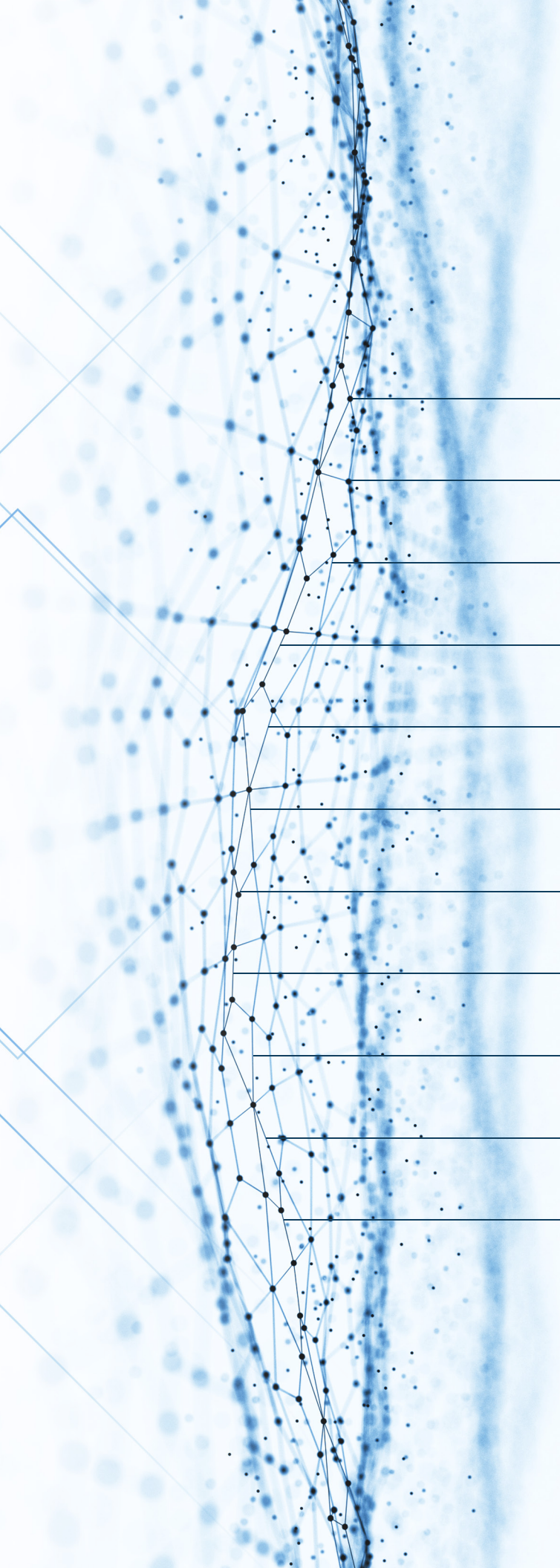
THE STATE OF CYBER SECURITY IN THE FINANCIAL INSTITUTION INDUSTRY

2021 SURVEY REPORT

Tandem™



Contents

About this Report

Tandem surveyed cybersecurity professionals working in the financial institution industry. The goal of the survey was to discover:

- Information about the Board of Directors' involvement in the institution's cybersecurity program.
- How institutions manage cybersecurity and what financial resources are provided to increase security posture.
- Training standards and best practices across the industry.
- The effectiveness of implemented best practices.
- How financial institutions manage incident response.
- Trends in cybersecurity and IT management being implemented by financial institutions.

The survey was conducted from November 1, 2020 to April 30, 2021 and generated 237 responses. All respondents are based in the United States.

Percentages were rounded to the nearest whole number. Not all percentage totals in this report equal 100%, as only significant answer options are represented in the findings.

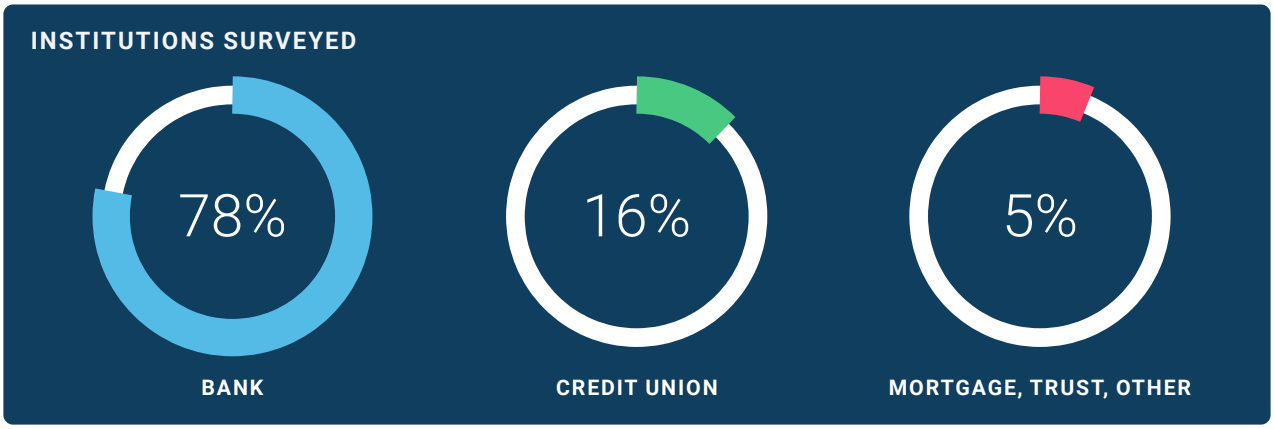
When applicable, answers were also compared with historical data for context. If you would like to participate in the next survey, visit https://tandem.app/survey-sign-up.

The survey was conducted by Tandem, LLC. For more information about Tandem, see page 29.

Demographics

TYPES OF INSTITUTIONS

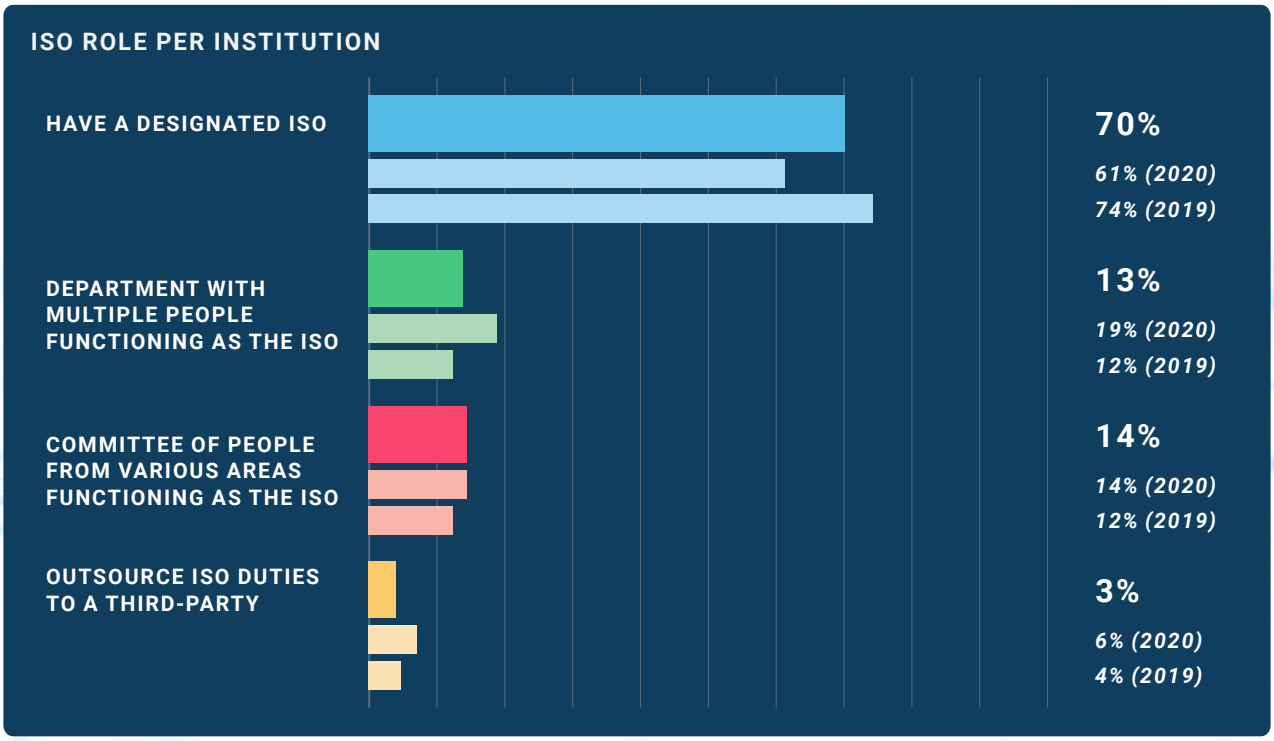
Of those who responded, 78% worked for a bank, 16% worked for a credit union, and the remaining respondents worked for other financial institutions such as mortgage companies or trust companies.



As shown, the collected data most significantly represents professionals working for banks.

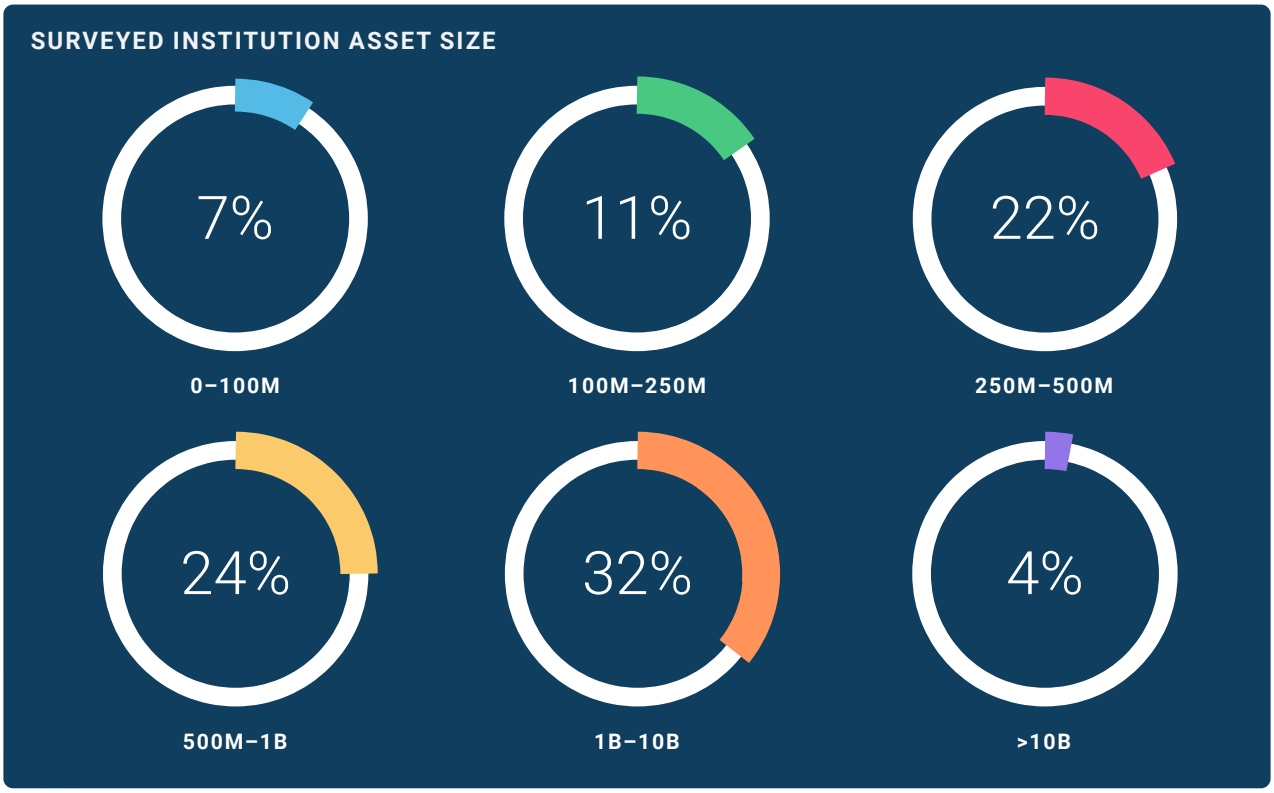
INFORMATION SECURITY OFFICER (ISO) ROLE

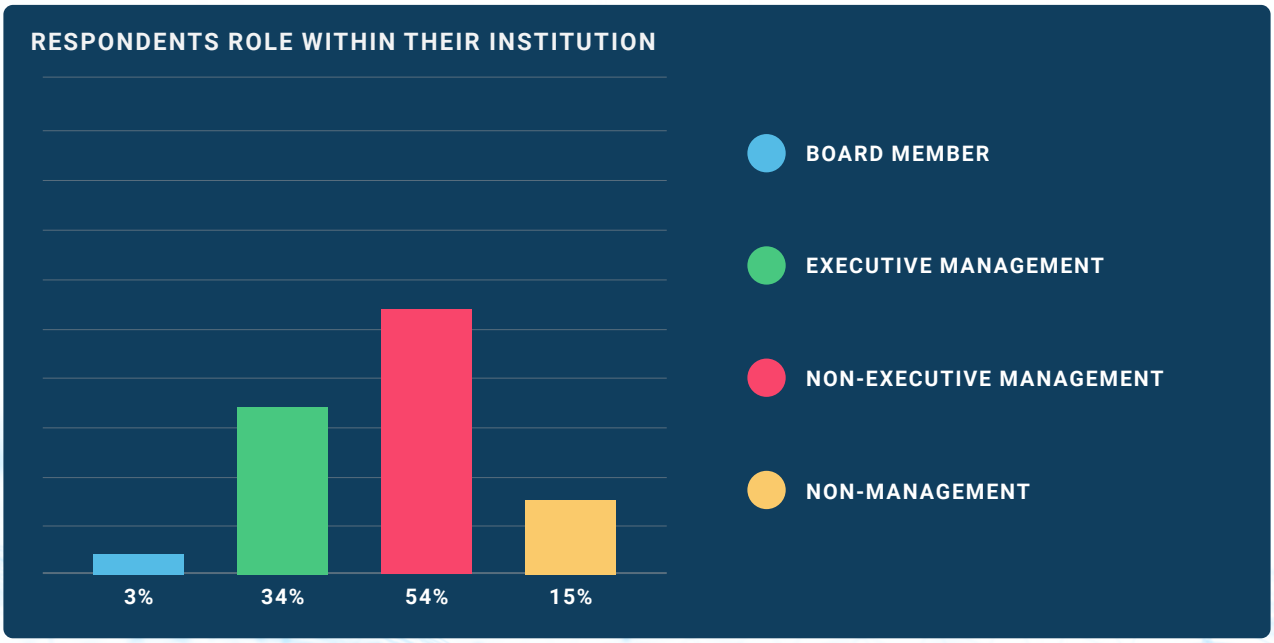
The survey defined cybersecurity as a subset of information security; therefore, for consistency and simplicity, the survey does not differentiate between the role of Cybersecurity Officer and Information Security Officer.



ASSET SIZE OF INSTITUTIONS SURVEYED

The majority of respondents were from regional community banks, but a strong representation are from larger community institutions, with 36% of responding institutions' asset sizes $1B+.



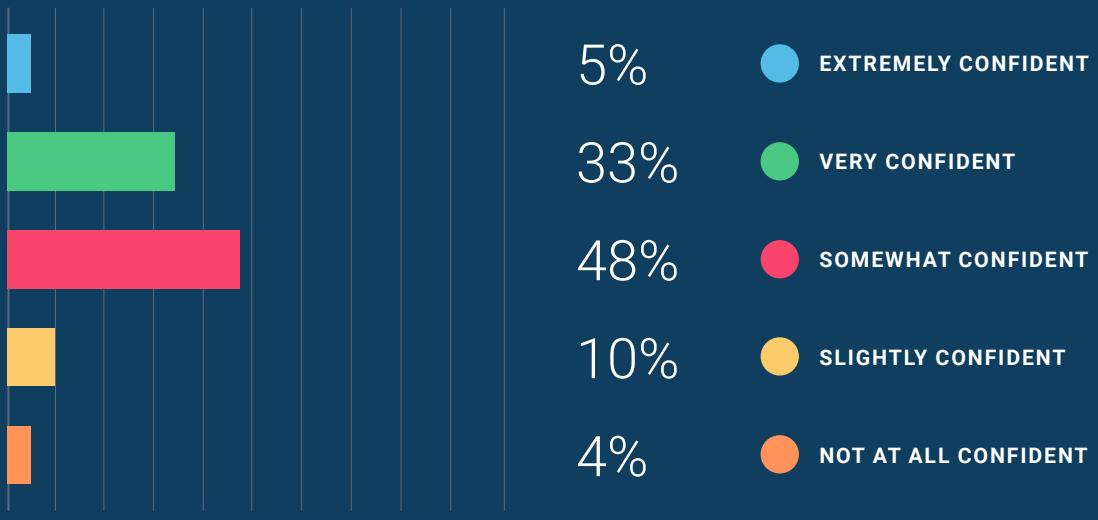


Board Oversight in Financial Institutions

BOARD OVERSIGHT FINDINGS

INSTITUTIONS WITH BOARD MEMBERS WHO HAVE EXPERIENCE IN CYBERSECURITY OR IT

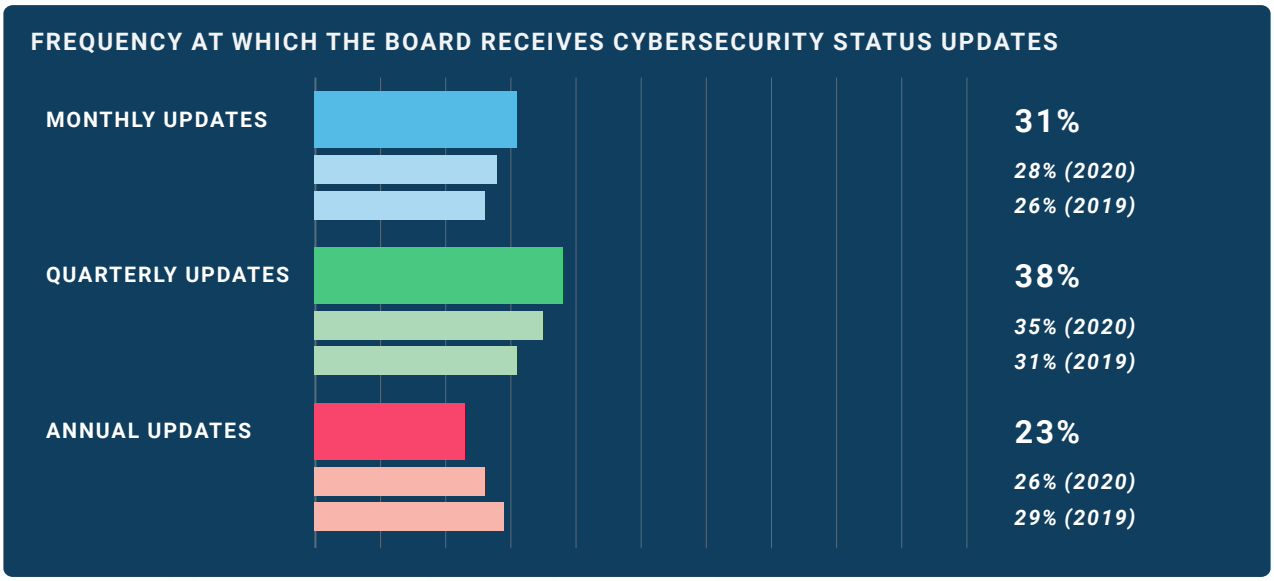
CONFIDENCE IN BOARD OF DIRECTORS' UNDERSTANDING OF THE INSTITUTION'S CYBERSECURITY POSTURE



INSTITUTIONS WHERE BOARD MEMBERS HAVE SET A CYBERSECURITY RISK APPETITE

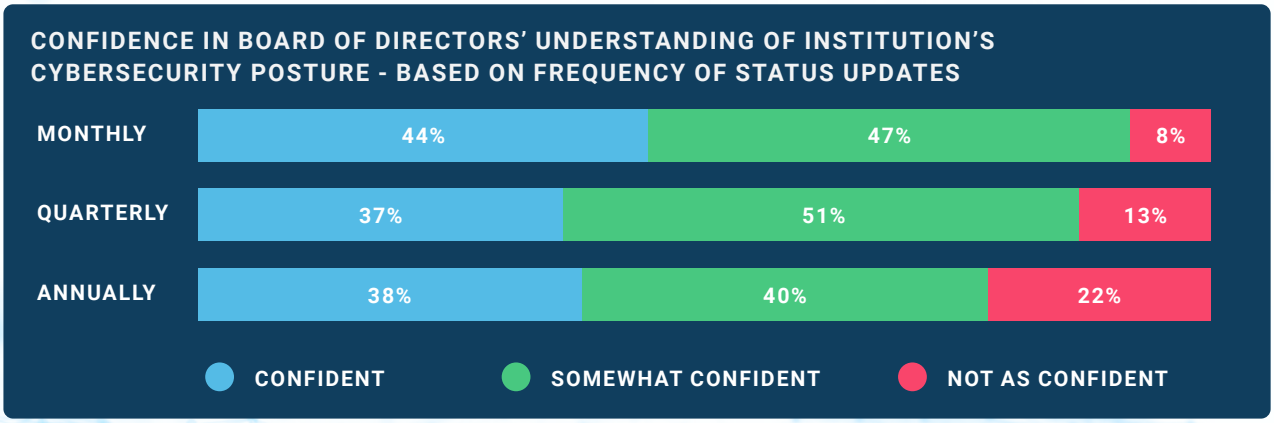
SIGNIFICANT FINDING

When we asked how frequently the Board receives updates on the institution's cybersecurity status, the results showed the majority of respondents (68%) update their Board quarterly or monthly. Over the past three years, there has been a shift toward providing cybersecurity updates to the Board more frequently.



DIVING FURTHER

Institutions who provide monthly updates to the Board of Directors are more likely to have a higher confidence in the Board's understanding of the institution's cybersecurity posture. Additionally, one-in-five institutions who provide annual updates to the Board of Directors are not confident in their Board's understanding of the institution's cybersecurity posture.



TAKEAWAY

Providing more frequent updates to the Board of Directors seems to be a mutually beneficial arrangement. As the Board becomes more aware of the institution's cybersecurity posture, confidence in their understanding of cybersecurity matters also increases.

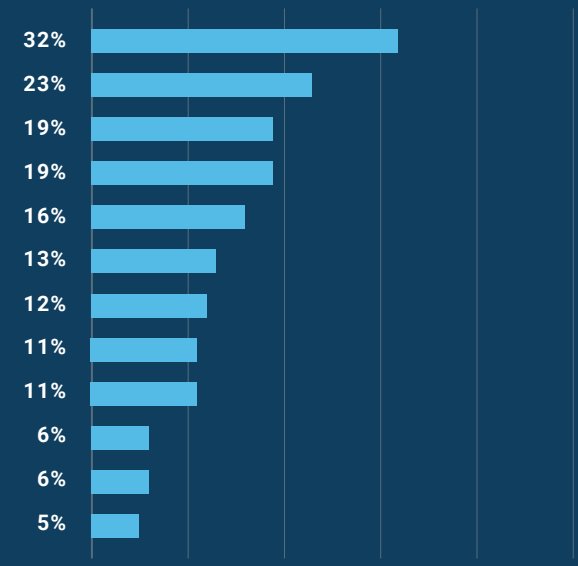
ISO Management and Staffing

ISO MANAGEMENT AND STAFFING FINDINGS

INSTITUTIONS OUTSOURCING THEIR CYBERSECURITY PROGRAM

- COMPLETELY MANAGED IN-HOUSE (22%)
- MANAGED IN-HOUSE WITH SUPPORT FROM THIRD-PARTIES (64%)
- MANAGED BY A THIRD-PARTY WITH SUPPORT FROM IN-HOUSE (14%)
- COMPLETELY MANAGED BY A THIRD-PARTY (1%)

DEGREES OR CERTIFICATIONS HELD BY ISO OR MEMBERS OF INSTITUTION'S ISO COMMITTEE

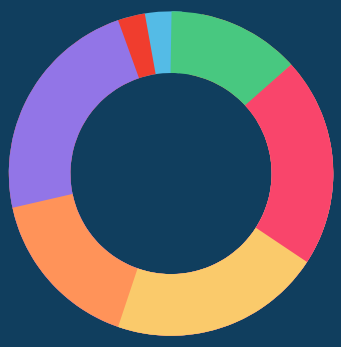


32%	BACHELOR DEGREE OUTSIDE OF IT OR CYBERSECURITY
23%	BACHELOR DEGREE IN IT OR CYBERSECURITY
19%	CISSP (ISC)2
19%	NONE
16%	SECURITY+ (COMPTIA)
13%	OTHER
12%	CISA (ISACA)
11%	MASTER DEGREE OUTSIDE OF IT OR CYBERSECURITY
11%	CISM (ISACA)
6%	MASTER DEGREE IN IT OR CYBERSECURITY
6%	CERTIFIED ETHICAL HACKER (CEH)
5%	CRISC (ISACA)

Displayed on a 50% maximum scale

**Respondents were asked to choose all that apply*

YEARS OF EXPERIENCE FOR THE INSTITUTION'S ISO



- 0 – 1 YEAR (4%)
- 2 – 5 YEARS (13%)
- 6 – 10 YEARS (21%)
- 11 – 15 YEARS (21%)
- 16 – 20 YEARS (14%)
- 21+ YEARS (21%)
- NOT APPLICABLE (5%)

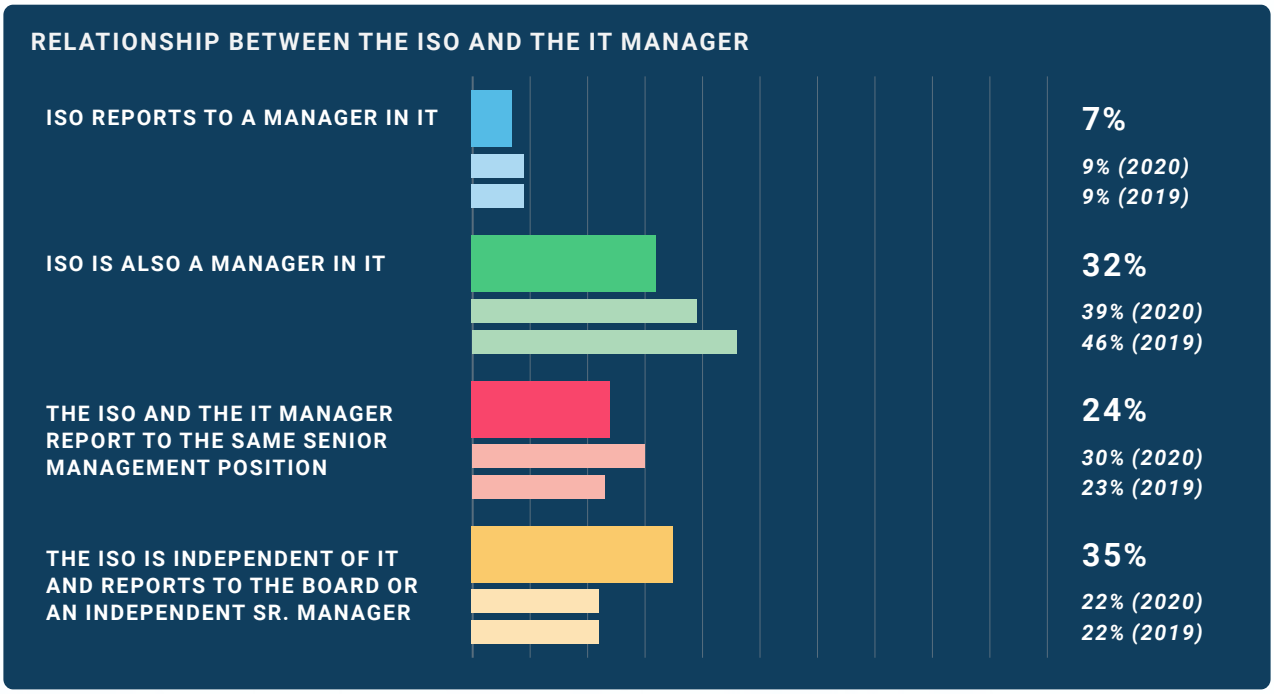
CYBERSECURITY ADDRESSED IN INSTITUTION'S STRATEGIC PLAN

YES

NO

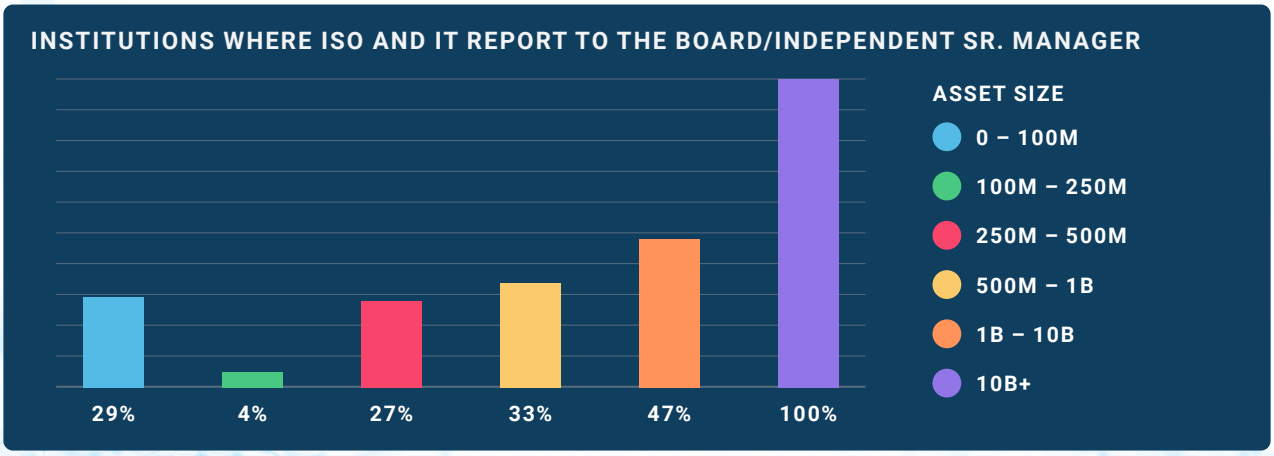
SIGNIFICANT FINDING

When we asked about the relationship between the ISO and the IT manager, the results showed that 35% of ISOs are independent from IT and report to an independent senior manager. This separation between the two responsibilities has increased considerably since 2019.



DIVING FURTHER

Larger institutions are more likely to structure their organization so that the ISO and IT report to the Board or to an independent senior manager.

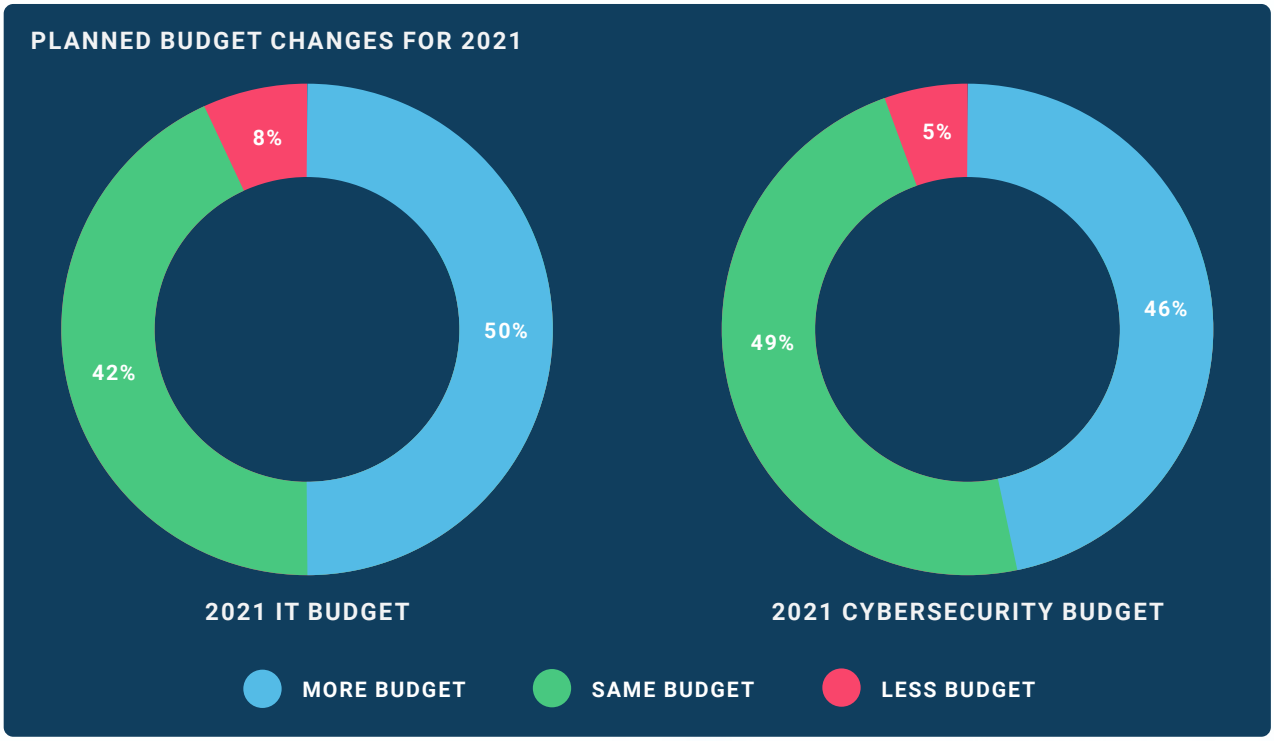


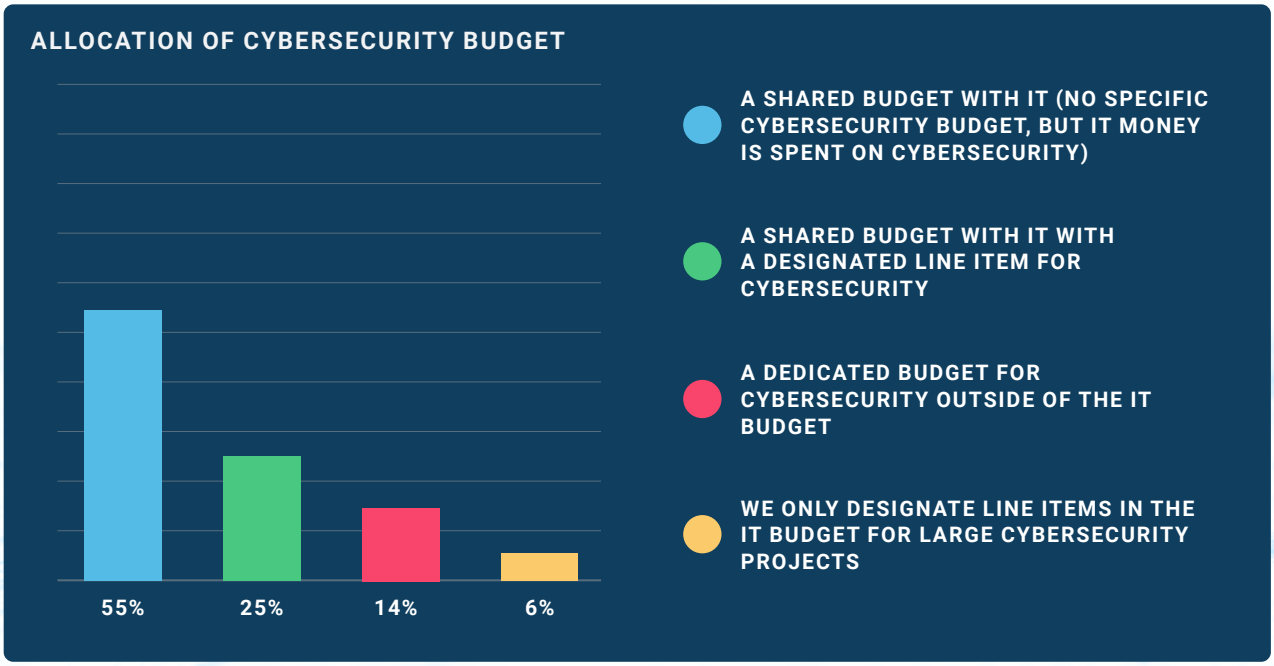
TAKEAWAY

The overlap in expertise and resources needed to support both IT and information security can make it difficult to justify the separation of these two functions. While smaller organizations particularly struggle with the cost of separating IT and information security, they should weigh the improved ability to reach the organization's strategic goals through this delineation.

Budgeting

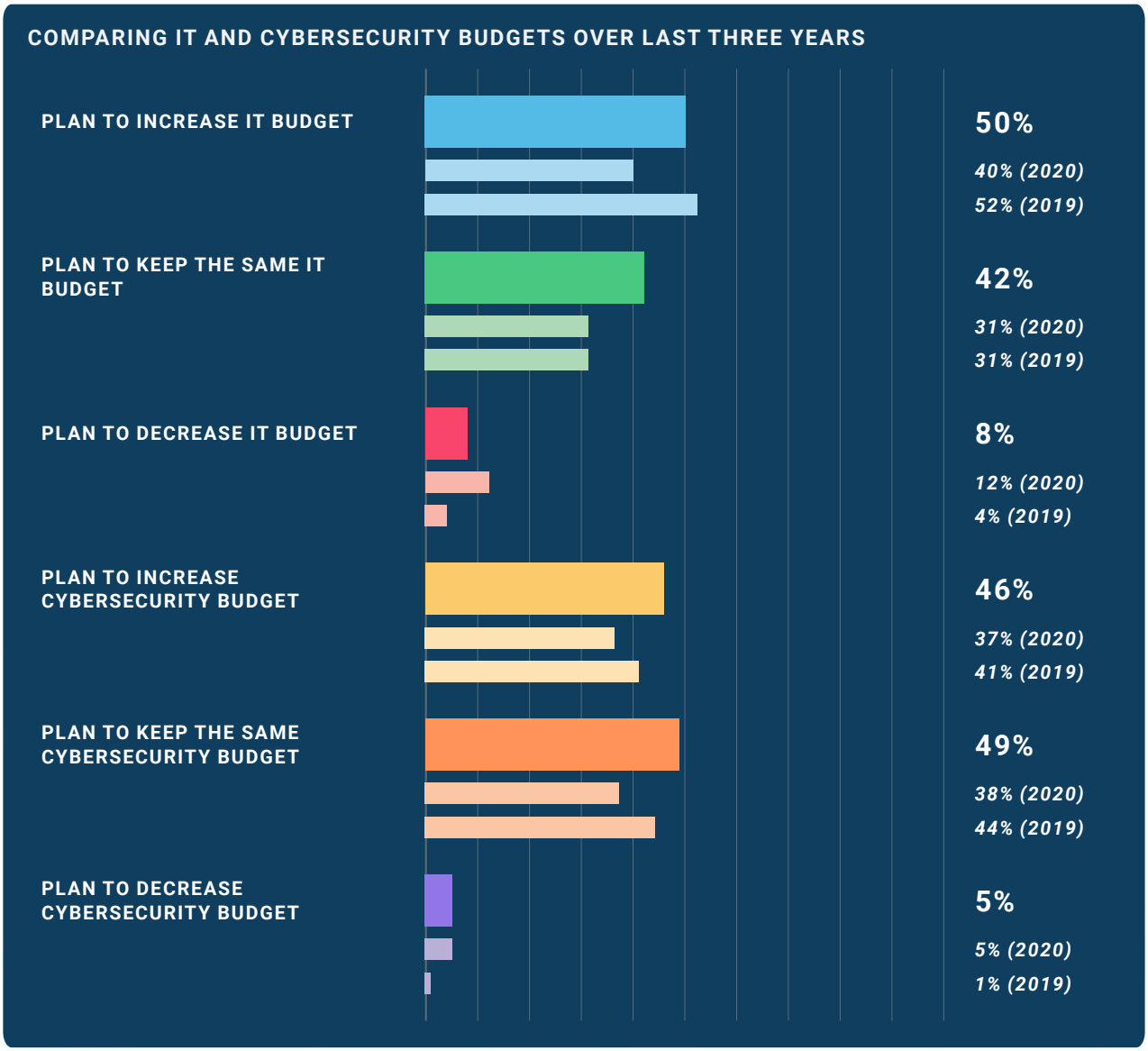
BUDGETING FINDINGS





SIGNIFICANT FINDING

When we asked about budgeting, the results showed that approximately 50% of institutions plan to increase their IT budget in 2021, and 46% plan to increase their cybersecurity spending. These metrics are in line with previous years.



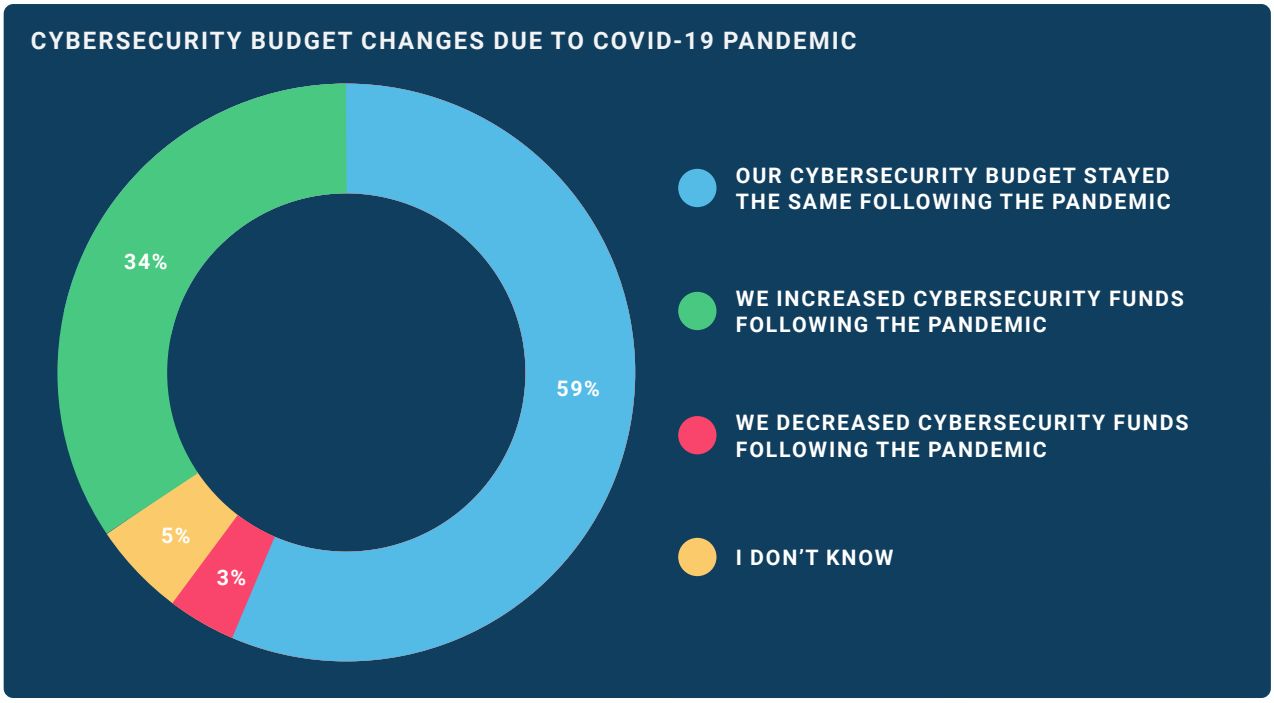
BUDGETING CONTINUED ON NEXT PAGE

Budgeting

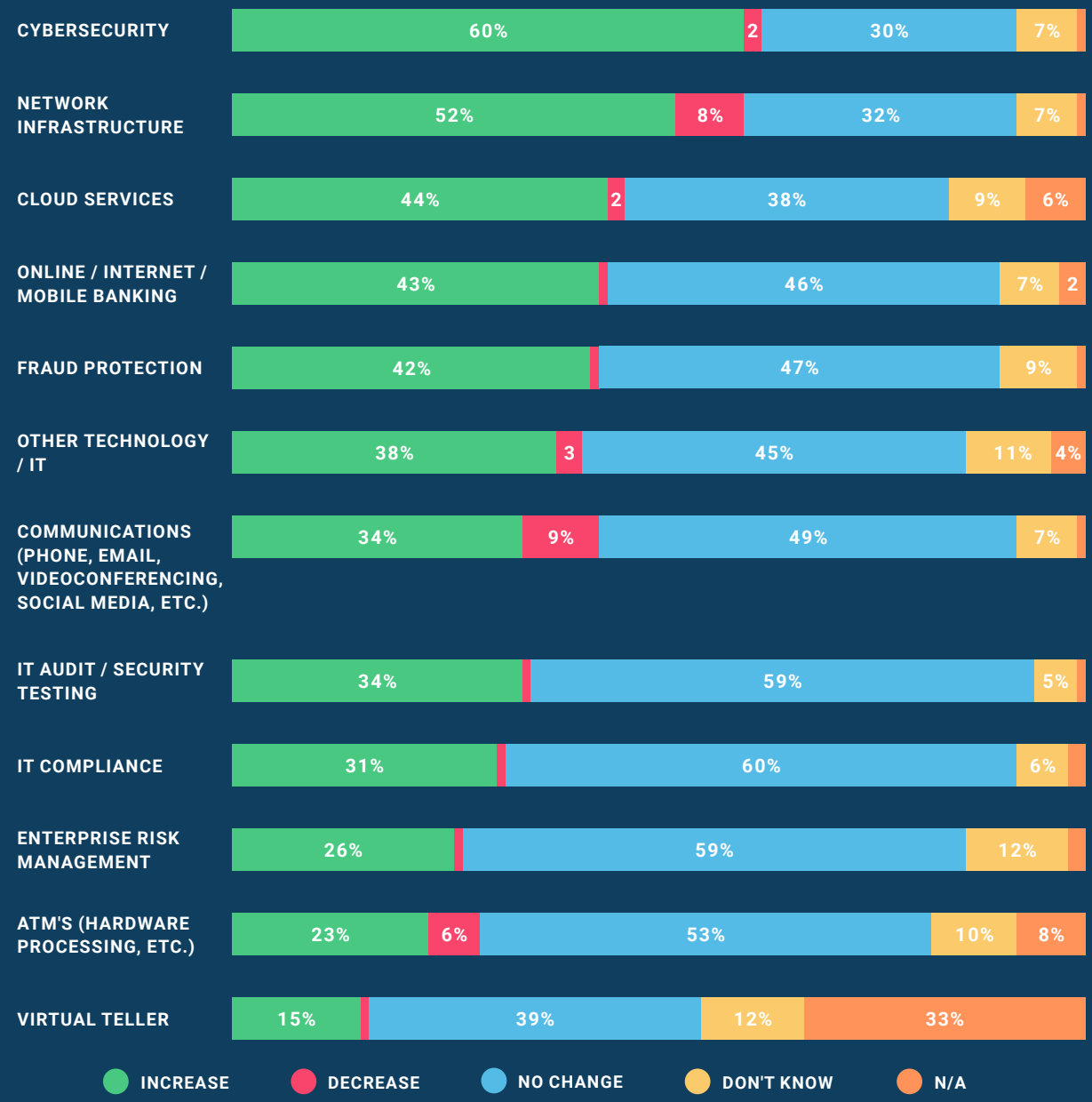
DIVING FURTHER

At the beginning of 2020, most institutions were making business decisions in response to COVID-19. The pandemic was a factor for cybersecurity budgets with 34% stating that COVID-19 caused the institution to increase cybersecurity funding.

We also learned that 44% of institutions plan to increase budget for cloud services which is up from 38% in 2020. This increase could indicate institutions are moving towards cloud-based solutions to better support remote work environments.



ANTICIPATED IT SPENDING CHANGES FOR THE NEXT 12 MONTHS



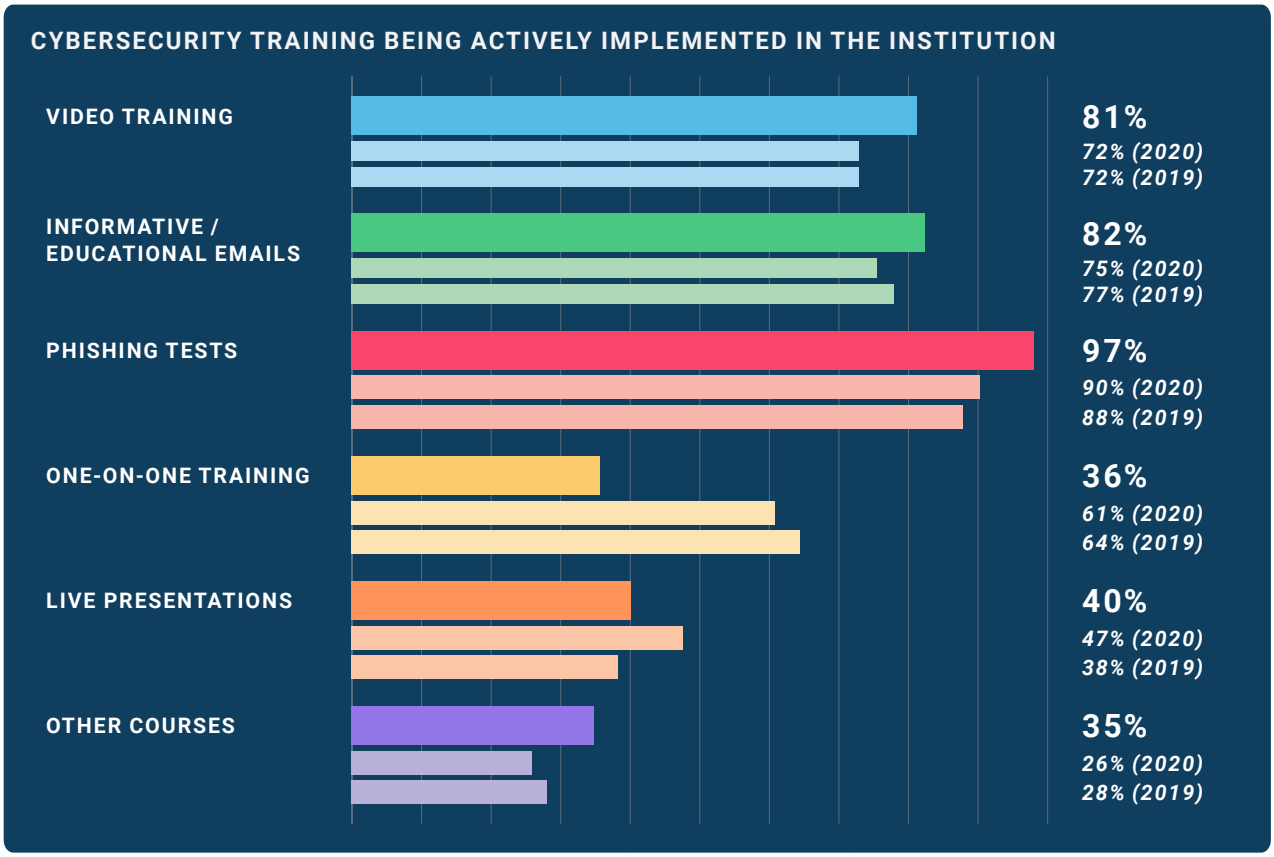
TAKEAWAY

The sudden shift to remote environments due to COVID-19 presented new challenges for both IT and information security. Some institutions increased budgets to cover the costs of implementing and securing new remote work technologies. Other institutions find themselves trying to mitigate increased risk while working within the same budget.

To ensure an effective security posture while attempting to reduce cost, institutions are likely to increase outsourcing. Outsourcing should be approached with due care, as it can introduce a different set of risks.

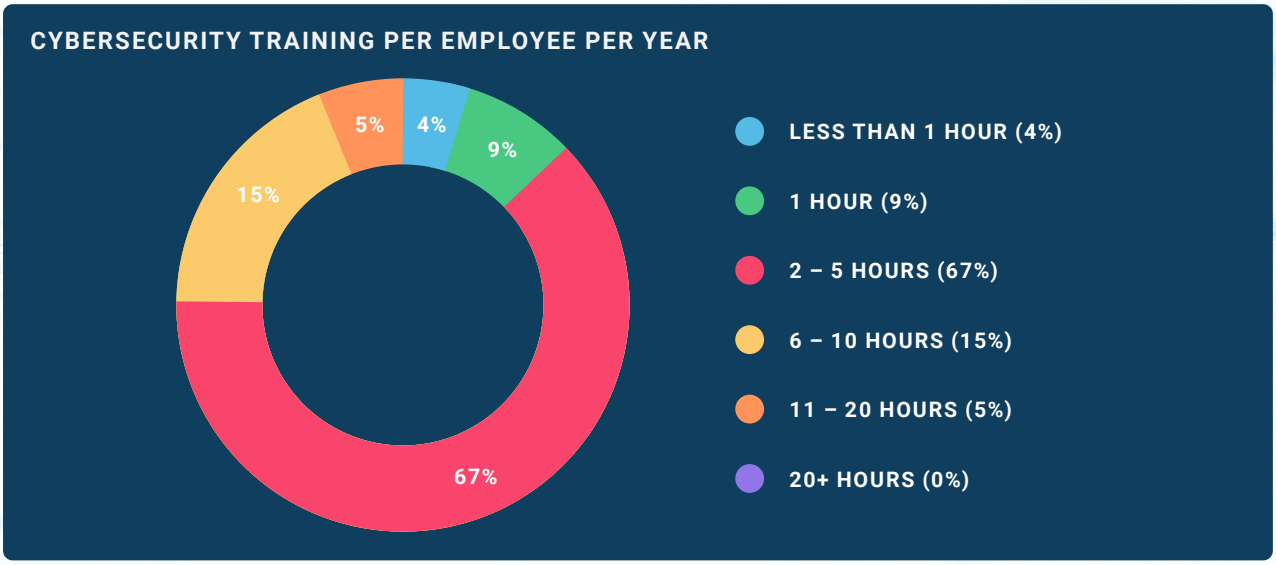
Training

TRAINING FINDINGS



SIGNIFICANT FINDING

When we asked how much time was spent on security awareness training, the results showed a majority of respondents (67%) administer an average of 2-5 hours (per employee) of information security training on an annual basis.



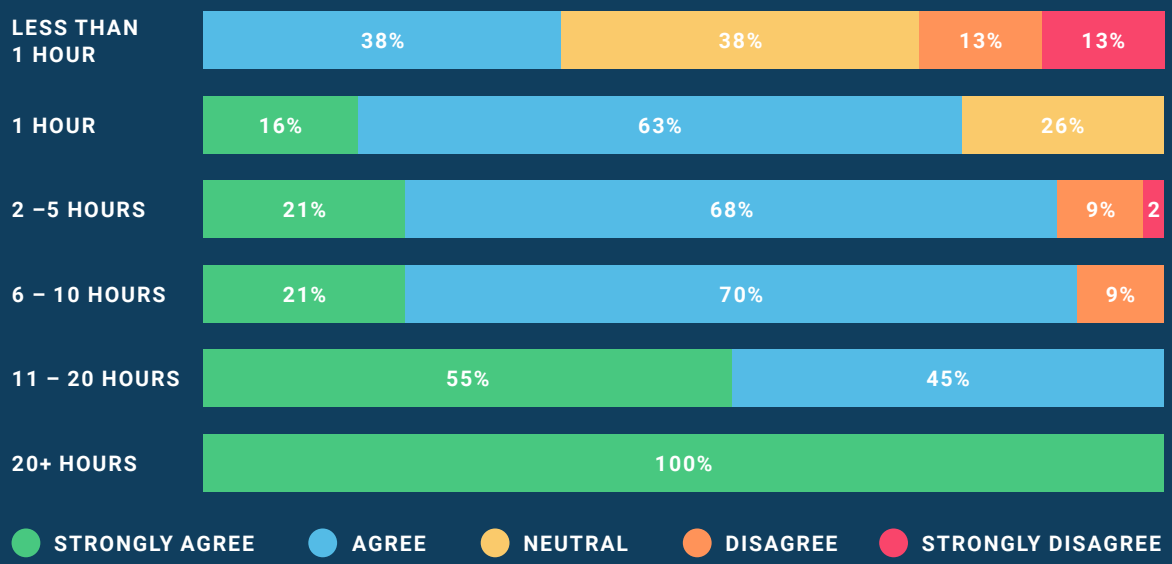
DIVING FURTHER

Institutions who administer information security training more often throughout the year tend to have more confidence in the effectiveness of their training.

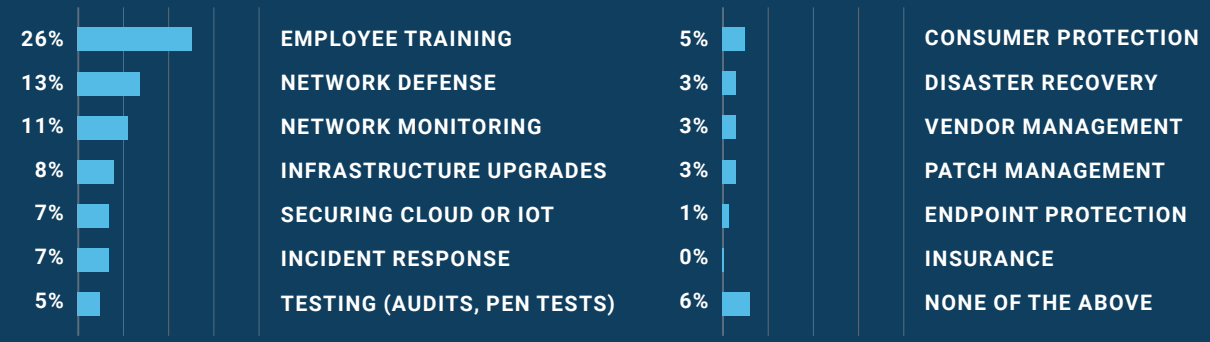
We also found that one-in-four institutions state they would provide additional employee training if given the choice of where to invest in additional cybersecurity resources.

HOURS OF CYBERSECURITY TRAINING PER YEAR IN ORDER TO REDUCE RISK

Respondents were asked to what degree they feel their institution's cybersecurity training directly reduces risk of cyber incidents.



ONE AREA OF CYBERSECURITY TO IMPROVE IF THERE WERE ADDITIONAL RESOURCES



Displayed on a 50% maximum scale

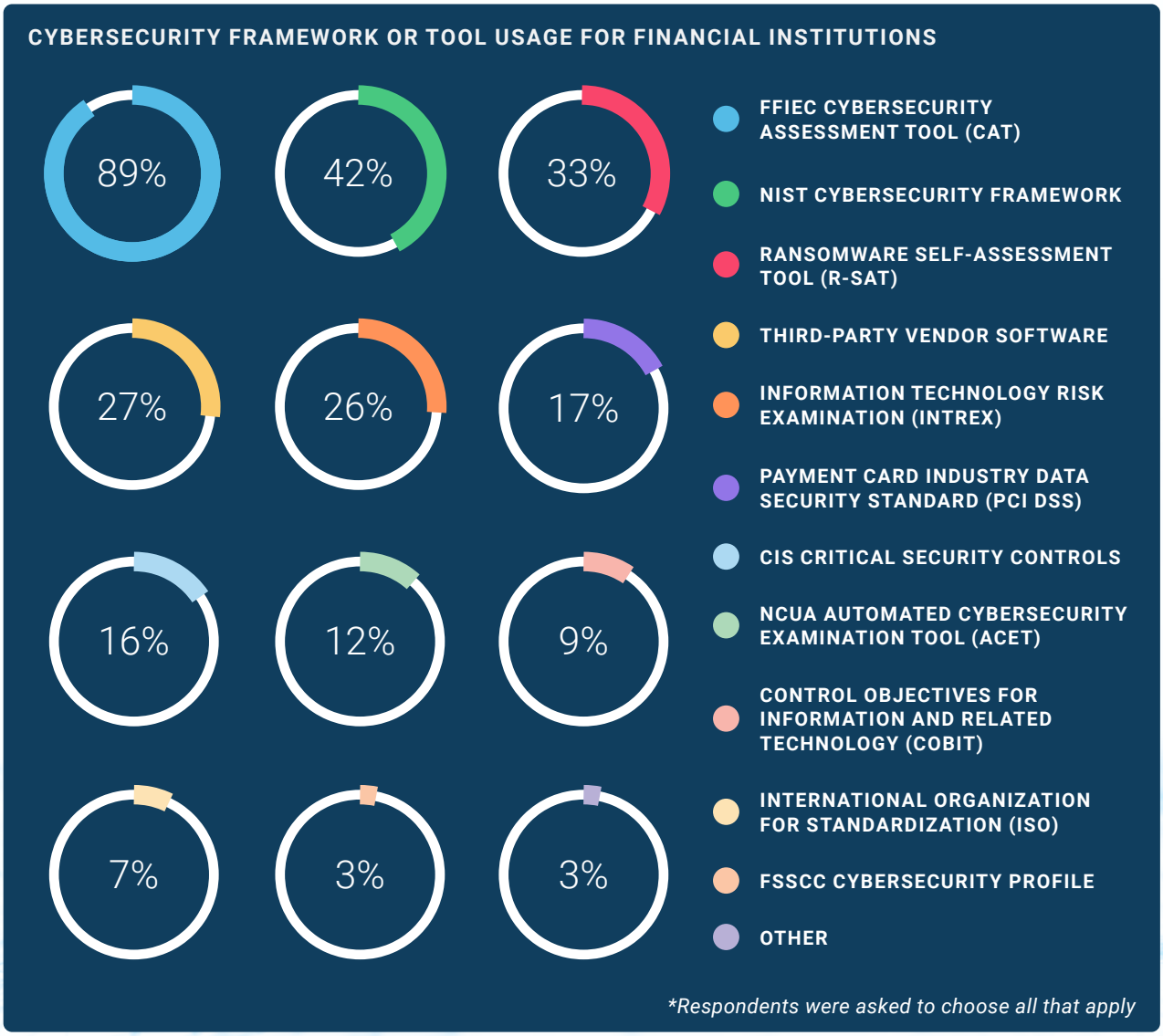
TAKEAWAY

Increasing training hours has a direct correlation to an institution's confidence in their employees' cybersecurity awareness. However, a lack of resources seems to be a roadblock to implementing additional training. To justify a request for additional resources, it may be beneficial to perform a root cause analysis, determine which incidents occurred due to a lack of awareness or education, and use the financial and strategic impact of those events to validate your request.

Cybersecurity Tools and Frameworks

SIGNIFICANT FINDING

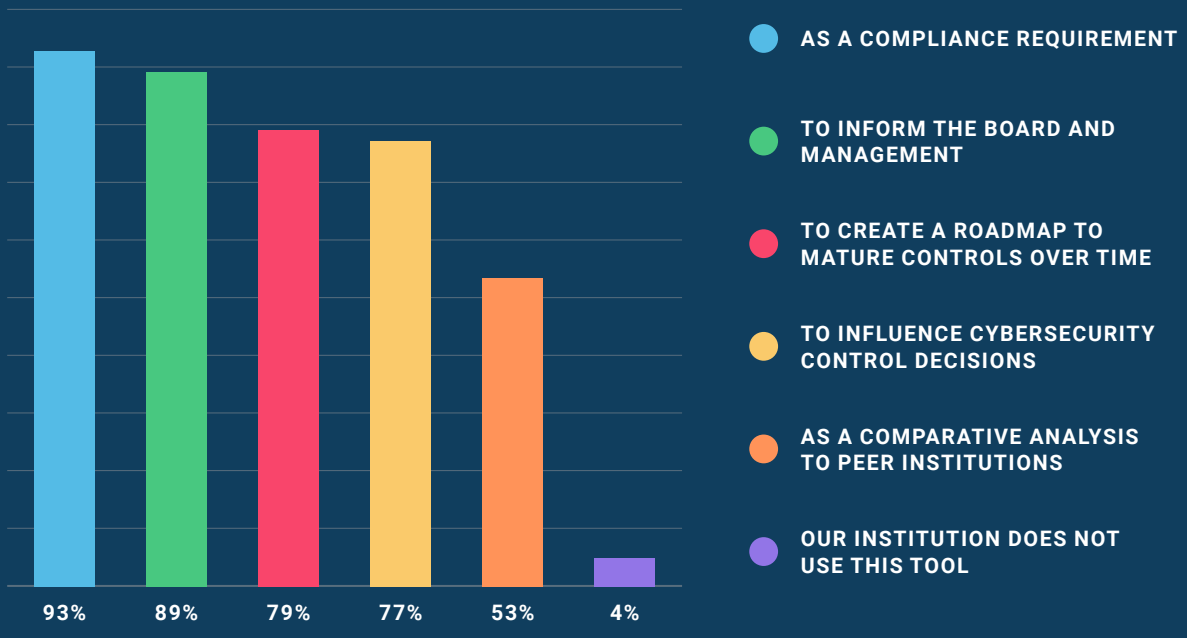
When we asked about cybersecurity frameworks used by financial institutions, the results showed a large majority (89%) of institutions use the FFIEC's Cybersecurity Assessment Tool as a cybersecurity framework or tool. The NIST Cybersecurity Framework and the Ransomware Self-Assessment Tool (R-SAT) are also well adopted among institutions.



DIVING FURTHER

Of the institutions who use the FFIEC CAT, the primary perceived value of the assessment is to fulfill compliance requirements. However, many financial institutions also believe the tool provides value in informing the Board and management about the institution's cybersecurity posture and creating a control maturity roadmap.

INSTITUTION'S USAGE OF THE FFIEC CYBERSECURITY ASSESSMENT TOOL (CAT)



**Respondents were asked to choose all that apply*

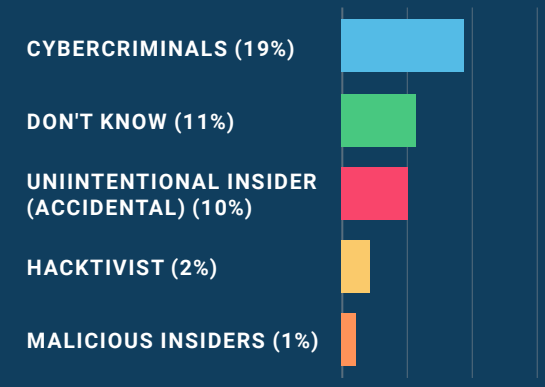
TAKEAWAY

While using the FFIEC CAT for compliance reasons is valuable, financial institutions can gain more value from the tool by leveraging it to assist with communication, improve control maturity, and influence decisions. Using a standard framework to measure the institution's cybersecurity standing will reduce risk and allow you to leverage external authority when proposing investments in cybersecurity.

Incident Response

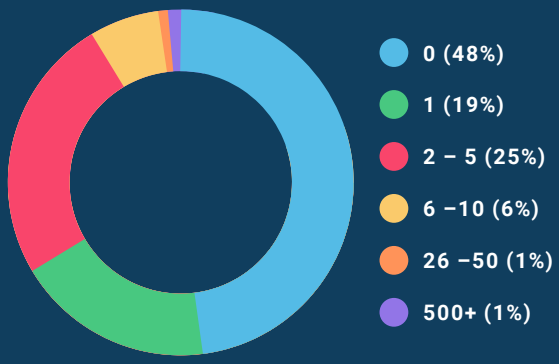
INCIDENT RESPONSE FINDINGS

TOP 3 INCIDENTS EXPERIENCED IN 2020

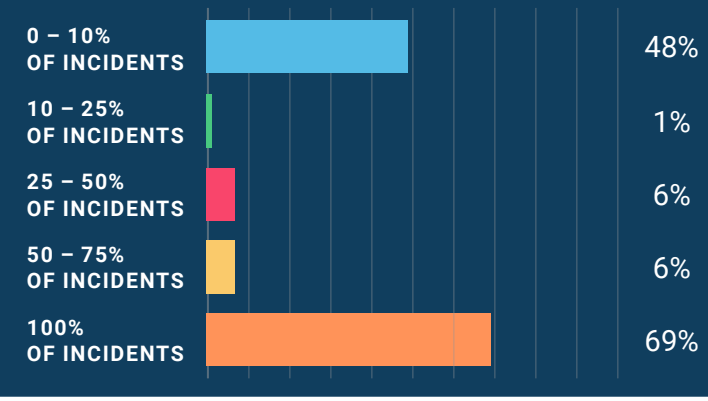


Displayed on a 30% maximum scale

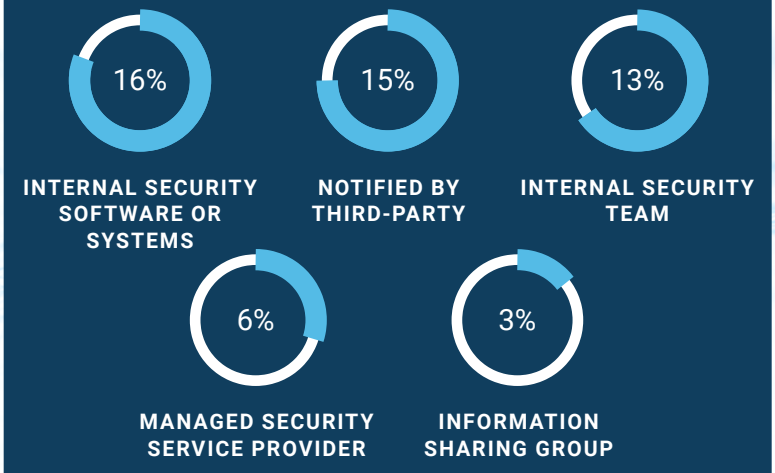
NUMBER OF INCIDENTS THAT NEGATIVELY IMPACTED THE INSTITUTION



PERCENTAGE OF INCIDENTS REPORTED TO THE BOARD

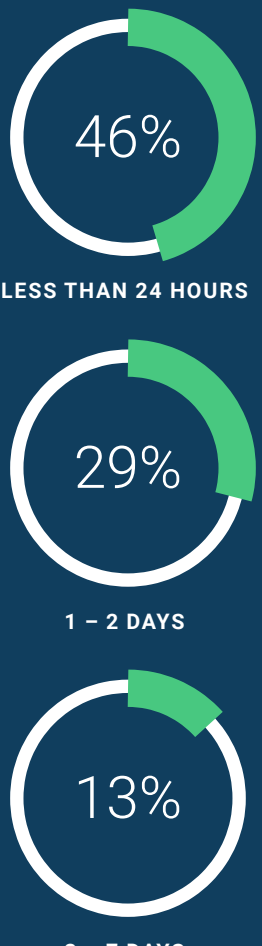


HOW SIGNIFICANT INCIDENTS WERE DISCOVERED

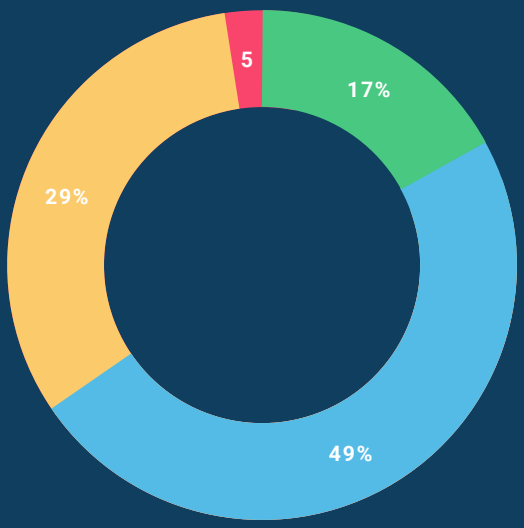


Displayed on a 20% maximum scale

AVERAGE TIME TO DISCOVER INCIDENTS

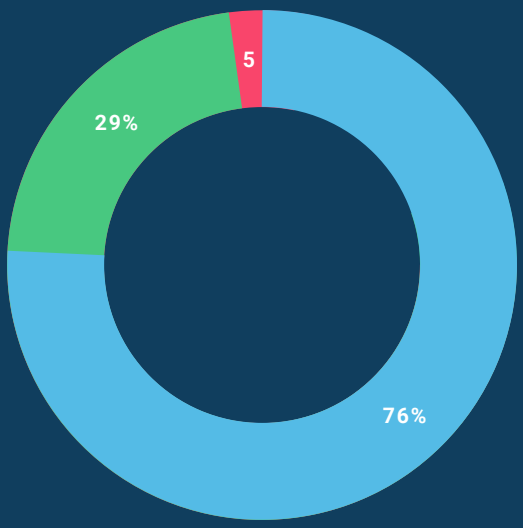


INCIDENT RESPONSE PLAN EFFECTIVENESS



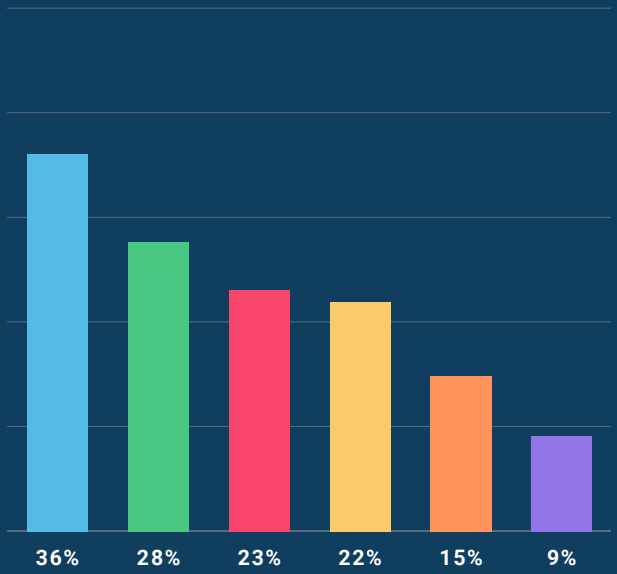
- EXTREMELY EFFECTIVE
- VERY EFFECTIVE
- SOMEWHAT EFFECTIVE
- NOT VERY EFFECTIVE

INCIDENT RECOVERY COSTS



- $0 – $5,000
- $5,001 – $50,000
- $50,001 – $100,000

BIGGEST BARRIERS TO MITIGATING AND REMEDIATING CYBERSECURITY INCIDENTS



- LACK OF APPROPRIATE CYBERSECURITY PERSONNEL
- TOO MUCH CYBER THREAT INFORMATION TO ADEQUATELY PROCESS
- LACK OF TRAINING RESOURCES FOR EMPLOYEES
- OVER RELIANCE ON VENDOR SOLUTIONS / SYSTEMS
- LACK OF FINANCIAL RESOURCES
- NETWORK, SYSTEMS, SOFTWARE, AND/OR SERVICES TOO COMPLEX TO SECURE

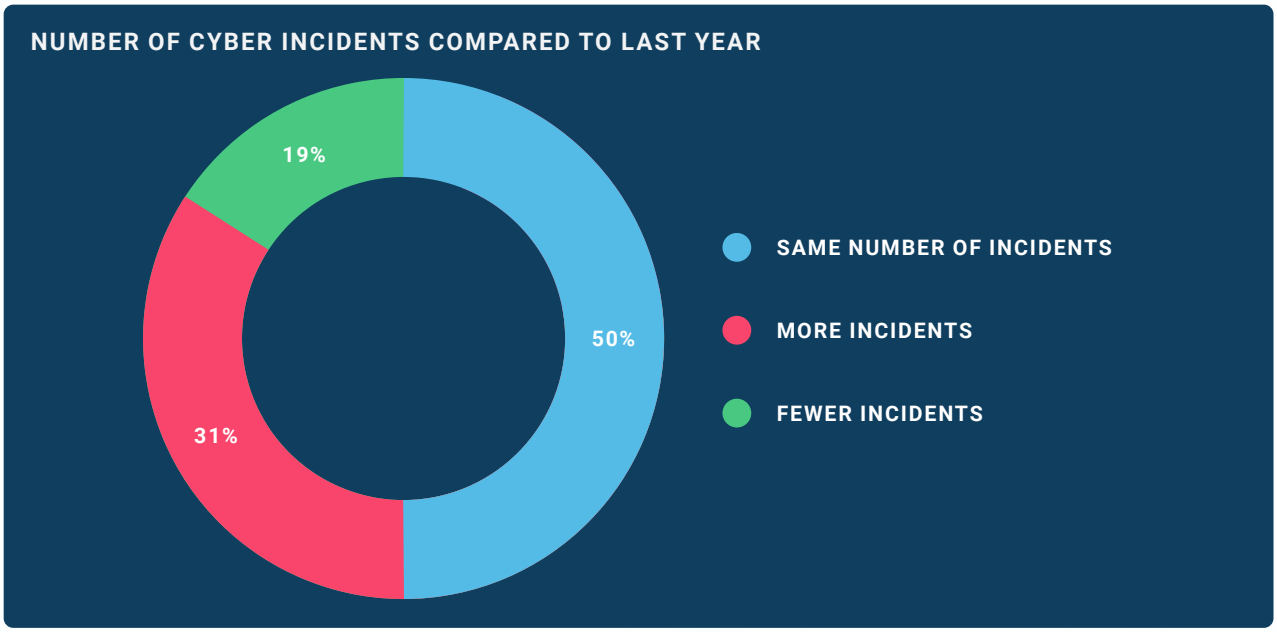
**Respondents were asked to choose up to three options*

INCIDENT RESPONSE CONTINUED ON NEXT PAGE

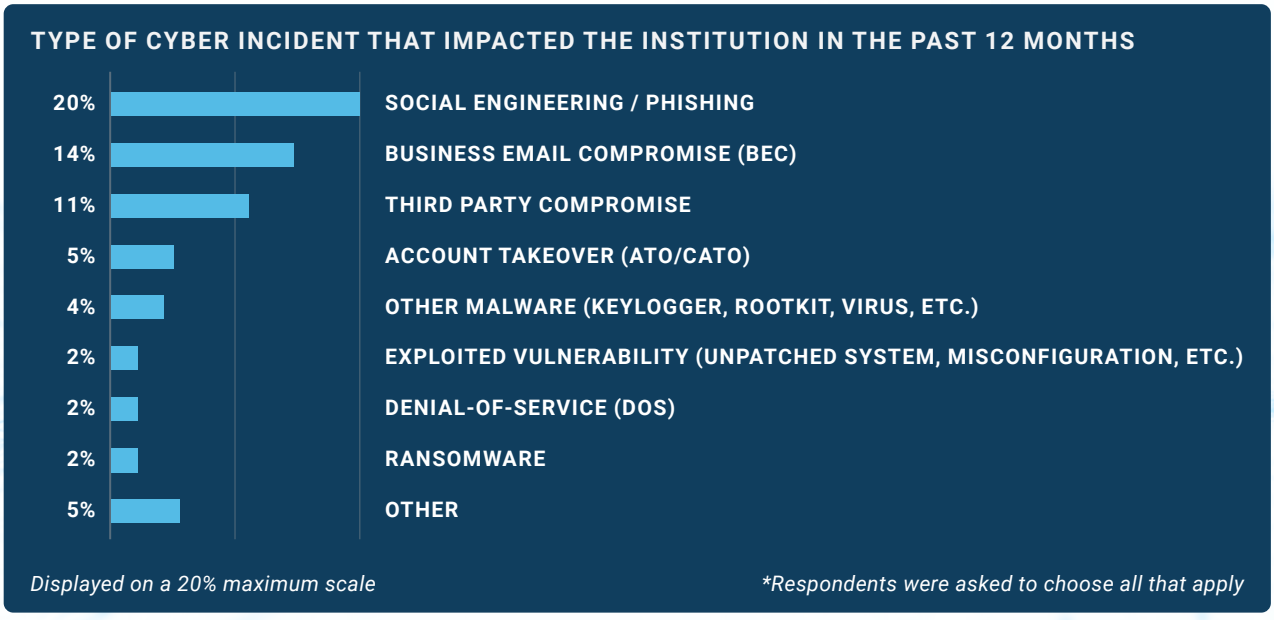
Incident Response

SIGNIFICANT FINDING

When we asked about the number of cyber incidents experienced in 2020, the results showed that 81% of respondents said they experienced the same or a greater number of cyber incidents in 2020 in comparison to 2019.

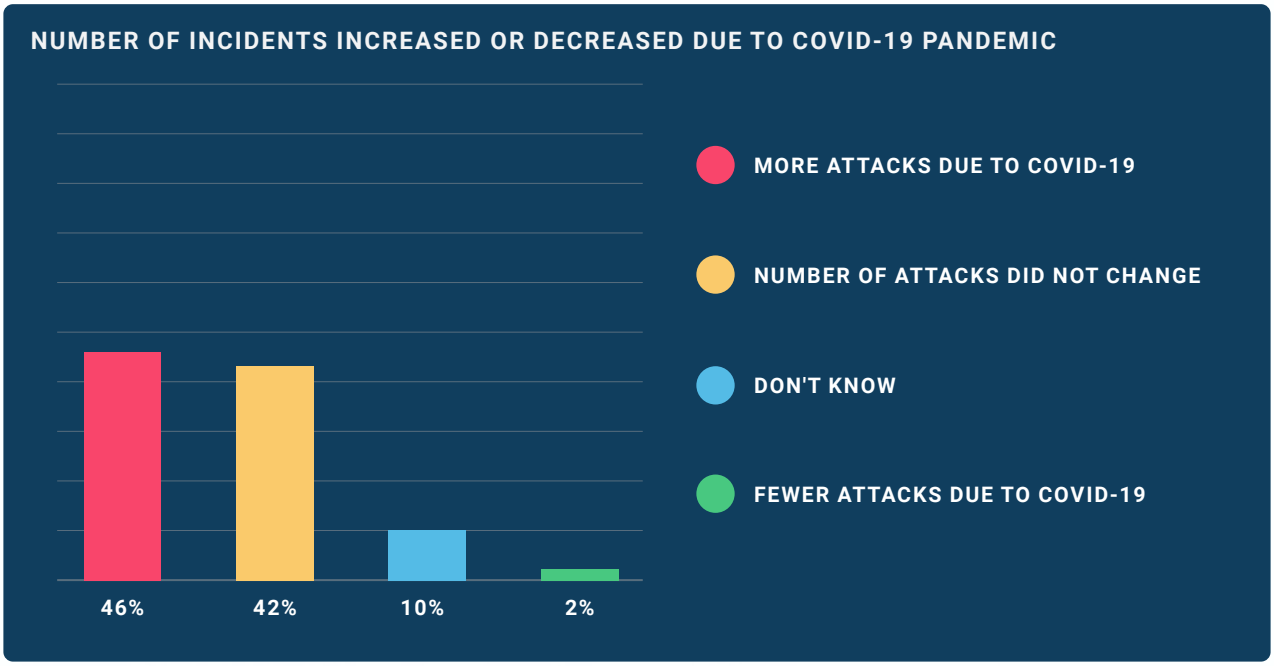


The top three incidents experienced by financial institutions were social engineering/phishing, business email compromise (BEC), and third party compromise.



DIVING FURTHER

Some respondents believed COVID-19 was a factor in the increased number of incidents in 2020.

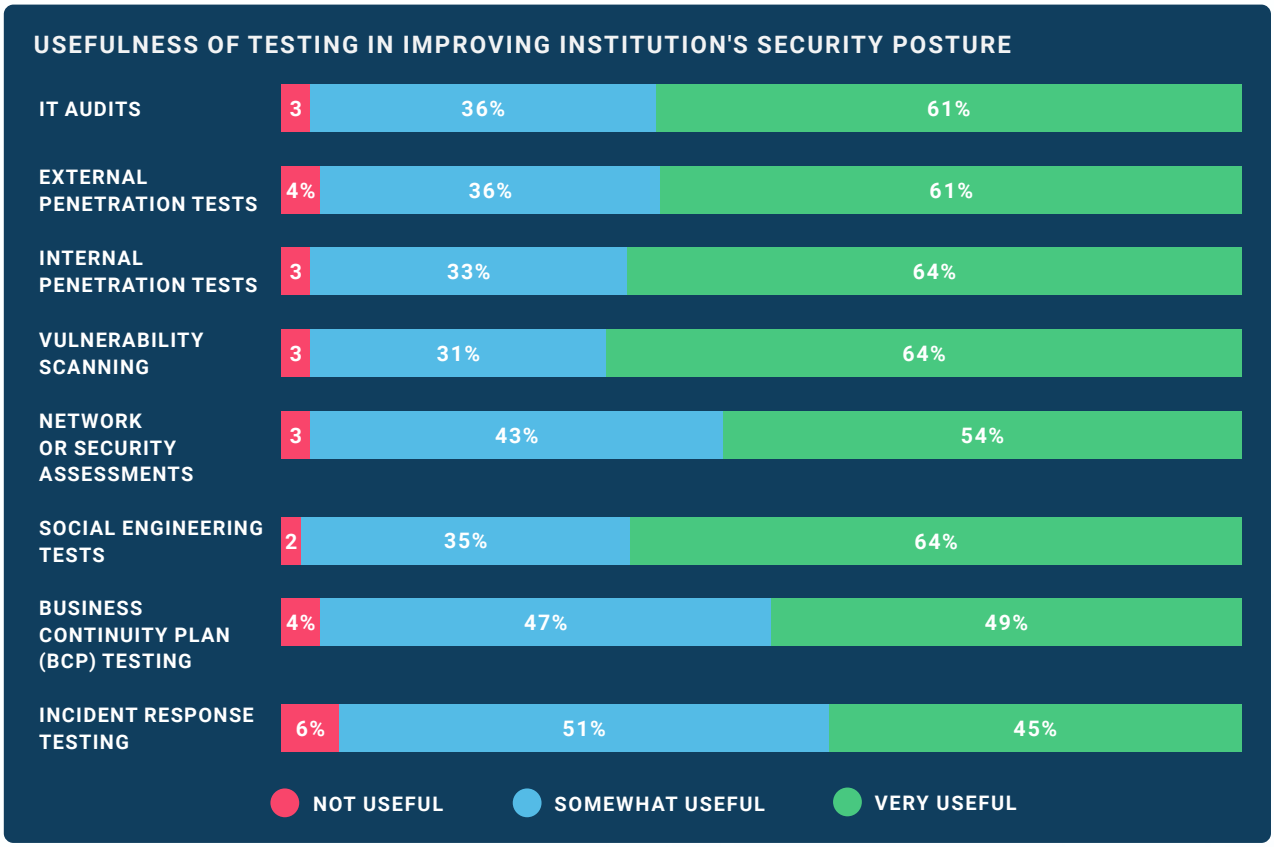


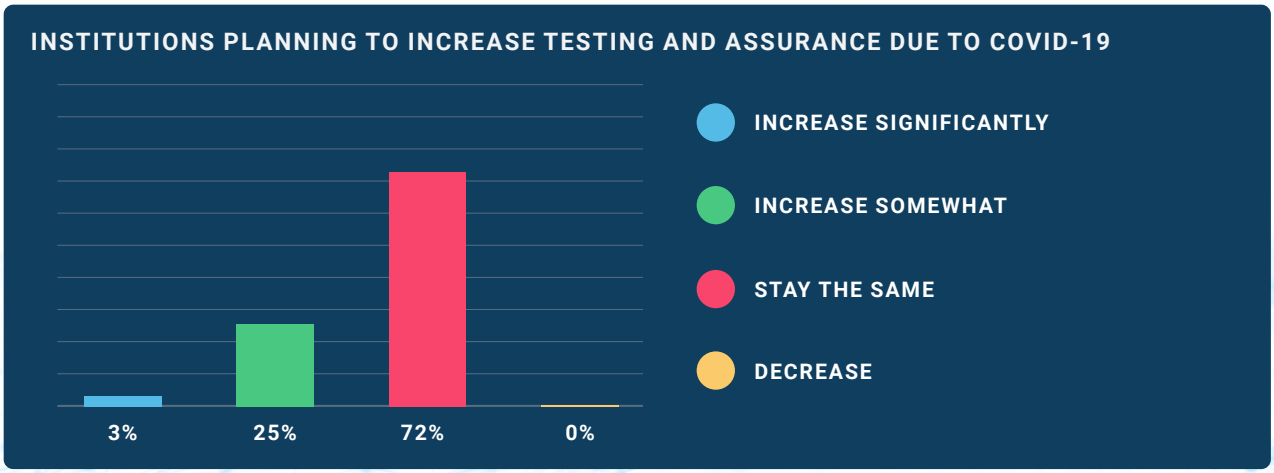
TAKEAWAY

Proper cybersecurity awareness training is more important than ever as threats continue to increase and bad actors take advantage of time-sensitive situations. The situation is compounded by increasingly remote IT environments due to COVID-19. Administering high-quality and regular cybersecurity awareness training, monitoring, and testing can reduce the impact of an incident.

Assurance & Testing

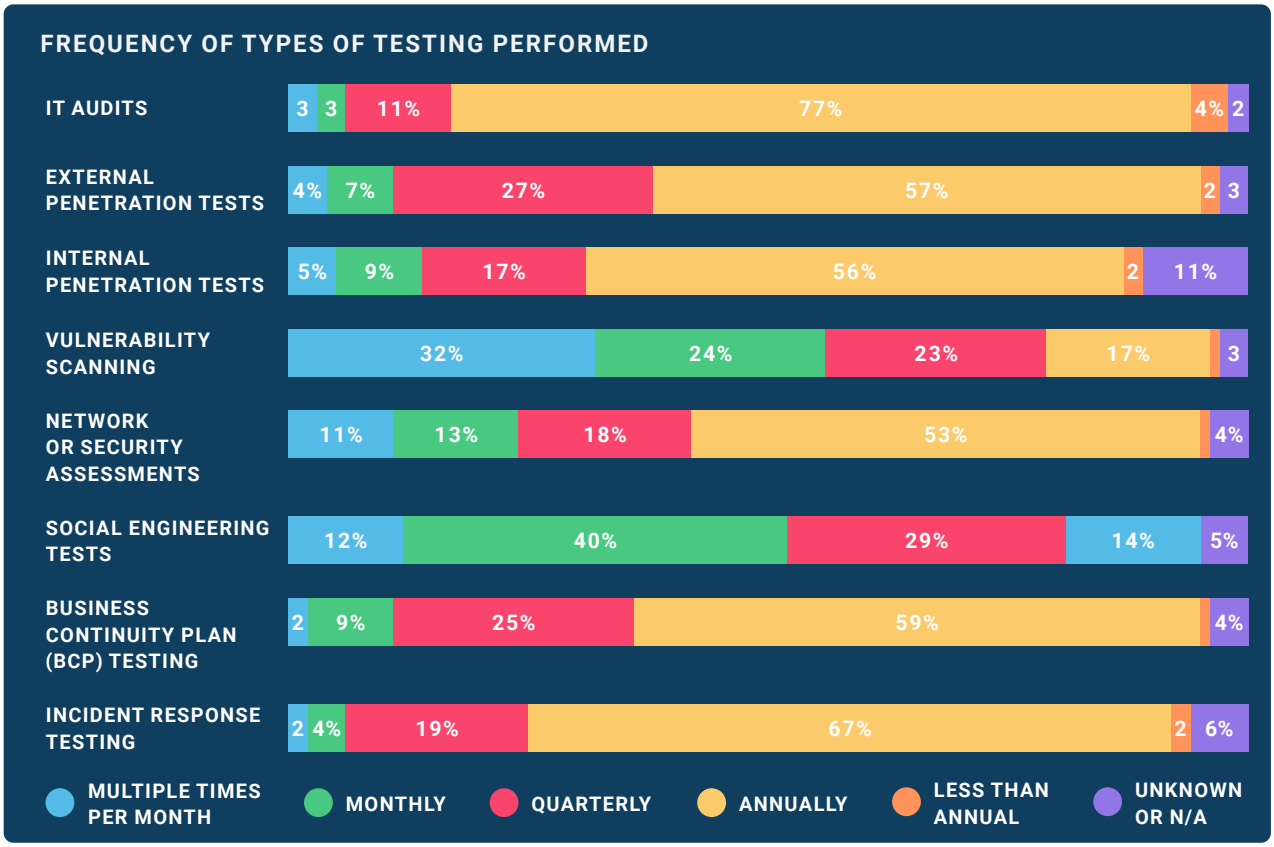
ASSURANCE & TESTING FINDINGS





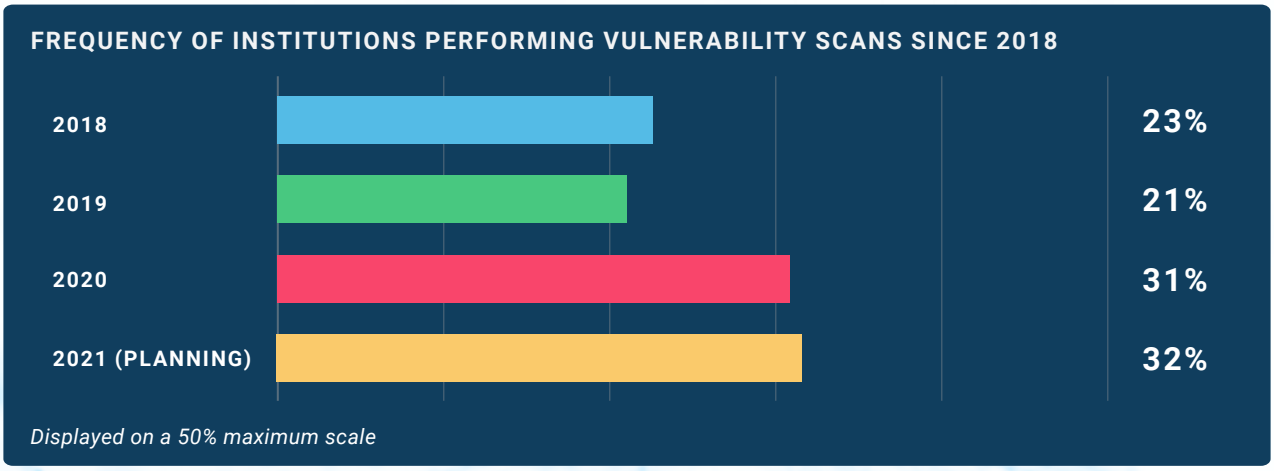
SIGNIFICANT FINDING

When we asked how financial institutions perform assurance and testing, the results showed that of the various forms, financial institutions most frequently performed vulnerability scans, social engineering tests, and network assessments. Larger, more complex tests and projects were done with less frequency.



DIVING FURTHER

According to data collected since 2018, institutions are performing more frequent vulnerability scanning.



TAKEAWAY

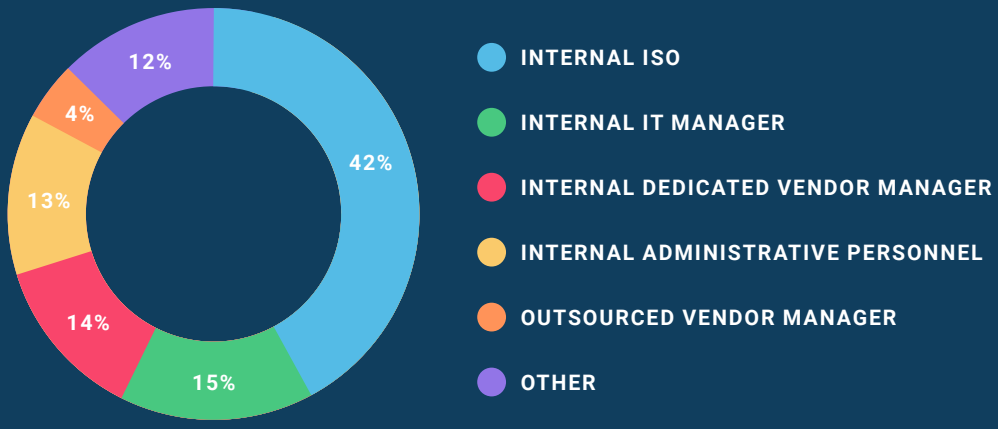
Affordable and accessible vulnerability scans are providing significant value to financial institutions. These tests offer an efficient way to identify security weaknesses, such as misconfigurations, unpatched systems, and unauthorized applications. This perspective on the overall health of the environment is proving especially valuable as operations continue in decentralized environments due to COVID-19.

Vendor Management

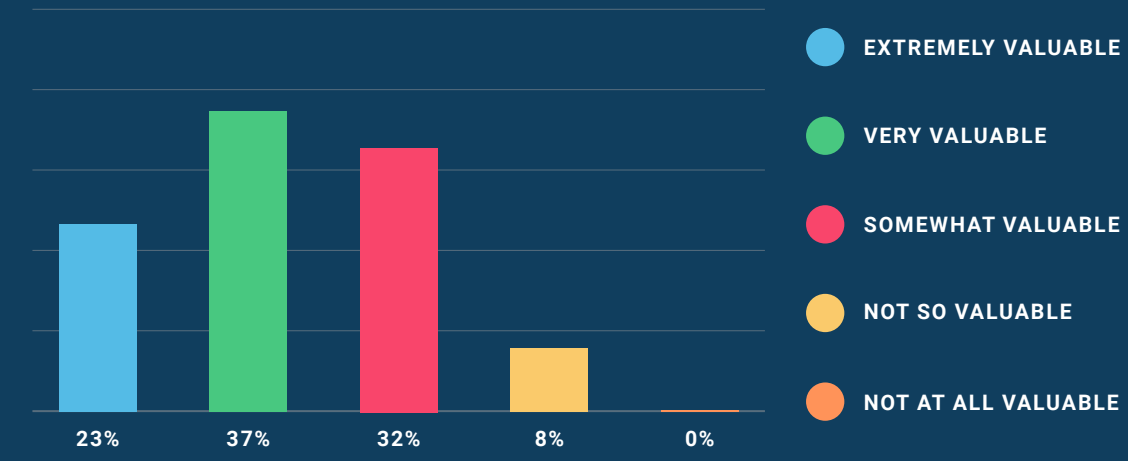
VENDOR MANAGEMENT FINDINGS

INSTITUTION'S VENDORS THAT EXPERIENCED A CYBERSECURITY INCIDENT THAT NEGATIVELY IMPACTED THE INSTITUTION OR ITS CUSTOMERS

INSTITUTION'S PRIMARY VENDOR MANAGER



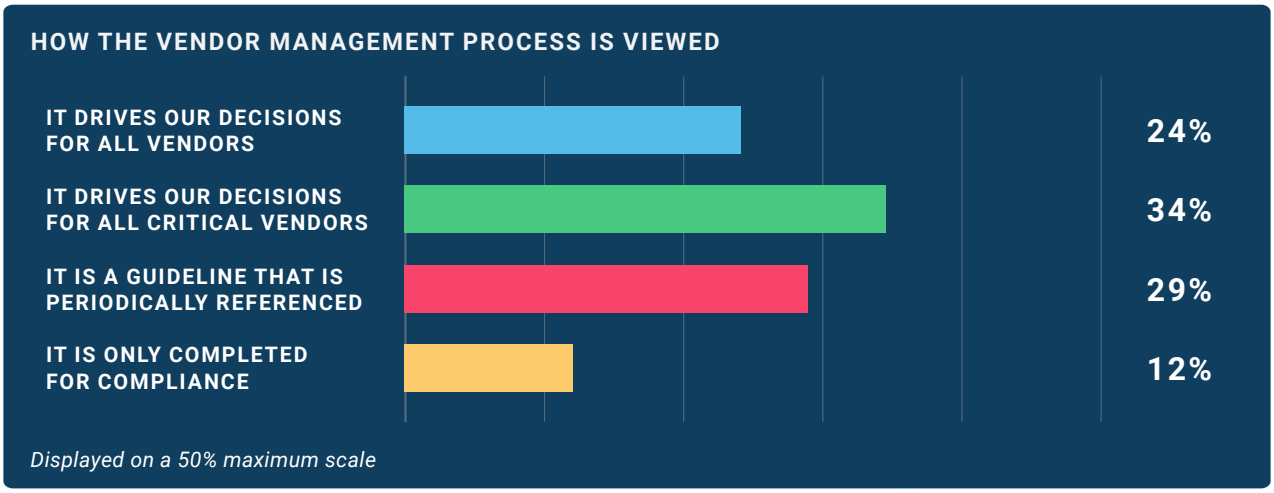
HOW VALUABLE THE VENDOR MANAGEMENT PROCESS IS TO THE INSTITUTION



Displayed on a 50% maximum scale

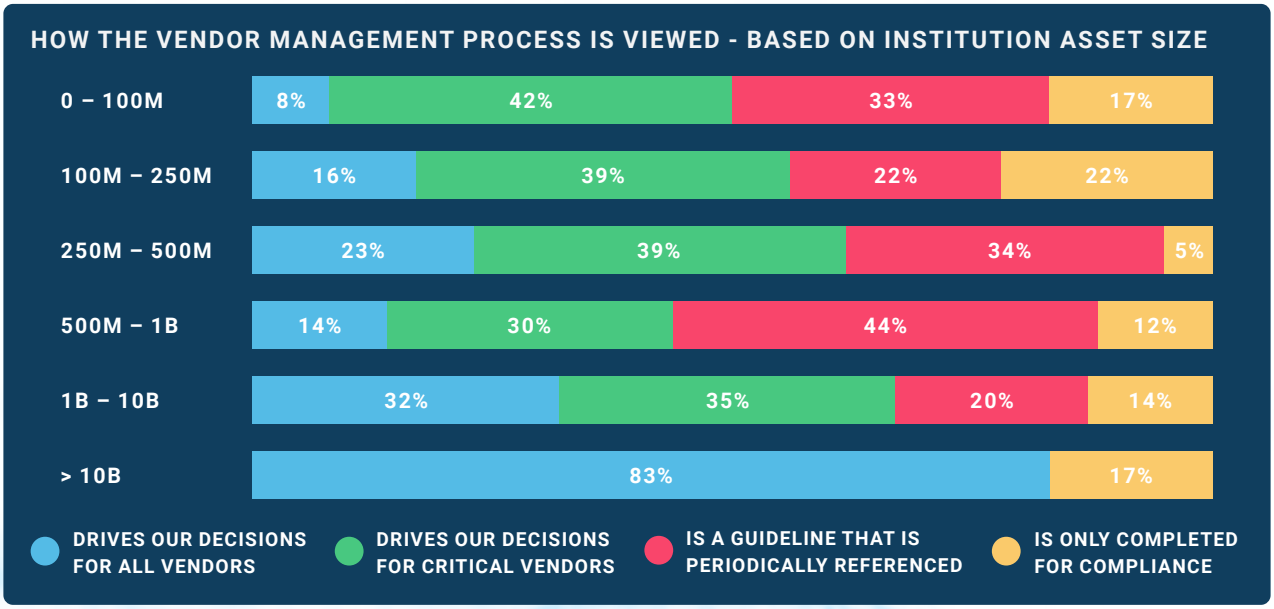
SIGNIFICANT FINDING

When we asked how the vendor management process is viewed, the results showed the majority of institutions (58%) view it as one which directly impacts decisions for all or critical vendors.



DIVING FURTHER

Smaller financial institutions are less likely to use their vendor management program to guide decisions on vendors and are more likely to view the program as a compliance requirement.



TAKEAWAY

There is a correlation between the perceived value of the vendor management process and the reasoning behind why the program is implemented. In a time when third-party compromise is among the most frequently experienced incidents by financial institutions, a value-driven vendor management program is key to managing cybersecurity risk introduced by third parties.

About the Authors

Visit our website to learn more about our authors and to book them for a speaking engagement.
https://tandem.app/speakers

ALYSSA PUGH

Security+
GRC Content Manager, Tandem, LLC

As a millennial, Alyssa grew up with technology at her fingertips. She has more than ten years of professional technical and information security experience. She currently serves as the GRC Content Manager for Tandem, where she participates in the development of cybersecurity content and educational resources. In addition to her passion for technology, Alyssa is also a wife, graphic designer, and video game enthusiast.

LETICIA SAIID

Security+
Chief of Staff, Tandem, LLC

After earning a B.A. and a M.A. in Mathematics, Leticia joined CoNetrix, where she served as the Tandem Software Support Manager for several years. She built and directed Tandem's first team of support specialists. Leticia now serves as Chief of Staff where she focuses on corporate strategy, employee development, and training. In her free time, she enjoys mentoring college students, teaching phonics, and solving jigsaw puzzles.

RUSS HORN

CISA, CISSP, CRISC
President, Tandem, LLC

Russ found a passion for technology at an early age, programming and playing on a Commodore 64. He went on to earn a B.A. in Mathematics and an M.S. degree in Management Information Systems. He spent time as a network administrator, systems analyst, university instructor, and IT Auditor prior to serving as President for CoNetrix and Tandem. Along with his interest in technology and cybersecurity, Russ is a husband, father, and runner.

BRIAN WHIPPLE

Marketing Manager, Tandem, LLC

Brian has over 10 years of experience in marketing. He started out his career by helping company founders secure funding for their startup businesses at a business incubator in Texas. He then spent time working within organizations and has focused on digital marketing and demand generation. When he is not working, Brian spends time with his wife and four children.

About Tandem

Tandem is a cybersecurity and compliance software designed specifically to help organizations improve their information security, stay in compliance, and lower overhead costs.

Our web-based application is designed to manage the compliance burden of information security regulations and improve the security posture of each organization and its users. Tandem is a business-to-business software as a service (SaaS) company and provides 12 unique, yet integrated, products as part of the software suite.

A Subsidiary of CoNetrix

Tandem is one of four companies owned by CoNetrix, LLC. CoNetrix has been known for innovative solutions and excellent quality since 1977. Tandem is no exception.

We believe there is a solution for every problem. As our clients began experiencing the burden of information security compliance, we began working to provide innovative solutions for them.

We initially supported our clients by helping them maintain their information security program documents. It didn't take long to realize a software solution could improve efficiency and help more people. In 2007, we began developing the do-it-yourself compliance application for information security, now known as Tandem.

Discover more about our products and watch demos at **tandem.app**

For media inquiries, contact Brian Whipple at **marketing@tandem.app**