

THE STATE OF

CYBER SECURITY

IN THE FINANCIAL INSTITUTION INDUSTRY

2022 SURVEY REPORT





Contents

- 4** About the Report
- 5** Demographics
- 6** Board Oversight
- 8** Cybersecurity Oversight
- 10** Budgeting
- 12** Tools & Frameworks
- 14** Training
- 16** Vendor Management
- 18** Assurance & Testing
- 20** Conclusion
- 21** All Survey Responses
- 26** About the Contributors
- 27** About Tandem

About the Report

This report includes the results of a survey of cybersecurity professionals working in the financial institution industry. The survey resulted in 310 responses which led to several informative observations to help community financial institutions improve their cybersecurity posture.

PURPOSE

The purpose of the survey was to discover information about:

- Board and senior management oversight of a financial institution's cybersecurity program.
- How financial institutions manage cybersecurity.
- Financial resources provided to increase security posture.
- Training standards and best practices across the industry.
- The effectiveness of implemented best practices.
- Trends in cybersecurity and technology implemented by financial institutions.



TIMEFRAME

This survey was conducted between March 30, 2022 and June 30, 2022.



PARTICIPANTS

All 310 survey participants work for a financial institution based in the United States.



AUTHOR

The survey was conducted by Tandem, LLC. For more information about Tandem, visit Tandem.App.

METHOD

Survey results were reviewed by a team of cybersecurity experts and analysts at Tandem. The results displayed in this report feature trends across years and correlations between questions. Only significant answer options are represented in the observations. This means percentages are rounded to the nearest whole number and not all percentage totals in this report equal 100%.

To participate in future surveys, visit Tandem.App/Survey-Sign-Up.

STRUCTURE

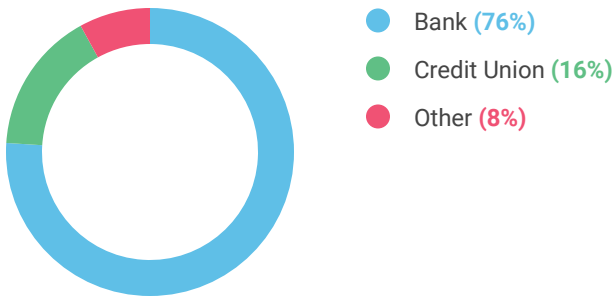
The report is structured into sections for each survey topic. Each topic is divided into three subsections to better share results. The subsections include:

- **Observations**, which provides an overview of findings from the survey.
- **Diving further**, which goes deeper into the observations by highlighting trends, cross-referencing responses across the survey, or by comparing responses with prior years.
- **Takeaways**, which provides a summary and some tangible recommendations for improving cybersecurity posture.

Demographics

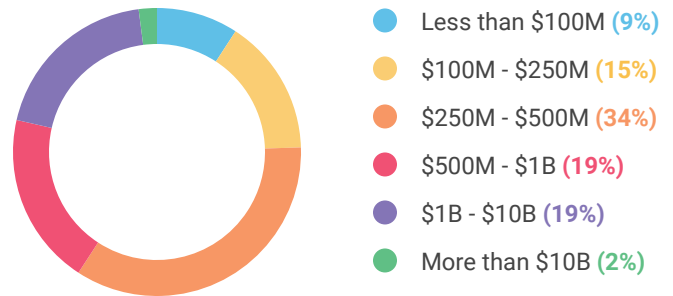
INSTITUTIONS SURVEYED: TYPES

Of those who responded, 76% work for a bank, 16% work for a credit union, and the remaining participants work for other financial institutions (e.g., mortgage companies, trust companies, etc.).



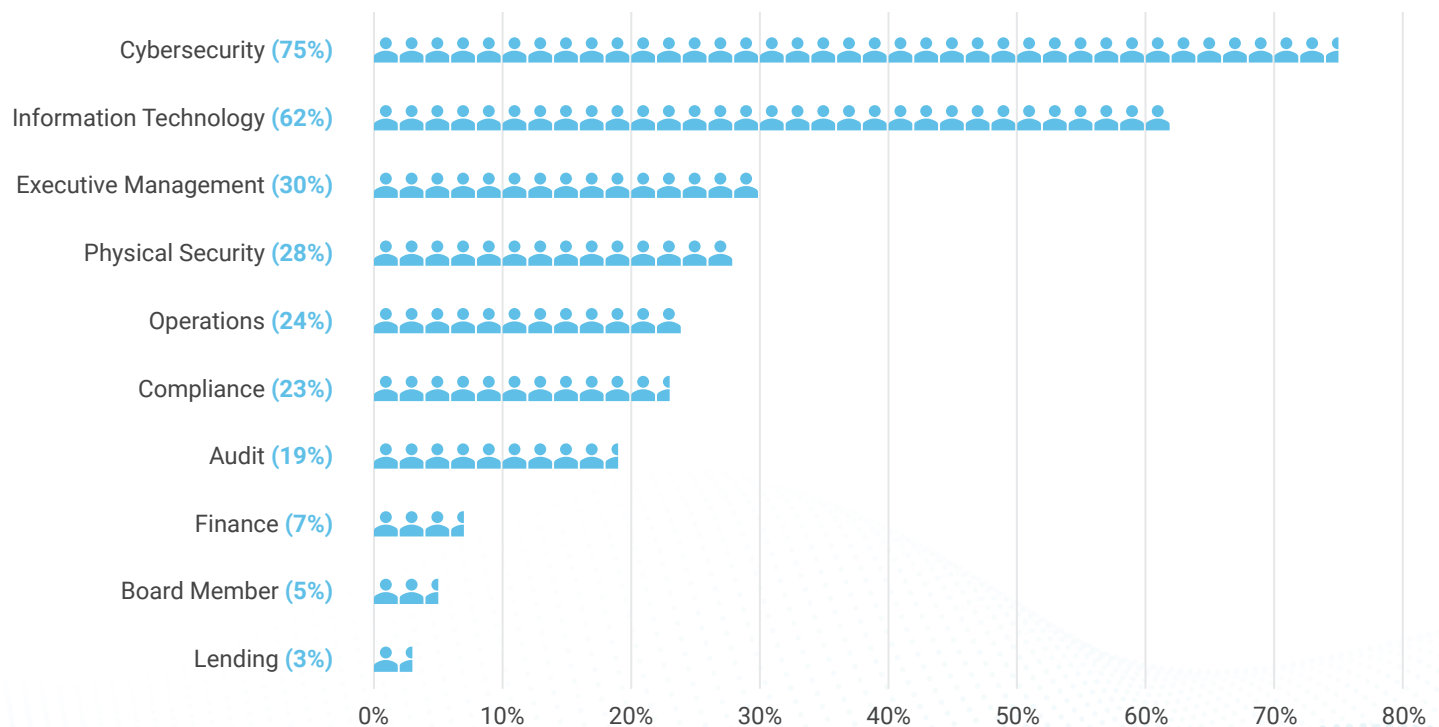
INSTITUTIONS SURVEYED: ASSETS

Most respondents were from regional community banks, but a good representation came from larger community institutions, with 21% of responding institutions reporting over \$1 billion in assets.



ROLES & RESPONSIBILITIES

Survey participants worked primarily within cybersecurity or information technology roles. However, participants also reported serving in roles in operations, compliance, audit, and finance, with 5% of respondents serving as Board Members. Participants were asked to select all that applied.

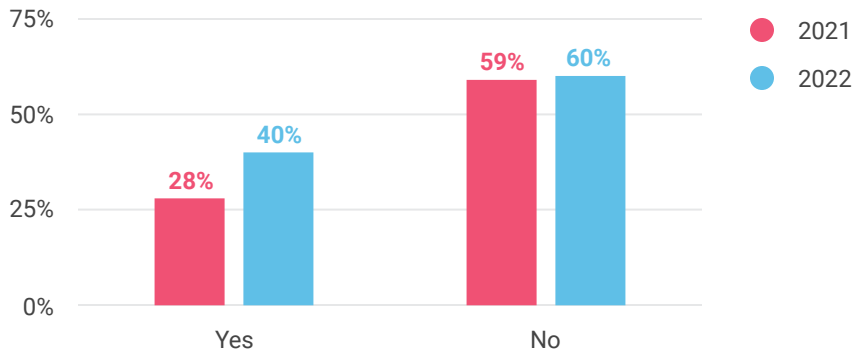


Board Oversight

OBSERVATIONS

This year represents the highest percent of participants who state the Board has someone with IT or cybersecurity experience, up 8% over last year's survey. While this is a positive trend, most respondents still state their Board does not have anyone with IT or cybersecurity experience.

PERCENT OF INSTITUTIONS WHO HAVE BOARD MEMBERS WITH IT / CYBER EXPERIENCE

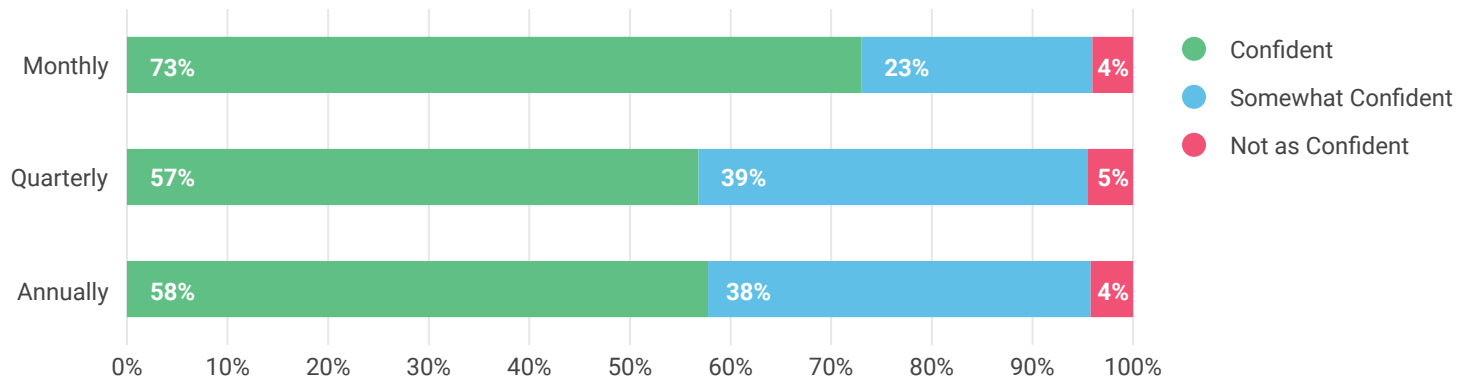


WHAT THIS MEANS

It is becoming more common to have technology representation on the Board, but it is still only happening in 40% of institutions.

This year's data also seems to indicate a direct correlation between more frequent reports to the Board and confidence in the institution's overall cybersecurity posture.

CONFIDENCE IN CYBERSECURITY POSTURE BY BOARD REPORT FREQUENCY



WHAT THIS MEANS

The more often a Board is informed on cybersecurity, the more confident cybersecurity professionals are about the Board's ability to make informed decisions on technology matters.



CONTRIBUTOR QUOTE TIM LEONARD

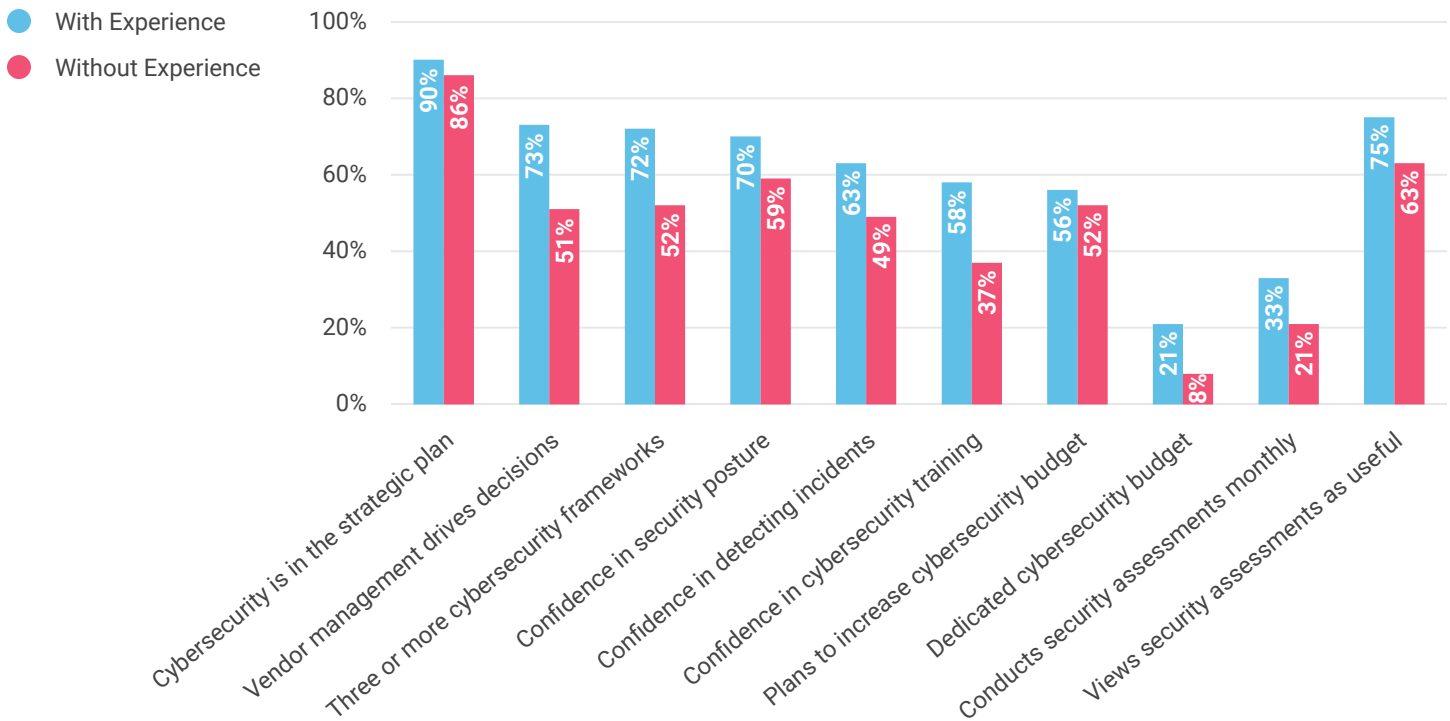
A Board Member with effective business acumen, who understands IT and cybersecurity is not a unicorn. Go find one.



DIVING FURTHER

In comparing the question about the Board’s experience against all other questions in the survey, almost all questions received a more cybersecurity-minded response when the institution had a Board Member with IT or cybersecurity expertise.

INSTITUTION ANSWERS ABOUT BOARD MEMBER IT / CYBER EXPERIENCE COMPARED WITH OTHER SURVEY RESPONSES



TAKEAWAY

Effective cybersecurity governance starts at the top. When cybersecurity and IT are represented at the Board-level, there is a trickle-down effect which results in a heightened culture of cybersecurity across the entire financial institution. Influence from the Board of Directors is a must-have for financial institutions desiring to improve cybersecurity and remain technologically competitive in today’s evolving financial market.

RECOMMENDATION

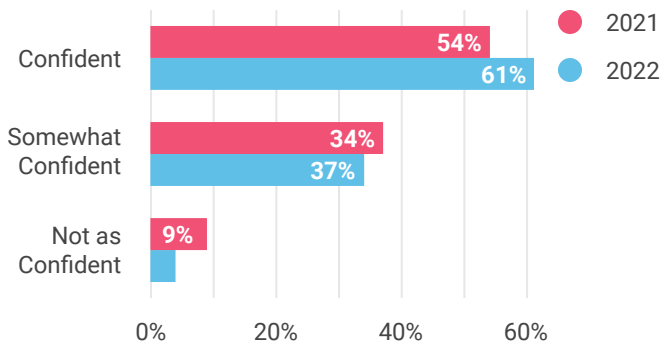
When possible, report cybersecurity matters to the Board more often and encourage technology representation on the Board.

Cybersecurity Oversight

OBSERVATIONS

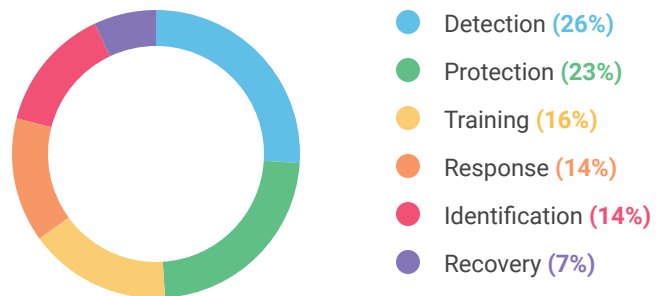
While 61% of respondents stated they were confident in the institution's overall security posture, only 54% stated they felt confident the institution could detect an incident as it was happening.

CONFIDENCE IN SECURITY POSTURE BY ABILITY TO DETECT INCIDENTS



When asked where they would allocate more resources, if available, 26% of survey participants replied with "Detection" controls. This is more than any other area of planned improvement.

WHERE ADDITIONAL RESOURCES WOULD BE ALLOCATED

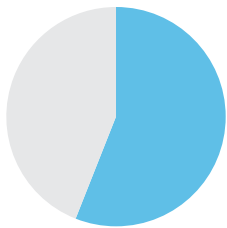


WHAT THIS MEANS

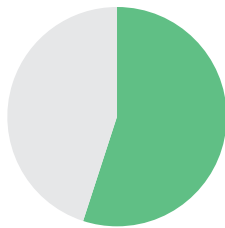
People seem to be more confident in the institution's ability to prevent or respond to a security incident than to detect one as it is happening.

Participants were also asked to select the top three circumstances negatively impacting the success of the institution's cybersecurity strategy. The four most selected answers were related to a lack of time.

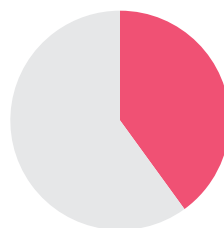
CIRCUMSTANCES NEGATIVELY IMPACTING CYBERSECURITY STRATEGY SUCCESS



Lack of time to manage daily tasks (56%)



Lack of time to analyze data (55%)



Lack of time to keep up with regulatory compliance (40%)



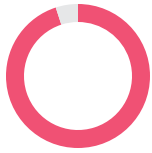
Lack of time to keep up with technology changes (35%)

WHAT THIS MEANS

More than any other circumstance (e.g., money, support, staffing, etc.), a lack of time is experienced as the biggest roadblock to achieving effective cybersecurity oversight.

DIVING FURTHER

Participants were asked to pick the top three circumstances which negatively impacted the success of their cybersecurity strategy. Of the 11 answer options provided:



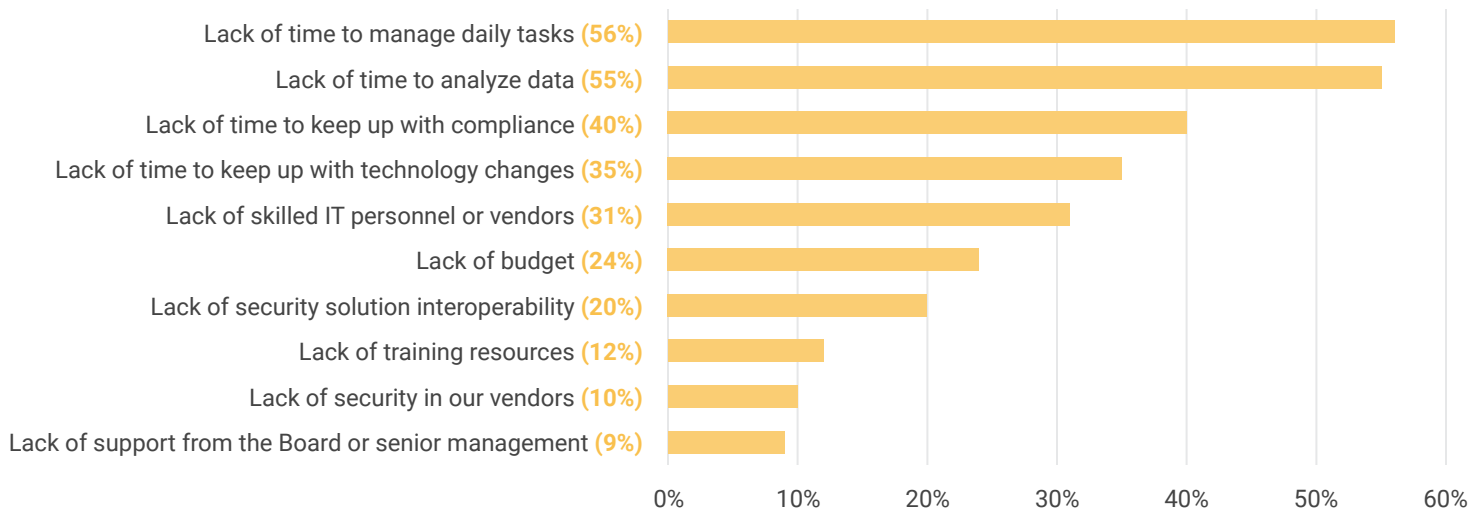
95% selected a "lack of time" answer as one of the three choices.



24% selected a "lack of time" answer for all three choices.

Significant runners up to "lack of time" include lack of skilled personnel, lack of budget, and lack of system integration as circumstances which negatively impact the success of the cybersecurity strategy.

CIRCUMSTANCES NEGATIVELY IMPACTING CYBERSECURITY STRATEGY SUCCESS



TAKEAWAY

"Lack of time" is a difficult circumstance to address. The go-to solutions often involve adding more staff and/or outsourcing, both of which actually create more of a time burden for the immediate future with the hope of a payout later. To address the immediate concern of "lack of time" without adding more personnel to train, manage, and coordinate, here are some strategies to consider.

- **Be realistic** about time requirements as part of strategic planning. Do not plan based on the shortest time a project could take. Build in time for unexpected roadblocks.
- **Review current tasks** to identify activities which are not necessary for cybersecurity staff to complete, then eliminate them. Redistribute tasks to departments or persons with the skills, interests, and time to better manage the tasks. Review current processes to identify steps which could be removed or rearranged to improve efficiency and leave decision-making power for more important tasks.
- **Acknowledge only so much can be done** within the contracted work time. Set appropriate expectations with senior leadership about how much can reasonably be accomplished and agree to respect those limitations.

RECOMMENDATION

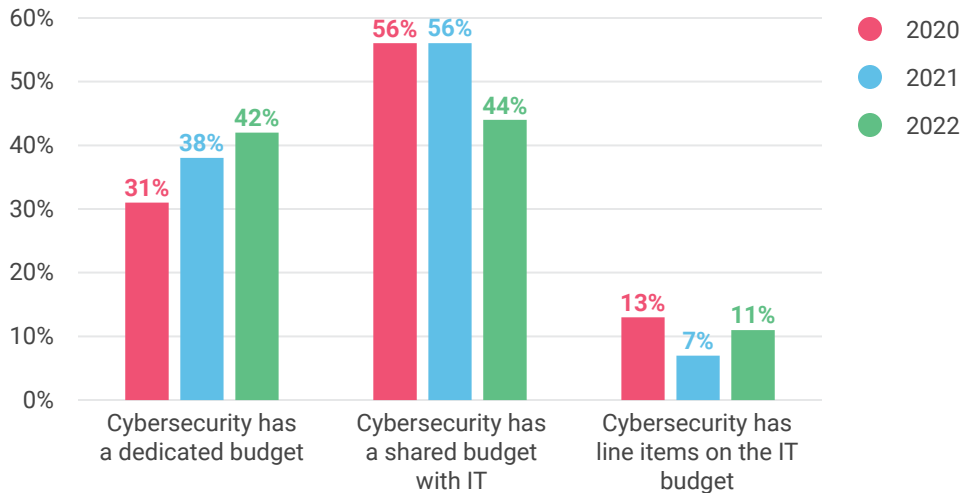
Take steps to maintain a healthy workload, as this has a direct impact on the effectiveness of the institution's cybersecurity oversight.

Budgeting

OBSERVATIONS

Over the last three years, there has been a trend toward separating the cybersecurity budget from the IT budget.

RELATIONSHIP OF CYBERSECURITY & IT BUDGETS



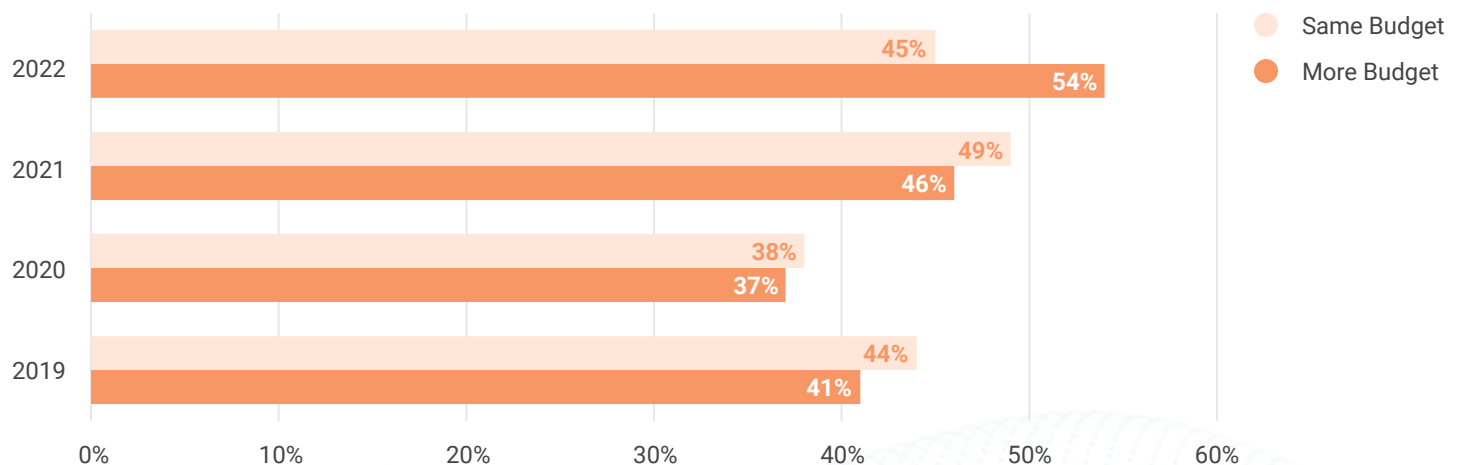
WHAT THIS MEANS

The people involved with strategic planning and budgeting are beginning to recognize cybersecurity as a separate cost from IT expenditures.

DIVING FURTHER

More than half of survey participants plan to increase their cybersecurity budget. Along with this, for the first time since the survey began in 2019, more financial institutions plan to increase their cybersecurity budget rather than keeping it the same.

PLANS FOR NEXT YEAR'S CYBERSECURITY BUDGET



WHAT THIS MEANS

Financial institutions are increasing monetary investments in cybersecurity and plan to spend more on cybersecurity in 2022 than in previous years.



CONTRIBUTOR QUOTE TREY MAUST

The longitudinal nature of this report is highly effective at exposing trends over time - whether good or bad. This allows us to compare and contrast our own responses against industry benchmarks. Most of us may know what is required by statutory or regulatory mandate and what is considered a best practice in the industry, but to see what practices are actually in place at a meaningfully large representative sample of cybersecurity-aware institutions is extremely helpful confirmation.



TAKEAWAY

Budgets for cybersecurity are growing and maturing. This could be a result of increased cybersecurity risk, increased understanding of cybersecurity by the Board of Directors, and/or inflation. Whatever the case, cybersecurity budgetary needs are being addressed and enhanced, which is a healthy direction for the industry.

RECOMMENDATION

Be cautious with how additional cybersecurity funds are allocated. While budgets are growing, the challenge institutions now face is how to use one resource (money) to help compensate for the lack of another resource (time). Cybersecurity funds should be spent on time-saving investments.

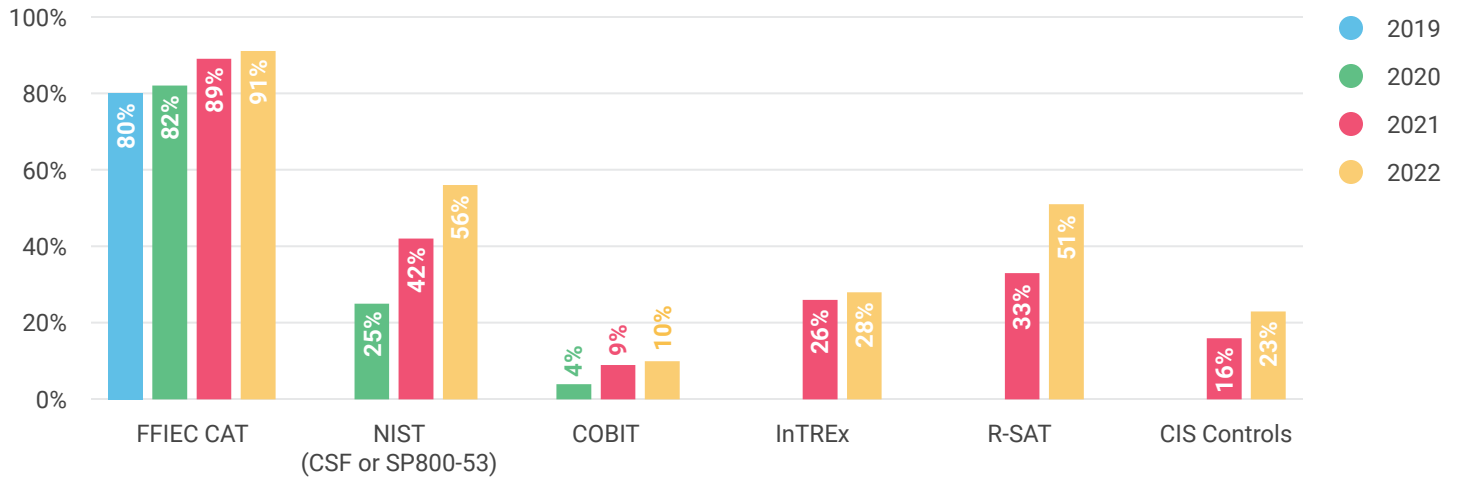
Tools & Frameworks

OBSERVATIONS

Over the past four years, there has been a steady increase in adoption of cybersecurity frameworks and assessment tools.

ADOPTION OF CYBERSECURITY FRAMEWORKS & TOOLS

Note: Not all frameworks and tools were asked about on prior surveys.



CONTRIBUTOR QUOTE CARLOS MORALES

It is interesting and encouraging to see a positive trend of adoption of multiple frameworks over the last few years. Seeing this data validates that institutions must not rely on just one framework, but incorporate guidance from various frameworks and tools in order to build a comprehensive program.

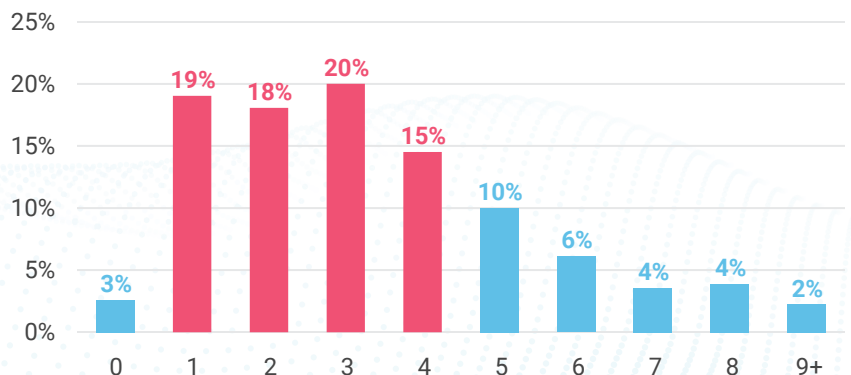


Of the 13 possible answer options, 72% of survey participants reported using one to four cybersecurity assessment tools and frameworks. A quarter of all respondents (25%) report using five or more.

WHAT THIS MEANS

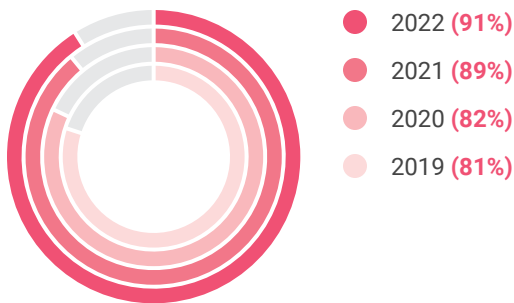
Financial institutions are increasingly turning to frameworks and tools as a significant component of the institution's cybersecurity program.

FRAMEWORKS PER PARTICIPANT



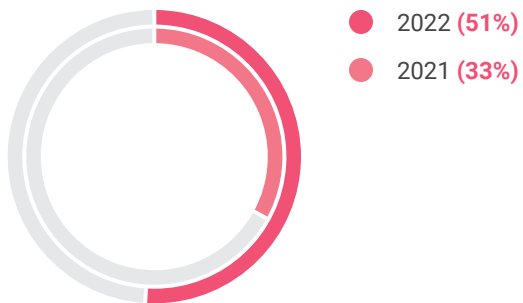
DIVING FURTHER

FFIEC CAT ADOPTION RATE



The most used assessment tool remains the FFIEC Cybersecurity Assessment Tool (CAT), also known by credit unions as the ACET. The CAT continues to gain acceptance year-over-year and is used by almost every survey participant (91%).

CSBS R-SAT ADOPTION RATE



The tool which gained the most traction between 2021 and 2022 was the CSBS Ransomware Self-Assessment Tool (R-SAT) with an adoption rate moving from 33% in 2021 to 51% in 2022.

Both assessment tools were developed specifically for financial institutions and were encouraged to be used by governing bodies. Other frameworks and tools seeing increased adoption include resources from NIST (56%) and the CIS Controls (23%).

WHAT THIS MEANS

Assessment tools specific to the financial industry are the most used by financial institutions. Still, there has been significant growth in institutions adopting technology-industry frameworks.

TAKEAWAY

Tools developed specifically by and for the financial institution industry are more likely to be used by financial institutions. There are several possible reasons for this, including:

- They are encouraged by the industry and are therefore more known.
- They are directly related to the products, services, and risks associated with the industry.
- They are easily accessible and offer the benefits of peer usage.

The continued increase in adoption of tools and frameworks indicates financial institutions find value from these resources, as they provide a benchmark for cybersecurity controls.

RECOMMENDATION

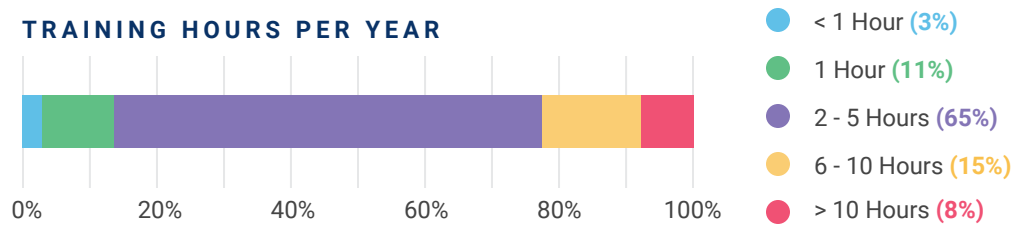
When choosing to complete a cybersecurity tool or framework, be strategic about the decision. Keep the purpose of the assessment in mind. Framework fatigue is a real thing and could be a contributing factor in the lack of time cybersecurity professionals are experiencing.

Training

OBSERVATIONS

Training hours remain steady across the years with most institutions conducting two to five hours of training per employee each year.

TRAINING HOURS PER YEAR



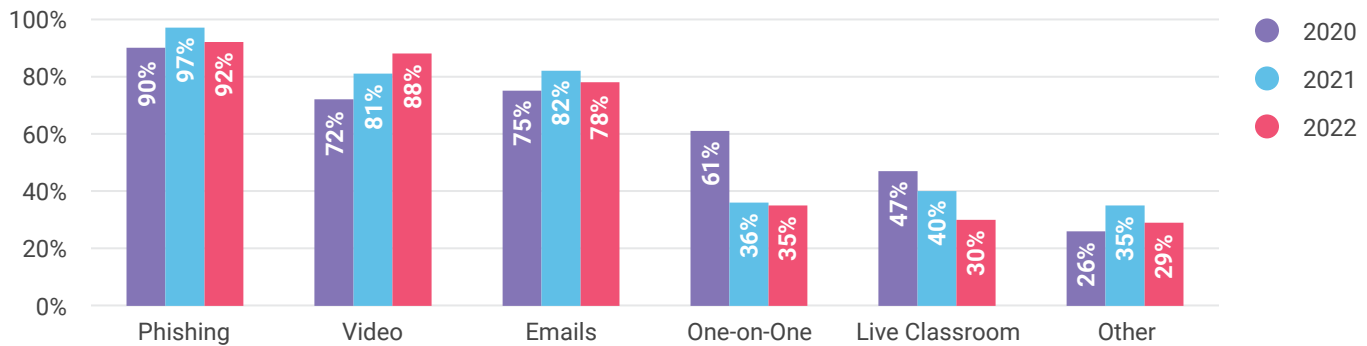
CONTRIBUTOR QUOTE CHRIS COLE

As a bank, our employees are our most valuable asset. The survey shows how much security awareness training improves overall security posture, so it is important we provide our employees with the best training possible to strengthen our security.



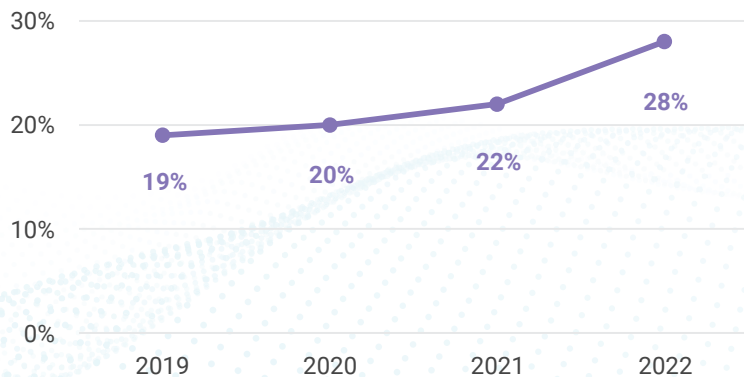
Phishing tests (92%) continue to remain the most popular type of security awareness training, followed closely by video training (88%) and educational emails (78%). When comparing data with previous years, the only type of training which increased in use from 2021 to 2022 was video training. All other forms of training had a reported decrease.

SECURITY AWARENESS TRAINING POPULARITY BY TYPE



That said, there is a steady increase in the percent of institutions who “strongly agree” with the statement: “My financial institution’s cybersecurity training directly reduces the risk of cyber security incidents.”

CONFIDENCE IN CYBER TRAINING'S ABILITY TO REDUCE RISK OF INCIDENTS



WHAT THIS MEANS

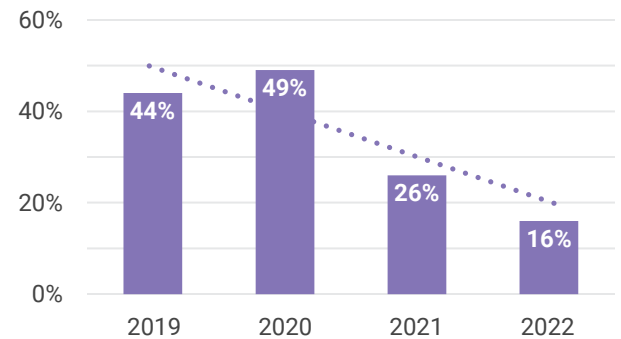
While training techniques remain largely the same, training quality seems to be improving.

Over the last four years, participants were asked how they would spend additional cybersecurity resources if they had them. Employee training topped the list from 2019 through 2021. However, this year, employee training came in third place (16%) behind technical controls for detection (26%) and protection (23%).

WHAT THIS MEANS

People do not wish to spend as much on employee training this year. This could be for several reasons, such as plans to invest in technical controls, changes in risk, or more cost-effective training resources available from federal agencies, banking associations, and businesses.

PLANNED INVESTMENT IN TRAINING

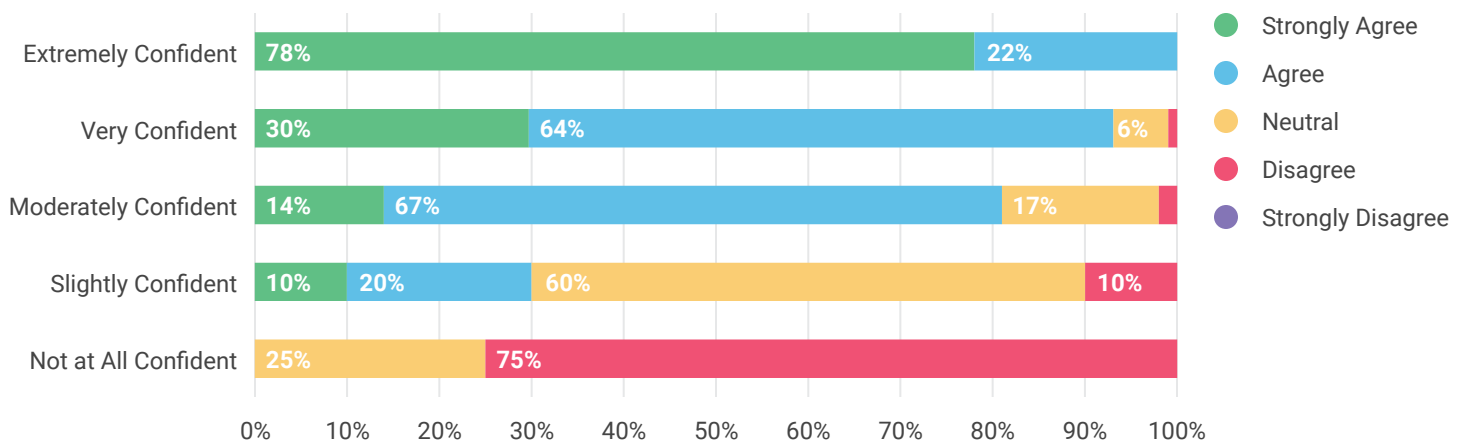


DIVING FURTHER

There is a positive correlation between confidence in an institution’s overall cybersecurity posture and agreement with training effectiveness. Cybersecurity professionals who strongly agree their training reduces cyber incidents are also likely to feel confident in their overall security posture.

Conversely, those who tend to believe their training does nothing to reduce cyber incidents also feel "not at all" confident about their overall security posture.

CONFIDENCE IN SECURITY POSTURE BY EFFECTIVENESS OF CYBERSECURITY TRAINING



DIVING FURTHER

People are both the best defense and weakest link in a financial institution’s cybersecurity program. Ensuring employees are properly prepared through training remains a critical component in improving the institution’s overall cybersecurity posture.

RECOMMENDATION

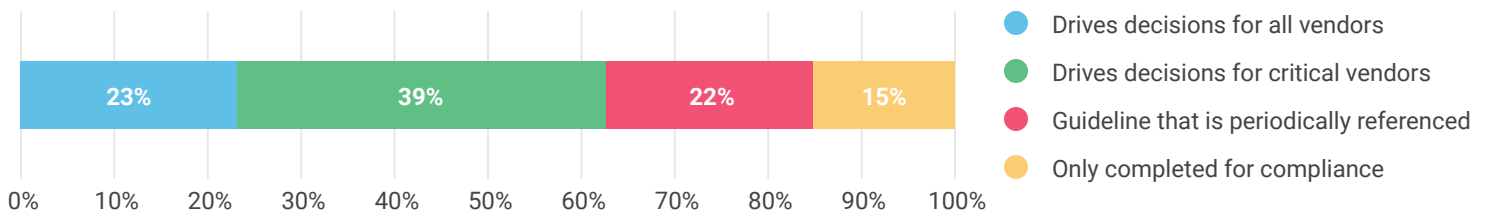
As training is a long-standing component of many cybersecurity programs, a good next step for most would be to look for ways to continue improving training effectiveness, in a time and cost-friendly manner. Start a conversation with other security professionals who feel confident about the effectiveness of their cybersecurity training and discuss ways to make your training more valuable.

Vendor Management

OBSERVATIONS

Most participants report the vendor management program is used to drive decision making (62%), but part of the industry (15%) still uses vendor management only to achieve compliance with laws and regulations.

HOW THE VENDOR MANAGEMENT PROGRAM IS USED



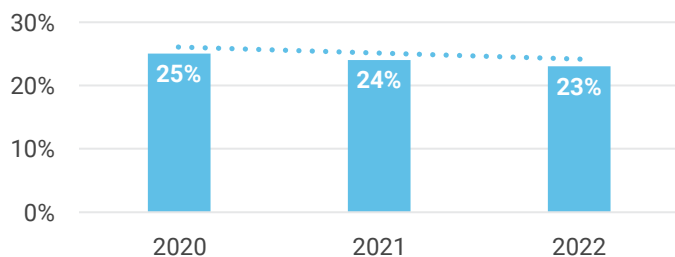
WHAT THIS MEANS

Most of the industry understands the risk posed by third parties and finds value in vendor management beyond just compliance purposes.

DIVING FURTHER

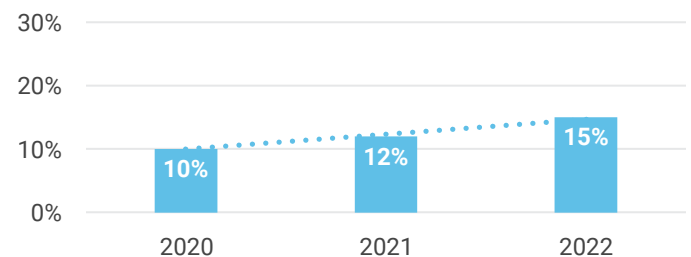
When comparing data across years, there seems to be a slight negative trend in two of the answer options about how the vendor management program is used.

DRIVES DECISIONS FOR ALL VENDORS



Participants who reported using the program to drive decisions for all vendors decreased from 25% in 2020 to 23% in 2022.

ONLY COMPLETED FOR COMPLIANCE



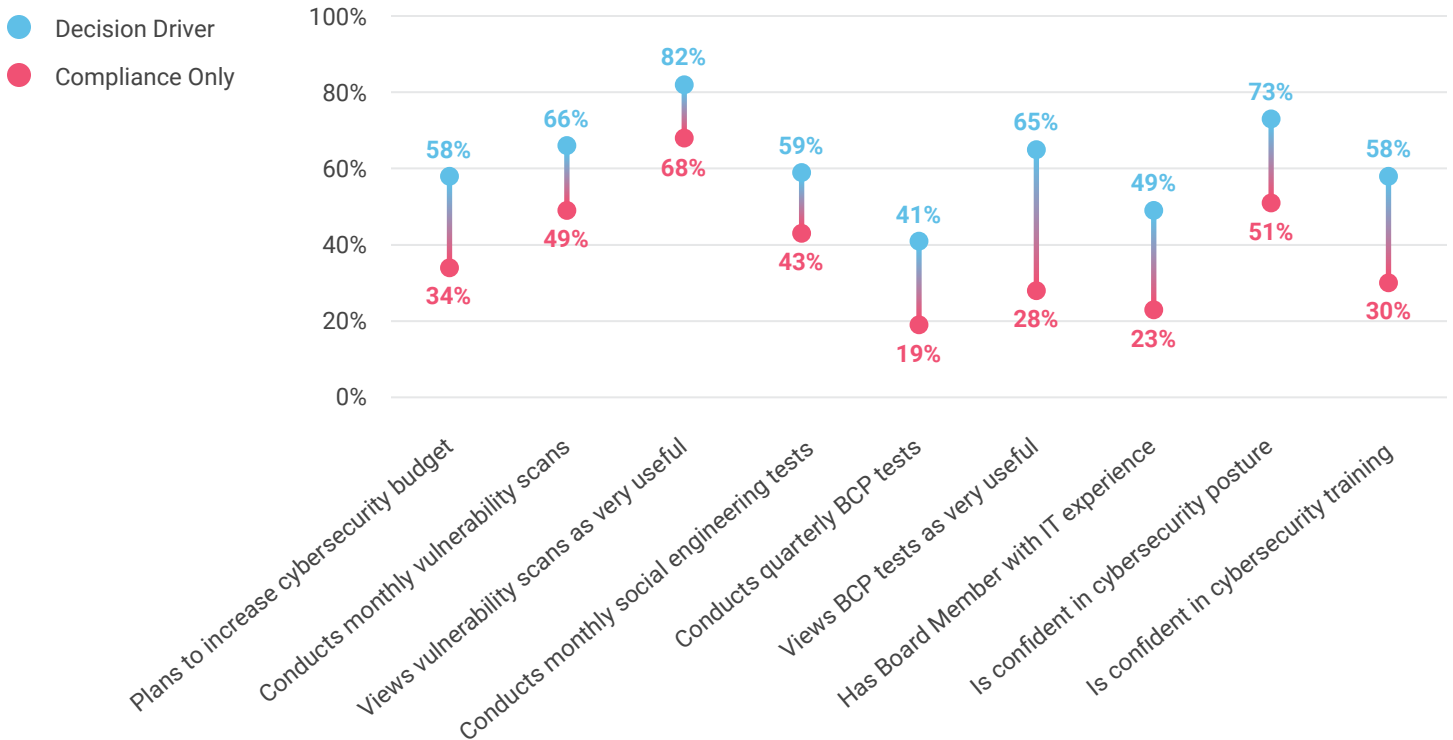
Participants who reported using the program only for compliance purposes increased from 10% in 2020 to 15% in 2022.

WHAT THIS MEANS

Some financial institutions feel unsure about the value of their vendor management program. The exact reason is unknown. Some factors could involve shifting expectations around emerging topics (e.g., fintechs, digital assets, subcontractors, supply chains, incidents, etc.), outsourcing the program to third parties, or a lack of clarity on how vendor management influences cybersecurity.

There is a correlation between the responses to this question and responses to other questions related to the institution's cybersecurity posture. Most participants who said vendor management is a decision-driver also had a positive view of other security practices. Conversely, participants who said vendor management is for compliance only had a less positive view of other practices.

RELATIONSHIP OF VENDOR MANAGEMENT PROGRAM AND OTHER SECURITY PRACTICES



WHAT THIS MEANS

Institutions who recognize cybersecurity programs as useful reap the benefits of those tools in the form of improved cybersecurity posture and confidence in their programs. Institutions who maintain cybersecurity programs only for compliance purposes have poorer cybersecurity posture, in addition to experiencing these programs as a burden.

TAKEAWAY

When programs are designed with compliance as the primary objective, they often miss the greater mark of security. However, when programs are designed security-first, financial institutions often experience compliance as a result. As third-party incidents, zero-day vulnerabilities, and supply chain disruptions increasingly impact financial institutions, vendor management can no longer exist only for the purposes of checking a compliance box. Vendor management must be seen as a critical component of each financial institution's cybersecurity strategy and operational viability.

RECOMMENDATION

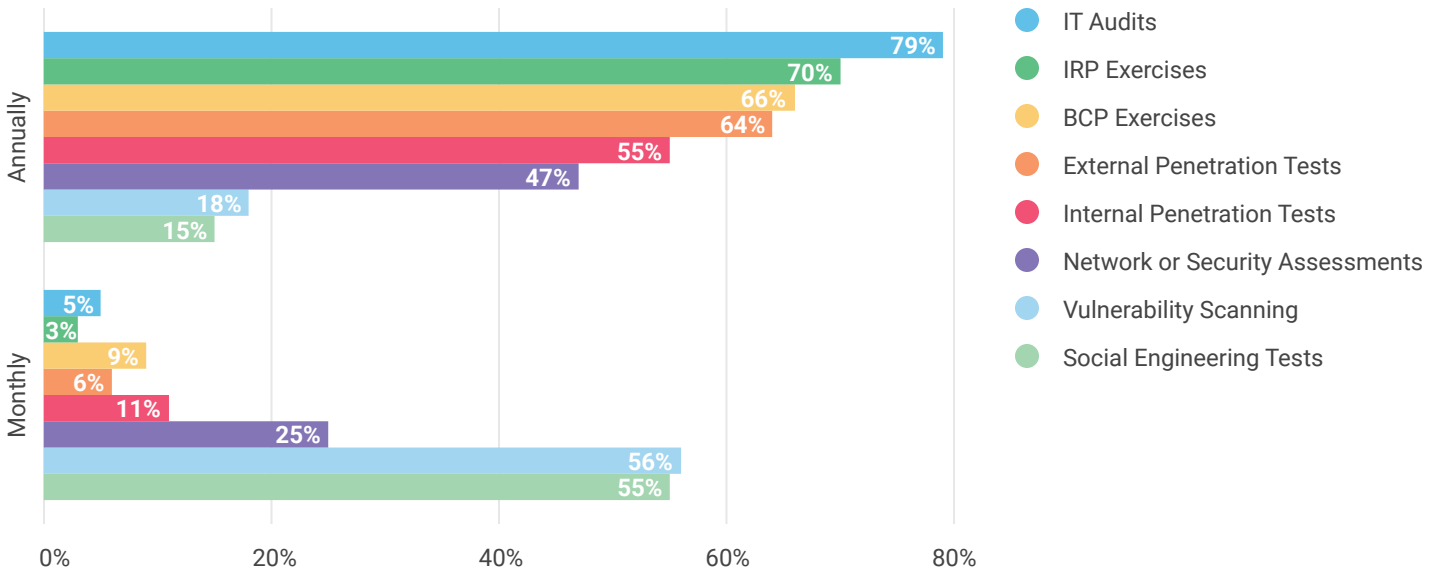
If you currently maintain a vendor management program for compliance only, consider changing your mindset and updating your program to make it useful for decision making. This culture shift is shown to have a positive effect on your entire cybersecurity posture.

Assurance & Testing

OBSERVATIONS

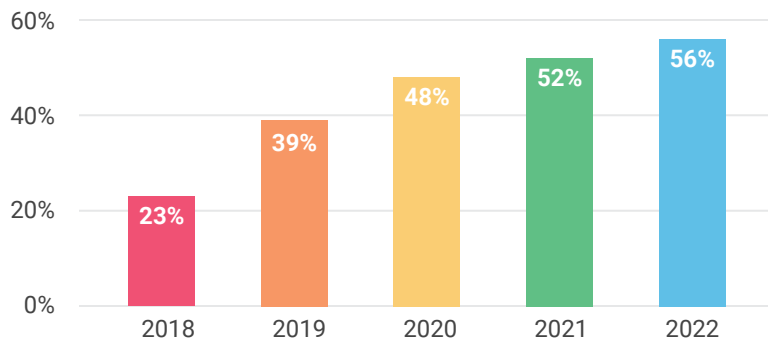
Financial institutions report performing most forms of assurance and testing annually. The two types of testing which participants reported performing more frequently are Vulnerability Scanning (56%) and Social Engineering Testing (55%).

TESTING FREQUENCY BY TYPE



Over the years, there has been a trend towards administering Social Engineering Testing (e.g., phishing tests) more frequently.

SOCIAL ENGINEERING TESTS: MONTHLY OR MORE FREQUENT



Note: The 2019 survey asked about the current and previous year, which is why 2018 data is included, even though the report began in 2019.

WHAT THIS MEANS

Vulnerability scanning and social engineering tests are leading the pack in testing frequency. This is likely due to low cost, autonomy offered by software solutions, and value perceived from a security standpoint.



CONTRIBUTOR QUOTE ED MCMURRAY

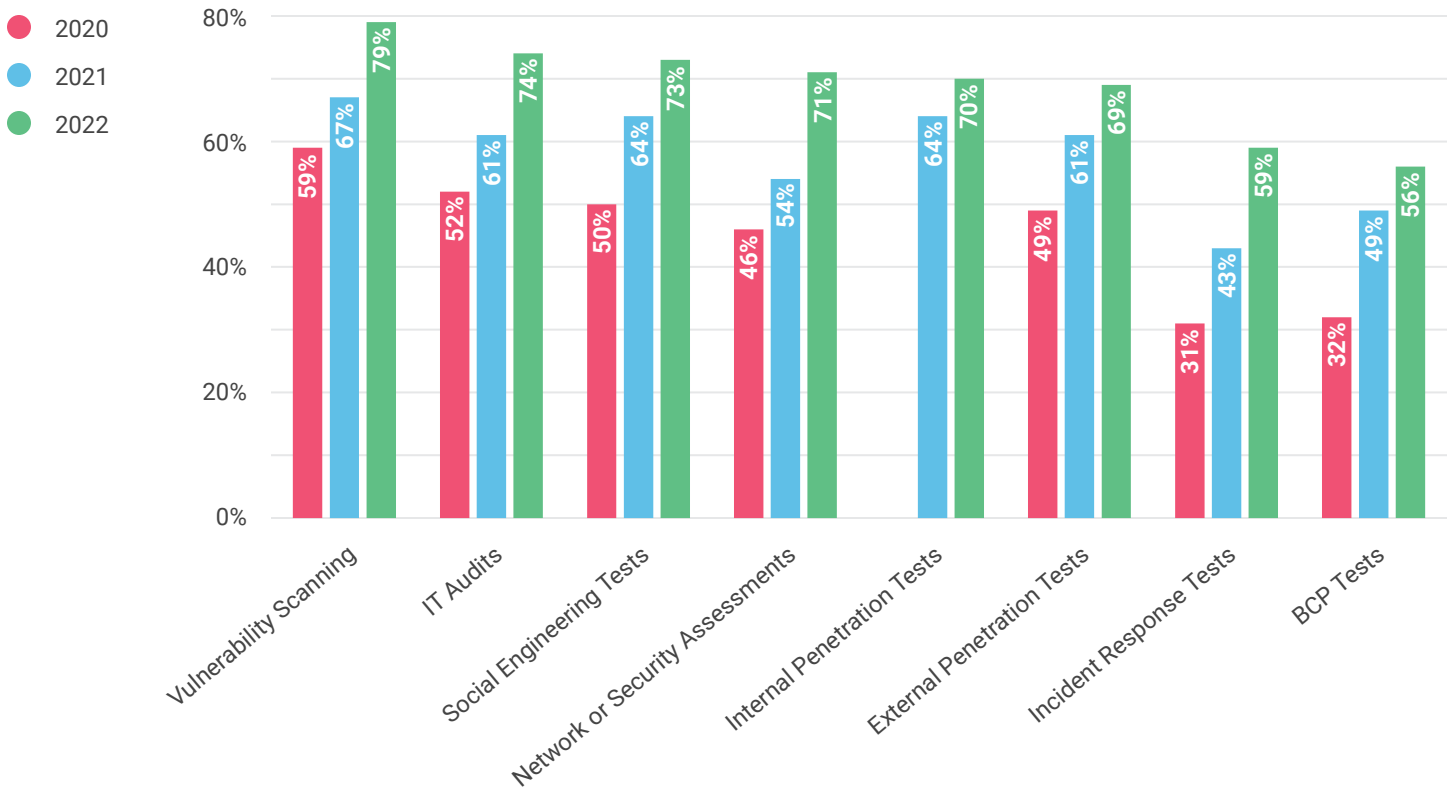
Financial institutions are continuing to mature the way they get value from security audits and testing. In years past, they were often seen as regulatory requirements - check the box. Now, they are being used as inputs into risk assessments and as ways to monitor critical security controls.



DIVING FURTHER

Across all assurance and testing activities, there is an increasing confidence in the usefulness of these tests, with Vulnerability Scanning (79%) perceived as the most valuable, followed by IT Audits (74%) and Social Engineering Tests (73%). Institutions find Incident Response Tests (59%) and BCP Tests (56%) the least valuable. Yet, while the least valuable, still more than half of institutions consider them to be valuable.

TESTING TYPES PERCEIVED TO BE "VERY USEFUL" IN IMPROVING SECURITY



TAKEAWAY

Perceived value in assurance and testing is steadily increasing over time. This could be due to several factors, such as:

- **Need:** As cybersecurity risk increases, the need for testing is more understood.
- **Purpose:** Testing is being used to improve security instead of as a compliance requirement.
- **Awareness:** Testing can be used to bring hidden vulnerabilities to light.
- **Execution:** There have been improvements in the testing process over time.
- **Communication:** Results are viewed as an objective metric in communicating with the Board.

Whatever the factors, the institution's cybersecurity posture both directly and indirectly benefits when assurance and testing is viewed as a value-add for the business.

RECOMMENDATION

If you do not currently consider your assurance and testing activities to be "very useful," start a conversation with other security professionals who do. Learn and discuss ways you can make your testing more valuable.

Conclusion

A review of survey data from the past four years shows distinctive trends in the state of cybersecurity.

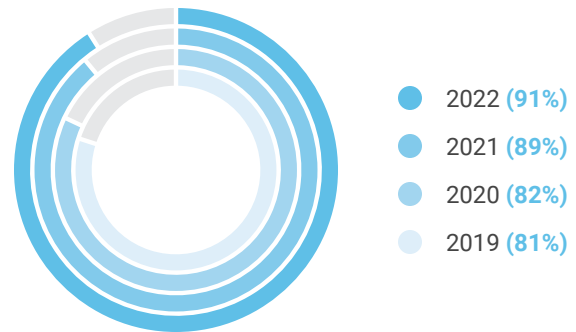
Trends in controls. Cybersecurity professionals report improvements in control implementation. More financial institutions are turning to cybersecurity tools and frameworks to benchmark controls against industry best practices. They also report plans to invest in technical “Detection” controls (e.g., network monitoring, IDS, SIEM, etc.) and “Protection” controls (e.g., anti-malware, firewall, patch management, etc.).

Trends in culture. Cybersecurity professionals report a culture shift from compliance-first to security-first. Financial institutions who value the elements of their cybersecurity programs are more likely to experience a heightened culture of security across the institution. They also report plans for additional financial resources and inclusion of cybersecurity in the institution’s strategic plan, which demonstrates top-down support of cybersecurity culture.

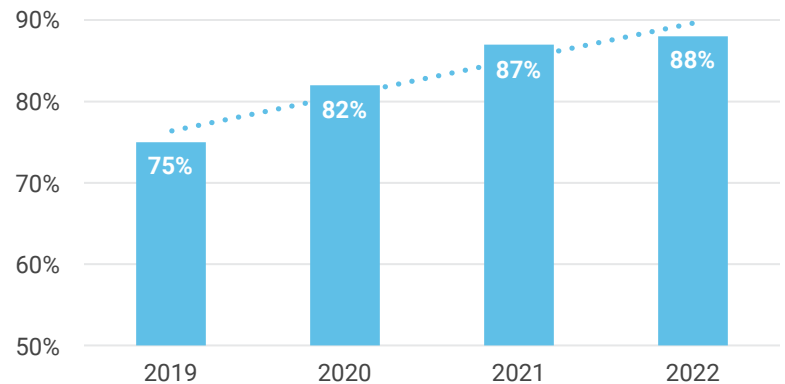
Trends in confidence. Cybersecurity professionals report increasing confidence in the Board of Directors’ understanding of the financial institution’s cybersecurity posture. They also report increasing confidence in cybersecurity training and in the value of assurance and testing activities.

What this information tells us is that the state of cybersecurity is evolving. Cybersecurity is now being seen as a critical component of a financial institution’s strategy and long-term success. The overall state of cybersecurity in the financial institution industry is strong, and we anticipate continued improvement in coming years.

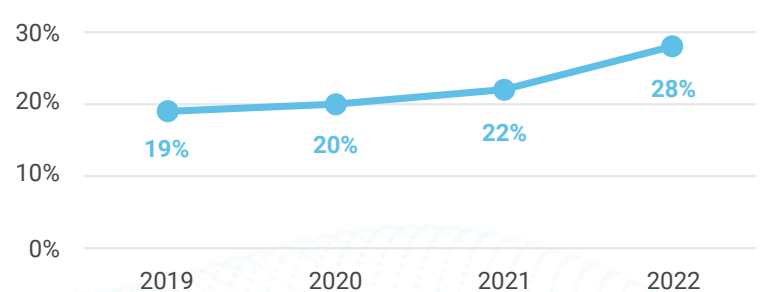
CYBERSECURITY ASSESSMENT TOOL ADOPTION



CYBERSECURITY IN THE STRATEGIC PLAN



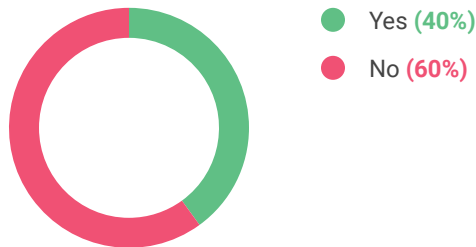
CYBER TRAINING REDUCES RISK OF INCIDENTS



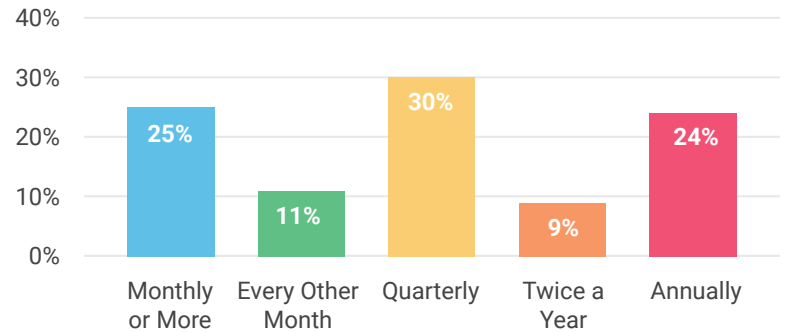
All Survey Responses

BOARD OVERSIGHT

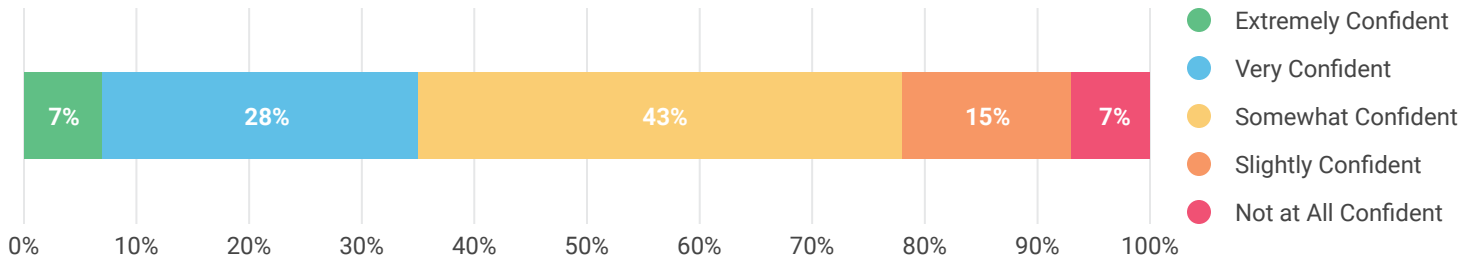
Does your Board have at least one member with professional cybersecurity or IT experience?



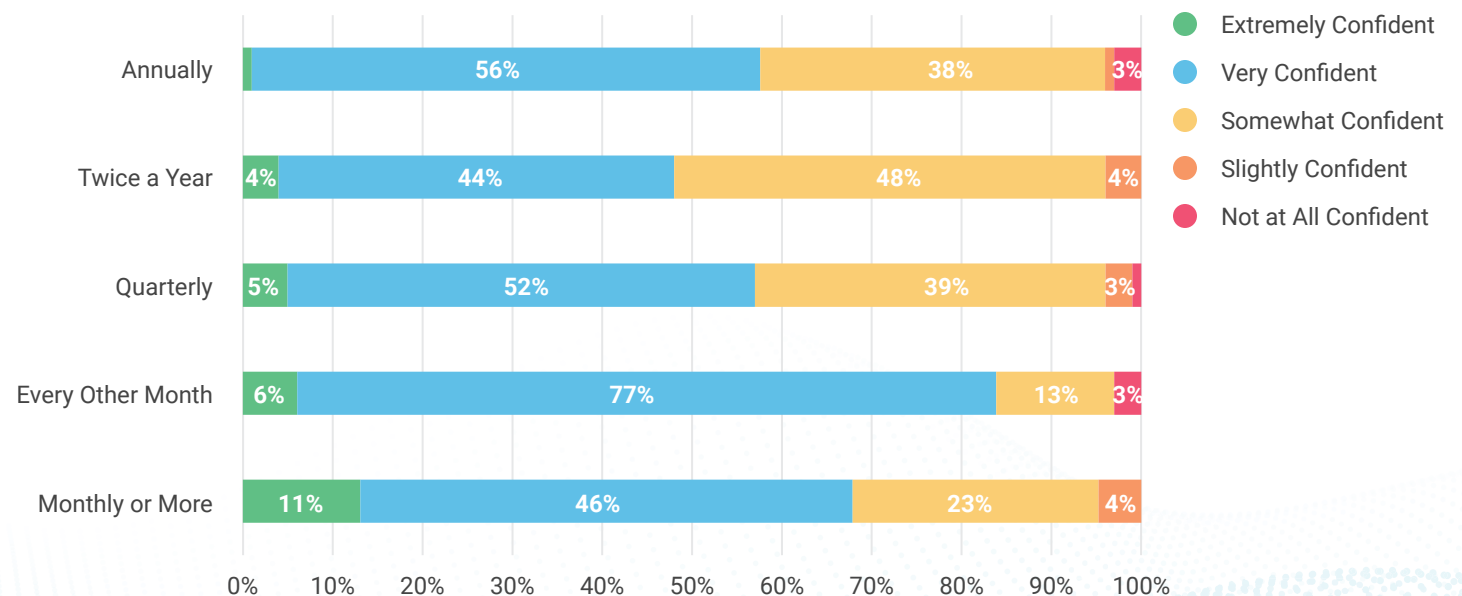
How frequently is your institution's Board of Directors updated on the institution's cybersecurity status?



How confident are you that the Board understands your institution's cybersecurity posture in order to make informed decisions?



Confidence in Overall Security Posture by Board Reporting Frequency



CYBERSECURITY OVERSIGHT

How confident are you in your institution's overall security posture?



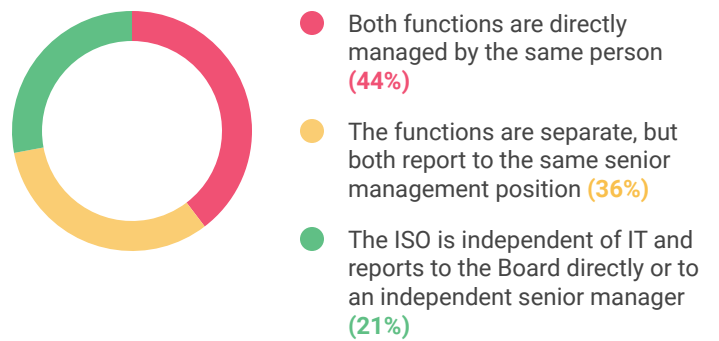
For your institution, which of the following best describes your ISO?



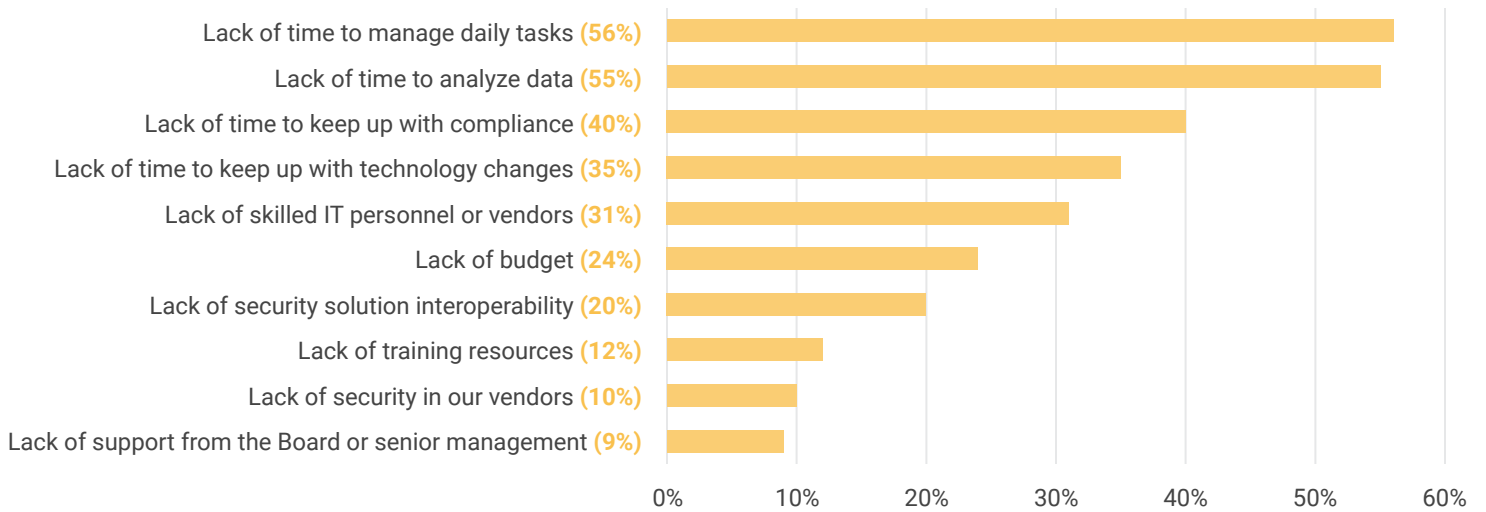
Is cybersecurity addressed in your institution's overall strategic plan?



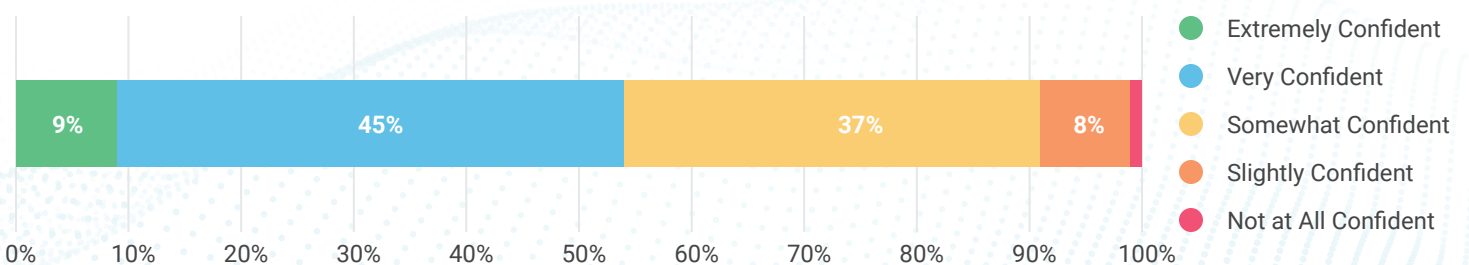
Which of the following best describes the organizational structure between the ISO and IT?



Which of the following circumstances are negatively impacting the success of your cybersecurity strategy?

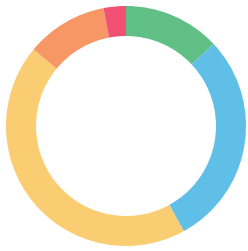


How confident are you that your institution would be able to detect an incident as it is happening?



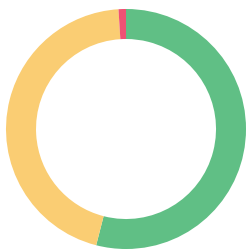
BUDGETING

How is your cybersecurity budget allocated?



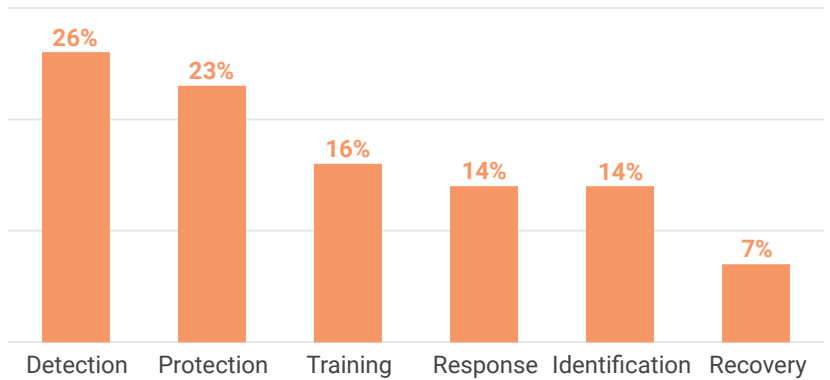
- We have a dedicated budget for cybersecurity outside of the IT budget. (13%)
- We have a shared budget with IT with a designated line item for cybersecurity. (29%)
- We have a shared budget with IT without a designated line item for cybersecurity. (44%)
- We only designate line items in the IT budget for large cybersecurity budget projects. (11%)
- No money is allocated to cybersecurity. (3%)

Is your institution's 2022 cybersecurity budget more or less than your 2021 cybersecurity budget?



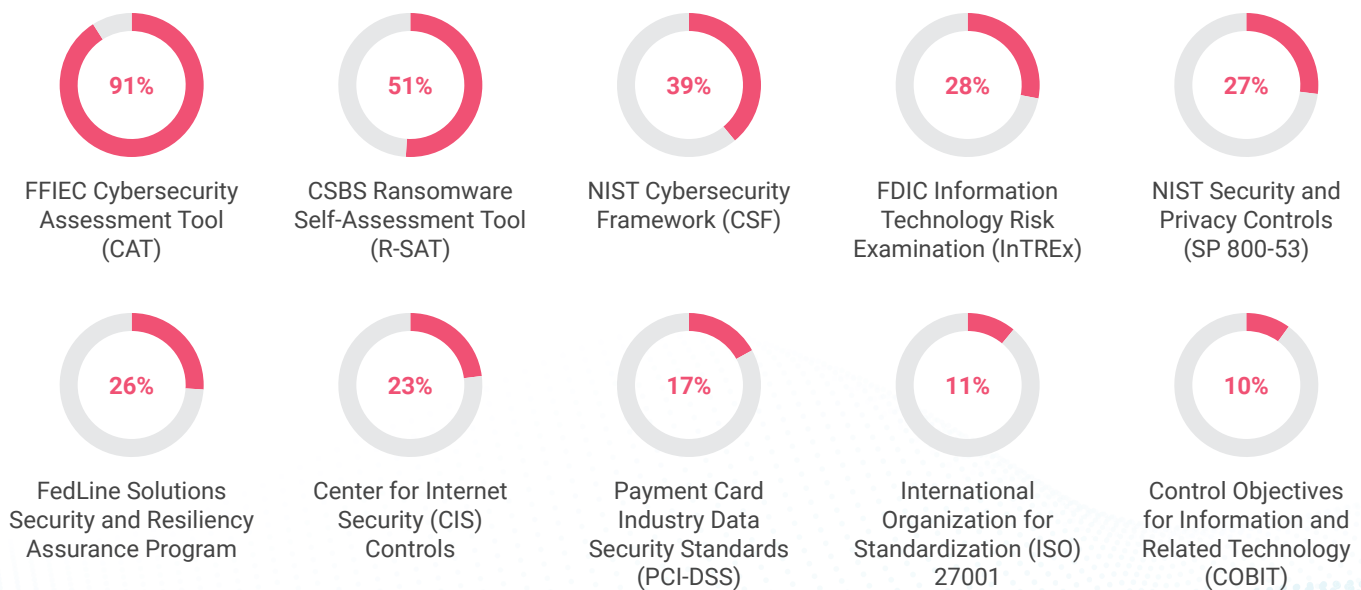
- More (54%)
- Same (45%)
- Less (1%)

If you could have additional resources to improve one area of cybersecurity, where would you apply these resources?



CYBERSECURITY TOOLS & FRAMEWORKS

Which cybersecurity frameworks and/or tools does your financial institution use?

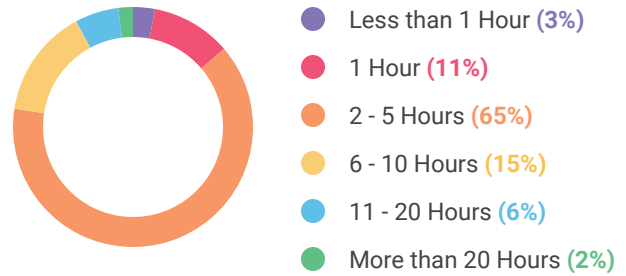


TRAINING

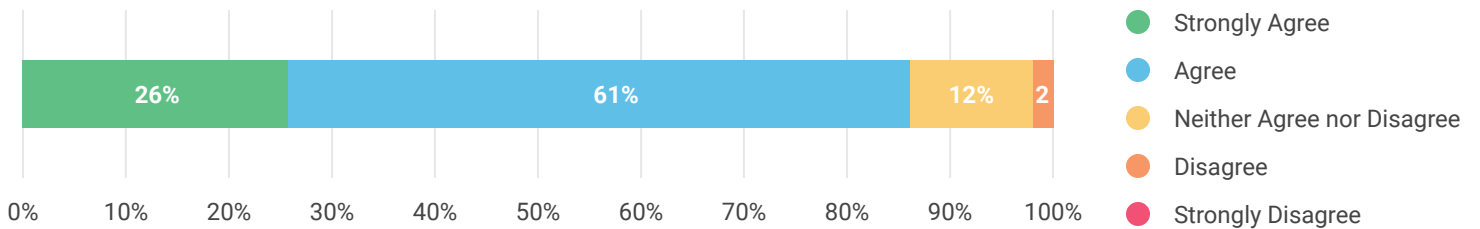
How confident do you feel your cybersecurity training is for the average employee?



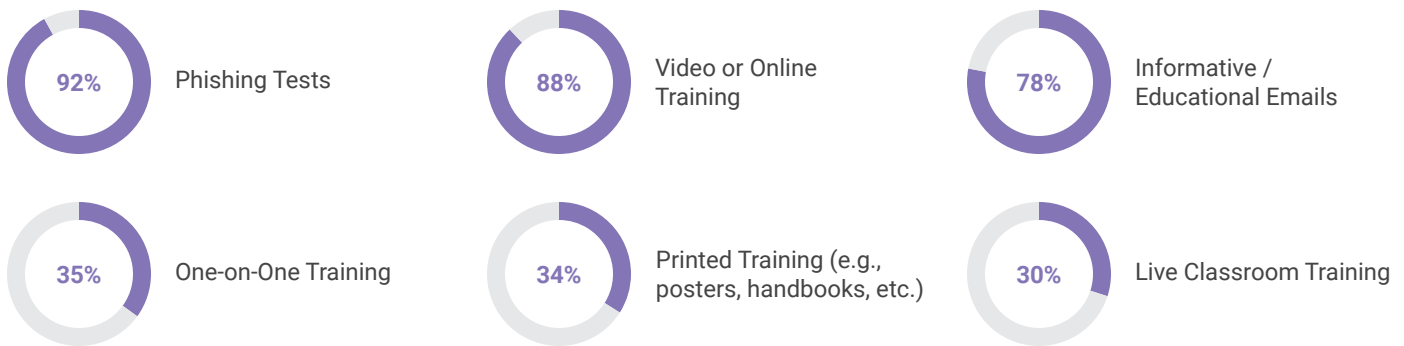
How many hours of information security training does the average employee receive each year?



Please indicate to what extent you agree or disagree with the following statement:
"My financial institution's cybersecurity training directly reduces the risk of cyber security incidents."

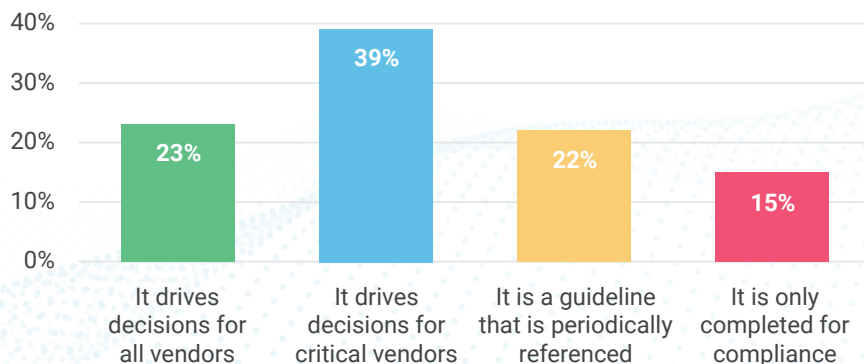


Which of the following cybersecurity training activities are actively implemented in your institution?



VENDOR MANAGEMENT

How do you view the vendor management program?

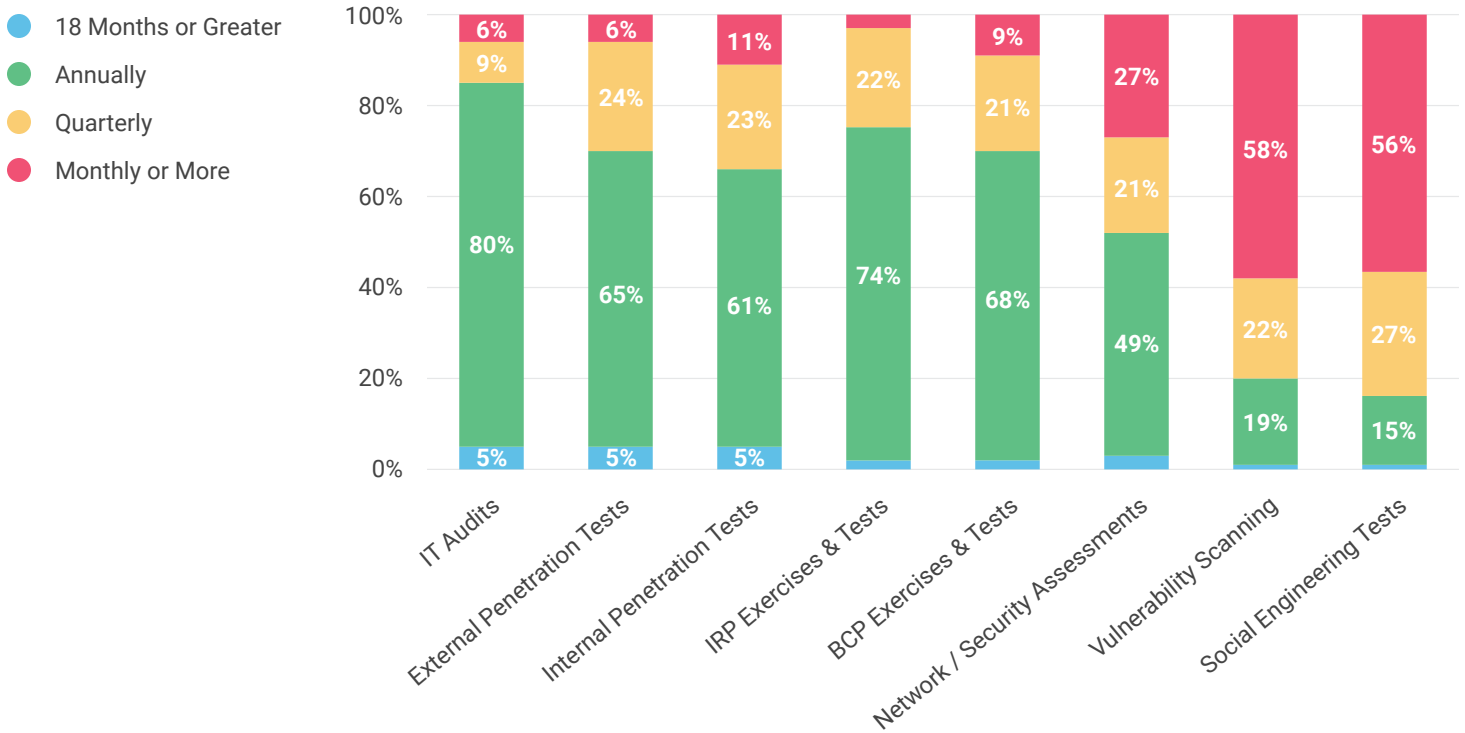


Have any of your vendors experienced an incident that significantly impacted your institution or your customers?

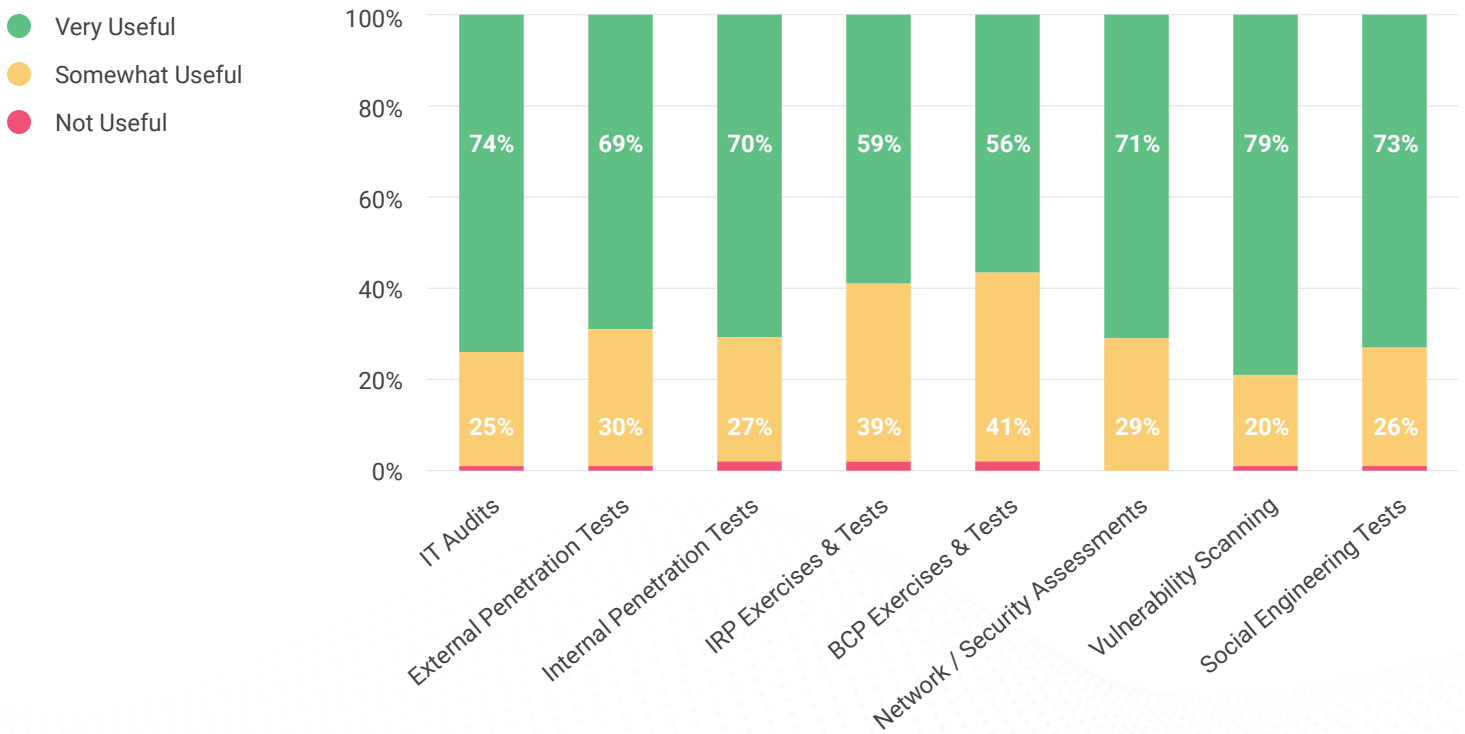


ASSURANCE & TESTING

How frequently do you plan to conduct each of the following types of assurance and testing activities in 2022?



How useful were each of the following in improving your institution's security posture?



About the Contributors

AUTHORS

To learn more about the authors and to book them for a speaking engagement, visit Tandem.App/Speakers.



RUSS HORN
President



LETICIA SAIID
Chief of Staff &
Chief Learning Officer



BRIAN WHIPPLE
Marketing Manager



BREANNA HARRISON
Marketing Coordinator



ALYSSA PUGH
GRC Content Manager



BRADY COOK
General Manager



KAUA AWBREY
Data Analytics Intern

CONTRIBUTORS

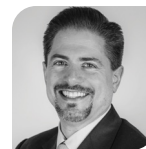
Tandem would like to thank the following individuals for reviewing and contributing commentary to this year's report.



CHRIS COLE
Chief Operations Officer
SouthWest Bank



TIM LEONARD
Chief Information Officer
Commercial Bank of Texas



TREY MAUST
Co-Founder & CEO
BankEvo



ED MCMURRAY
General Manager
CoNetrix Security





CARLOS MORALES
Chief Information Security Officer
First Liberty Bank


About Tandem


Tandem, LLC is one of four companies owned by CoNetrix, LLC. We develop an online information security governance, risk management, and compliance (GRC) web application designed to ease the burden of regulatory compliance and ultimately, improve your security.


We chose the name Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs, Tandem brings a suite of 11 products built by cybersecurity experts to help you organize and manage your information security program. See how Tandem can help you by visiting Tandem.App.


 **AUDIT MANAGEMENT**
Conduct and respond to audits through a unique framework designed to help you manage, track, and report on the results.


 **BUSINESS CONTINUITY PLAN**
Define and outline plans and procedures to effectively manage operations before, during, and after a disaster.


 **COMPLIANCE MANAGEMENT**
Identify, schedule, and track important compliance projects and deadlines, such as reporting, audits, training, and operations.


 **CYBERSECURITY**
Complete and report on the FFIEC Cybersecurity Assessment Tool using a streamlined framework. Report your growth plan and peer comparison data to management.


 **IDENTITY THEFT PREVENTION**
Create your Identity Theft Prevention Program document, along with customizable employee training for Identity Theft Red Flags.


 **INCIDENT MANAGEMENT**
Prepare for security incidents by developing an incident response plan. When incidents do occur, track and document them throughout your incident handling process.

 **INTERNET BANKING SECURITY**
Create risk assessments for different types of digital banking services offered by your institution. Offer education with expert-designed security awareness materials.

 **PHISHING**
Test and train your employees to recognize and avoid social engineering attacks by sending simulated phishing emails and enrolling users in training courses.

 **POLICIES**
Create and maintain your enterprise-wide policies in Tandem. Use our Information Security Policies set, tailored for your institution through a multiple-choice questionnaire.

 **RISK ASSESSMENT**
Perform an information security risk assessment, as well as individual information asset risk assessments with our easy-to-follow format in Tandem.

 **VENDOR MANAGEMENT**
Manage contracts, documents, risk assessments, reviews, and other information related to your third-party relationships.

STATE OF CYBERSECURITY

If you enjoyed this report and you would like to be part of next year's survey, sign up now at Tandem.App/Survey-Sign-Up.

