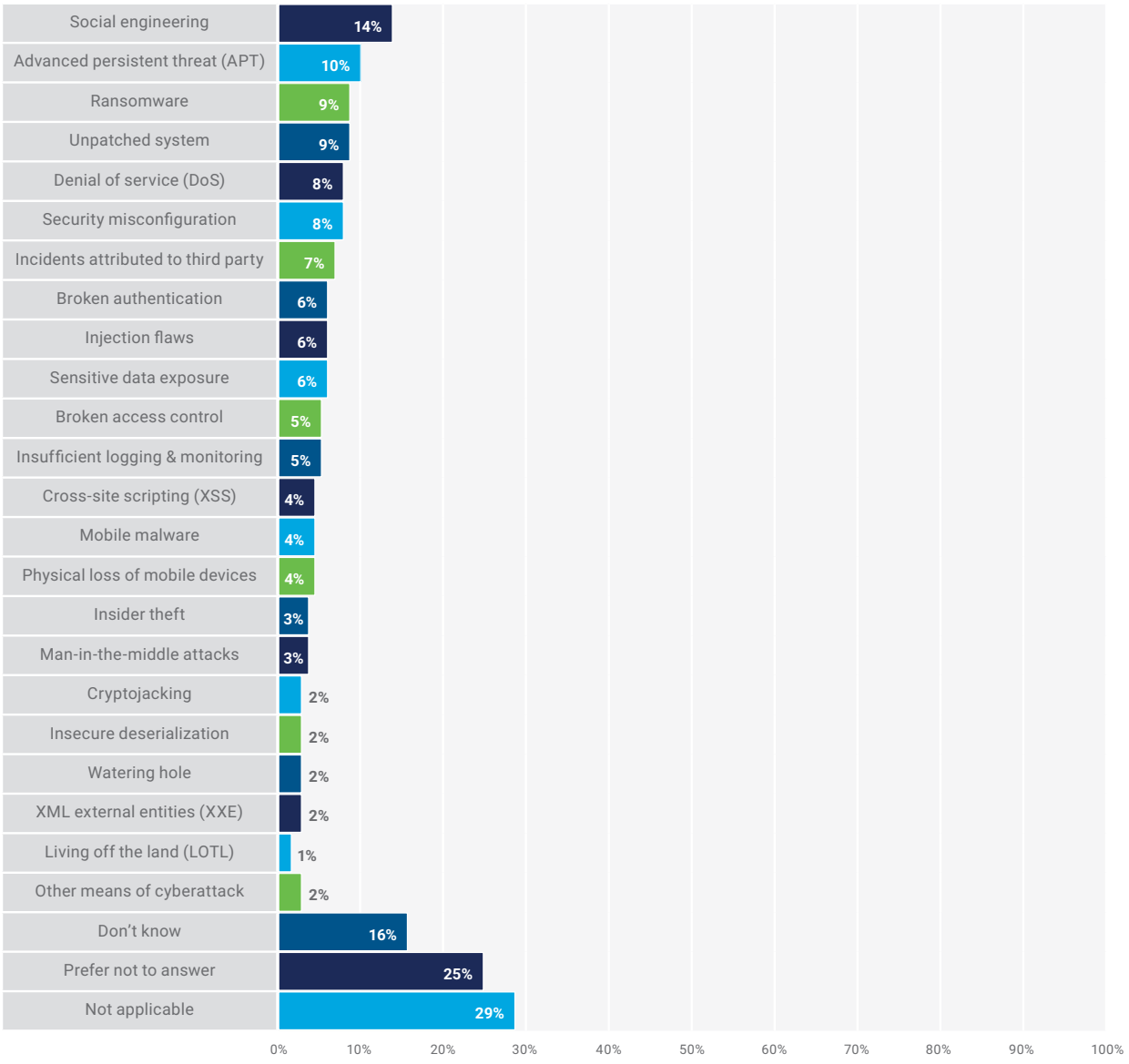


ISACA continued to offer the granularity in attack type survey response options (**figure 13**) introduced last year. Social engineering remains the predominant cyberattack method (14 percent), followed by: advanced persistent threat (APT) (10 percent), ransomware (9 percent), unpatched system (9 percent), denial of service (8 percent), and security misconfiguration (8 percent). Overall, responses about attack types almost mirror those in the ISACA *State of Cybersecurity 2020, Part 2* report, with two notable exceptions—insufficient logging and monitoring dips two percentage points in 2021, and insider theft also drops two percentage points in 2021. Respondents selecting "Prefer not to answer" decrease three percentage points, and respondents indicating "Not applicable" (29 percent) rise six percentage points. Although the percentage of respondents indicating a ransomware attack (9 percent) does not change from last year, it will be interesting to see if ransomware attacks increase next year's results, due to recent high-profile ransomware attacks.[7,8] Future reporting may show that this attack type can be higher profile in terms of press coverage but remain steady in its actual number.

[7] Fung, B.; D. Sands; "Ransomware attackers used compromised password to access Colonial Pipeline network," CNN, 4 June 2021, https://www.cnn.com/2021/06/04/politics/colonial-pipeline-ransomware-attack-password/index.html
[8] Durbin, D.A.; J. Bajak; "Largest meat producer getting back online after cyberattack," Associated Press (AP), 2 June 2021, https://apnews.com/article/jbs-sa-lifestyle-health-coronavirus-pandemic-technology-bf82114d3f54e5be2241bd5f9a0b2639

FIGURE 13: Attack Types

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



A Snapshot of Security Operations

State of Cybersecurity 2021, Part 1 notes that enterprises employ a variety of methods to fulfill their organizational responsibilities—the largest of which entails training to introduce existing, interested nonsecurity staff into security roles.

Industry reporting suggests that enterprises use technical and nontechnical employees to fill shortfalls.

Acknowledging this trend, ISACA sought insights about the amount of security-related work handled by IT operations. **Figure 14** illustrates the breadth of security responsibilities managed by IT operations; **figure 15** shows their normal IT activities.

Industry reporting suggests that enterprises use technical and nontechnical employees to fill shortfalls.

FIGURE 14: Security Work Performed by IT Operations

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

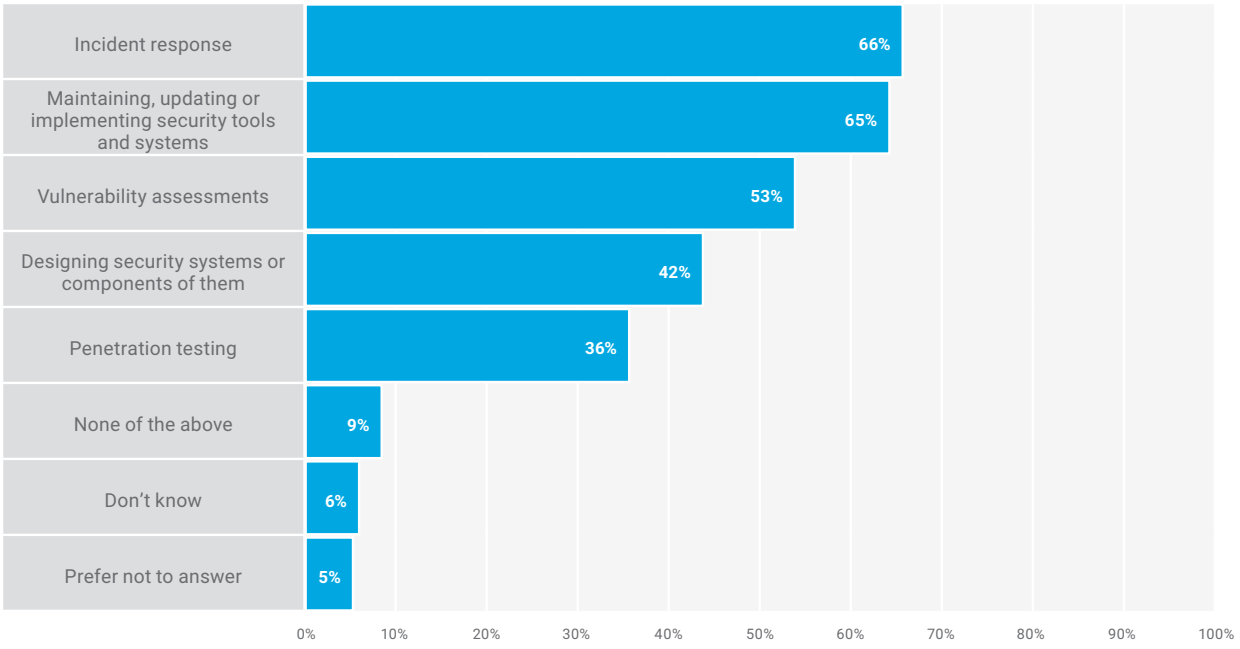
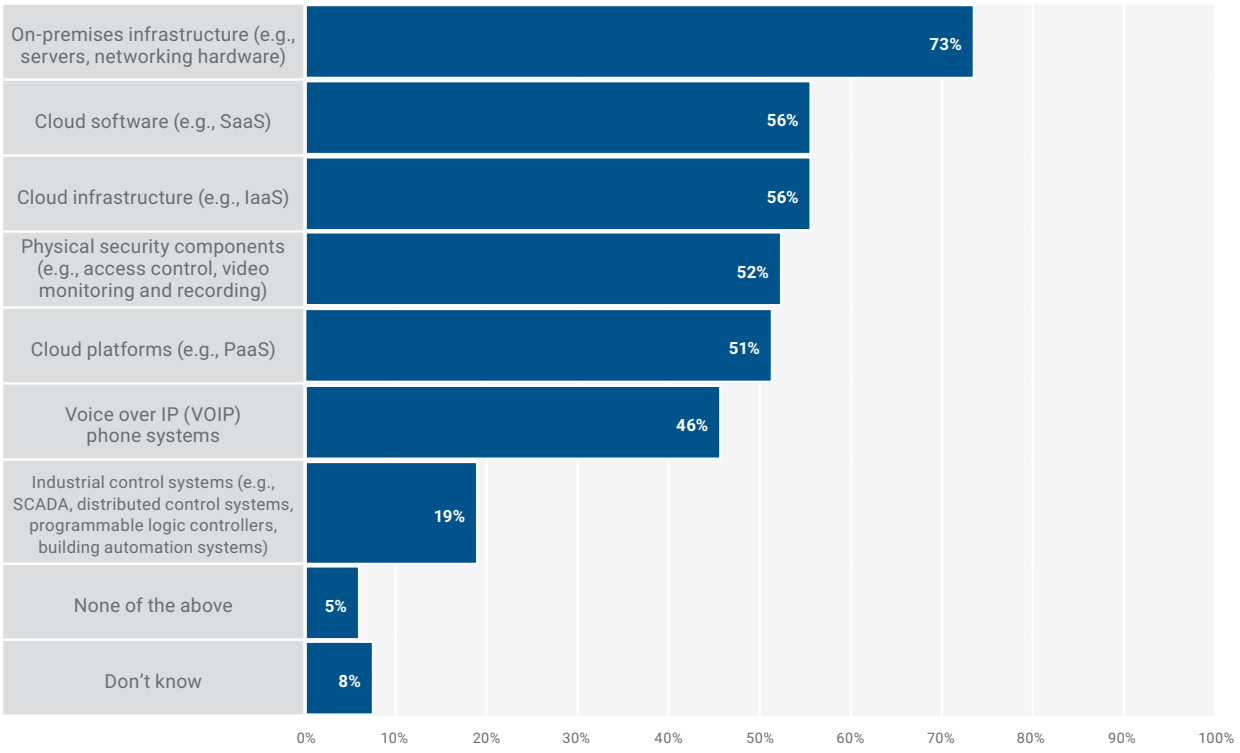


FIGURE 15: IT Operations Activity

Which, if any, of the following does your IT operations team manage or oversee? Select all that apply.



Whereas security was once a dedicated function isolated from IT operations, the colocation of work into formal network operations centers (NOCs) and security operations centers (SOCs) drives integrated response capabilities. Organizational approach and structure vary based on enterprise needs and resources.

Although it seems intuitive that smaller enterprises with few cyberresources are most disadvantaged, respondent data (**figure 16**) reveal that those enterprises with 500 to 5,000 employees are more likely to be significantly understaffed.

Nonetheless, survey responses reveal that most enterprises are performing the five major security functions in-house (**figure 17**), despite reporting that each function is somewhat understaffed (**figure 18**), which largely resembles the responses reported a year ago.

Whereas security was once a dedicated function isolated from IT operations, the colocation of work into formal network operations centers (NOCs) and security operations centers (SOCs) drives integrated response capabilities.

FIGURE 16: Organizational Staffing by Size

How would you describe the current staffing of your organization's cybersecurity team?

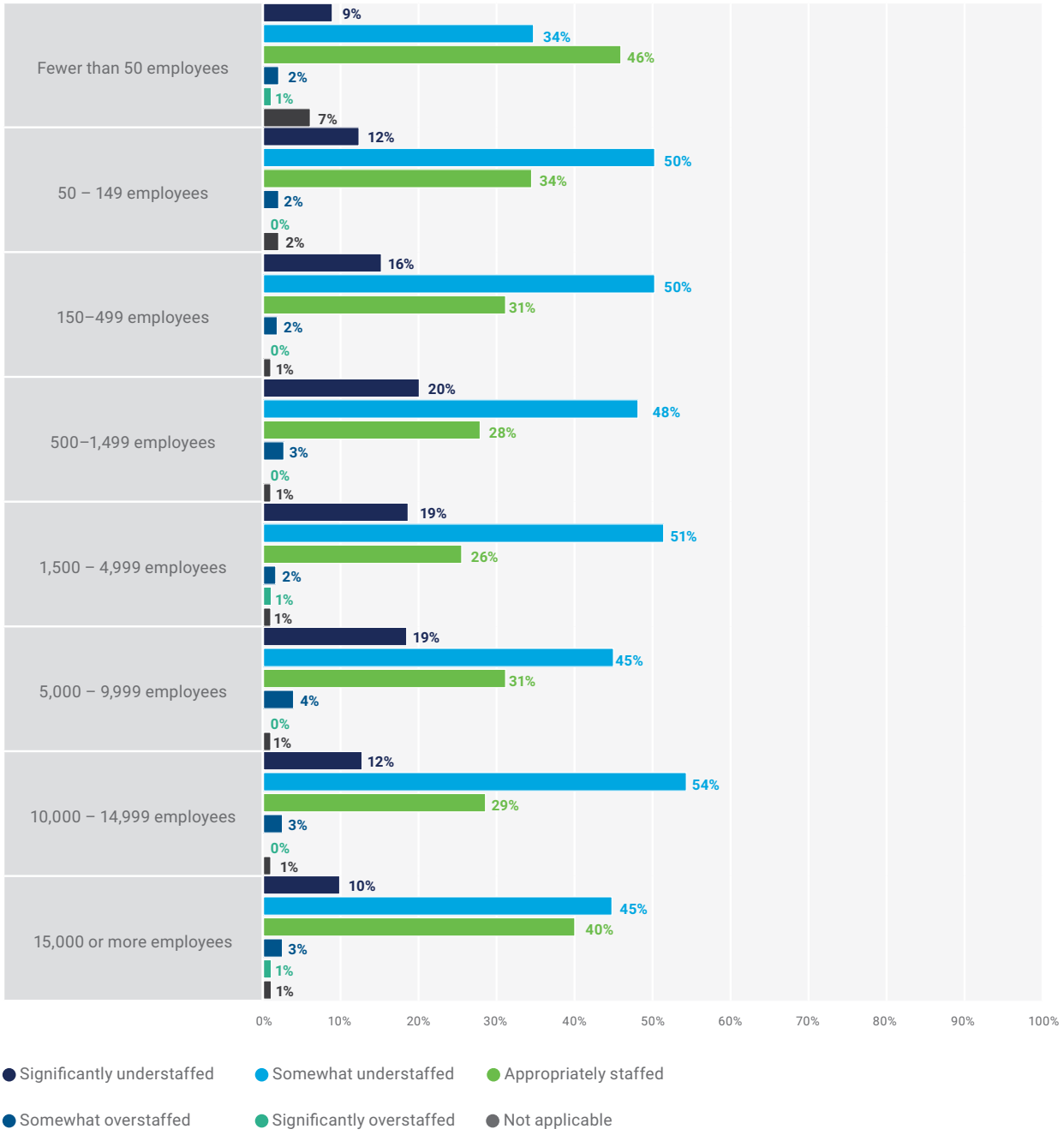


FIGURE 17: Security Function Staffing

For the following five major security functions, please indicate how they are staffed in your organization.

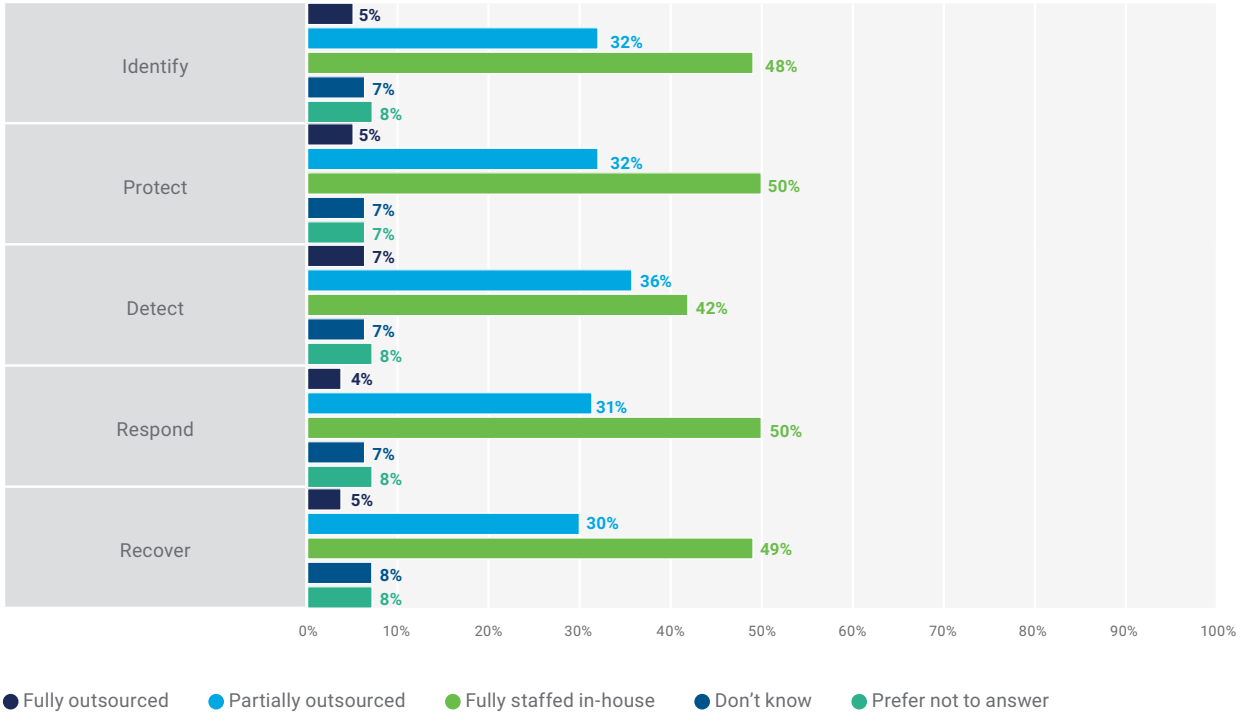
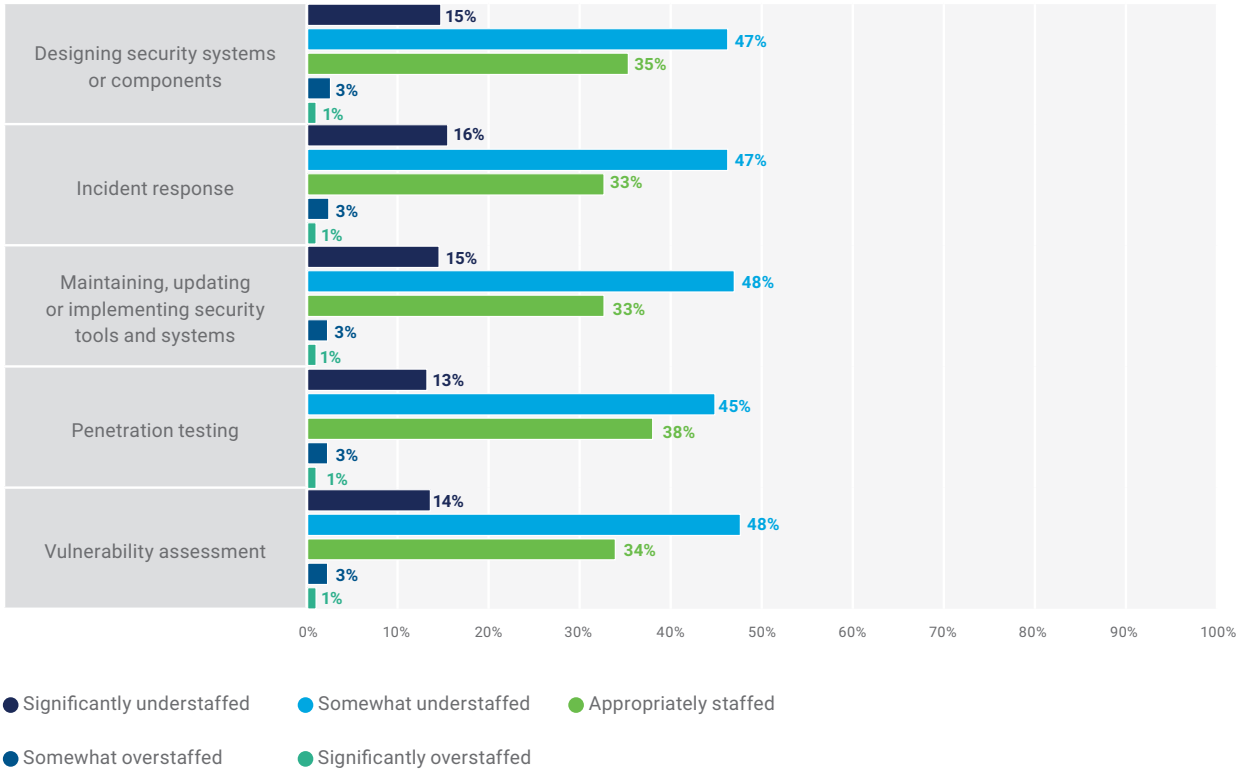


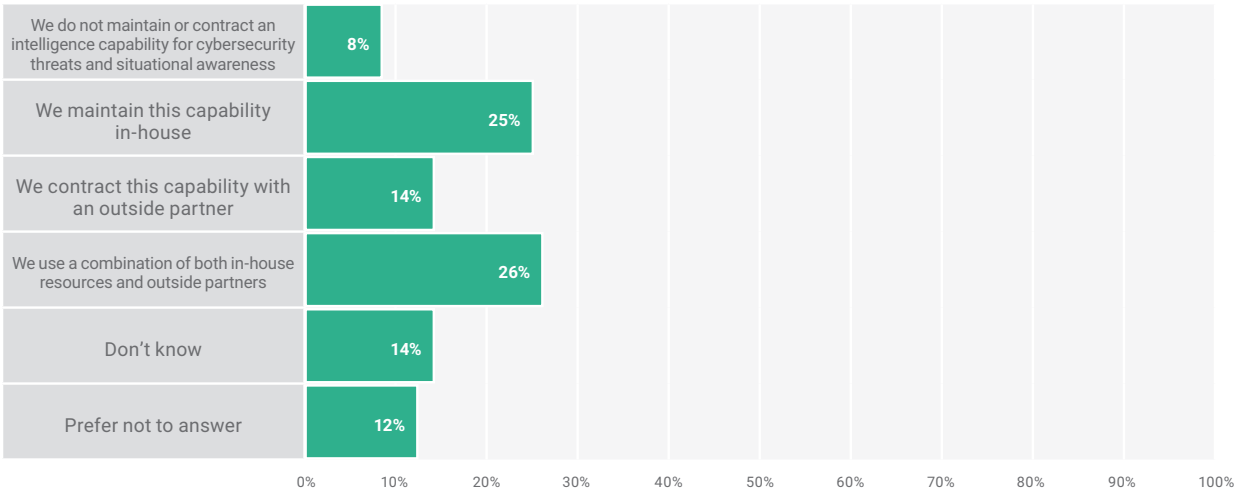
FIGURE 18: Security Staffing Levels Relative to Tasks Performed by IT Operations



Although respondent data reflect mostly in-house staffing, this varies for threat intelligence. When asked about their cybersecurity threat intelligence capability, 26 percent of respondents say that their enterprises use a combination of in-house and external resources, including services and subscriptions. An almost equal percentage of respondents (25 percent) report a wholly in-house capability for threat intelligence (**figure 19**).

FIGURE 19: Threat Intelligence Capabilities

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?



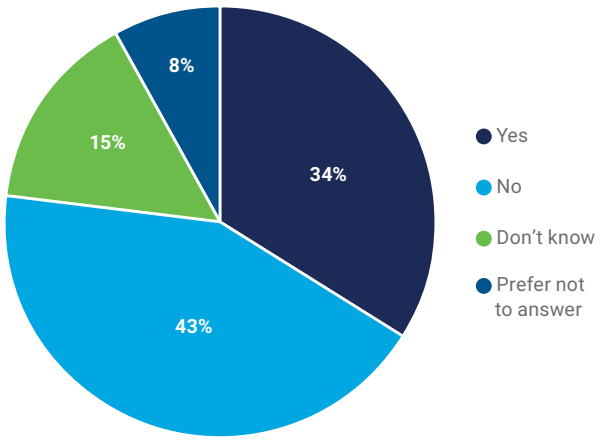
Use of artificial intelligence (AI) in security operations is increasing (**figure 20**)—up four percentage points from a year ago. Of interest here is the decline, from 12 percent last year to 8 percent this year, in the percentage of respondents who prefer not to answer this question, which may suggest that these capabilities were in research and development last year and not yet fully deployed. Regardless of the reason, it is promising that respondents are increasingly open when completing this annual survey.

How large-scale adoption alters the cybersecurity profession skills gaps will become clear as AI adoption increases. Technologies often do not replace human resources but instead shift the types of resources required. For example, AI may broadly decrease the number of analysts needed; however, human resources will be reallocated to designing, monitoring and auditing algorithms.

Technologies often do not replace human resources but instead shift the types of resources required. For example, AI may broadly decrease the number of analysts needed; however, human resources will be reallocated to designing, monitoring and auditing algorithms.

FIGURE 20: Use of AI in Security Operations

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



CISO or CIO—Does It Really Matter?

Much has been said about the importance of enterprises having a chief information security officer (CISO) and, as the role matures, to whom the CISO should report and the scope of CISO responsibilities.

Overall, reporting on the prevalence of the CISO role is scarce, with one relatively recent report highlighting that less than 70 percent of Fortune 500 enterprises employ an executive-level cybersecurity champion.[9, 10, 11]

Other notable sources highlight CISO compensation, roles, responsibilities and challenges but offer little insight into CISO staffing.[12, 13] Unfortunately, many businesses and industries learn the hard way that security cannot be merely bolted on with any expectation of success; therefore, more enterprises are likely to proactively formalize the role.

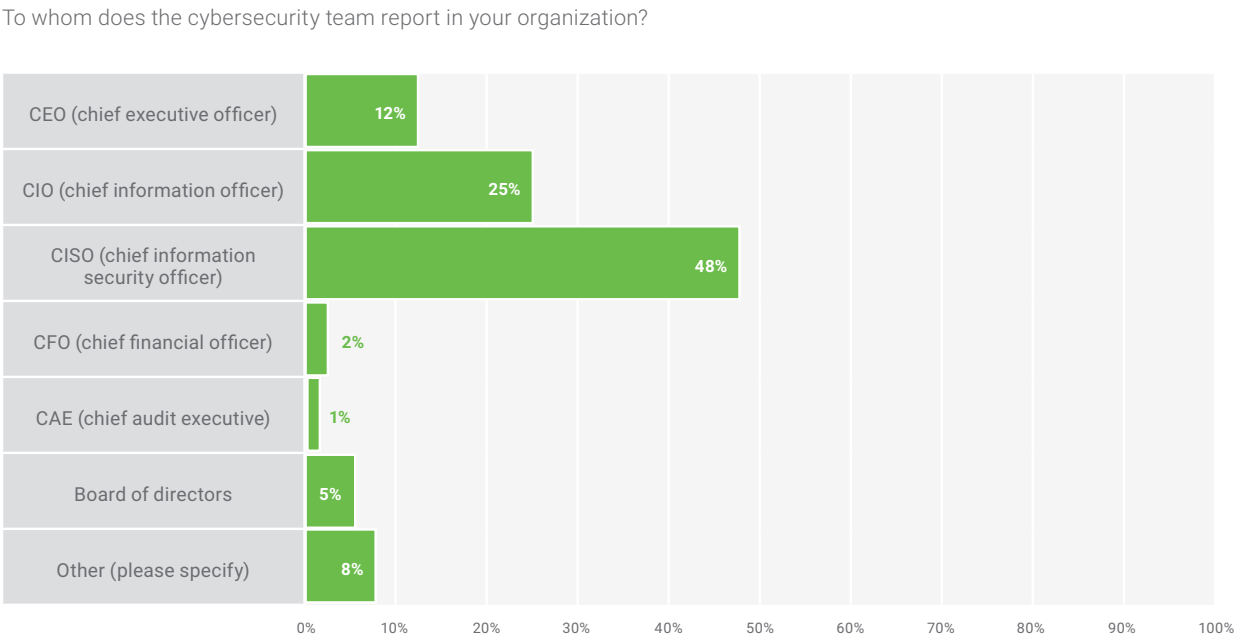
In the past, enterprise size was a primary factor in determining whether to add a CISO to the executive lineup, but regulatory requirements, industry, locale and corporate prioritization of security are also factors.

As **figure 21** shows, respondents largely indicate that their cybersecurity team reports to a CISO (48 percent); however, one in four respondents indicates that the cybersecurity team reports to the chief information officer (CIO).

Note the possibility that some enterprises whose cybersecurity teams report to a CIO also have a CISO who reports to the CIO rather than to another corporate executive. In the past, enterprise size was a primary factor in determining whether to add a CISO to the executive lineup, but regulatory requirements, industry, locale and corporate prioritization of security are also factors.[14]

[9] Morgan, S.; "CISO 500 Demographic Study Announced by Cybersecurity Ventures," Cybercrime Magazine, 17 February 2020, https://cybersecurityventures.com/ciso-500-demographic-study/
[10] Bitglass, "Bitglass Fortune 500 Cybersecurity Report: Leading Companies Failing to Demonstrate Commitment to Cybersecurity," 30 September 2019, www.bitglass.com/press-releases/bitglass-report-fortune-500-cybersecurity
[11] CISOMAG, "45% companies don't have cybersecurity leader: Study," 11 December 2017, https://cisomag.eccouncil.org/45-companies-dont-cybersecurity-leader-study/
[12] Cynet, "2021 Survey of CISOs with Small Security Teams: The Push for More Usable Cybersecurity Technologies," https://www.cynet.com/blog/2021-survey-CISOs-with-small-security-teams
[13] Aiello, M.; S. Thompson; "2020 North American Chief Information Security Officer (CISO) Compensation Survey," Heidrick & Struggles, www.heidrick.com/en/insights/cybersecurity/2020_north_american_chief_information_security_officer_ciso_compensation_survey
[14] Howlett, T.; "Do midsized companies need a CISO?" Security Boulevard, 13 January 2020, https://securityboulevard.com/2020/01/do-midsized-companies-need-a-ciso-3/

FIGURE 21: Cybersecurity Function Reporting



ISACA explores the relationship between the executive to whom enterprise cybersecurity teams report and the relevance of that position to perceived executive value and prioritization of security operations.

Respondent data reveal no strong differences between security function ownership (CISO or CIO) and the following:

- Organizational views on increased or decreased cyberattacks
- Confidence levels related to detecting and responding to cyberthreats
- Perceptions on cybercrime reporting

However, security function ownership (CISO or CIO) is related to notable differences regarding executive valuation of cyberrisk assessments (**figure 22**), board of director prioritization of cybersecurity (**figure 23**) and strategic alignment (**figure 24**).

Of interest is an increase in the industry practice whereby the CISO reports to anyone other than the CIO, especially when the CISO's scope includes governance, risk and compliance (GRC); business continuity/disaster recovery; fraud; trust; and safety or crisis management.[15]

Although the CISO's focus varies greatly by industry, security is no longer thought of as just an IT function, and CISOs largely report directly to the board of directors and/or audit committee.[16]

Of interest is an increase in the industry practice whereby the CISO reports to anyone other than the CIO, especially when the CISO's scope includes governance, risk and compliance (GRC); business continuity/disaster recovery; fraud; trust; and safety or crisis management.

[15] *Op cit* Aiello
[16] *Ibid.*

FIGURE 22: Executive Valuation of Cybersecurity Assessments by Overseer

Does your executive leadership team see value in conducting a cyberrisk assessment?

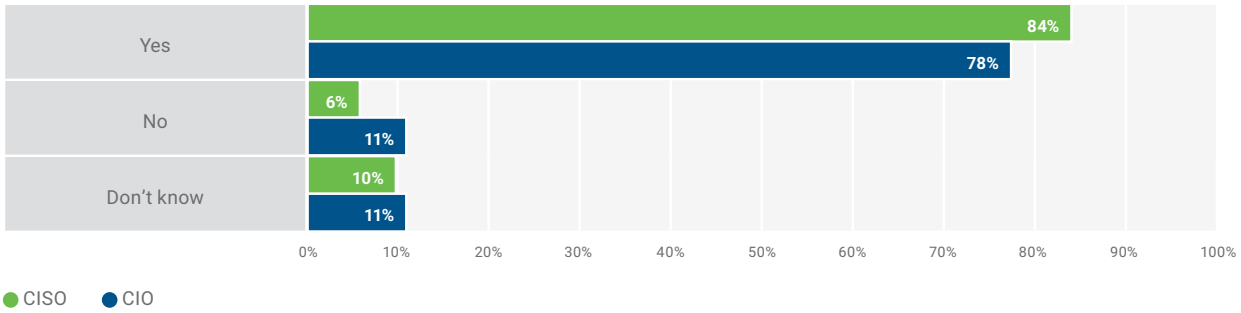


FIGURE 23: Board of Directors Prioritization of Cybersecurity by Overseer

Do you believe that your board of directors has adequately prioritized organization cybersecurity?

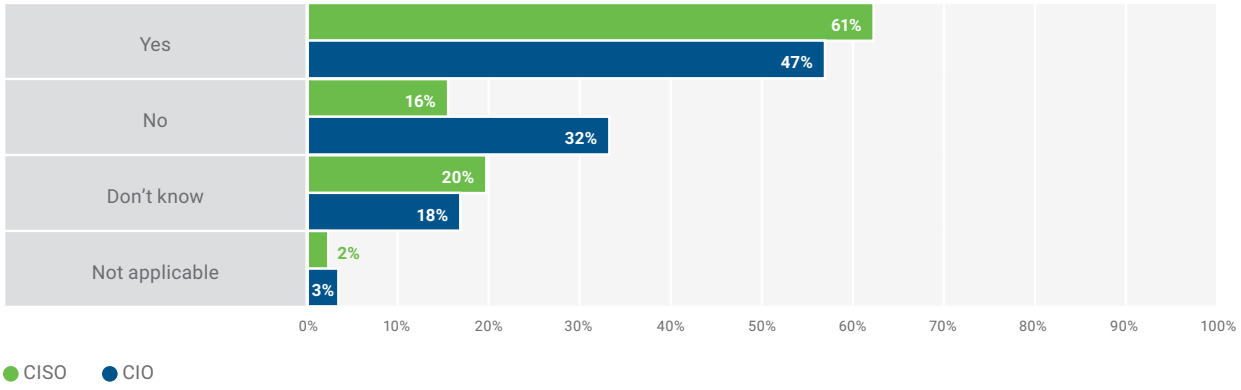
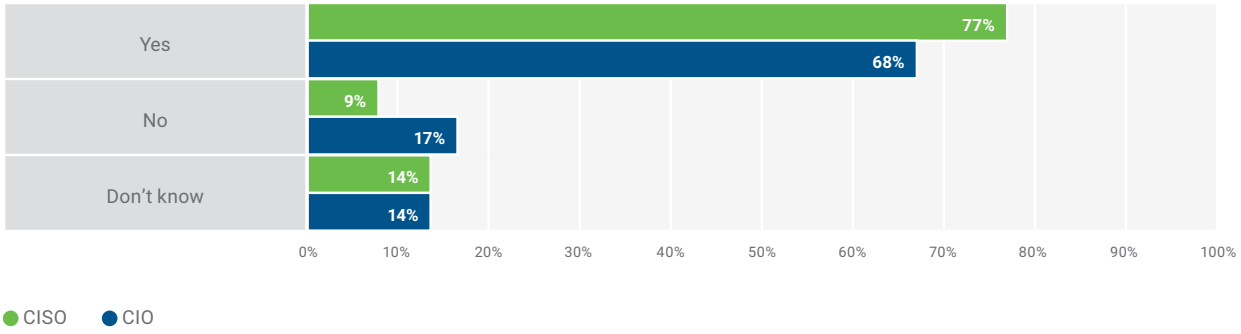


FIGURE 24: Strategic Alignment Between Cybersecurity and Enterprise Objectives

Is your organization's cybersecurity strategy aligned with your organizational objectives?



Cybersecurity Maturity Is a Business Imperative

In business, maturity indicates the degree of reliability or dependability that a process will achieve the desired goals or objectives. Given the ever-growing cyberthreat landscape, enterprises must be able to determine and subsequently communicate the effectiveness of their security investments.

With cybersecurity budgets showing signs of leveling (**figure 25**), it is prudent for cybersecurity leaders to empower data-driven decision making when assessing or adjusting security program components. This year, ISACA expanded the topics covered in its annual survey to glean insights about this important, yet often elusive, aspect of business survival.

Sixty-five percent of enterprises assess their cybermaturity (**figure 26**). Those that perform these assessments are more likely to have appropriately staffed security teams and are more likely to report appropriately funded cybersecurity budgets. Furthermore, respondents with a pulse on security program measurement and maturity are more than two times more confident in the ability of their organization to detect and respond to cyberattacks.

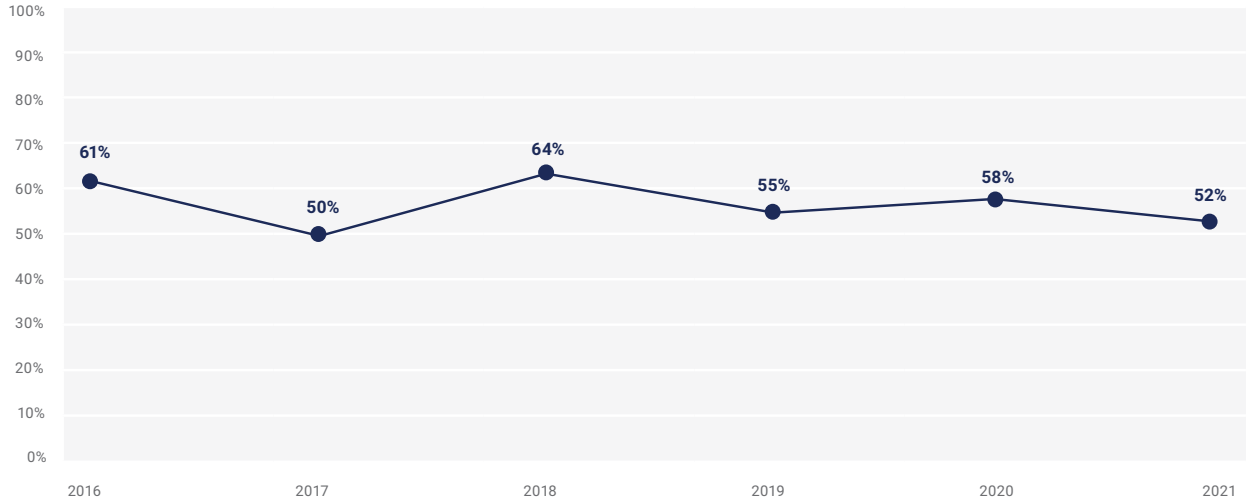
Given the ever-growing cyberthreat landscape, enterprises must be able to determine and subsequently communicate the effectiveness of their security investments.

Assessing cybermaturity is not without its challenges. The top three obstacles that respondents identify are (**figure 27**):

- Challenge of integrating risk with maturity and keeping up with industry threats and trends (30 percent)
- Difficulty differentiating maturity from compliance to management (29 percent)
- Organizational expertise necessary to understand and assess maturity (27 percent)

The survey results do not imply that executive leadership does not value cyberrisk assessments, because leadership overwhelmingly does value this assessment (**figure 28**).

FIGURE 25: Forecasted Security Budget Increases



However, perceived value does not necessarily translate to attentiveness—39 percent of respondent enterprises perform cyberrisk assessments annually, which hardly seems prudent, given an ever-changing threat landscape. To be fair, organizational size and resource challenges, such as sufficient workforce, skills gaps, time and money, can limit some enterprises to annual assessments. Given that an overwhelming 76 percent of respondents cite regulatory compliance as the primary driver for conducting cyberrisk assessments (**figure 29**), one must consider the likelihood that a compliance-based mind-set prevails over the more appropriate risk-based approach to cybersecurity.

FIGURE 26: Assessing Cybermaturity

Does your organization currently assess its cybermaturity?

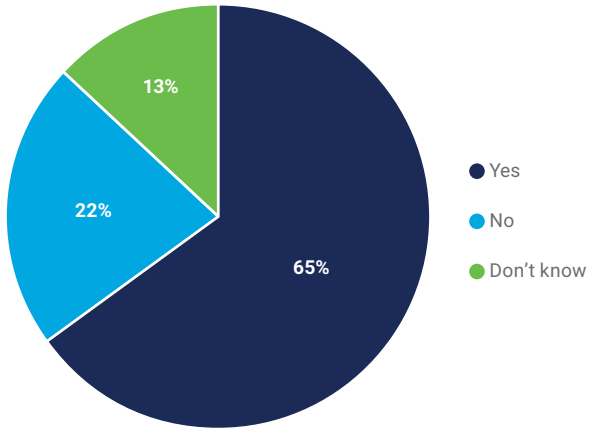


FIGURE 27: Obstacles to Defining Organizational Cybermaturity

Which, if any, of the following are obstacles to defining the cybermaturity of your organization? Select all that apply.

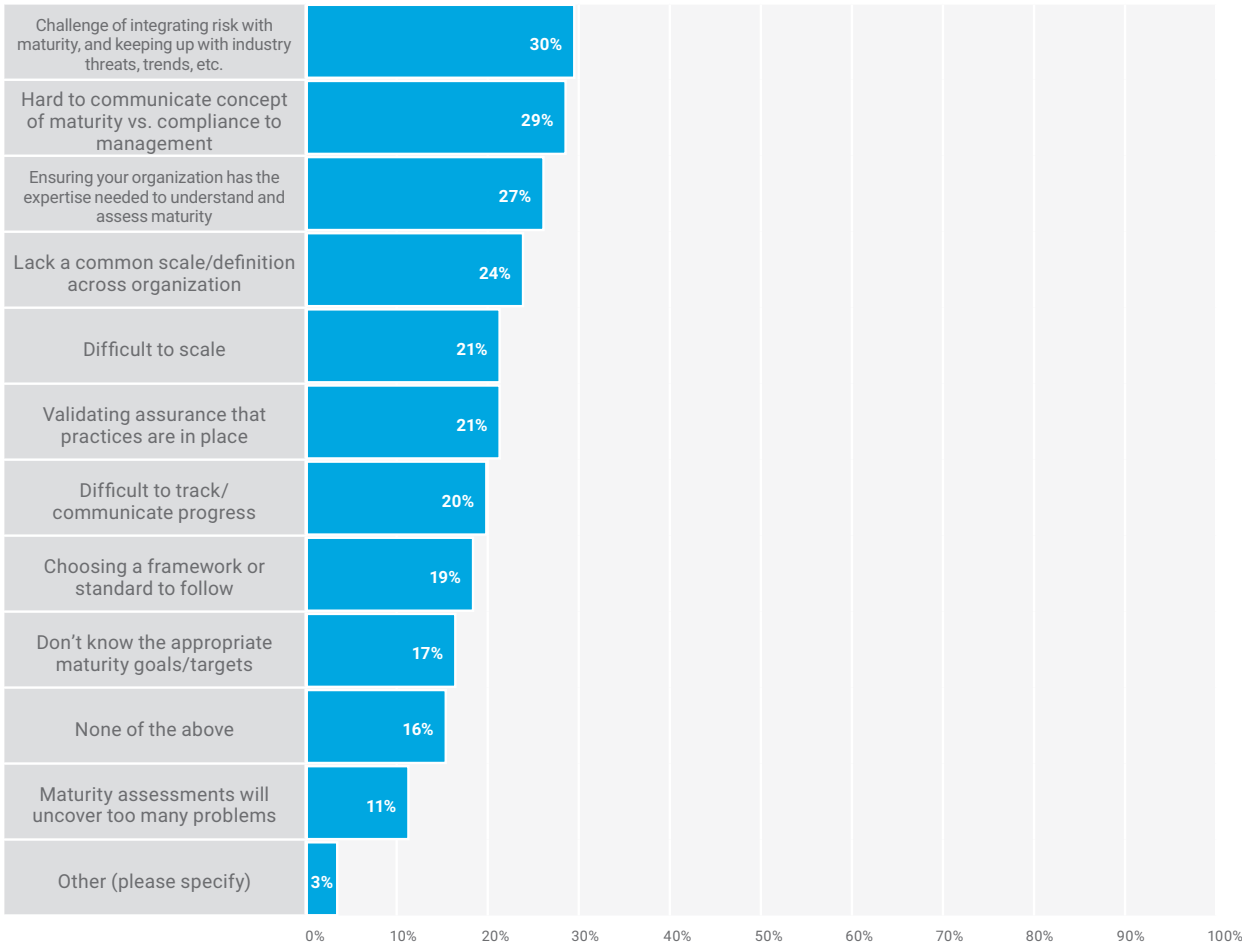


FIGURE 28: Executive Leadership Valuation of Cyberrisk Assessments

Does your executive leadership team see value in conducting a cyberrisk assessment?

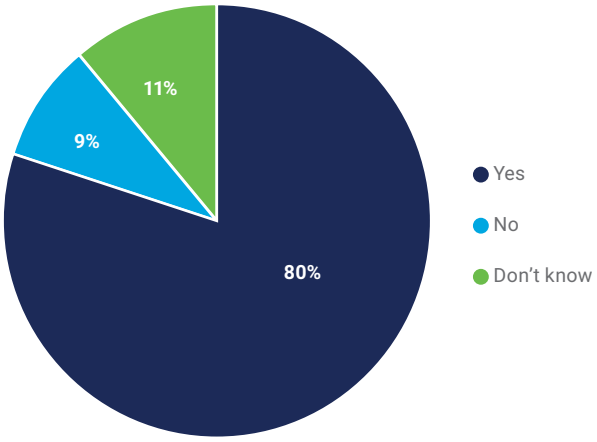
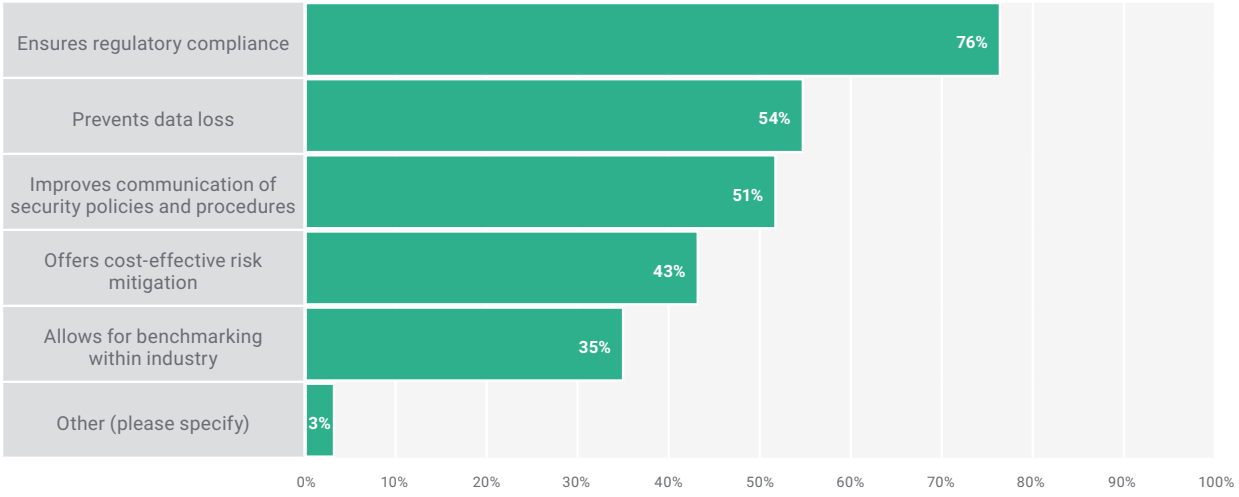


FIGURE 29: Cyberrisk Assessment Drivers

Why does your organization conduct a cyberrisk assessment? Select all that apply.



Conclusion—Business as Usual Is Not Working

Change is ever present for cybersecurity professionals who partner daily with business leaders to meet organizational goals amid growing regulatory requirements and a fluid threat landscape. Much has already changed since ISACA collected these data at the end of 2020. High-profile cyberattacks, including those affecting SolarWinds, Microsoft and Colonial Pipeline, thrust cybersecurity to the forefront for government and business leaders, who have already prompted regulatory changes. Undoubtedly, there will be more.

This year's *State of Cybersecurity Survey* data reveal that COVID-19 is not substantially altering security plans and investments, which suggests that cybersecurity leadership did not panic when a global pandemic disrupted business-as-usual thinking and fundamentally altered where work is predominantly done. The current survey data show that enterprise IT operations absorbed some security tasks, and the C-suite leader to whom a security team reports has tangible influence at a strategic level but not at the tactical level. Finally, although the importance of assessing cybersecurity maturity is unquestioned, it has notable challenges—including integrating risk and maturity, explaining how cybersecurity maturity assessment differs from compliance, and obtaining the necessary organizational resources.

Acknowledgments

ISACA would like to recognize:

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

John De Santis
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE
Chief Information Security Officer, UNOPS, Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, 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 that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 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. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

About HCL

HCL Technologies (HCL) empowers global enterprises with technology for the next decade, today. HCL's Mode 1-2-3 strategy, based on its deep-domain industry expertise, client-centricity and entrepreneurial culture of Ideapreneurship™, enables businesses to transform into next-gen enterprises. HCL offers its services and products through three business units: IT and Business Services (ITBS), Engineering and R&D Services (ERS) and Products & Platforms (P&P). ITBS enables global enterprises to transform their businesses through offerings in the areas of applications, infrastructure, digital process operations and next generation digital transformation solutions. ERS offers engineering services and solutions in all aspects of product development and platform engineering. P&P provides modernized software products to global clients for their technology and industry specific requirements. Through its cutting-edge co-innovation labs, global delivery capabilities and broad global network, HCL delivers holistic services in various industry verticals, categorized as Financial Services, Manufacturing, Technology and Services, Telecom and Media, Retail and CPG, Life Sciences and Healthcare, and Public Services. As a leading global technology company, HCL takes pride in its diversity, social responsibility, sustainability, and education initiatives. For the 12 months ended Dec. 31, 2020 HCL had consolidated revenue of US$10.02 billion. Its 159,682 Ideapreneurs operate out of 50 countries. For more information, visit www.hcltech.com.

DISCLAIMER

ISACA has designed and created *State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity* (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-2021

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/

CyberSecurity & GRC Services
by HCL Technologies

HCL

Inspiring business confidence through **dynamic cybersecurity**

Leader

Rated as a Leader by six leading industry analyst reports in FY'21 (Everest, ISG, Avasant)

6 CSFCs +
40 GDCs

450+
Global Customers

4500+
Experienced & Certified Engineers

for more info: **Cybersecurity-GRC@hcl.com**

www.hcltech.com