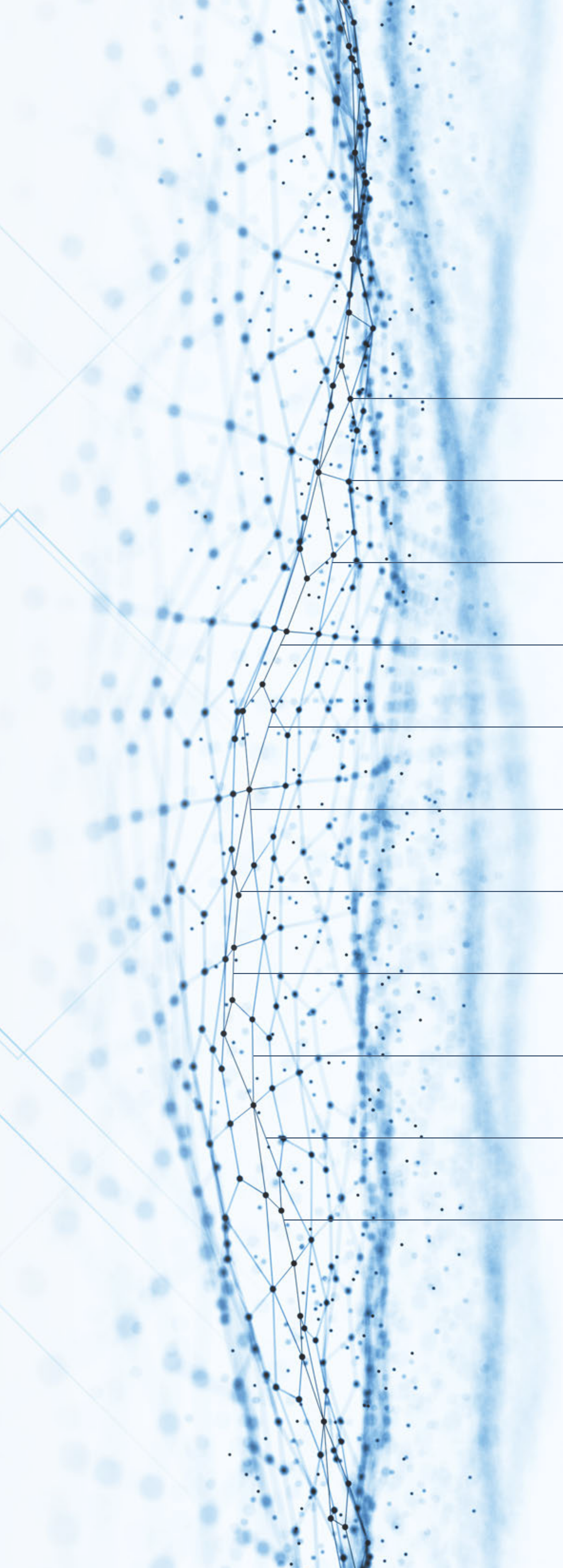
THE STATE OF

CYBERSECURITY

IN THE FINANCIAL INSTITUTION INDUSTRY

2020 SURVEY REPORT

Tandem™



Contents

About the 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, 2019 to January 31, 2020 and generated 252 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, contact info@tandem.app.

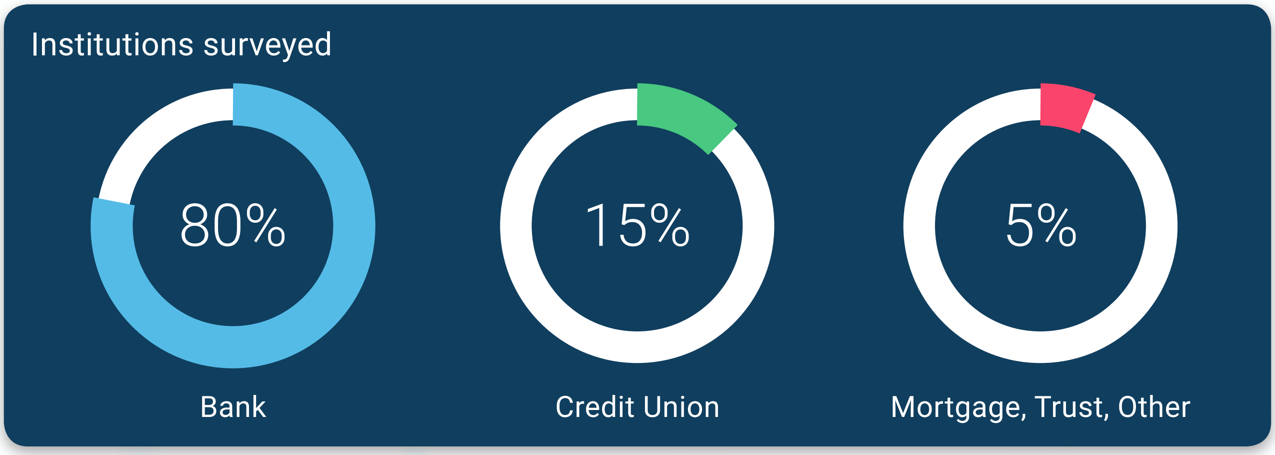
The survey was conducted by Tandem, LLC. For more information about Tandem, see page 24.

For questions or media inquiries, contact us at **tandem.app/contact**

Demographics

Types of Institutions

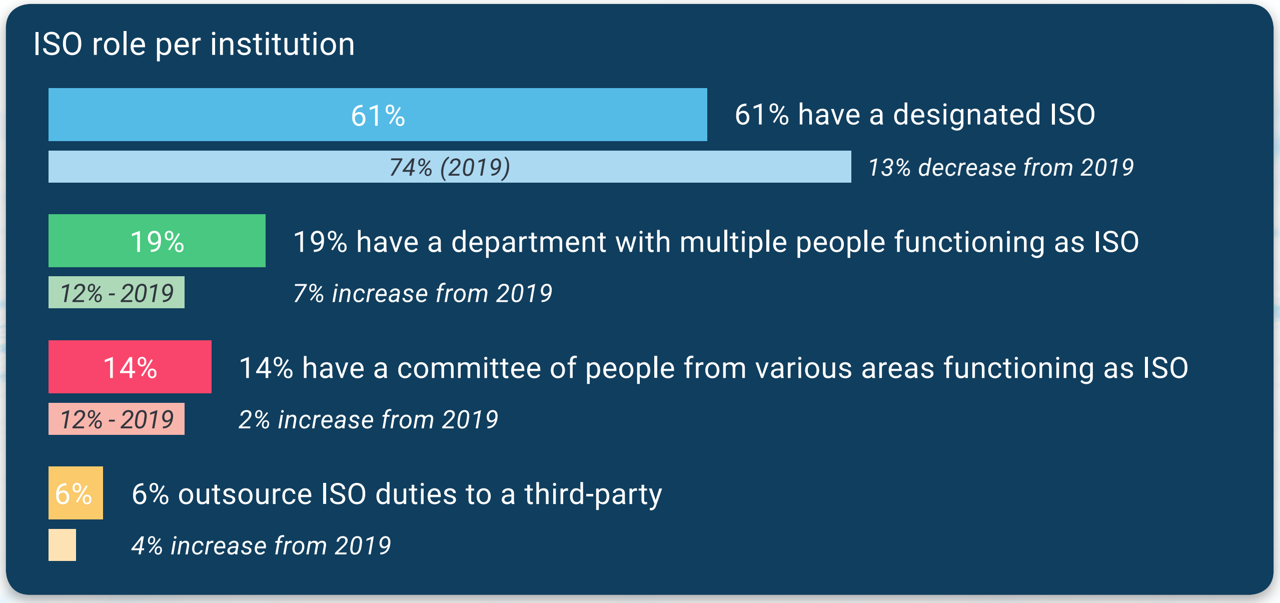
Of the 252 respondents that participated in the survey, 80% of respondents worked for a bank, 15% worked for a credit union, and the remaining percentage worked for other financial institutions, such as mortgage companies or trust companies at the time of the survey.



As shown, the collected data 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. In this survey, Information Security Officer (ISO) is synonymous with cybersecurity officer. According to survey results:



61% have a designated ISO

13% decrease from 2019

19% have a department with multiple people functioning as ISO

7% increase from 2019

14% have a committee of people from various areas functioning as ISO

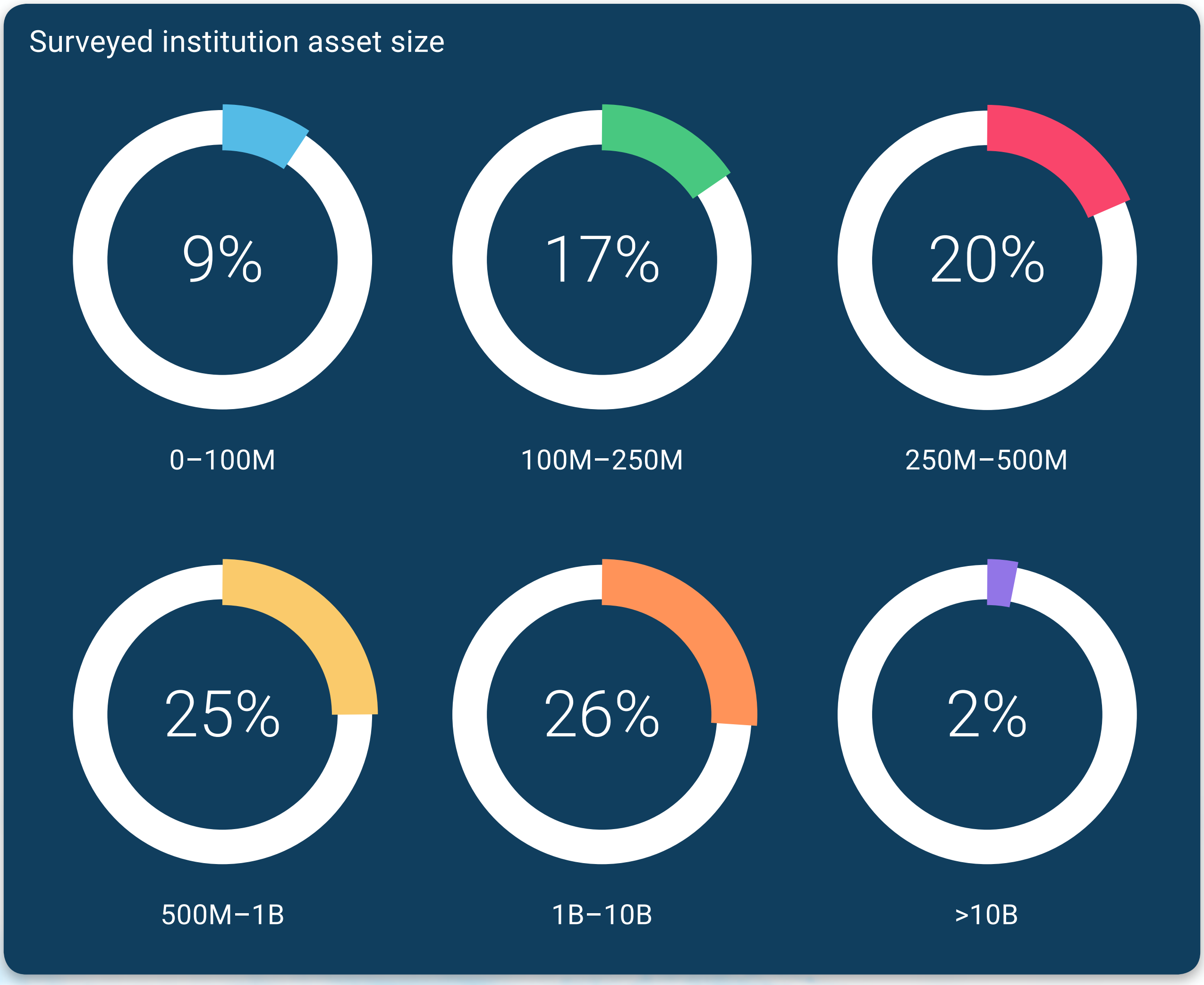
2% increase from 2019

6% outsource ISO duties to a third-party

4% increase from 2019

Asset Size of Institutions Surveyed

The survey focused on community financial institutions, with the majority of responding institutions reporting asset sizes between $250M and $10B.


Surveyed institution asset size

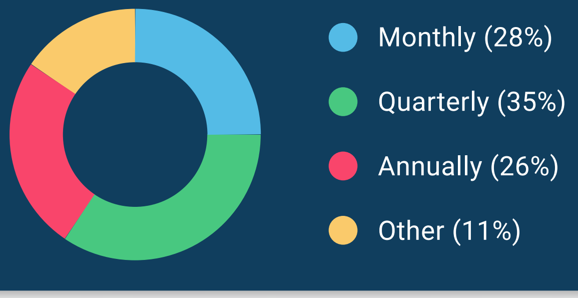
Board Oversight in Financial Institutions

Board understanding of, and involvement in, the financial institution's cybersecurity program is critical to the program's success. Our findings show increased Board involvement positively relates to improved funding for the cybersecurity program.

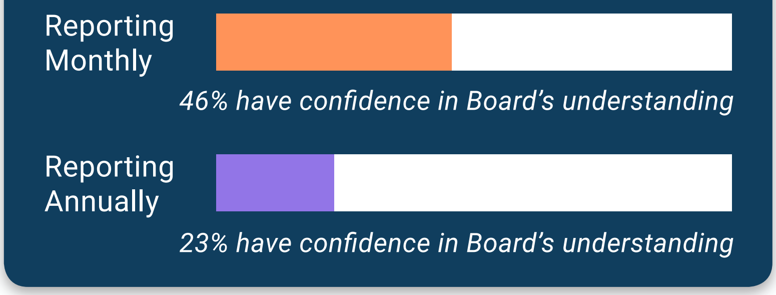
Significant Finding

The frequency with which cybersecurity reports were presented to the Board varied significantly with 28% percent of respondents saying they reported monthly, 35% quarterly, and 26% annually.

Cybersecurity Board reporting frequency



Confidence in Board's cybersecurity understanding



Diving Further

Of the institutions who report to the Board of Directors monthly, 46% are confident in the Board's understanding of the institution's cybersecurity posture. Only half as many (23%) are confident in their Board's understanding if they report annually.

Additionally, of the institutions who report to the Board of Directors monthly, 38% plan to increase cybersecurity budget in 2020. For those who report annually, only 27% plan to increase their 2020 cybersecurity budget.

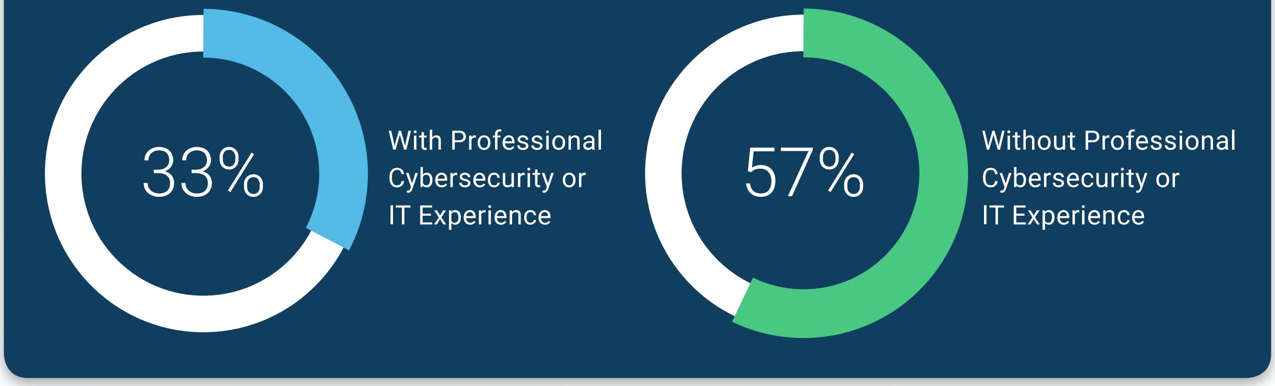
Takeaways

The more frequently the Board is exposed to information about the institution's cybersecurity posture, the better they understand and support it. Understanding a situation is foundational for support and improvement.

Board Member Experience

Findings show 33% of institutions have a Board member with professional cybersecurity or information technology experience, which is 4% more than 2019. Conversely, 57% of institutions do not have a Board member with IT or cybersecurity experience.

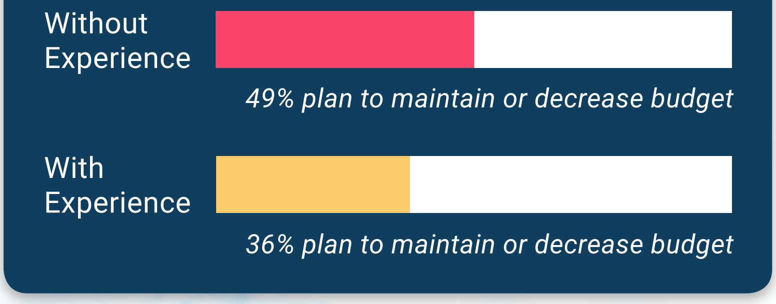
Institutions with Board members who have experience in cybersecurity or IT



Diving Further

Of the institutions who do not have a Board member with cybersecurity or IT experience, 49% plan to maintain or decrease the IT budget in 2020. Of institutions who have a Board member with relevant IT experience, only 36% plan to maintain or decrease the IT budget.

IT budget dependent on Board experience



Takeaways

Of the institutions who have a Board member with relevant cybersecurity or IT experience, 70% claim their Board members show more interest in how cybersecurity is being implemented within the institution. Institutions who have a Board member with IT experience are also more likely to receive additional resources to strengthen their cybersecurity posture than institutions without a Board member with this kind of experience.

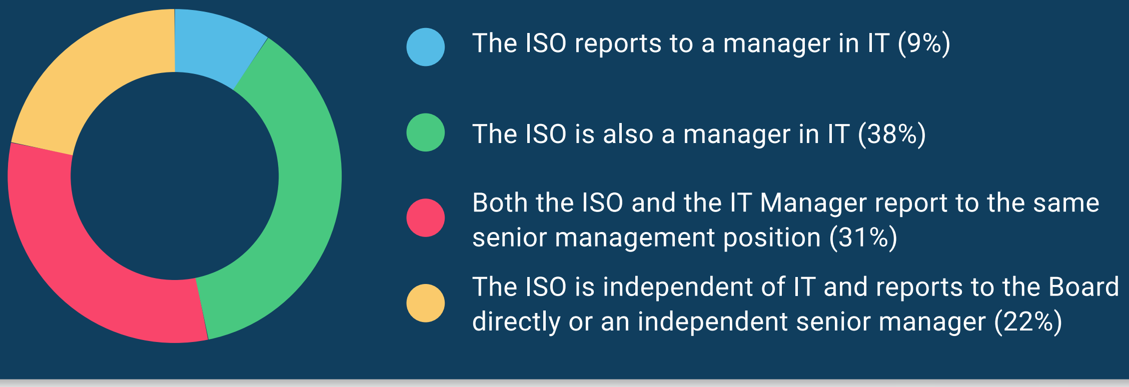
ISO Management and Staffing

Staffing and managing qualified employees in charge of the cybersecurity program is a common challenge for financial institutions. The survey results give insight into how the ISO role is being filled in the industry.

Significant Finding

According to the data, 48% of ISOs are either the IT Manager or report directly to the IT Manager. This number decreased by 7% from 2019 (55%).

Relationship between the ISO and the IT Manager



Diving Further

If the ISO does not report to the IT Manager, it is very likely they will report to the President/CEO, CRO, COO, CFO, or Board.

Takeaways

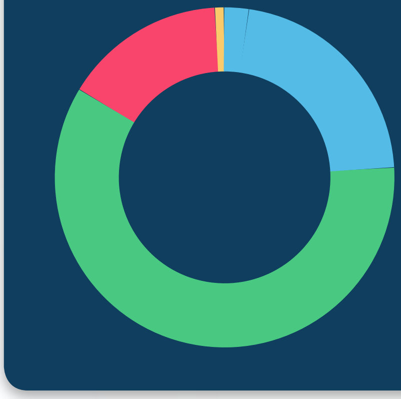
According to respondents, 53% of ISOs report to either the Board or a manager who is independent of the IT department. The FFIEC IT Examination Handbook, Management booklet states “the CISO should report directly to the board, a board committee, or senior management and not IT operations management.”

It is considered a best practice for financial institutions to separate the IT role from the cybersecurity role entirely, and more institutions are choosing to follow this model.

In-House vs. Third-Party Management

According to the data, 23% of institutions manage their cybersecurity program completely in-house, a 5% decrease from 2019. The data shows a slight trend towards institutions working with third-party service providers.

Institutions outsourcing their cybersecurity program



🔵 Completely managed in-house (23%)
5% decrease from 2019 (28%)

🟢 Managed in-house with support from third-parties (60%)
2% increase from 2019 (58%)

🔴 Managed by a third-party with support from in-house (16%)
4% increase from 2019 (12%)

🟡 Completely managed by a third-party (<1%)
Approximately 2% decrease from 2019

Diving Further

In 2020, 61% of institutions have a designated ISO which is a 13% decrease from 2019. While the number decreased for institutions with designated ISOs, the number increased for institutions who depend on third parties for managing a cybersecurity program.

Takeaways

Financial institutions are starting to seek support from third-party providers to help manage their cybersecurity, and they are moving away from a single person maintaining the ISO role.

This move could be an indicator institutions find it more cost effective to work with an existing third-party cybersecurity expert than to develop one for themselves.

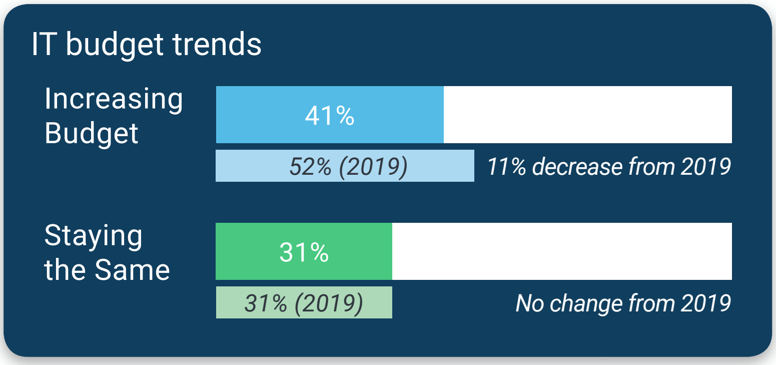
As the trend to seek third-party cybersecurity services continues to grow, institutions will need to be diligent in their vendor management processes to ensure they partner with high quality service providers.

Budgeting - IT

The data below shows budget data and trends, giving insight into how institutions are using their funds to support their cybersecurity programs.

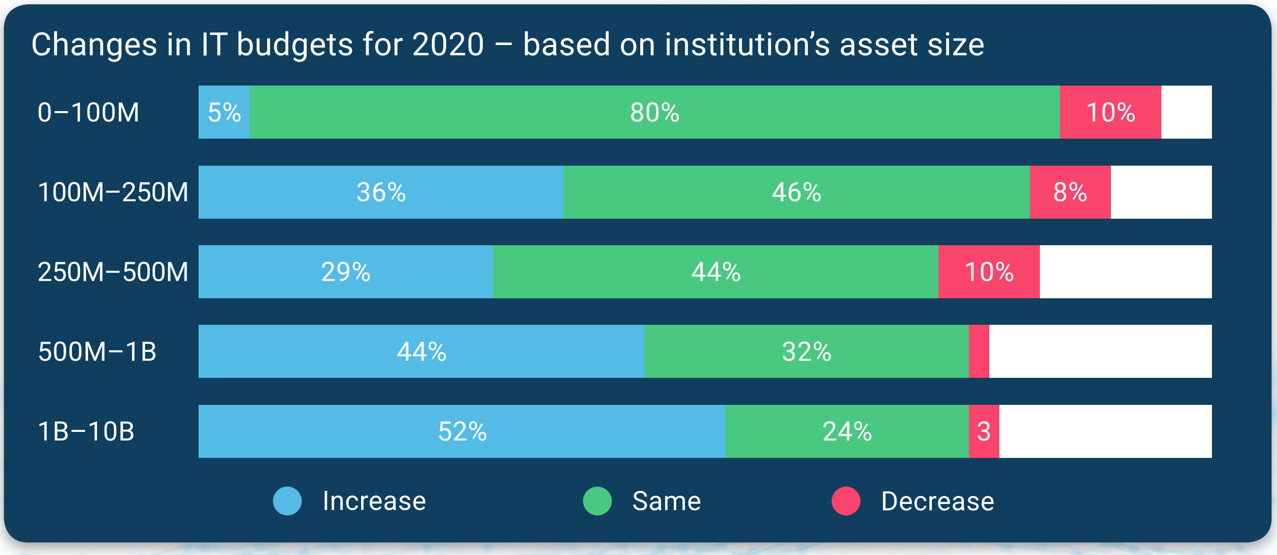
Significant Finding

Approximately 41% of institutions reported their IT budget for 2020 has increased, 31% reported it has stayed the same, and 11% reported a decrease in budget.


IT budget trends

Diving Further

While a large portion of institutions are increasing their IT budgets in 2020, the trend has slowed slightly compared to 2019. This decrease is especially true for institutions with an asset size between $250M - $500M where only 29% plan to increase their budget, which is down 28% from 2019 (57%). Results show that 10% of institutions within this asset range have decreased their budget in 2020.


Changes in IT budgets for 2020 – based on institution's asset size

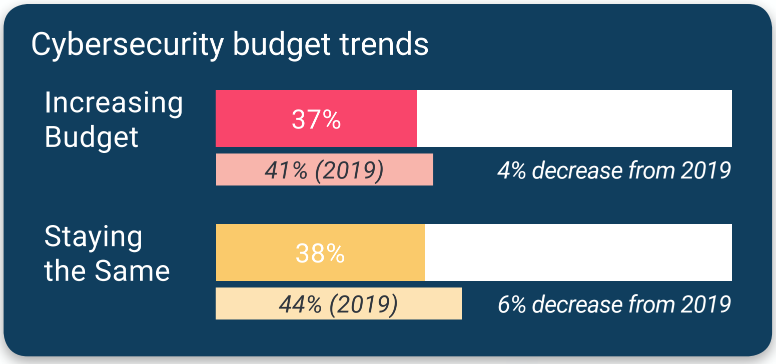
Takeaways

Most institution's IT budgets will continue to grow or stay the same in order to maintain or improve technology. Based on survey results, it is unclear why institutions in the $250M - $500M range appear to be shifting their budgets away from IT, but the study indicates less IT spending is expected in 2020 for this group.

Budgeting - Cybersecurity

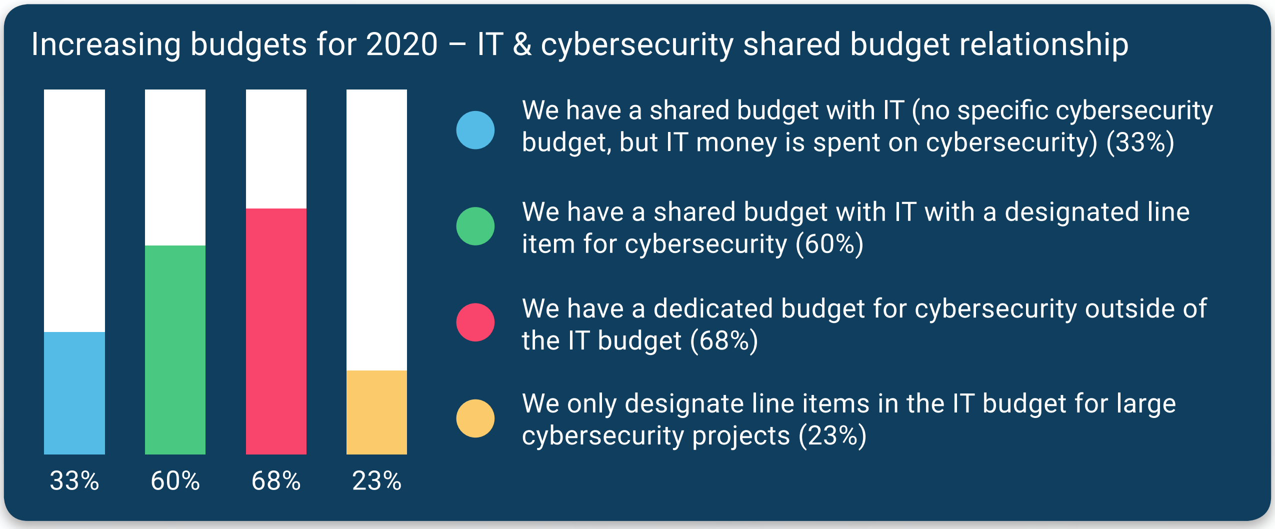
Significant Finding

Findings show 37% percent of financial institutions will increase their cybersecurity budget in 2020; 38% will maintain the same budget.


Cybersecurity budget trends

Diving Further

Institutions who have a dedicated cybersecurity budget separate from the IT budget are more likely to increase their budget (68%) than those who only have a shared budget with IT (33%) or those who only designate a line item for major cybersecurity projects (23%).


Increasing budgets for 2020 – IT & cybersecurity shared budget relationship

Takeaways

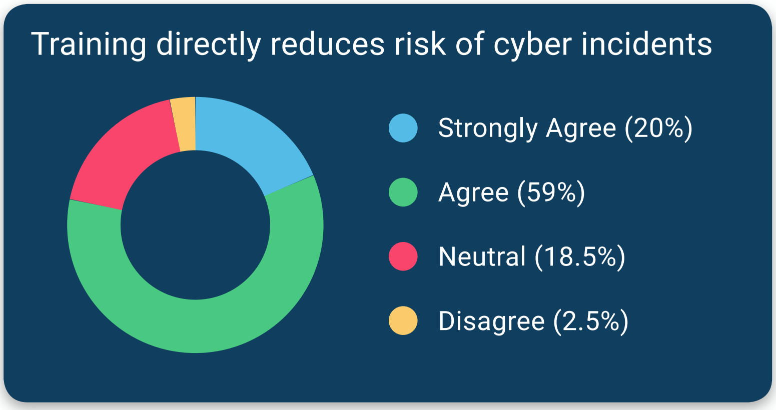
ISOs who wish to increase resources and budget for cybersecurity should work with senior management to fully separate the cybersecurity budget from the IT budget. If a separate budget is not possible, then a separate line item is the next most effective option.

Training

Employee training is a critical part of any layered security program to help prevent and reduce the damage of cybersecurity incidents in a financial institution. The findings below give insight into how institutions are managing their training programs, and the impact training makes.

Significant Finding

Most institutions (79%) believe their cybersecurity training directly reduces the risk of cybersecurity incidents.

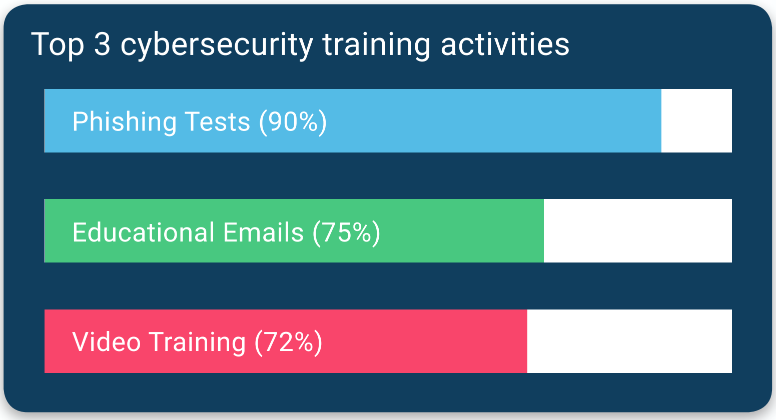


Training directly reduces risk of cyber incidents

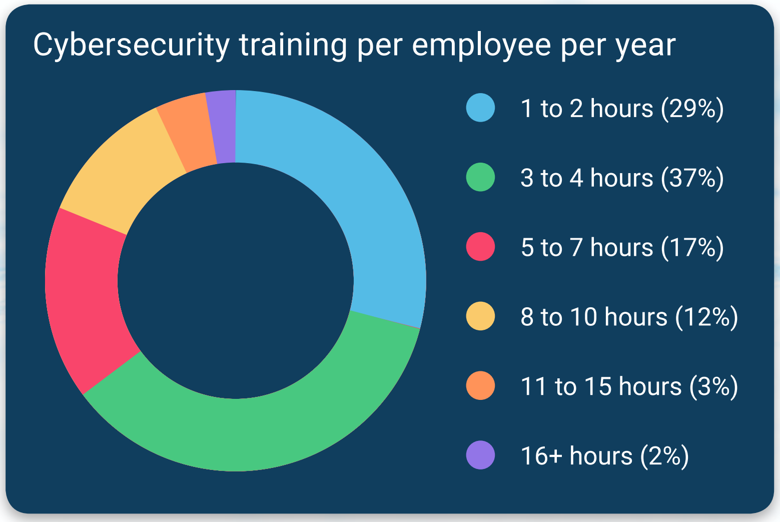
Diving Further

The top three cybersecurity training activities were phishing tests (90%), educational emails (75%), and video training (72%).

When asked how many hours of cybersecurity training per year an employee receives on average, 37% of respondents said 3 to 4 hours.



Top 3 cybersecurity training activities

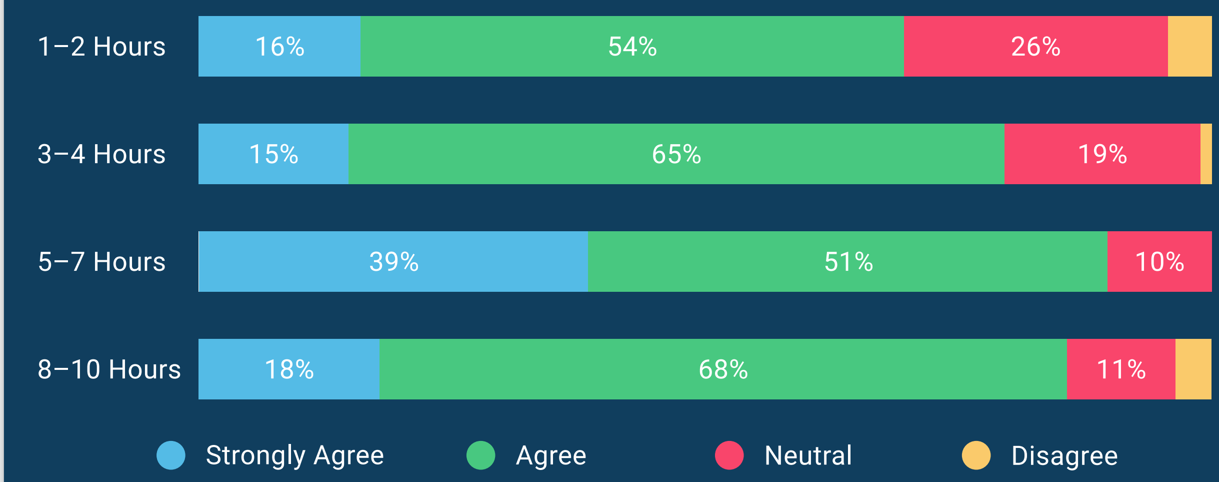


Cybersecurity training per employee per year

Diving Further

Of the institutions who provided 5-7 hours of cybersecurity training per year to each employee, 38% strongly agree that their training reduces risk. Of the institutions who provided 3-4 hours, 15% strongly agreed that their training reduces risk.

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.

Takeaways

The survey indicates increasing the amount of time spent training per employee per year by just a couple hours could greatly improve the effectiveness of the training and, subsequently, reduce risk.

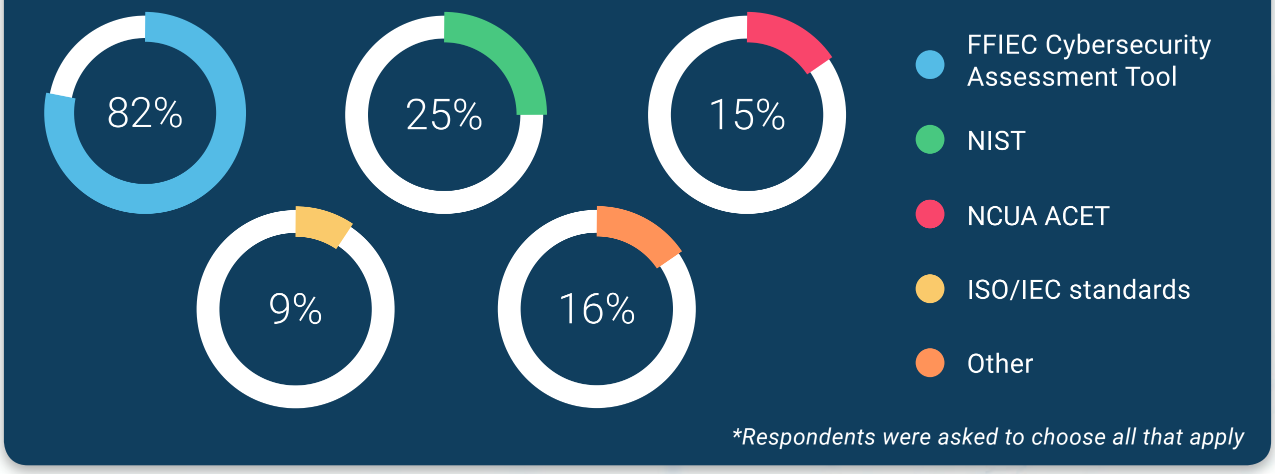
Cybersecurity Tools and Frameworks

Various organizations now provide cybersecurity tools and frameworks used by financial institutions. The data below gives insight into which tools are being used and how they are being used to improve cybersecurity.

Significant Finding

A large majority of institutions (82%) use the FFIEC Cybersecurity Assessment Tool (CAT) as the primary method of evaluating the maturity of their cybersecurity program.

Cybersecurity framework or tool usage for financial institutions



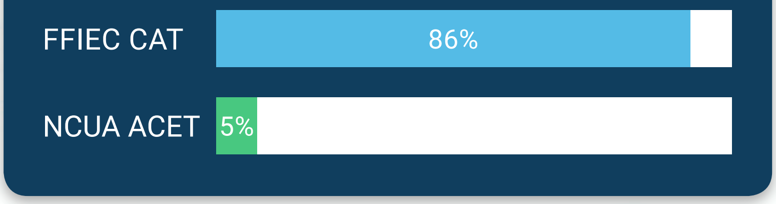
*Respondents were asked to choose all that apply

Diving Further

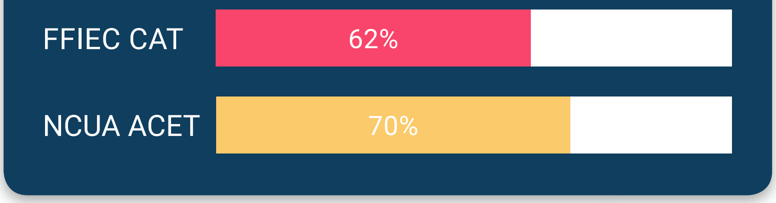
When separated by type of financial institution, we see 86% of banks use the CAT; while 70% of credit unions use the Automated Cybersecurity Examination Tool (ACET).

** Based on the FFIEC CAT, ACET is an assessment tool provided by the NCUA for use in examinations. The tool builds on the CAT with additional commentary and a document request list.*

Banks usage of FFIEC CAT vs. NCUA ACET*



Credit Unions usage of FFIEC CAT vs. NCUA ACET*

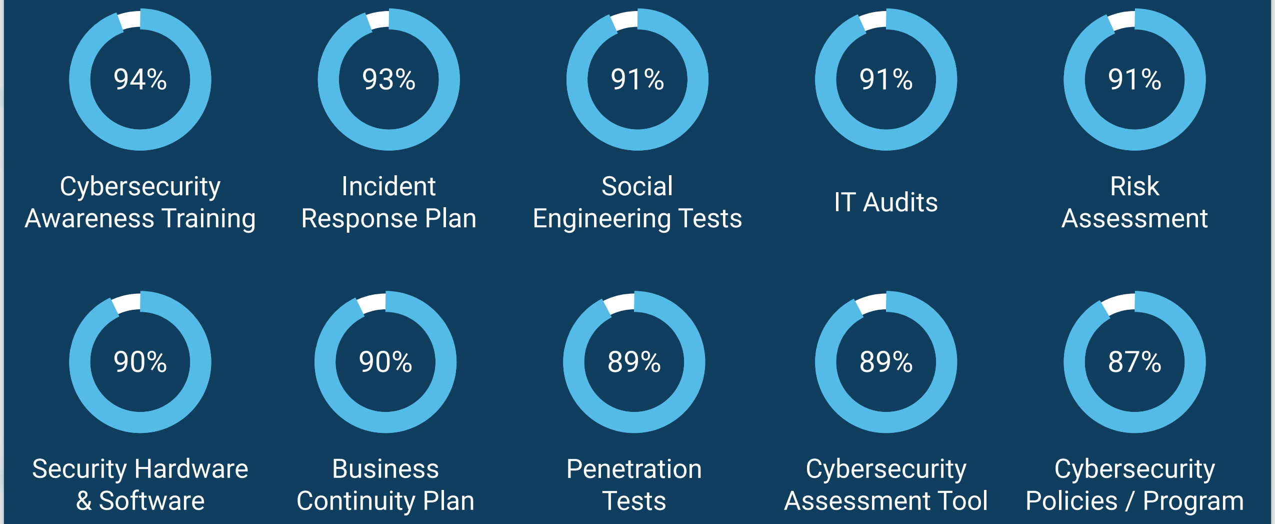


Takeaways

Most institutions have adopted a cybersecurity framework to improve their cybersecurity posture and meet examiner expectations.

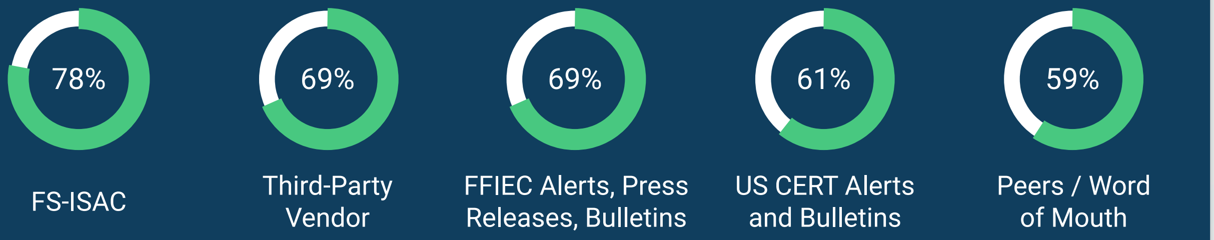
When asked, 87% of institutions said they use a framework as a compliance requirement. The 2020 survey indicates credit unions have been quick to adopt the NCUA's ACET, since it is now becoming an expected part of the examination process.

Top 10 contributions to an institution's overall cybersecurity posture



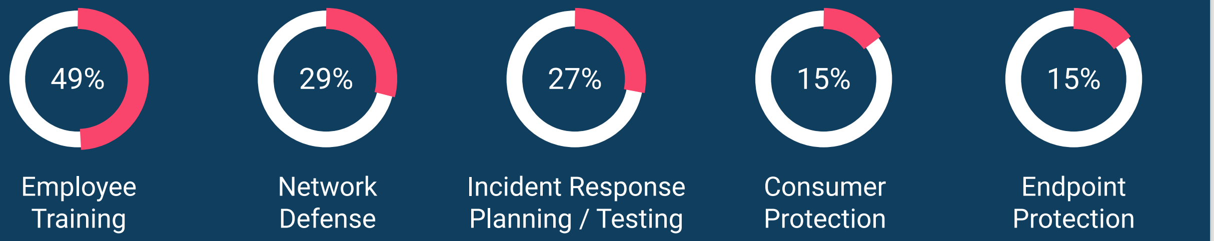
**Respondents were asked to choose all that apply*

Top 5 sources institutions use to learn about new cyber threats



**Respondents were asked to choose all that apply*

Top 5 areas needing additional resources to improve cybersecurity



**Respondents were asked to choose their top two choices*

Incident Response

Significant Finding

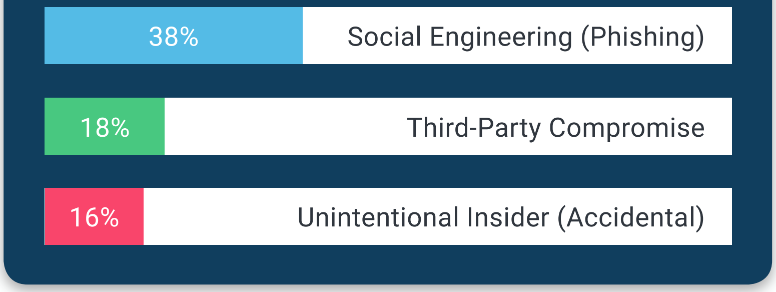
The top three incidents experienced by institutions in 2019 were social engineering (phishing), third-party compromise, and accidental security incidents by employees.

Of those who experienced an incident, 35% claimed it negatively impacted their customers or members.

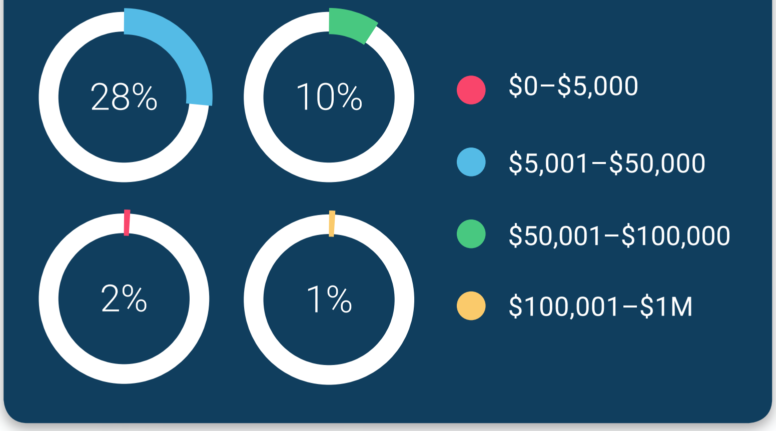
Diving Further

When asked how often institutions performed social engineering tests in 2019, 29% said they perform tests once per year and 30% test quarterly.

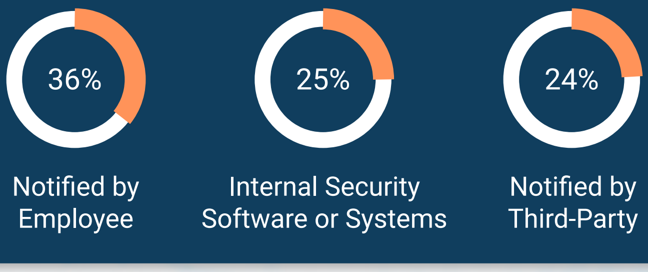
Top 3 incidents experienced in 2019*



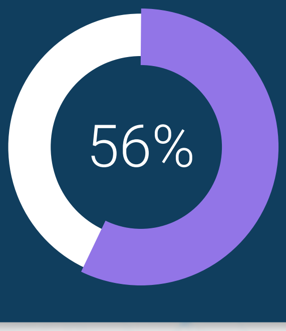
Incident recovery costs in 2019



Top 3 ways significant incidents were discovered



Percentage of incidents discovered within 24 hours*



Respondents were asked to choose all that apply

Takeaways

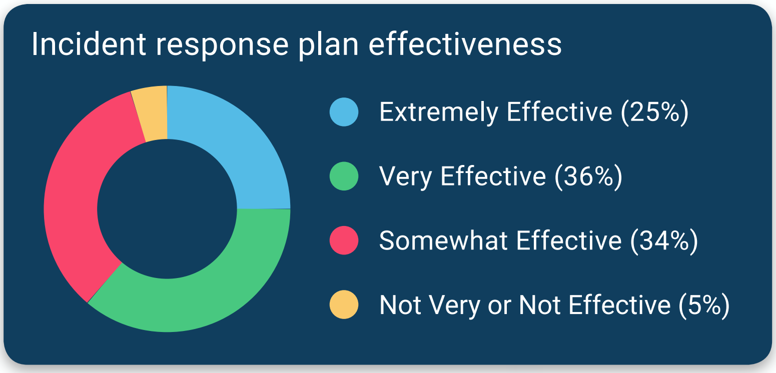
Phishing attacks are still the top cyber threat to institutions. While respondents indicated the financial damage from reported phishing incidents was relatively small, other operational and reputation risks remain high. Increasing the number and frequency of social engineering tests makes your employees more resilient to cyber attacks.

Incident Response Plan

Significant Finding

When asked, 61% of institutions felt their incident response plan was extremely or very effective, and 5% felt their incident response plan was not effective.

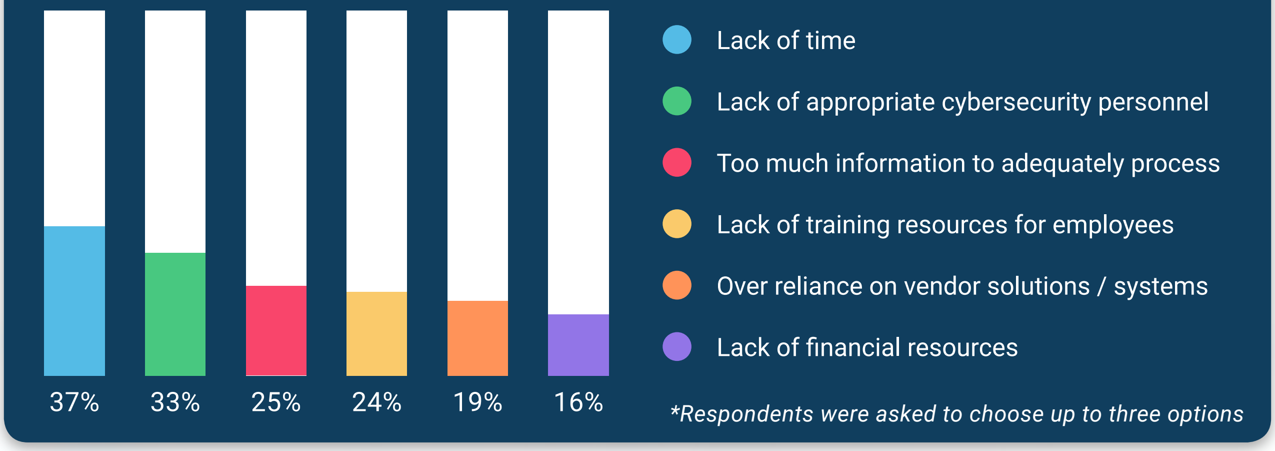
Incident response plan effectiveness



Diving Further

Of the institutions who said their plan was ineffective to adequately mitigate or remediate cybersecurity incidents, the top three barriers included: lack of time (37%), lack of appropriate cybersecurity personnel (33%), and too much threat information to process (25%).

Biggest barriers to mitigating and remediating cybersecurity incidents



Respondents were asked to choose up to three options

Takeaways

A cybersecurity incident is inevitable, but institutions continue to struggle with securing resources to help build a strong incident response plan.

For institutions that hope to increase their IT or cybersecurity budget, we recommend following the best practices outlined in this report. To specify, we recommend reporting to the Board more frequently, separating out the cybersecurity budget from the IT budget, and including a Board member with relevant IT experience.

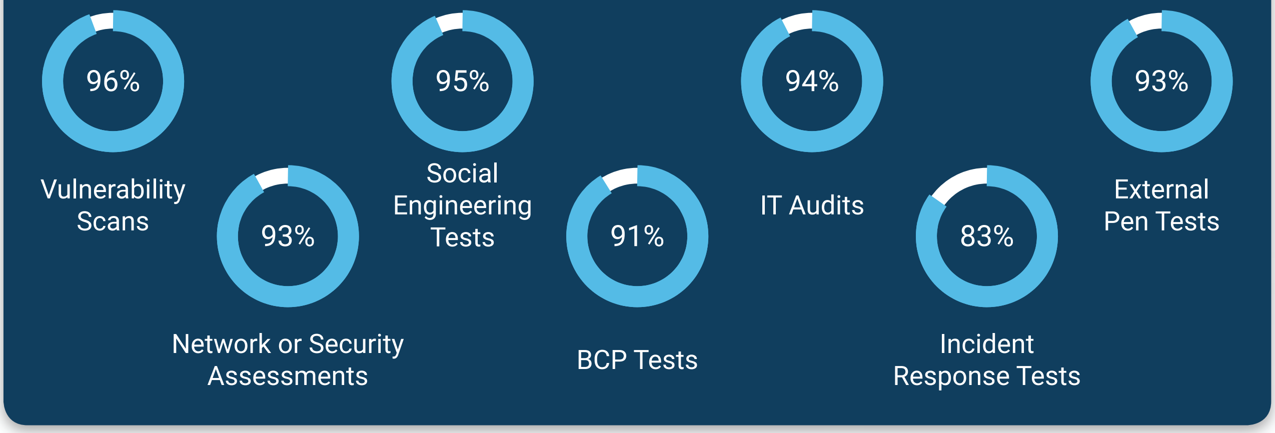
Assurance & Testing

Performing frequent internal and external cybersecurity audits, assessments, and tests is key to evaluating controls and being prepared for attacks. The data shows financial institutions are implementing many of the testing best practices known in the cybersecurity industry.

Significant Finding

Of the various forms of assurance and testing, financial institutions, on at least an annual basis, most frequently performed vulnerability scans (96%), social engineering tests (95%), and IT audits (94%). Larger, more complex, tests and projects were done with less frequency.

Most performed testing activities in 2019 (at least annually)



Diving Further

BCP tests and exercises saw one of the biggest increases in regularity with a jump from 15% performing quarterly tests in 2018 to 21% performing quarterly tests in 2019. Furthering the trend, 28% plan to perform BCP tests quarterly in 2020.

Similarly, institutions plan to increase quarterly incident response testing. In 2019, 14% performed a quarterly incident response test. In 2020, 27% plan to perform quarterly incident response tests or exercises.

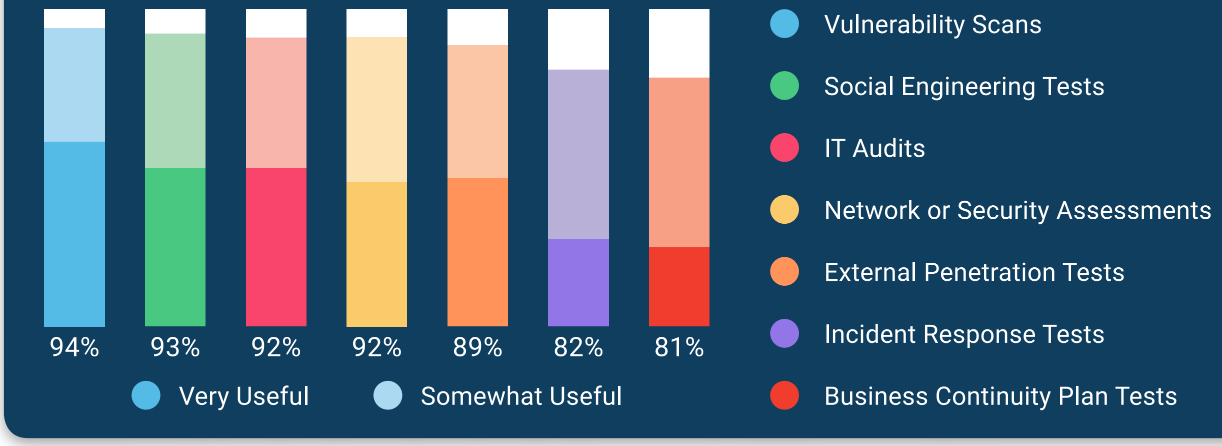
Takeaways

Institutions are increasing testing in several areas with BCP and incident response receiving the most time and resources. Other tests, such as external penetration tests and network assessments, continue to be important factors for assurance and testing programs, but results show little anticipated growth in frequency.

Value of Testing

The most valued testing activities for improving security posture are vulnerability scans, IT audits, and social engineering tests.

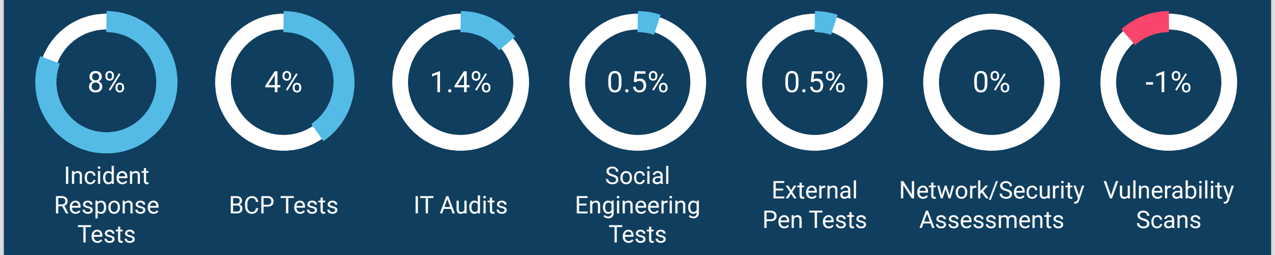
Usefulness of tests in improving an institution's security posture



Diving Further

Even though institutions feel vulnerability scans, IT audits, and social engineering tests are the most valued, institutions are only increasing frequency of these services marginally in 2020.

Increase or decrease in planned testing activities from 2019 to 2020



Shown on a 10% maximum scale

Takeaways

According to the data, social engineering tests, IT audits, and vulnerability scans were selected as the most valuable activities. Institutions should consider increasing the number of times in which their systems can be tested in order to strengthen their security posture.

Of course, simply increasing the frequency of tests and scans is not the only way to improve security posture. Institutions should also consider the quality and depth of each scan, test, or audit. More in-depth testing allows ISOs to leverage results so they can obtain additional funding and resources to improve the institution's security posture.

Vendor Management

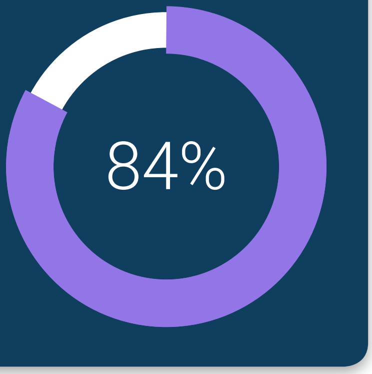
Vendor management is a core component of an institution's cybersecurity program and is reportedly one of the most frustrating aspects of an ISO's job. The data in this section highlights trends in institution vendor management processes.

Significant Finding

The majority of institutions (84%) reported they evaluate cybersecurity controls of vendors to ensure vendors are resilient against cybersecurity incidents.

Vendor cybersecurity evaluation

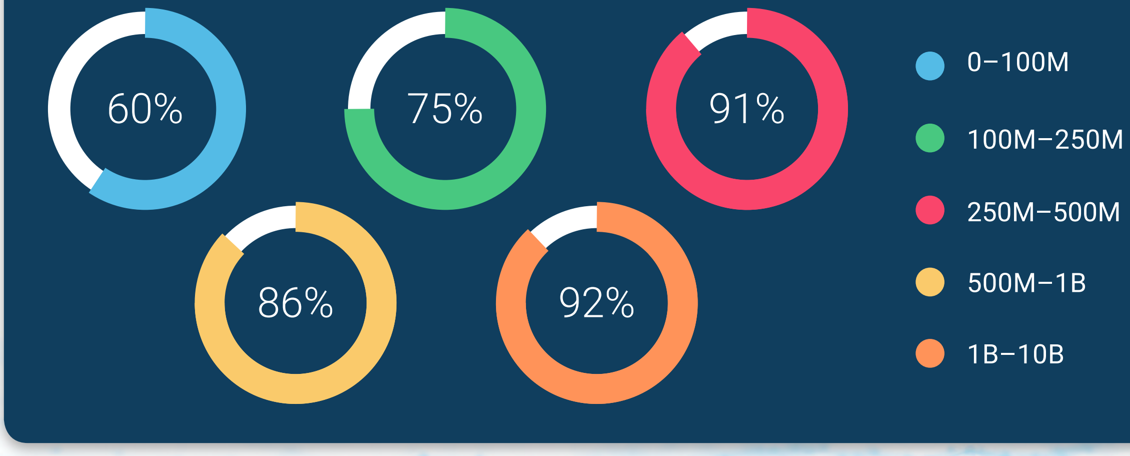
Percentage of institutions who report they evaluate cybersecurity controls of vendors



Diving Further

Smaller institutions are less likely to evaluate the effectiveness of their vendor's cybersecurity controls.

Likelihood of evaluating cybersecurity controls of vendors by asset size



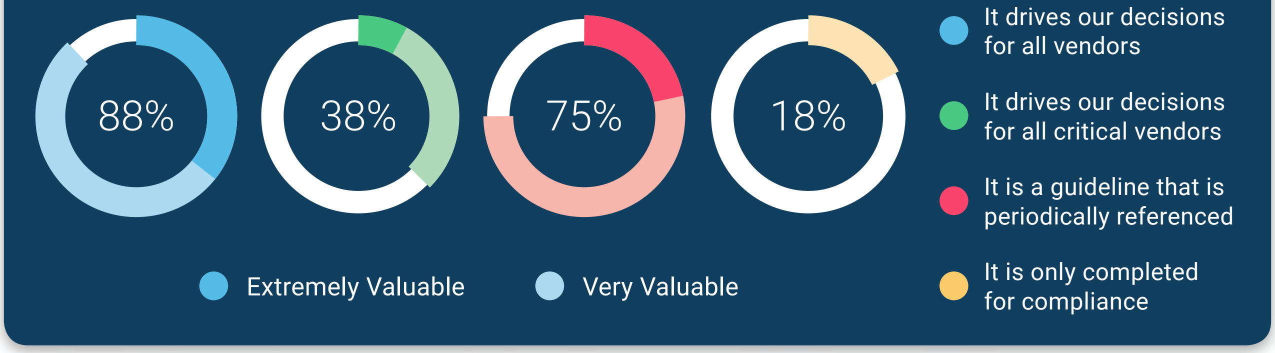
Takeaways

According to the results, it appears smaller institutions are less likely to review their vendor's cybersecurity controls, which could increase their exposure to additional risk. As the use of and dependency on third-parties continues to increase, all institutions should consider ways to improve their processes for assessing the sufficiency of third-party cybersecurity controls.

Vendor Management Process

Institutions who said using a vendor management program was very or extremely valuable were much more likely to use their vendor management process to guide all vendor decisions.

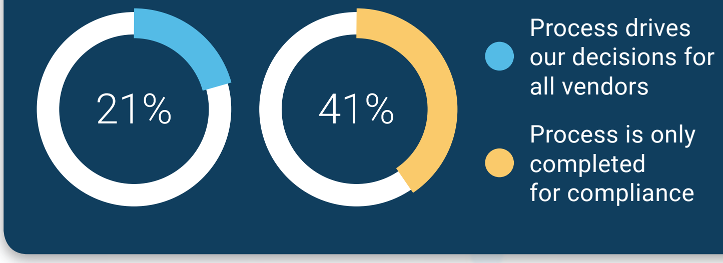
Value of the vendor management process



Diving Further

Of the institutions who said they only complete their vendor management process in order to maintain compliance, 41% had a vendor who experienced an incident which had a negative impact on the financial institution.

Institutions that were impacted by an incident to a vendor



Takeaways

Institutions who perceive the vendor management process as valuable are actively mitigating risk. Conversely, institutions who view their vendor management process simply as a compliance requirement are more likely to expose themselves to the types of risk the vendor management process is designed to avoid.

Financial institutions cannot abdicate their responsibilities assumed by third-parties. Instead, they must have a strong vendor management program to evaluate, oversee, and manage their third-party relationships. As part of this program, ISOs should view the vendor management process as important to the institution's overall security and should work to communicate this value with the rest of the organization.

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 11 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 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 questions or media inquiries, contact us at **tandem.app/contact**

Tandem™