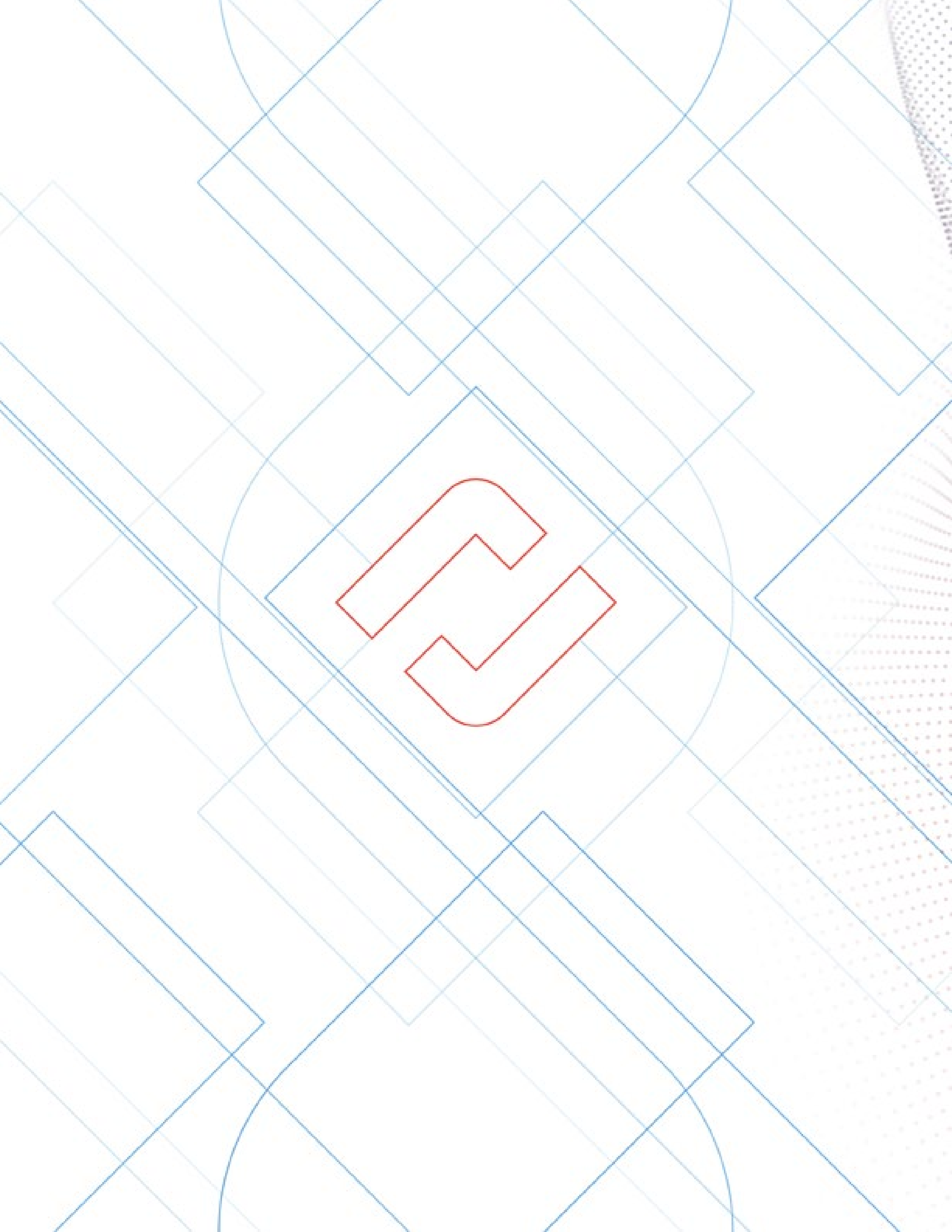
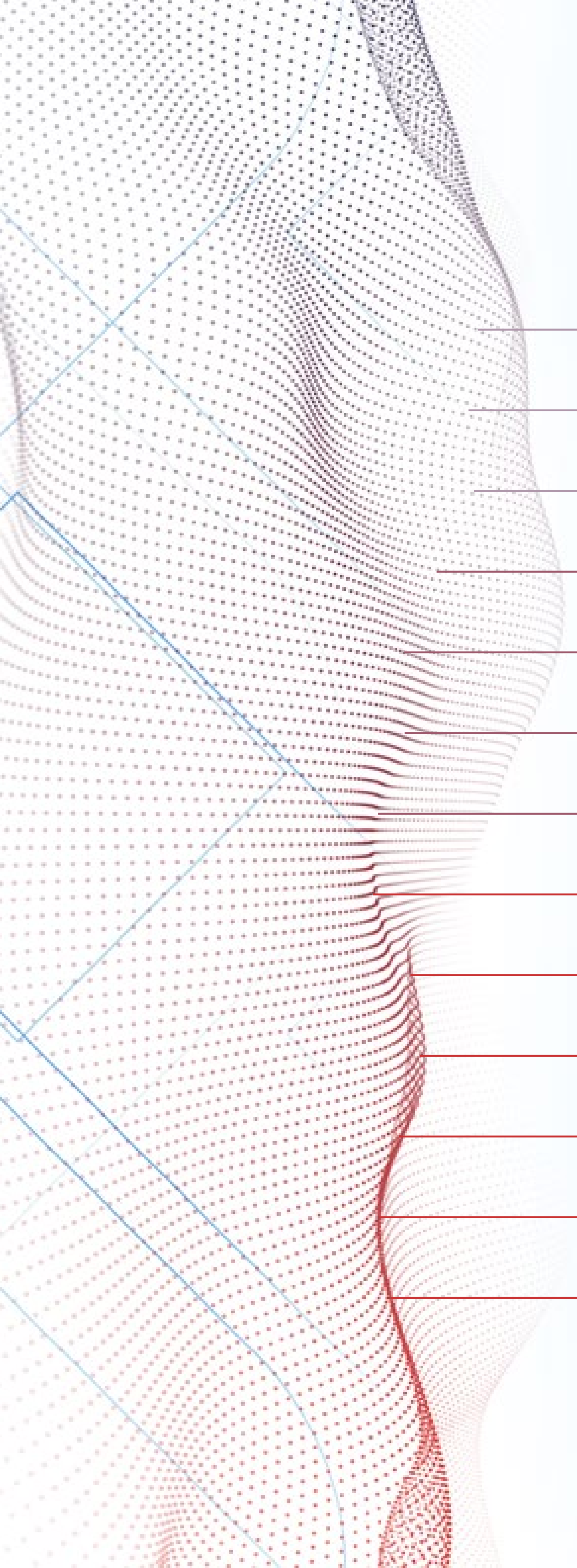
2023

CYBER SECURITY REPORT

FOR THE FINANCIAL INSTITUTION INDUSTRY

Tandem





Contents

About the Report

This report includes the results of a survey of cybersecurity professionals working in the financial institution industry. The survey resulted in 288 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 July 10, 2023 and August 31, 2023.

PARTICIPANTS

All 288 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

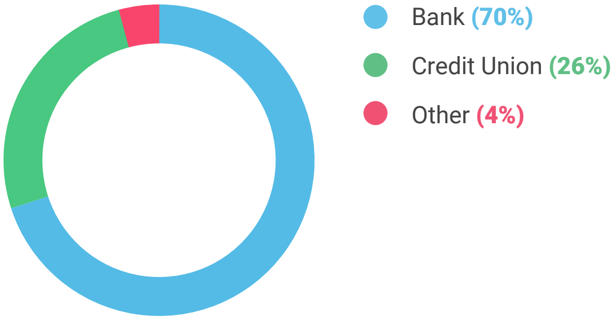
The report is structured into sections for each survey topic. Each topic is divided into three subsections to better share results. The subsections include:

- **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

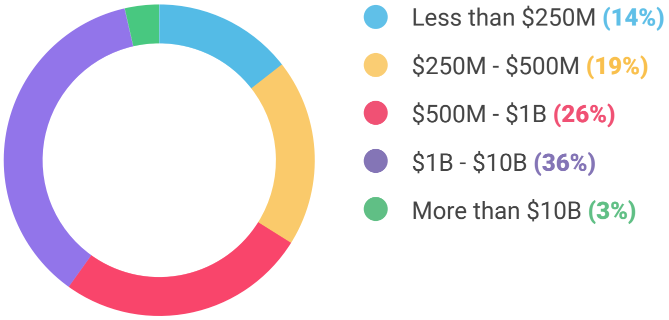
INSTITUTIONS SURVEYED: TYPES

Of those who responded, 70% work for a bank, 26% work for a credit union, and the remaining participants work for other financial institutions (e.g., mortgage companies, trust companies, etc.).



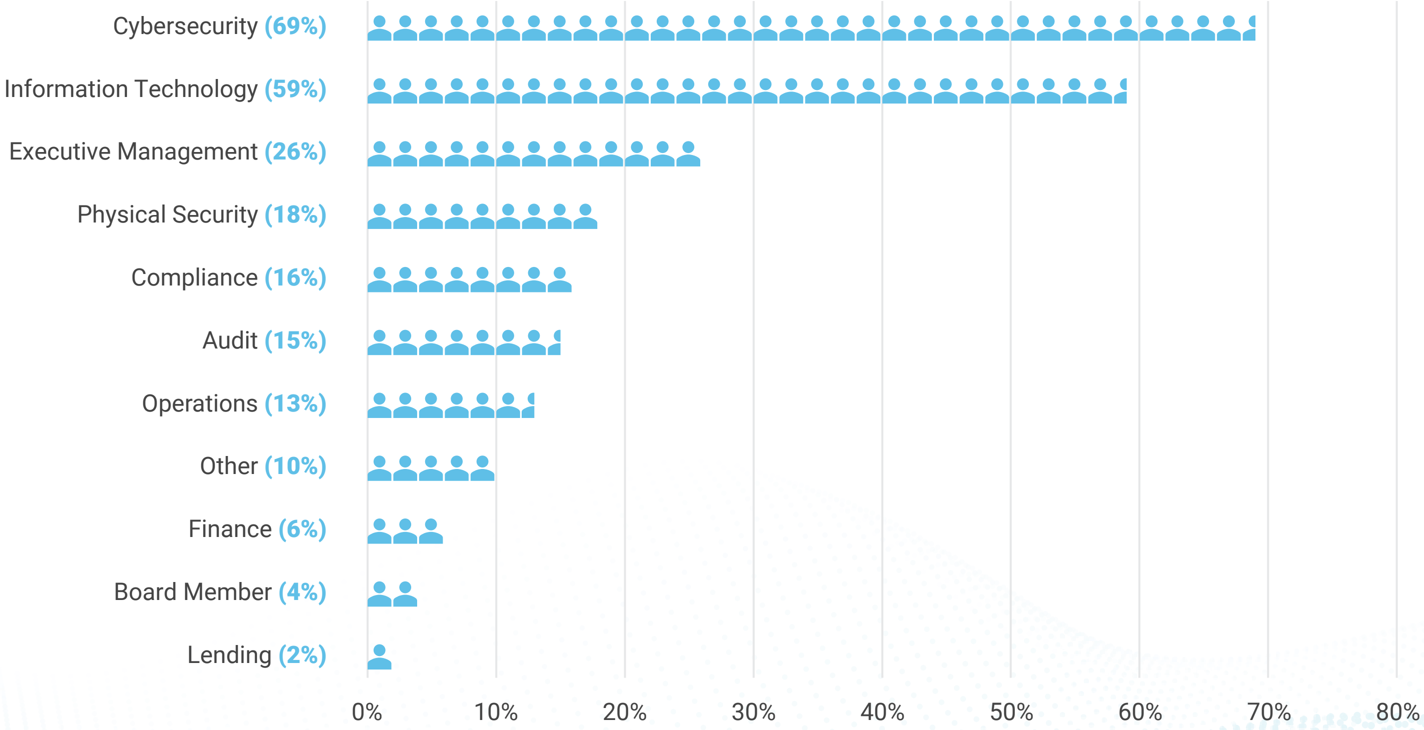
INSTITUTIONS SURVEYED: ASSETS

Most survey respondents were from small to medium sized regional community financial institutions, but a good representation came from larger community institutions, with 39% 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 4% of respondents serving as Board Members. Participants were asked to select all that applied.

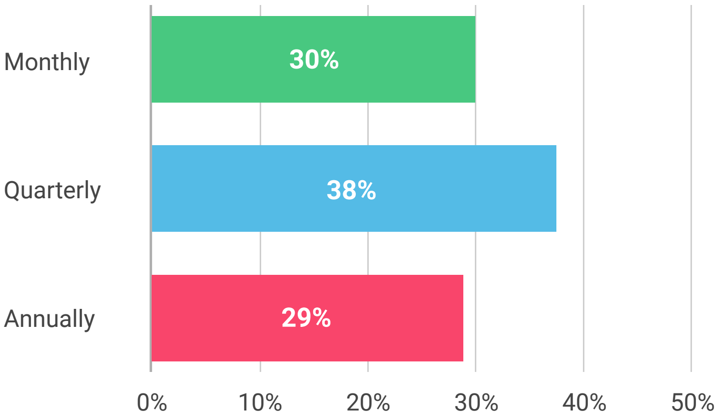


Board Oversight

OBSERVATION: BOARD OF DIRECTORS UPDATE FREQUENCY

The majority of financial institutions meet with their Board of Directors quarterly to give an update on the institution's cybersecurity status.

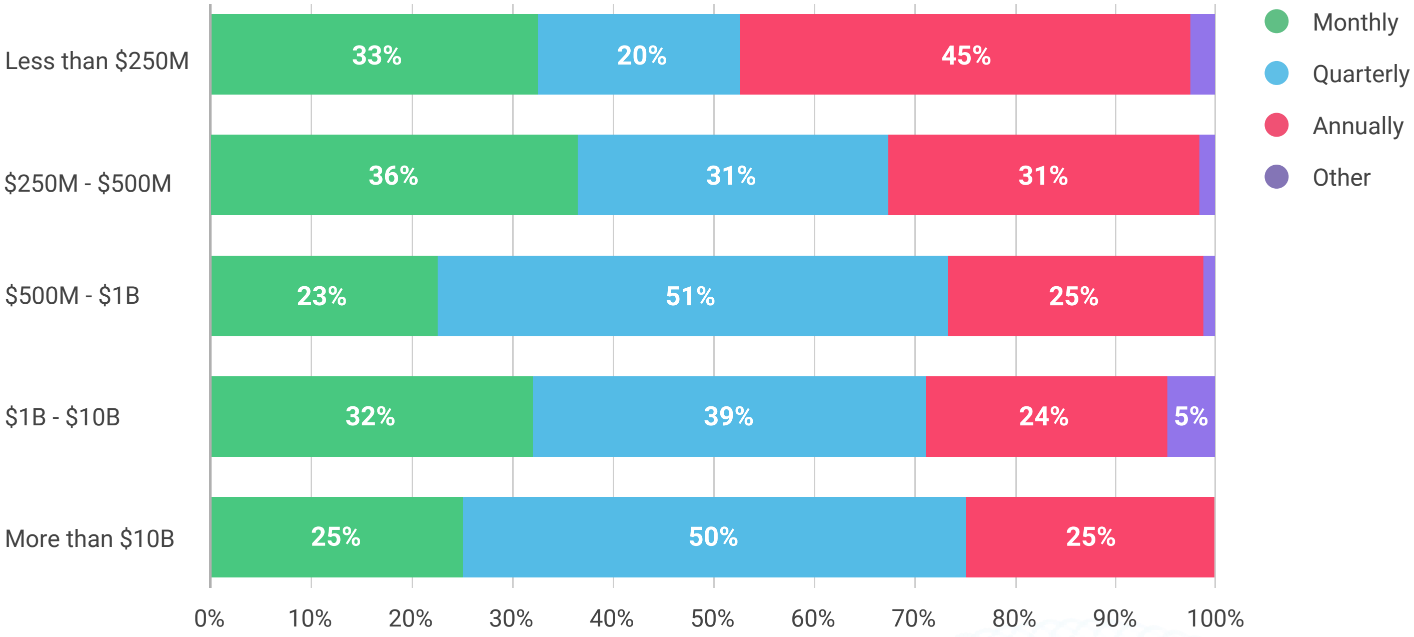
FREQUENCY OF BOARD UPDATES



DIVING FURTHER

Institution size may factor into the decision of frequency as 45% of institutions that have $250 million or less in assets will meet with their Board only annually.

REPORTING FREQUENCY BY ASSET SIZE

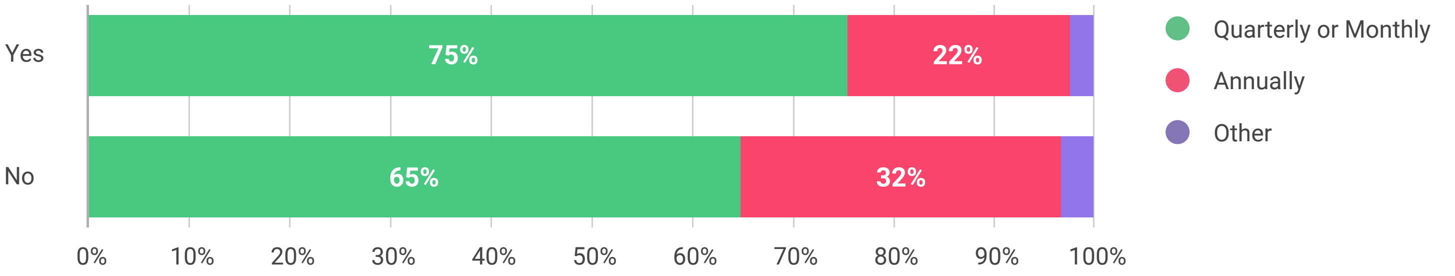


WHAT THIS MEANS

Smaller institutions typically have less complex technology environments, which may reduce the need to update the Board of Directors on cybersecurity issues as often as larger, more complex institutions.

Another potential factor of frequency is the presence of a Board member who has IT or Cybersecurity experience. Institutions who have at least one Board member with IT experience were 9% more likely to update their Board more than annually.

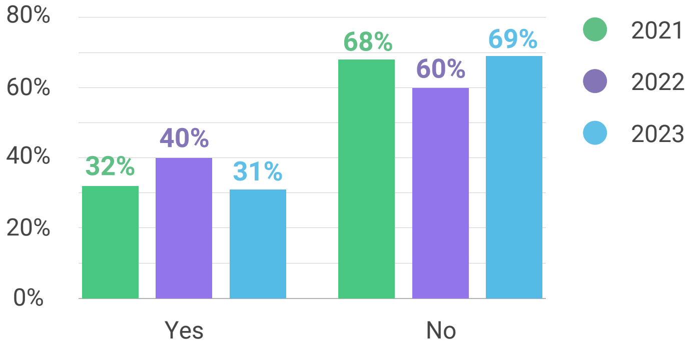
BOARD UPDATE FREQUENCY BY PRESENCE OF IT EXPERIENCED BOARD MEMBER



OBSERVATION: BOARD MEMBERS WITH IT EXPERIENCE

This year, there was a decrease in the number of institutions reporting to have at least one Board member with IT or cybersecurity experience, with only 31% of participants answering “Yes.” While there was a decrease this year, over the past three years the trend has been steady with approximately only 30-40% of institutions with a Board member with past IT experience.

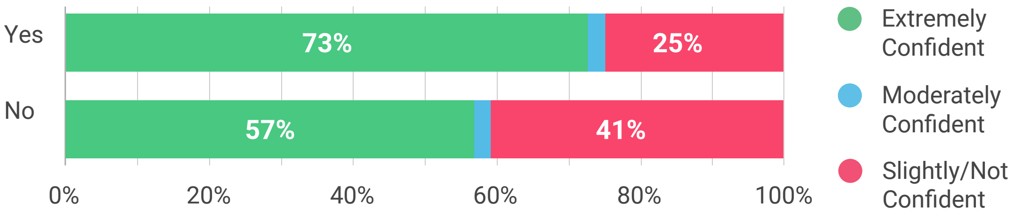
PERCENTAGE OF BOARD MEMBERS WITH IT EXPERIENCE



DIVING FURTHER

Financial institutions that reported to the Board more frequently are more confident about their overall cybersecurity posture.

CONFIDENCE IN CYBERSECURITY POSTURE BY BOARD REPORT FREQUENCY



TAKEAWAY

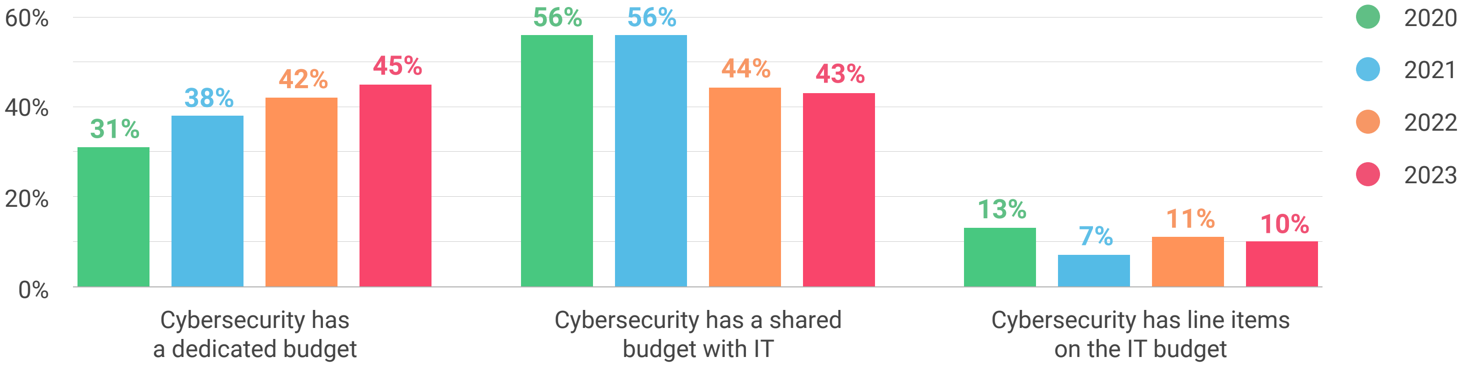
The more often a Board is informed on cybersecurity, the more confident the cybersecurity professionals of those organizations are about their Board's ability to make informed decisions on technology matters. This is balanced by the needs of the institution typically based on size. Larger institutions may need to meet with the Board frequently, whereas smaller institutions may have less complex environments and therefore need less involvement from the Board.

Budget

OBSERVATION: SEPARATE CYBERSECURITY BUDGETS

We continue to see a trend where cybersecurity is getting more focus in the budget. In the past, the majority of budgets just had cybersecurity included in the IT budget, but financial institutions are moving to either creating a separate line item or dedicated budget for cybersecurity.

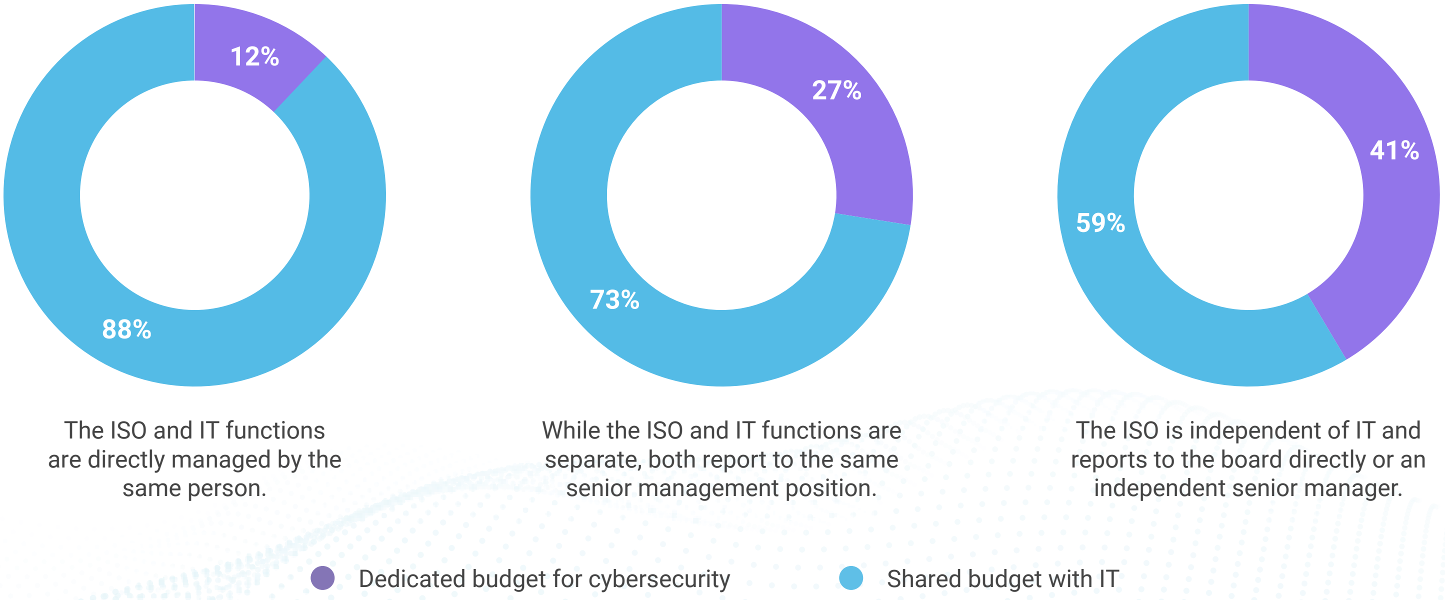
RELATIONSHIP OF CYBERSECURITY & IT BUDGETS



DIVING FURTHER: INDEPENDENT ISOs AND BUDGET

As you might expect, institutions with an ISO that has separation in reporting from the IT department is much more likely to have a dedicated cybersecurity budget than institutions where the ISO and IT functions are directly managed by the same person or report to the same person.

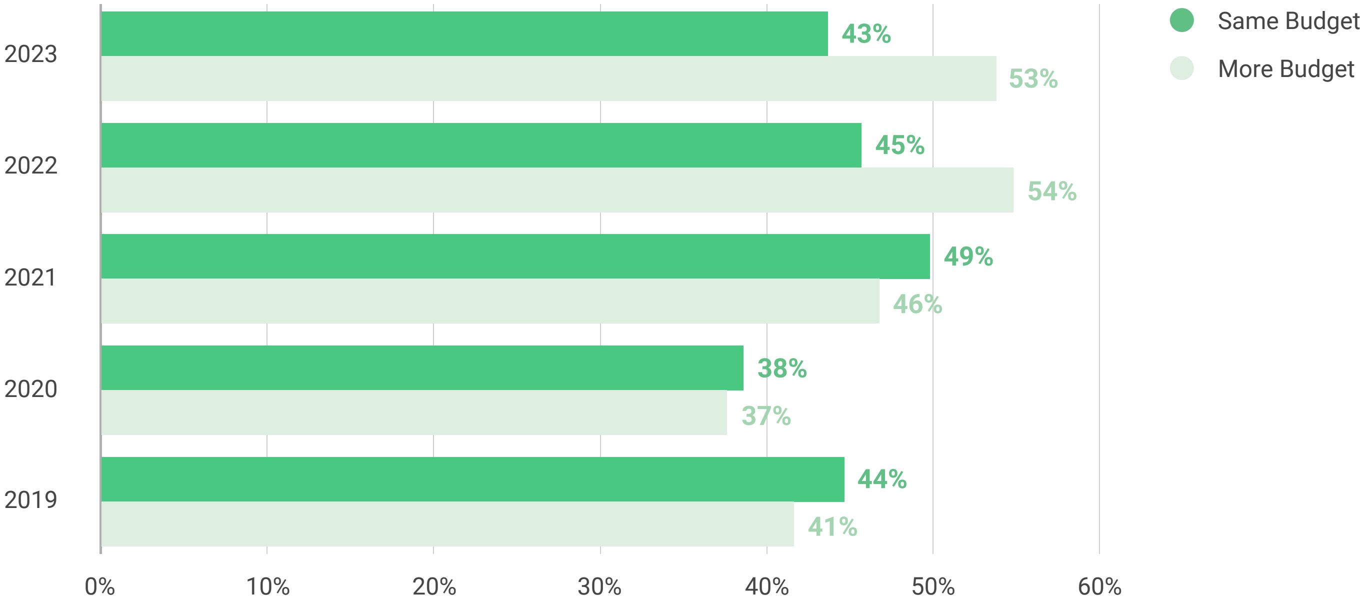
BUDGET DEDICATION BY ISO INDEPENDENCE



OBSERVATION: INSTITUTIONS ARE INCREASING BUDGETS

Over half of institutions increased their budget for cybersecurity in 2023. This continues the trend of financial institutions allocating more resources toward cybersecurity instead of simply maintaining the same budget year to year.

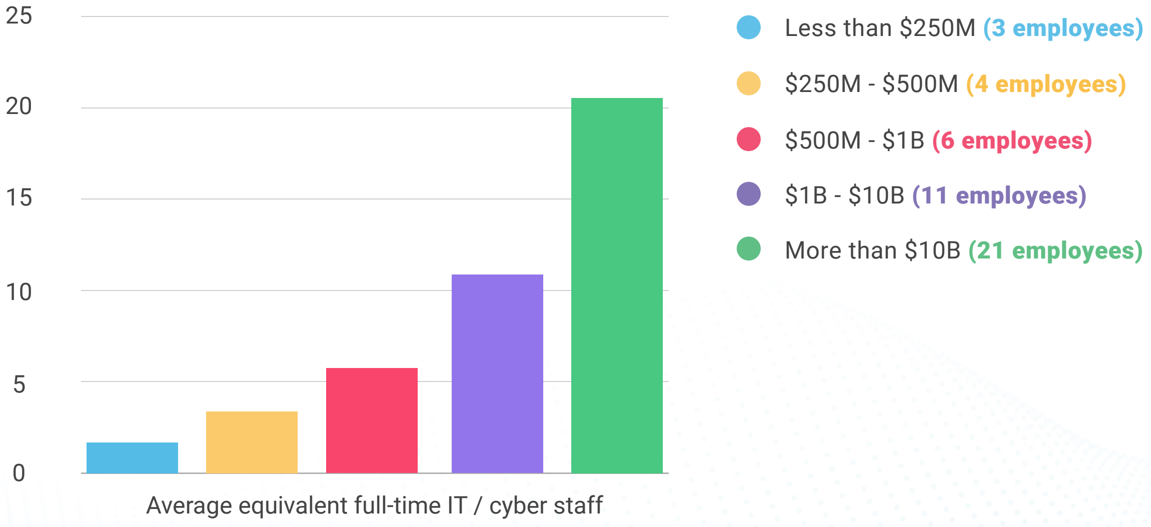
PLANS FOR NEXT YEAR'S CYBERSECURITY BUDGET



OBSERVATION: LARGER INSTITUTIONS HAVE MORE STAFF

As would be expected, larger institutions tend to have more full-time equivalent IT and information security staff.

AVERAGE FULL-TIME IT AND INFORMATION SECURITY STAFF BY ASSET SIZE

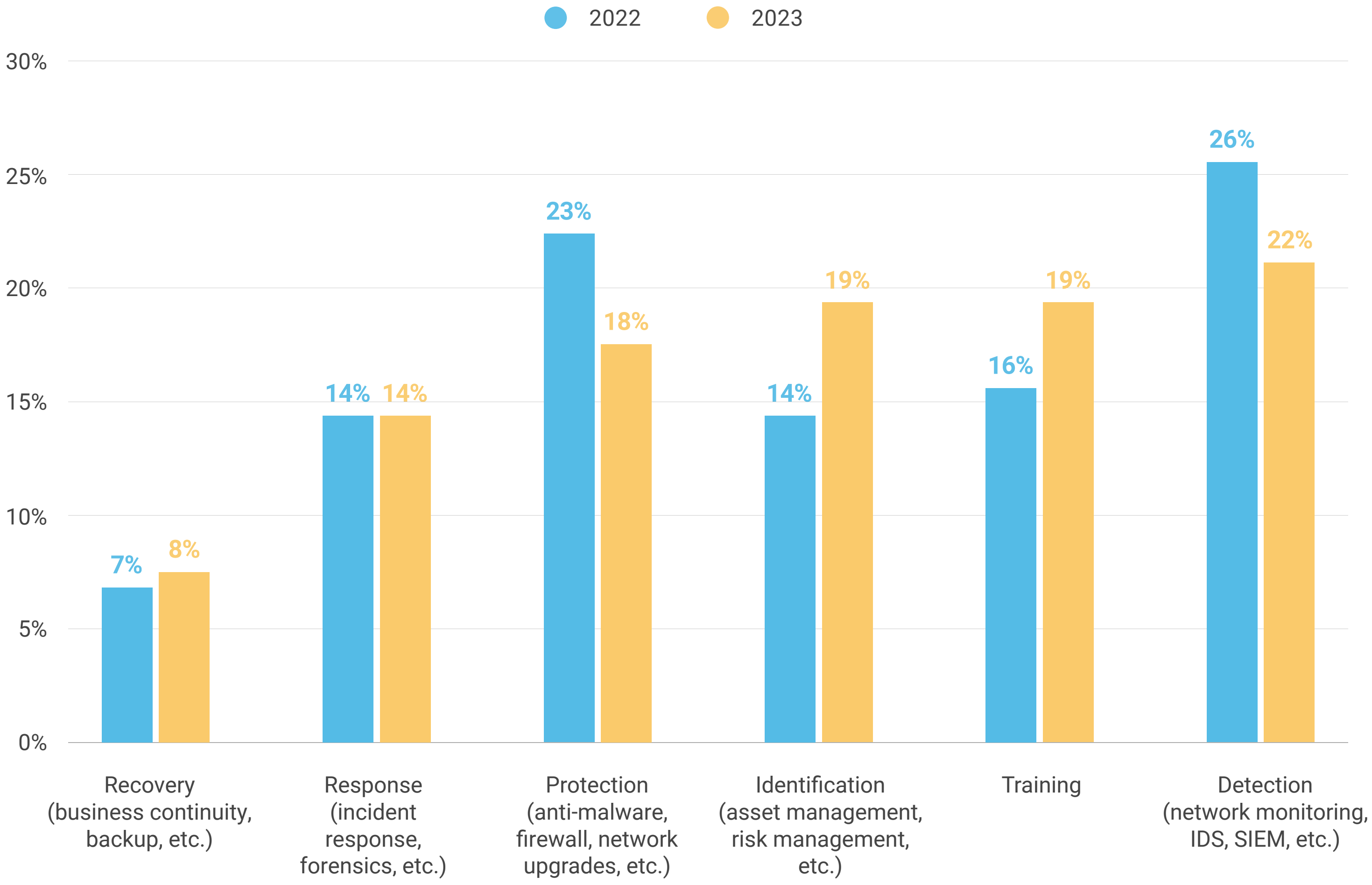


Cybersecurity Oversight

OBSERVATION: ADDITIONAL RESOURCES WOULD BE ALLOCATED EVENLY

Institutions selected Detection (e.g., network monitoring, IDS, SIEM, etc.) as their top area to improve, making it the top choice in both 2022 and 2023. However, this was a decrease compared to 2022, while Training and Identification both saw increases in 2023.

WHERE ADDITIONAL RESOURCES WOULD BE ALLOCATED



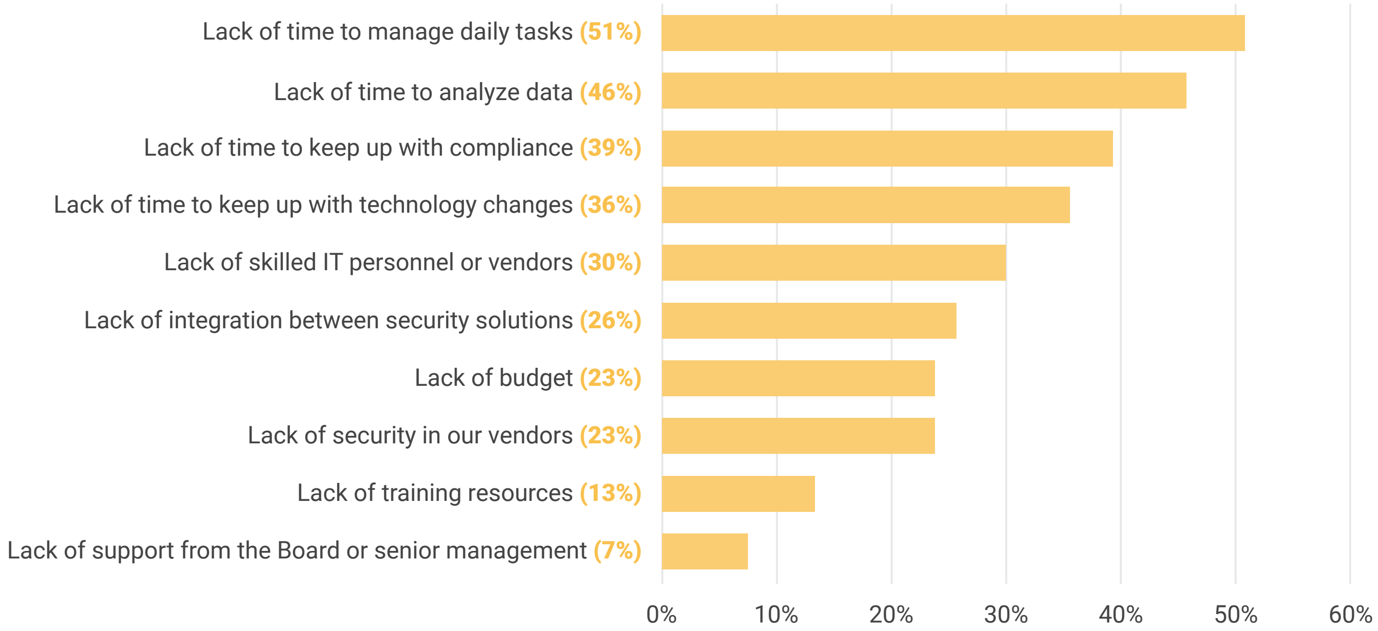
WHAT THIS MEANS

With Training and Identification seeing a jump in focus as areas to improve, we suspect cybersecurity professionals are looking to invest more in the administrative side of cybersecurity. Our largest threats involve people skills (e.g., phishing, compromised credentials, shadow IT, etc.) and the industry is redirecting focus to improve those areas.

OBSERVATION: LACK OF TIME STILL A PRIMARY PROBLEM

Participants were also asked to select the top three circumstances negatively impacting the success of the institution's cybersecurity strategy. Similar to 2022, the four most selected answers were related to a lack of time.

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.

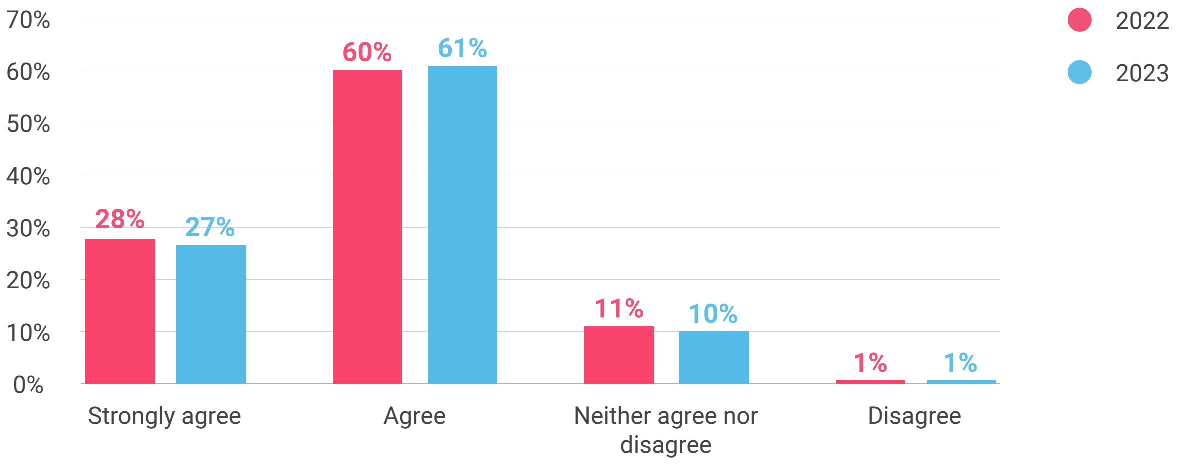
- **Be realistic** about time requirements as part of strategic planning. Do not plan based on the shortest time a project could take. Build in time for unexpected roadblocks.
- **Review current tasks** to identify activities which are not necessary for cybersecurity staff to complete, then eliminate 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.

Training

OBSERVATION: TRAINING REDUCES INCIDENTS

Almost identical with last year, the majority of institutions either strongly agree or agree with the statement, “my financial institution's cybersecurity training directly reduces the risk of cyber security incidents."

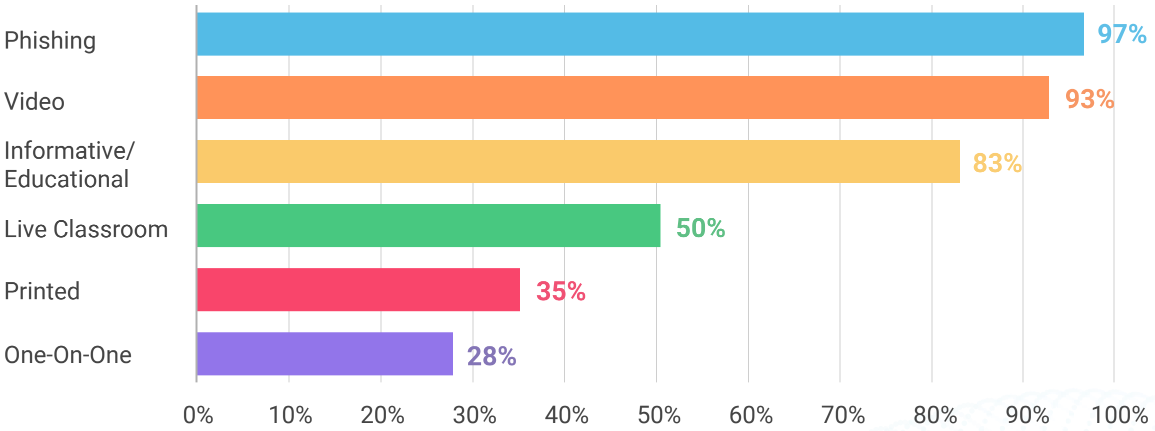
CYBERSECURITY TRAINING DIRECTLY REDUCES THE RISK OF CYBER SECURITY INCIDENTS



DIVING FURTHER

Of the institutions who include one-on-one training in their cybersecurity training program, 41% strongly agreed that their “training directly reduces the risk of cyber security incidents.” Institutions who did not implement one-on-one training seemed to have less confidence with only 28% strongly agreeing that their training directly reduces cyber security incidents.

SECURITY AWARENESS TRAINING POPULARITY BY TYPE



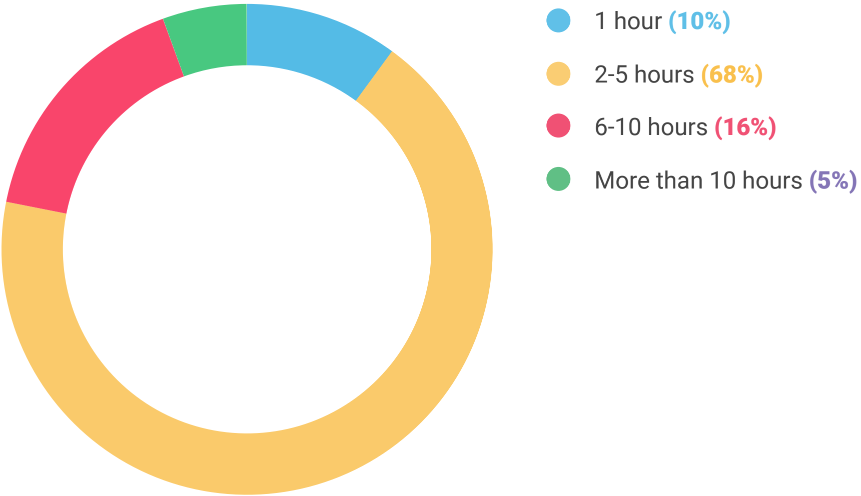
TAKEAWAY

While one-on-one training takes more time, it still holds an important place in your security awareness training program. We recommend having one-on-one training in response to repeat phishing failures, as opposed to assigning another self-paced training option. The one-on-one allows you to discover where the employee is struggling and make course corrections.

OBSERVATION: MORE TRAINING LEADS TO MORE CONFIDENCE

Over the past three years, the amount of security awareness training has been consistent for institutions. In 2023, 68% of institutions said they implement two to five hours of training per year.

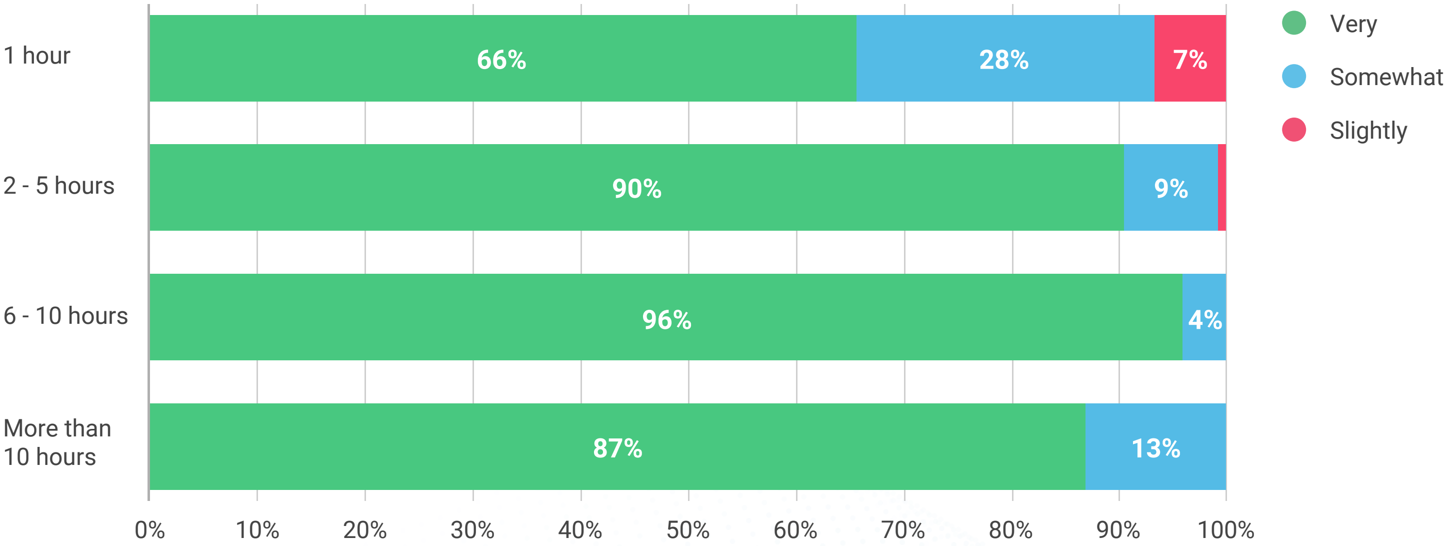
TRAINING HOURS PER YEAR



DIVING FURTHER

Not surprisingly, institutions that offered more than one hour of training increased their confidence in their security awareness training by 25%. Meanwhile, there is no significant difference in cybersecurity confidence to provide over five hours of training versus just two to five hours per year.

CONFIDENCE IN SECURITY AWARENESS TRAINING BY HOURS OF TRAINING



TAKEAWAY

It takes at least two hours per year of training for each employee to experience positive results from your security awareness training program.

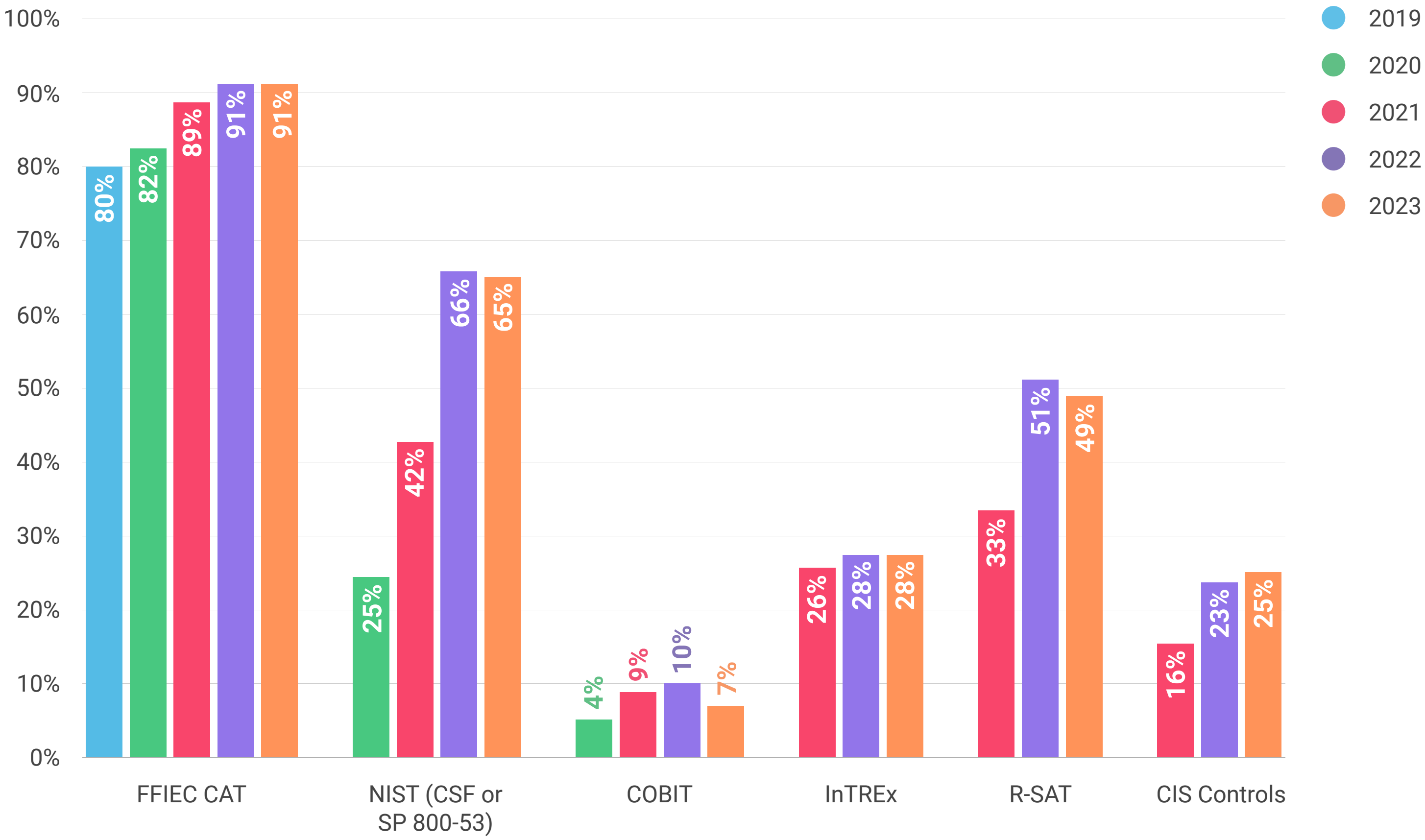
Cybersecurity Tools & Frameworks

OBSERVATION: CAT AND NIST LEAD IN FRAMEWORK USE

The FFIEC CAT continues to be the most used framework by financial institutions with 91% of respondents stating use of the framework. The use of NIST frameworks continues to be a strong second with 65% of respondents using a NIST framework.

ADOPTION OF CYBERSECURITY FRAMEWORKS & TOOLS

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



WHAT THIS MEANS

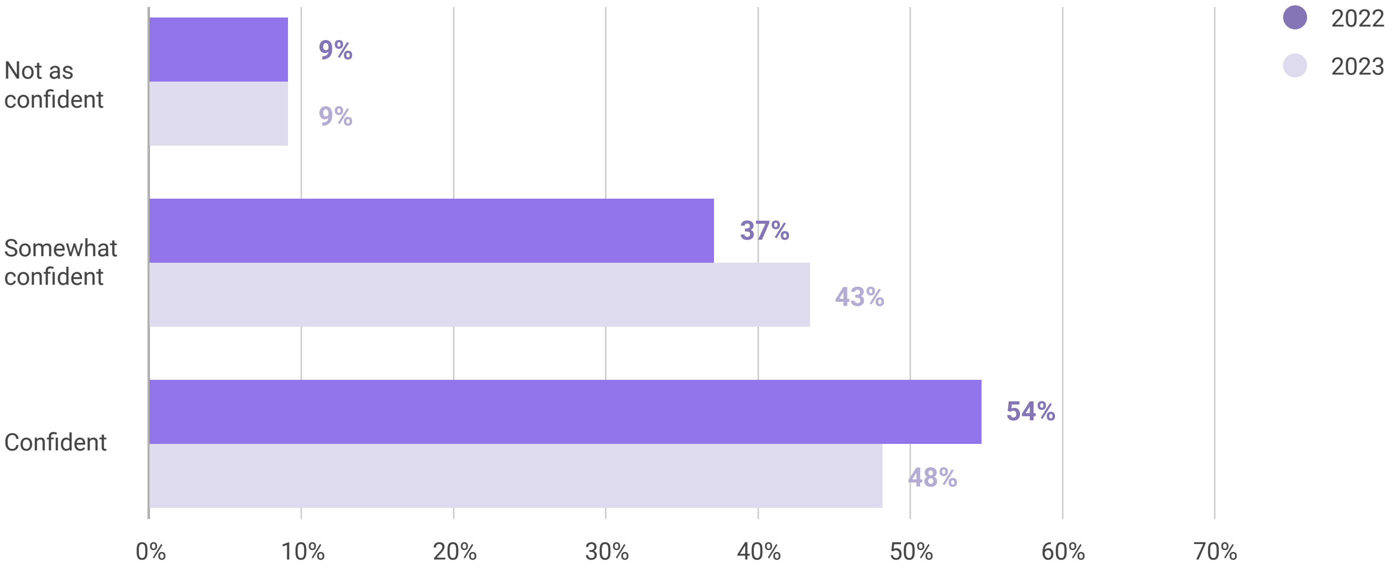
Assessment tools specific to the financial industry are the most used by financial institutions. Still, there has been significant growth in institutions adopting technology-industry frameworks.

Incident Reponse

OBSERVATION: DECREASED CONFIDENCE IN DETECTION

Financial institutions seem to be less confident in their ability to detect an incident as it is happening this year compared to last year.

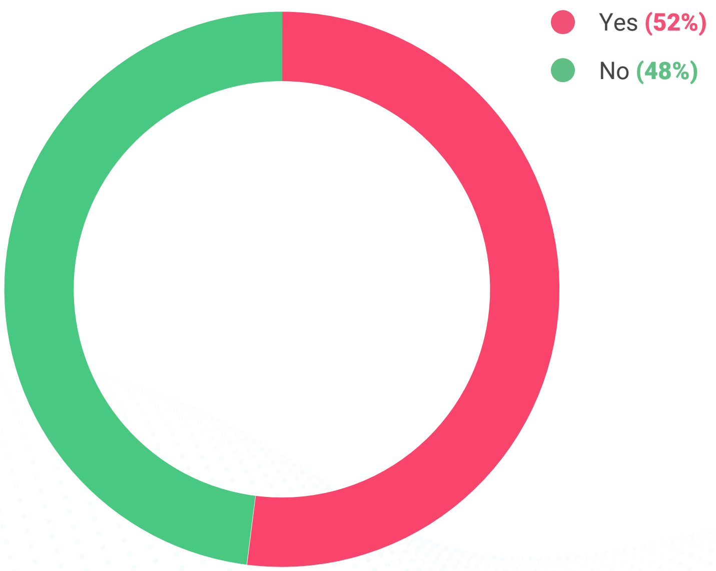
CONFIDENCE IN DETECTING AN INCIDENT OCCURRING



DIVING FURTHER

Of those that said they experienced more incidents this year, 52% of institutions said they experienced confirmed loss or exposure of data due to an incident with a vendor.

LOSS / EXPOSURE FROM VENDOR INCIDENTS

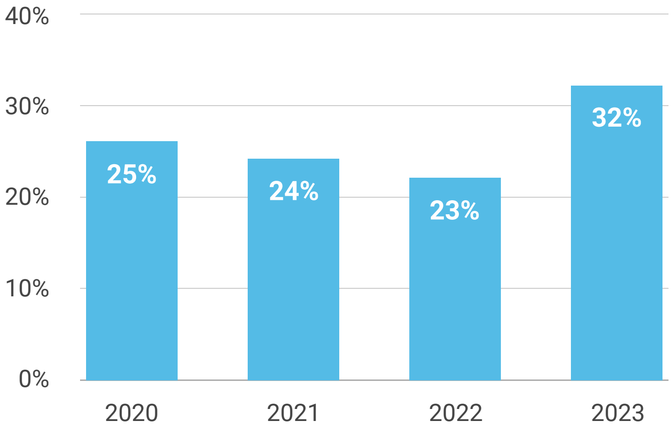


Vendor Management

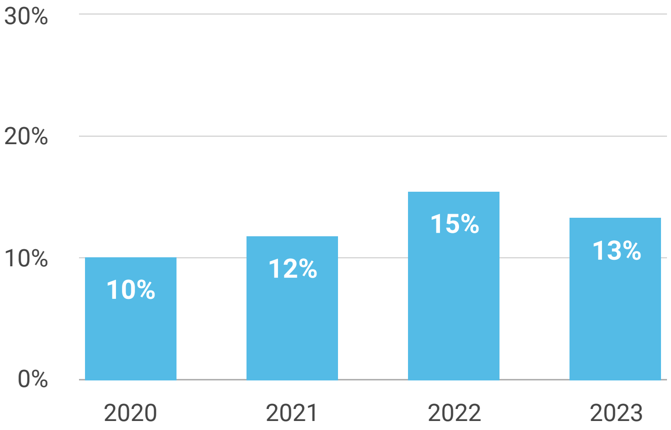
OBSERVATION: INTENTIONAL OVERSIGHT IMPROVES INCIDENT VISIBILITY

Institutions are becoming more intentional about their vendor management as 32% are now using their vendor management program to drive decisions. This is up from last year which was at 20% of institutions.

DRIVES DECISIONS FOR ALL VENDORS



ONLY COMPLETED FOR COMPLIANCE

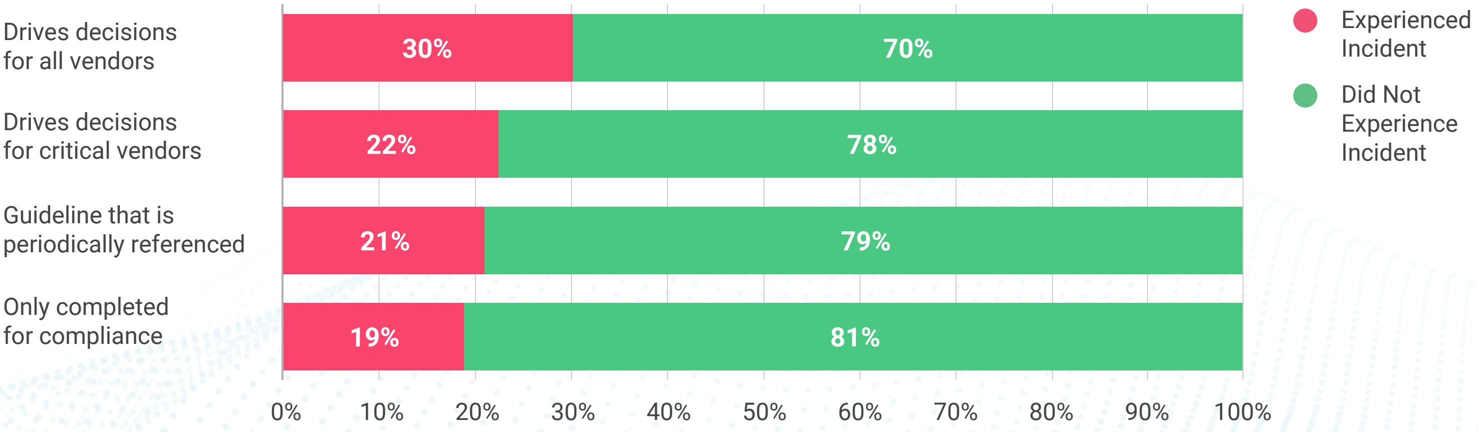


DIVING FURTHER

Of the institutions who said they use their vendor management program to make decisions, 30% said they experienced an incident with a vendor. Of the institutions who said they use their vendor management program for compliance only, 19% said they experienced an incident with a vendor. At first look, this observation seems counterintuitive, as we would expect better use of a program would reduce incidents. However, this stat does not necessarily mean the institutions who only used their vendor management program for compliance actually had less incidents with their vendors. It could be they were just not aware of them.

We propose institutions who have a more formal vendor program may be more aware of current incidents. Conversely, institutions who have not formalized their vendor program could be less aware of current incidents with their vendors.

INCIDENTS EXPERIENCED WITH A VENDOR BY THE WAY THE VENDOR MANAGEMENT PROGRAM IS USED

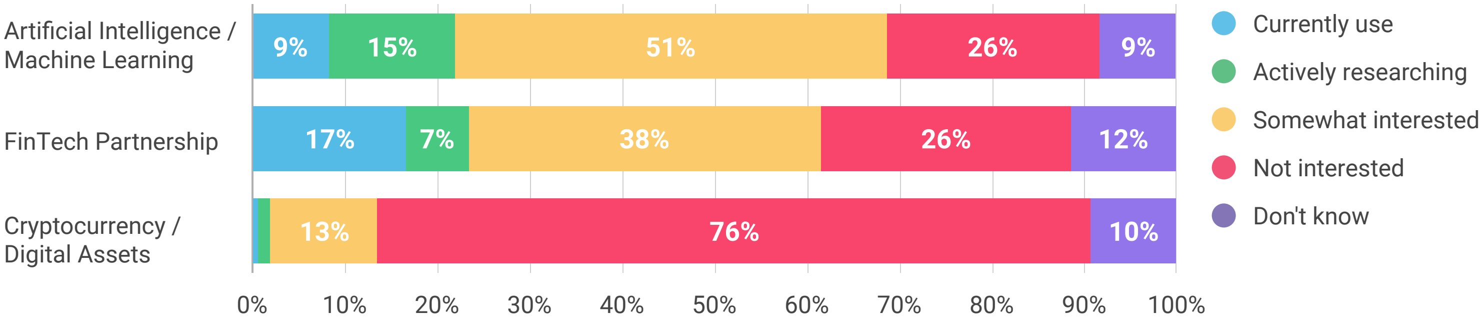


Emerging Technologies

OBSERVATION: INSTITUTIONS ARE MORE RECEPTIVE TO FINTECH AND AI THAN CRYPTOCURRENCY

76% of respondents said they were “Not Interested” when asked about providing cryptocurrency, as compared to 26% for using AI and 26% for partnering with a FinTech.

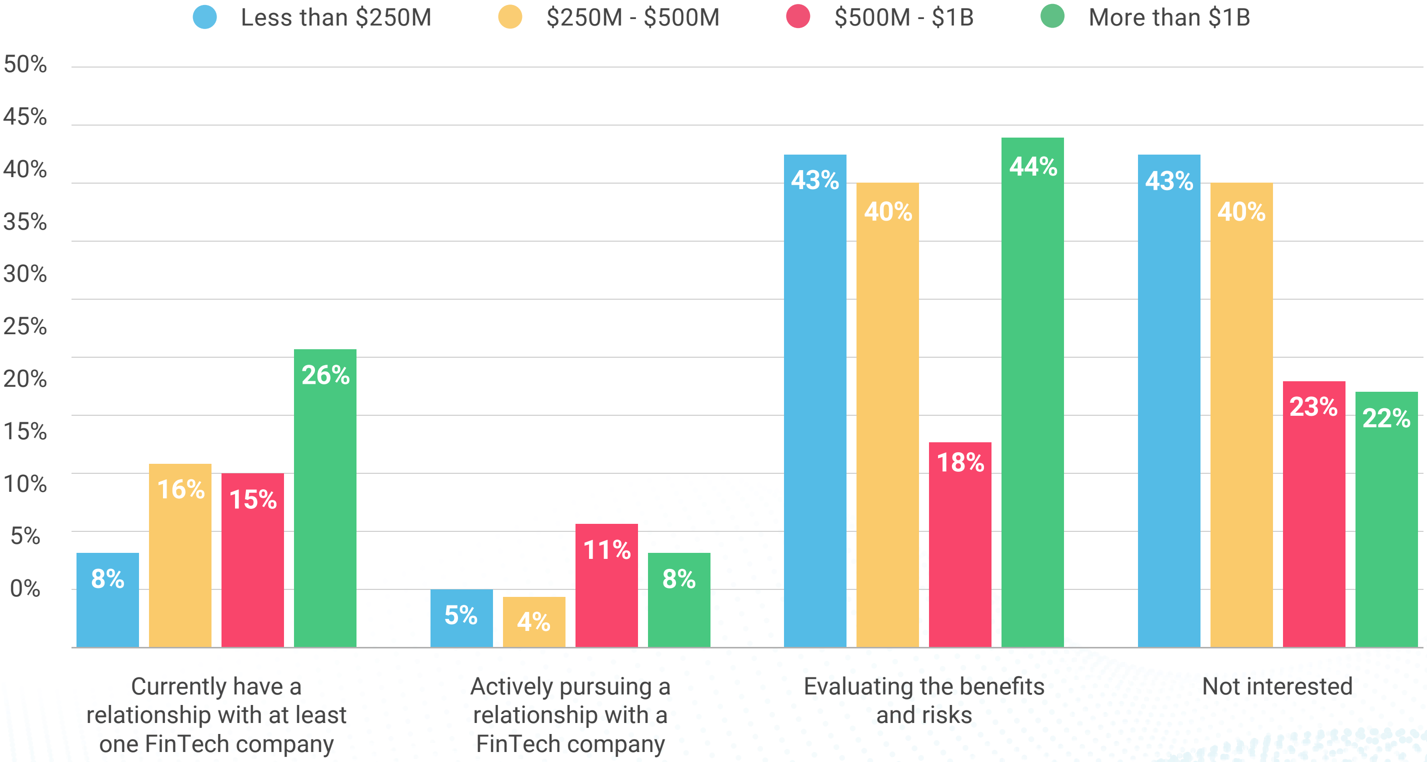
INTEREST IN EMERGING TECHNOLOGIES



DIVING FURTHER

While institutions of all sizes are using, pursuing, and evaluating FinTechs, the highest percentage of institutions already engaged with FinTechs, at 26%, are in the asset size of greater than $1 billion.

INSTITUTIONS USING / PURSUING / EVALUATING FINTECHS BY ASSET SIZE

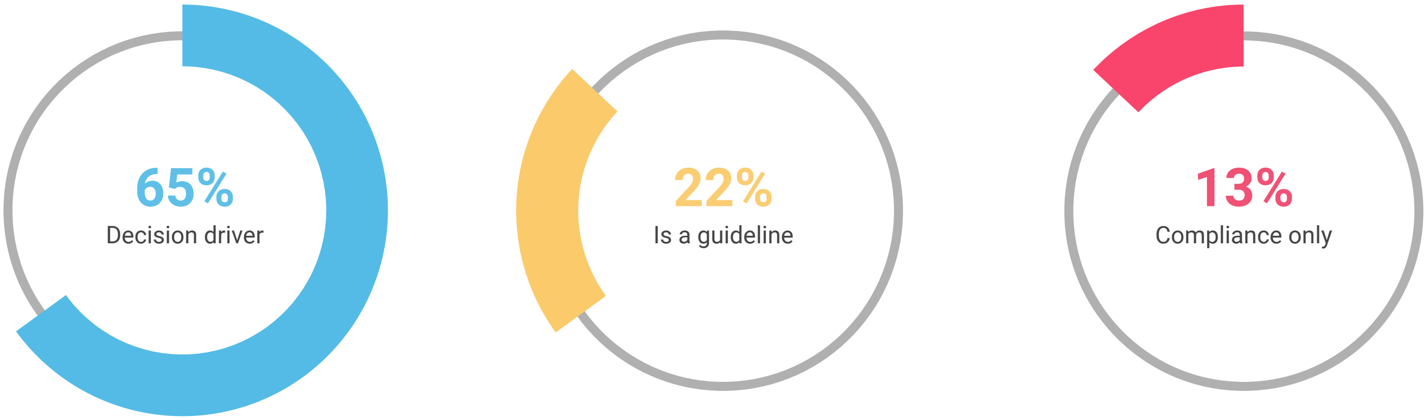


Cybersecurity Culture

OBSERVATION: INSTITUTIONS USING VENDOR MANAGEMENT PROGRAMS TO DRIVE DECISIONS HAVE A STRONGER CYBERSECURITY CULTURE

As part of the survey, we asked how respondents viewed their vendor management program. Did it drive decisions, was it just a guideline that was referenced, or did they only use it because it was required for compliance? While most respondents said they view the vendor management program as a driving factor, over one-third of respondents only use it as a guide or for compliance purposes.

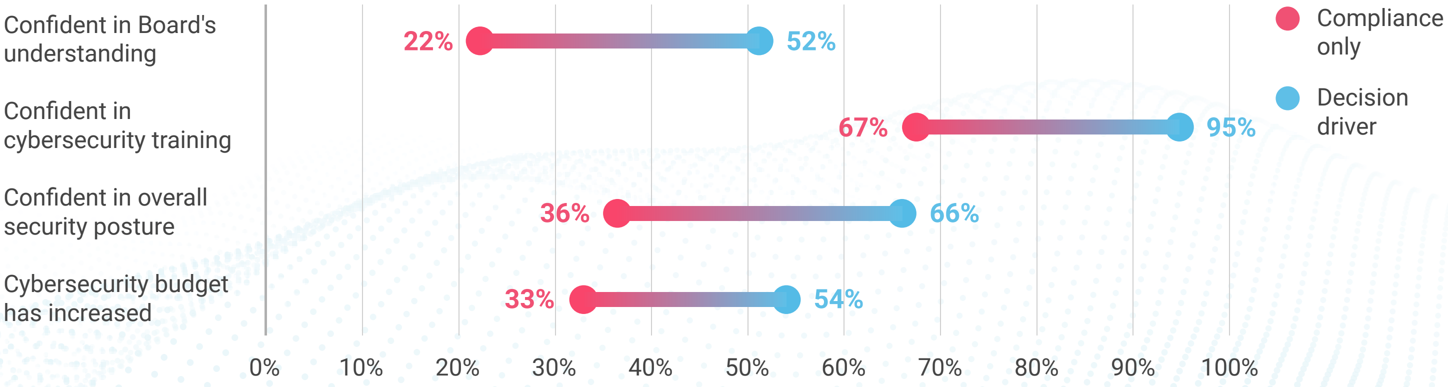
HOW DO YOU VIEW THE VENDOR MANAGEMENT PROGRAM



DIVING FURTHER

We wondered if this attitude towards the vendor management program affects other areas of an institution's cybersecurity program. We discovered overwhelming correlation that institutions who only use their vendor management programs for compliance tend to also have much less confidence in their cybersecurity programs. In contrast, institutions who use their vendor management program to drive decisions seem to have a much stronger cybersecurity culture. In addition, institutions who use their program for driving decisions also find testing of their programs and systems much more valuable. For example, the chart below shows how institutions who use their vendor management program for compliance only are 22% likely to be confident in the Board's understanding of the cybersecurity posture. Where as, institutions who use their vendor management program as a decision driver are 52% likely to be confident in the board's understanding

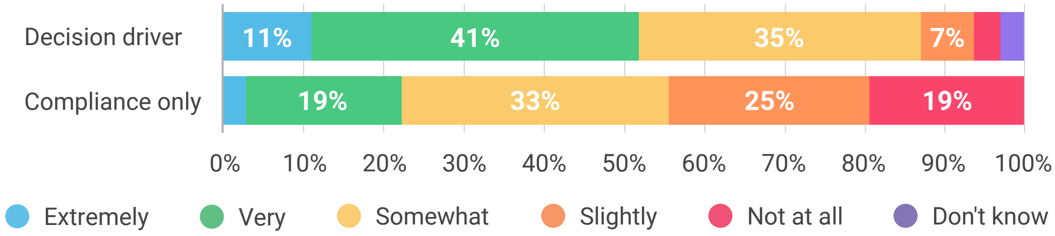
RELATIONSHIP OF VENDOR MANAGEMENT PROGRAM AND OTHER SECURITY PRACTICES



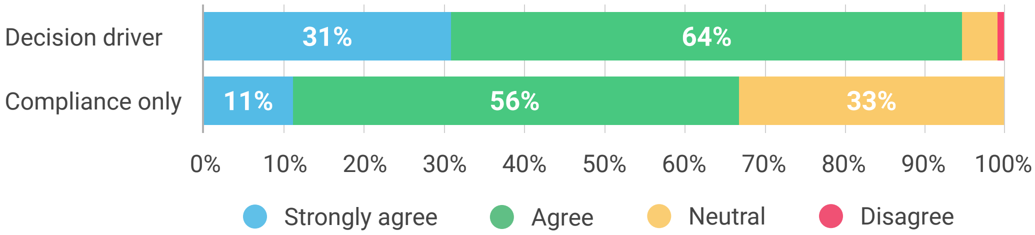
TAKEAWAY

The attitude we have towards programs directly impacts the strength of those programs. To improve a vendor management program or cybersecurity program, the program must first be seen as valuable. This means we should have a firm belief the program can and should be used to drive decisions versus existing just to “check a box” for compliance purposes.

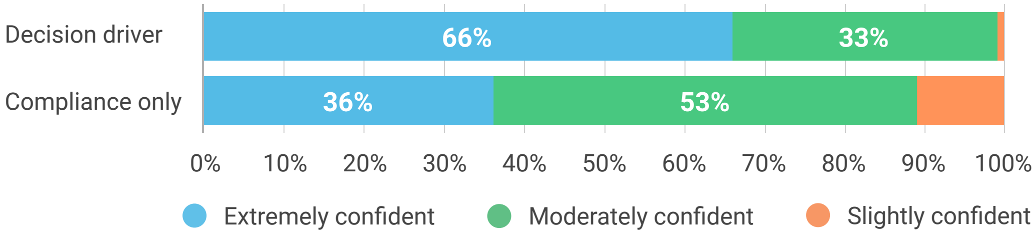
CONFIDENCE IN BOARD'S UNDERSTANDING INSTITUTION'S CYSBERSECURITY POSTURE IN ORDER TO MAKE INFORMED DECISIONS



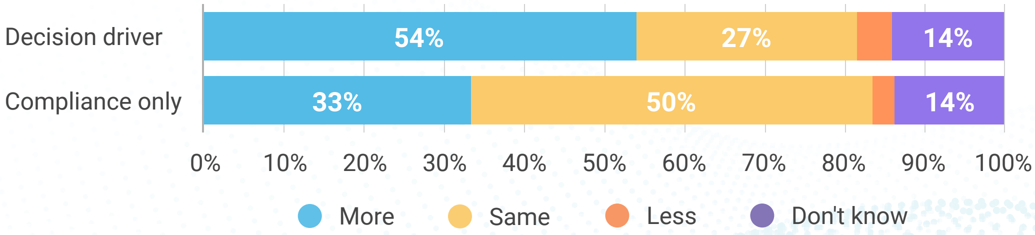
INSTITUTION'S CYBERSECURITY TRAINING DIRECTLY REDUCES THE RISK OF CYBER SECURITY INCIDENTS



CONFIDENCE IN INSTITUTION'S OVERALL SECURITY POSTURE



INSTITUTION'S 2023 CYBERSECURITY BUDGET MORE OR LESS THAN 2022 CYBERSECURITY BUDGET



About the Contributors

AUTHORS

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

ALYSSA PUGH, CISM, SECURITY+

GRC Content Manager

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.

RUSS HORN, CISA, CISSP, CRISC

President

Russ Horn 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.

LETICIA SAIID, SECURITY +

Chief of Staff & Chief Learning Officer

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 & Chief Learning Officer where she focuses on corporate strategy, employee development, and training. In her free time she enjoys mentoring college students, learning piano, and solving jigsaw puzzles.

BRIAN WHIPPLE

Marketing Manager

Brian has over 10 years of experience in Marketing and is the Marketing Manager for CoNetrix.
Since joining the CoNetrix team, Brian has led the company to provide a content-forward strategy by providing educational content on cybersecurity for CoNetrix customers. When not working to provide value for customers, he enjoys spending time with his wife and 4 children on their small farm.

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

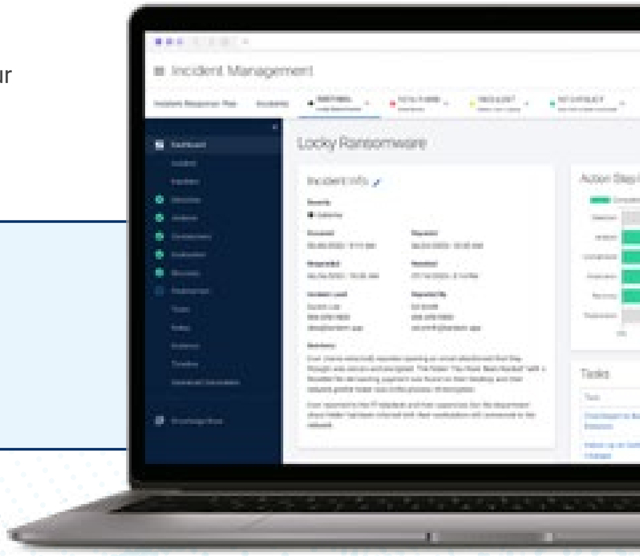
Perform an information security risk assessment, as well as individual information asset risk assessments with our easy-to-follow format in Tandem.

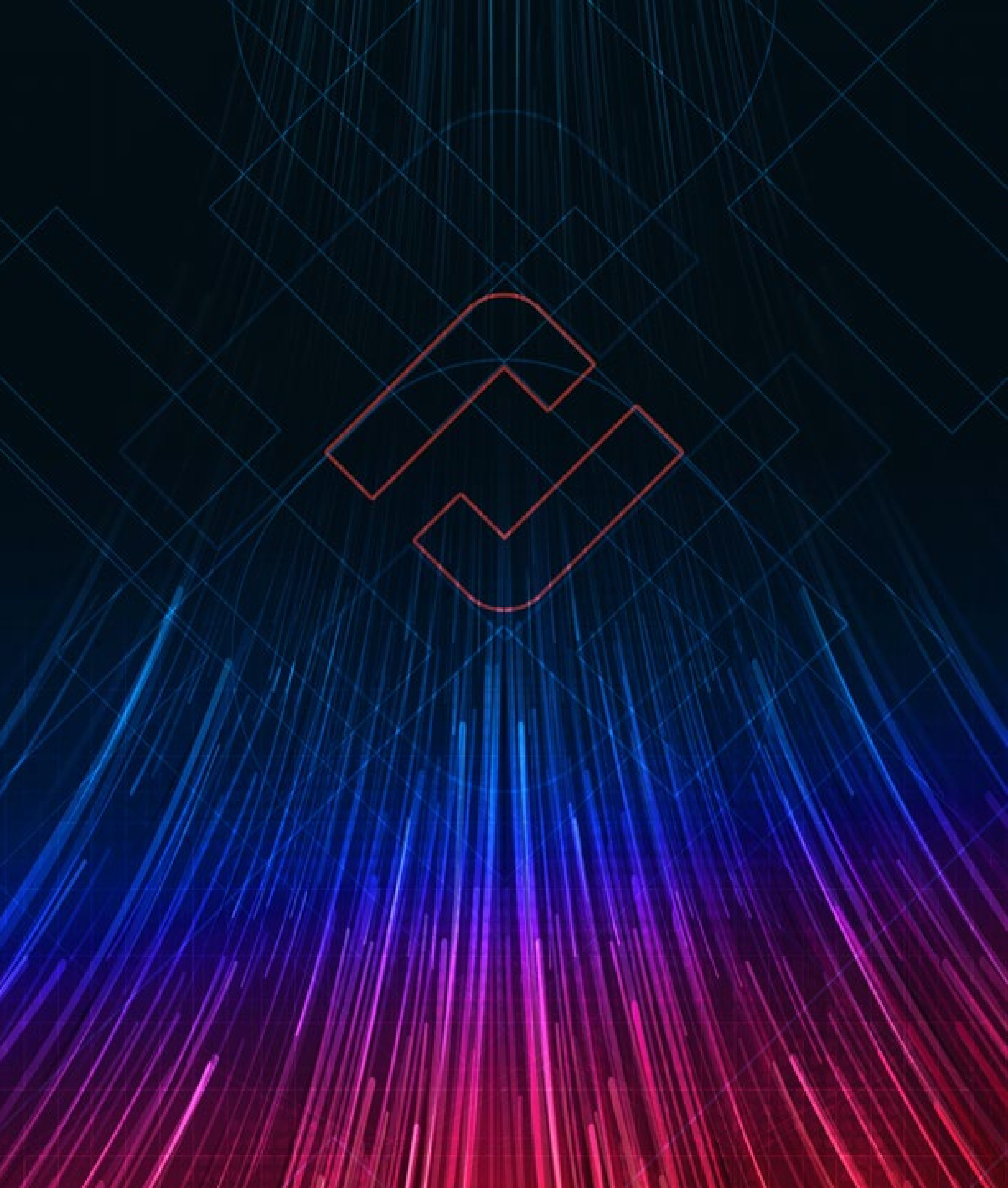
VENDOR MANAGEMENT

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**.





2023 Cybersecurity Report for the Financial Institution Industry