2024

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 238 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 18, 2024 and May 31, 2024.

Participants

All 238 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

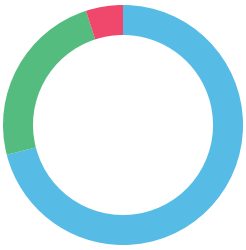
The report is structured into sections for each survey topic. Each topic is divided into three subsections to better share results.

- The **Observations** subsection provides an overview of findings from the survey.
- The **Diving Further** subsection goes deeper into the observations by highlighting trends, cross-referencing responses across the survey, or by comparing responses with prior years.
- The **Commentary** subsection provides additional perspective on the subject and may include summaries, opinions, and recommendations for improving cybersecurity posture.

Demographics

Institutions Surveyed: Types

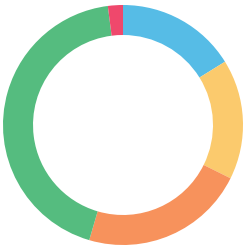
Of those who responded, 71% work for a bank, 24% work for a credit union, and the remaining participants work for other financial institutions (e.g., mortgage companies, trust companies, etc.).



- Bank (71%)
- Credit Union (24%)
- Other (5%)

Institutions Surveyed: Assets

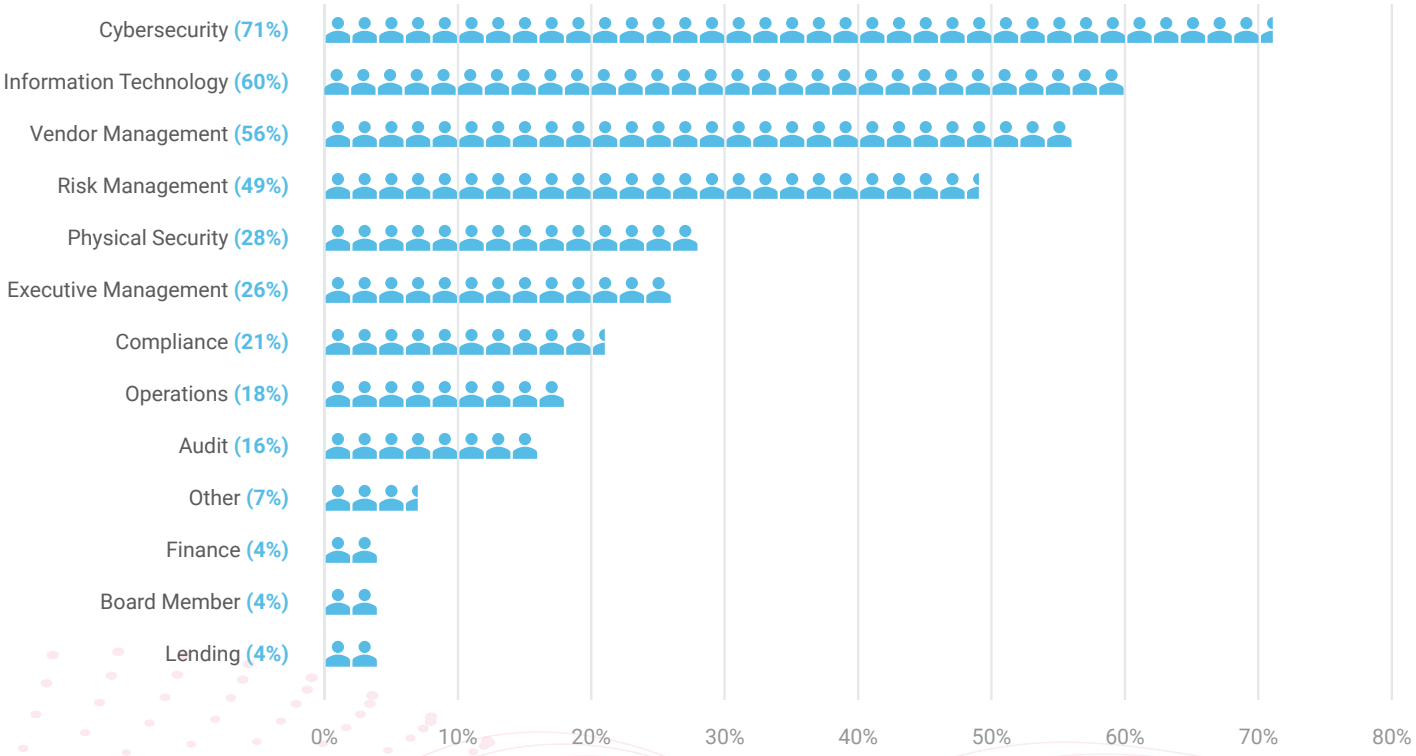
Survey respondents from small to medium-sized community institutions made up a small majority of total respondents (54%). However, 44% were from larger community institutions reporting over $1 billion in assets.



- Less than $250M (16%)
- $250M - $500M (16%)
- $500M - $1B (22%)
- $1B - $10B (44%)
- More than $10B (2%)

Roles & Responsibilities

Survey participants worked primarily within cybersecurity or information technology roles. Over half of participants also worked in vendor management and risk management roles. Participants were asked to select all that applied.

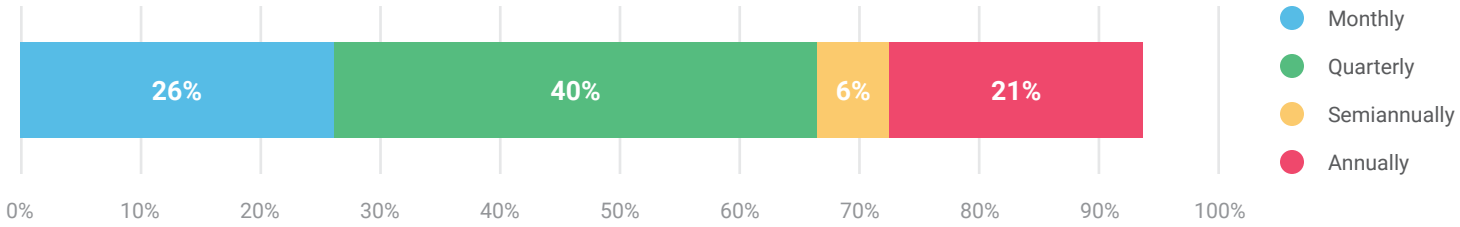


Board Oversight

Observation: Majority Update the Board Quarterly

The majority of financial institutions (40%) meet with their Board of Directors quarterly to give an update on the institution's cybersecurity status.

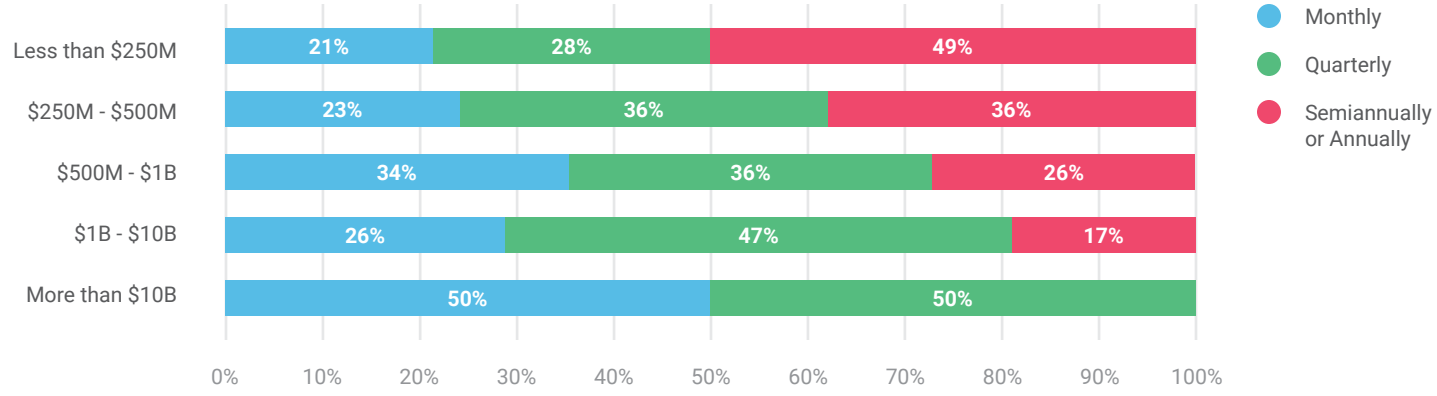
FREQUENCY OF BOARD UPDATES



Diving Further

Institution size may factor into the decision of frequency as 49% of institutions that have $250 million or less in assets report to their Board annually or semiannually.

REPORTING FREQUENCY BY ASSET SIZE



Commentary

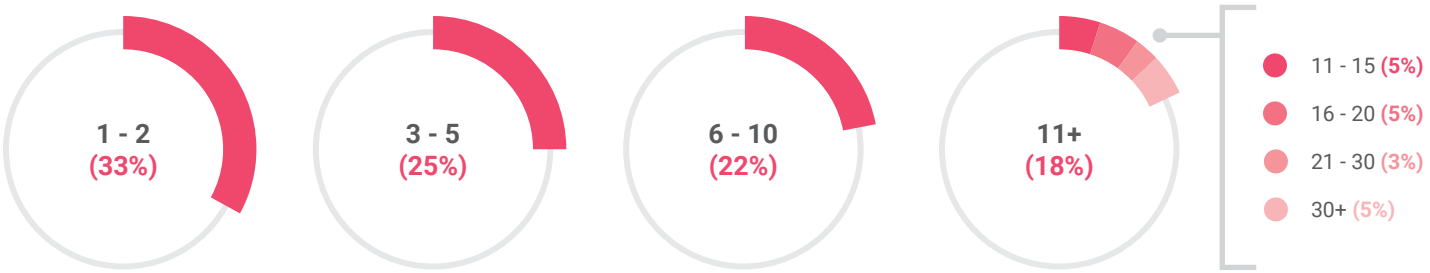
Trends continue to show a correlation between asset size and Board report frequency. Smaller institutions report to the Board of Directors less frequently than their larger counterparts. While the reasons for this can vary (e.g., resource constraints, less complexity, Board preferences, etc.), it is a good practice for institutions to report on a frequency that promotes effective awareness of the institution's cybersecurity posture.

Staffing

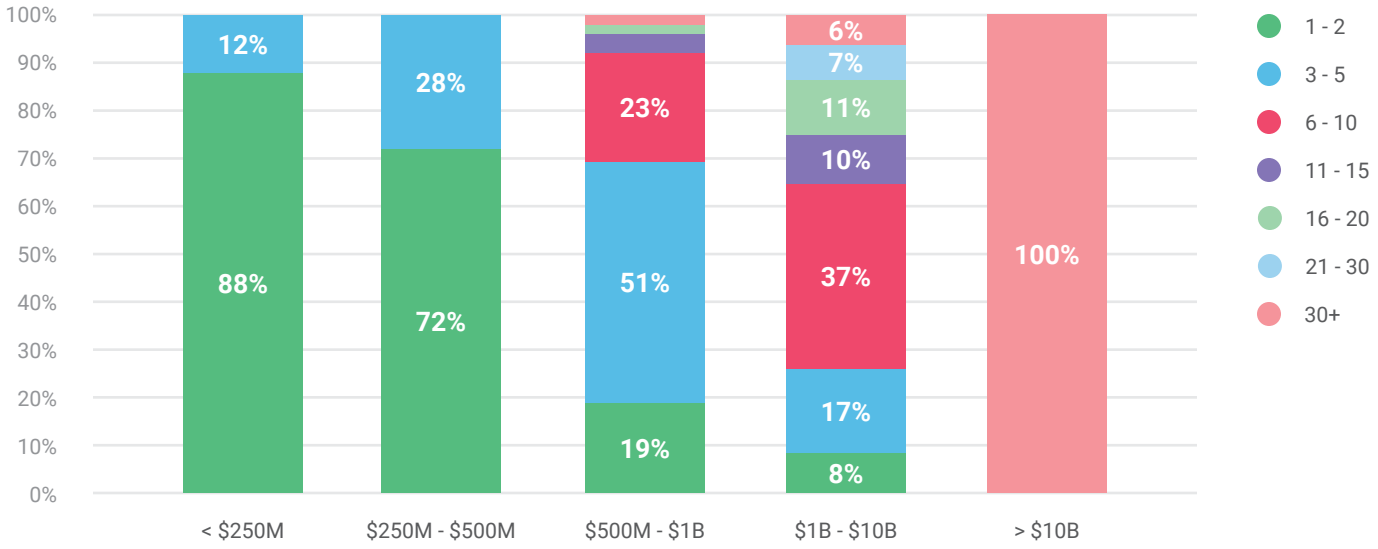
Observation: Majority of Financial Institutions have up to 10 Full-Time IT/Security Employees

Most institutions (80%) have 10 or less full-time IT or information security professionals working for their institution. As might be expected, the larger the institution, the more IT and information security professionals are employed at the company.

NUMBER OF FULL-TIME IT/SECURITY STAFF



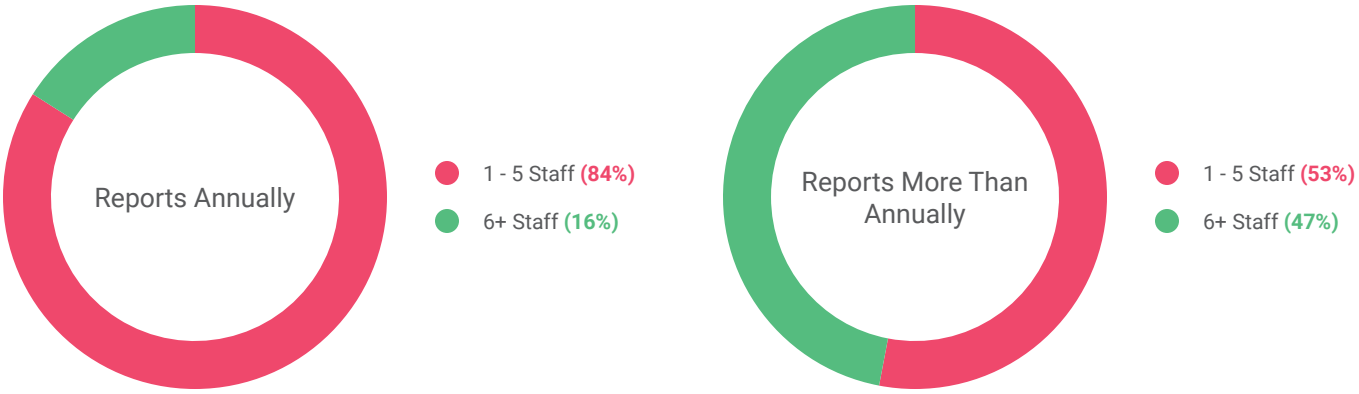
NUMBER OF FULL-TIME IT/SECURITY STAFF BY ASSET SIZE



Diving Further

Institutions who report more frequently to the Board of Directors tend to have more full-time employees on their team. Of those that report annually to the Board, 84% also report having five or fewer full-time employees. Of those that report more than once per year (i.e., semiannually, quarterly, or monthly), 47% also report having six or more full-time employees.

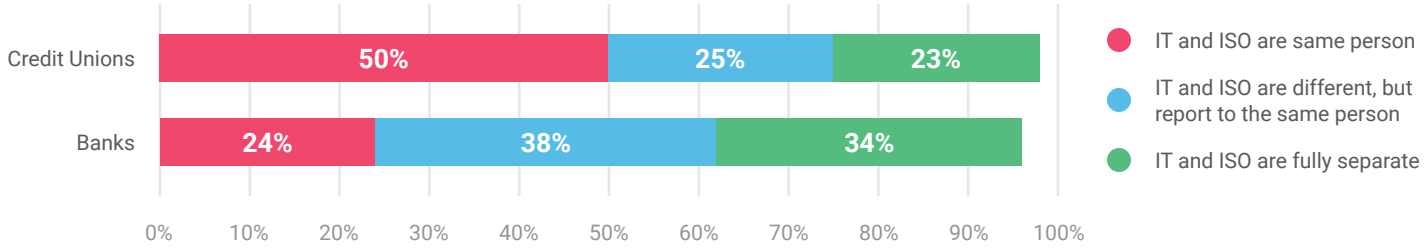
NUMBER OF FULL-TIME STAFF BY BOARD REPORT FREQUENCY



Observation: Credit Unions More Likely to Share IT and ISO Duties

According to survey results, credit unions are twice as likely as banks to have the ISO and IT roles held by the same person.

SEPARATION OF DUTIES BY INSTITUTION TYPE



Commentary

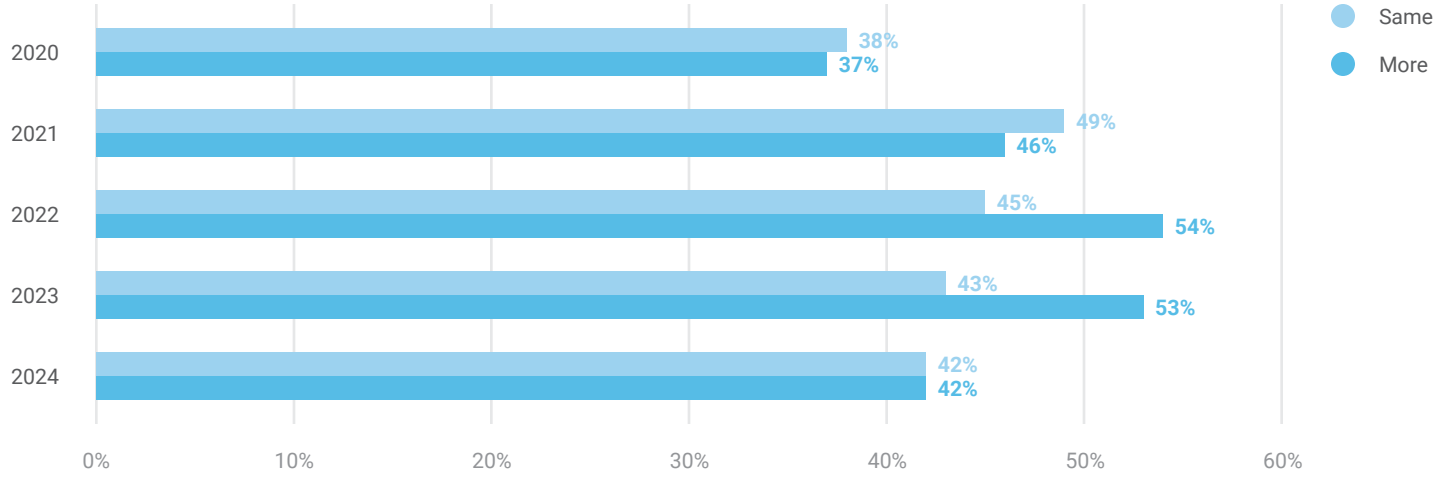
Several factors influence how many IT and/or security staff are employed at a financial institution (e.g., budget, complexity of IT environment, speed of organizational growth, etc.). Regardless of the reasons for varied frequency, reporting more often to the Board leads to a Board who is more informed of the organization's technology needs and, as a result, can be more willing to dedicate resources to IT and cybersecurity.

Budget

Observation: Budgets Fluctuate in 2024

While institutions have increased their cybersecurity budgets in 2024, the trend of increasing budgets shows signs of slowing slightly, as only 42% increased budgets in 2024 compared to 53% in 2023.

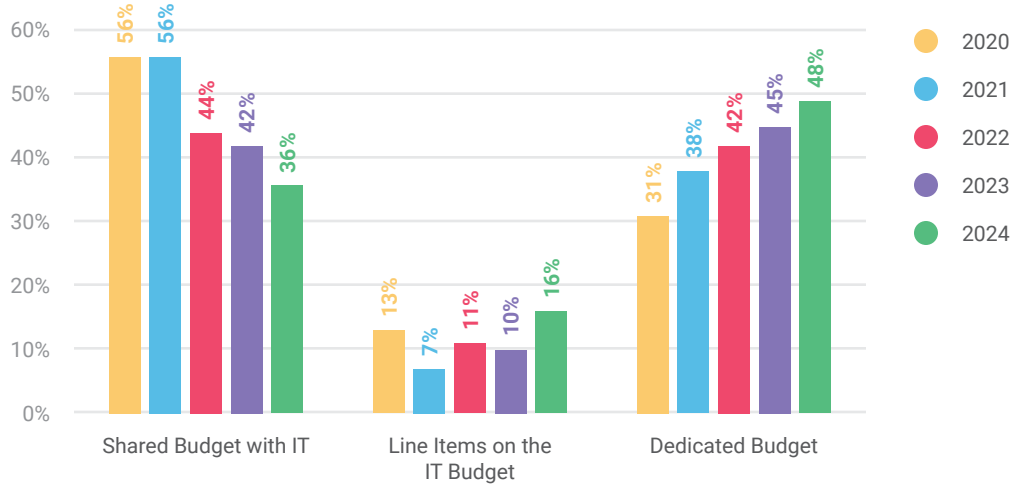
BUDGET CHANGES IN 2024



Diving Further

There has been a steady increase in the number of institutions who are creating a dedicated budget for cybersecurity with 48% now separating their budget from IT. This is a significant increase compared to 2020 where only 31% of institutions had a cybersecurity budget separate from IT.

CYBERSECURITY BUDGET ALLOCATION



Commentary

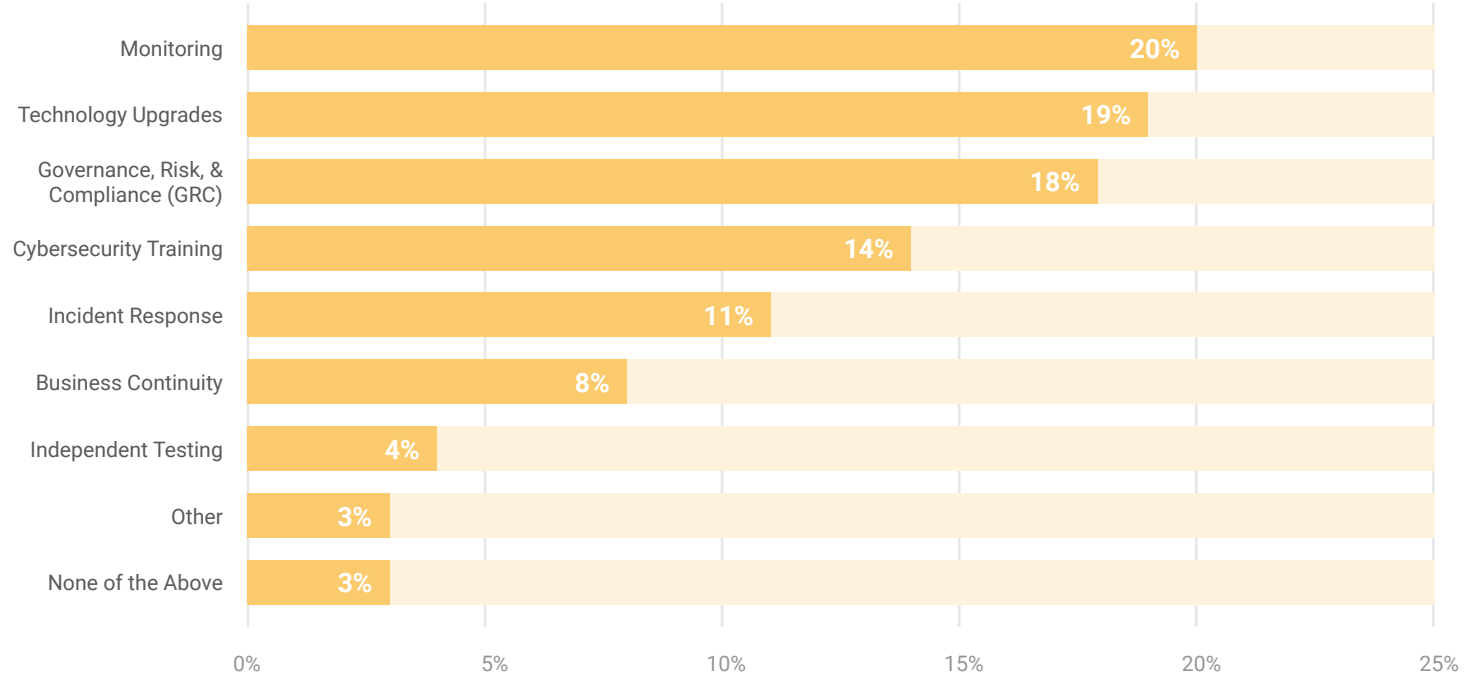
We have seen two big benefits result in institutions who set a dedicated cybersecurity budget. First, the clear resource allocations help to limit game-time conflicts over spending priorities. Second, having a dedicated cybersecurity budget demonstrates an institution's cybersecurity commitment to staff, shareholders, and clients. This is a win-win for all parties involved.

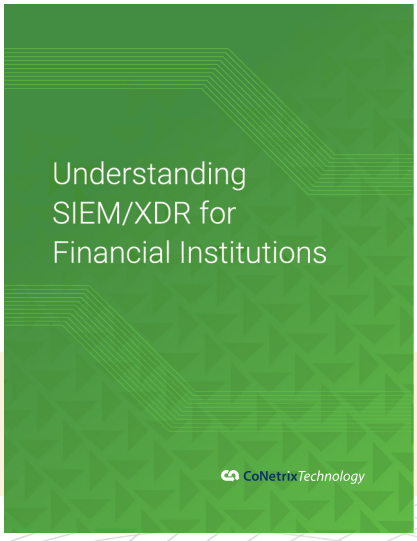
Cybersecurity Oversight

Observation: Various Resources Preferred to Improve Security

Financial institutions are split on how they would use additional resources, with monitoring solutions (e.g., SOC, SIEM, etc.) being selected as the top option. This indicates that one-in-five institutions are most concerned about their ability to detect malicious behavior on their networks.

CYBERSECURITY BUDGET ALLOCATION





Commentary

While the concept of "monitoring" tops the list of resources, monitoring can take many shapes and forms, often overlapping with other areas on this list, such as technology upgrades. Two common technical monitoring controls include Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) solutions. Tools likes these strengthen an institution's ability to detect and respond to cyber threats.

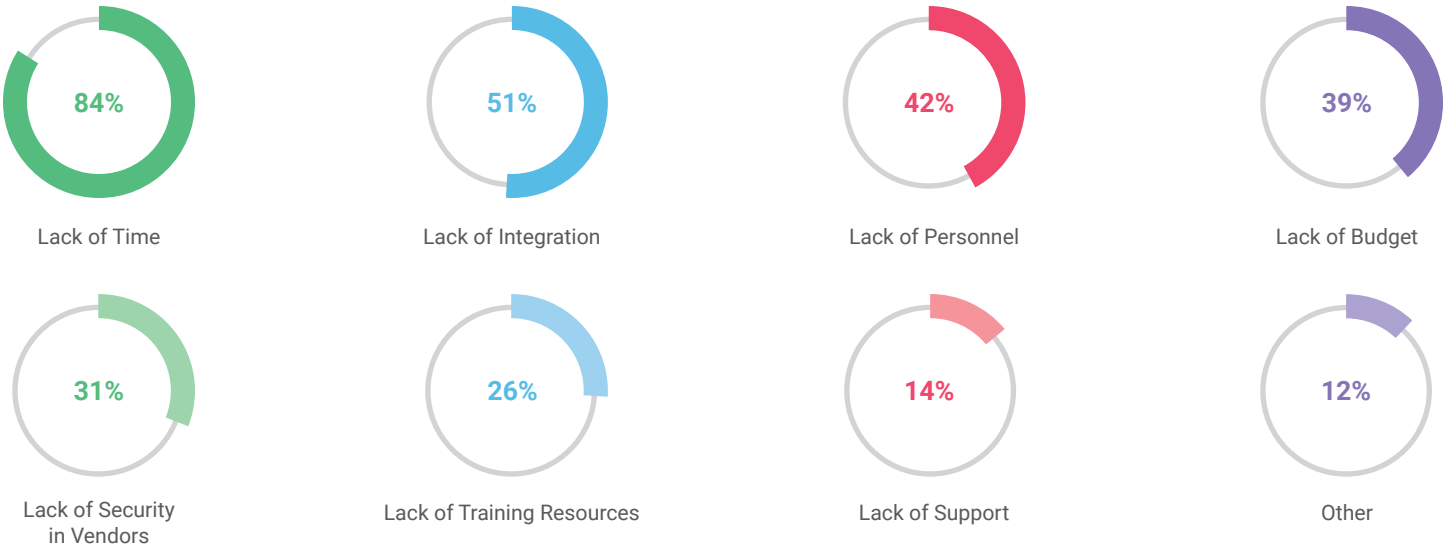
Learn more about these types of monitoring solutions with this free resource: CoNetrix.com/XDR.

Diving Further

Participants were also asked to select the top three circumstances negatively impacting the success of the institution's cybersecurity strategy. Similar to previous years, participants continue to express a "lack of time" as the most significant barrier to their cybersecurity program's success.

On the other end of the results, a "lack of support" (i.e., from the Board of Directors and senior management) continues to be seen as a less significant barrier. Only 6% of participants cited both "lack of support" and "lack of budget," which demonstrates an improvement in top-down cybersecurity support.

FACTORS IMPACTING CYBERSECURITY STRATEGY



Commentary

While most frequently selected, the "lack of time" factor is more of a resulting feeling than a cause. Security teams often take on complex work while armed with limited resources, funds, and staff. In this scenario, tasks can pile up fast, making it seem like if we just had more time, we could get it all done. As stress and inefficiency compound, feelings of being time-constrained intensify.

By taking steps toward fixing the root causes, cybersecurity professionals can better manage tasks and feel like they have more time, as a result. Here are some tips for addressing the next three issues, which may contribute to this "lack of time."

Lack of Integration (51%)
Look for ways to streamline workflows, standardize processes, and choose solutions that prioritize compatibility.

Lack of Personnel (42%)
Prioritize recruiting, training, and/or retention of team members, but recognize, this is a long-term investment that may require you to say "not right now" to some projects.

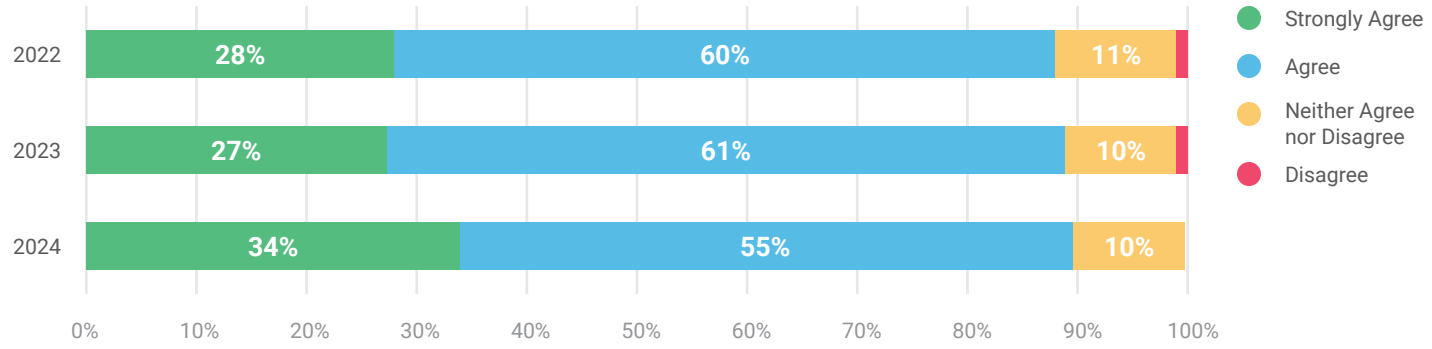
Lack of Budget (39%)
Focus on your most critical needs, negotiate better terms with vendors, and seek out cost-effective alternatives.

Training

Observation: Institutions Feel More Confident in Training

Over the past few years, financial institutions have become more confident in their cybersecurity training with 89% of participants agreeing or strongly agreeing their cybersecurity training directly reduces the risk of cyber incidents.

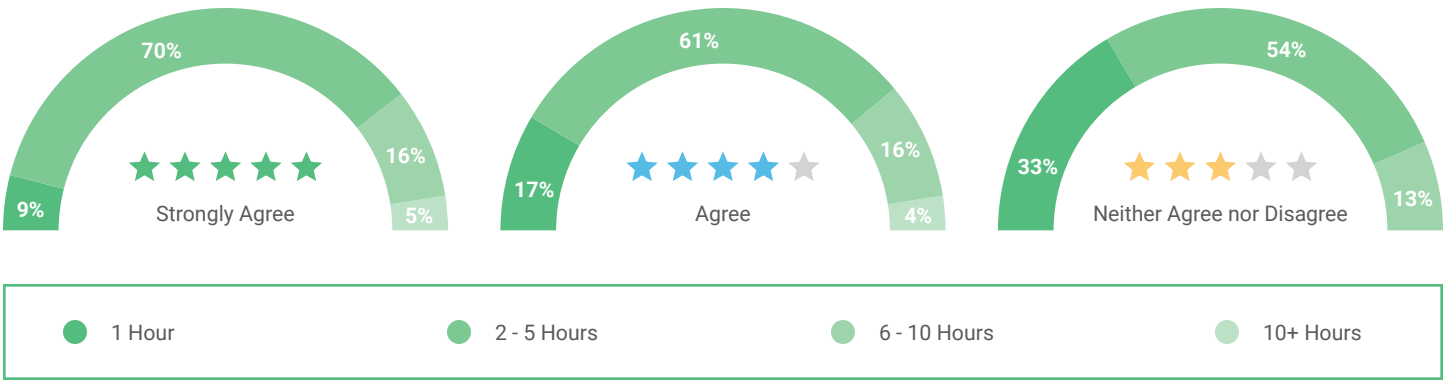
CONFIDENCE IN CYBERSECURITY TRAINING



Diving Further

Institutions who administer more hours of training are more likely to agree their cybersecurity training is effective. Among participants who "Strongly Agree" or "Agree" their training is effective, a significant majority (70% and 61%, respectively) administered 2-5 hours of annual training for each employee. Less confident participants more often reported spending less time conducting annual training, with a third reporting only 1 hour.

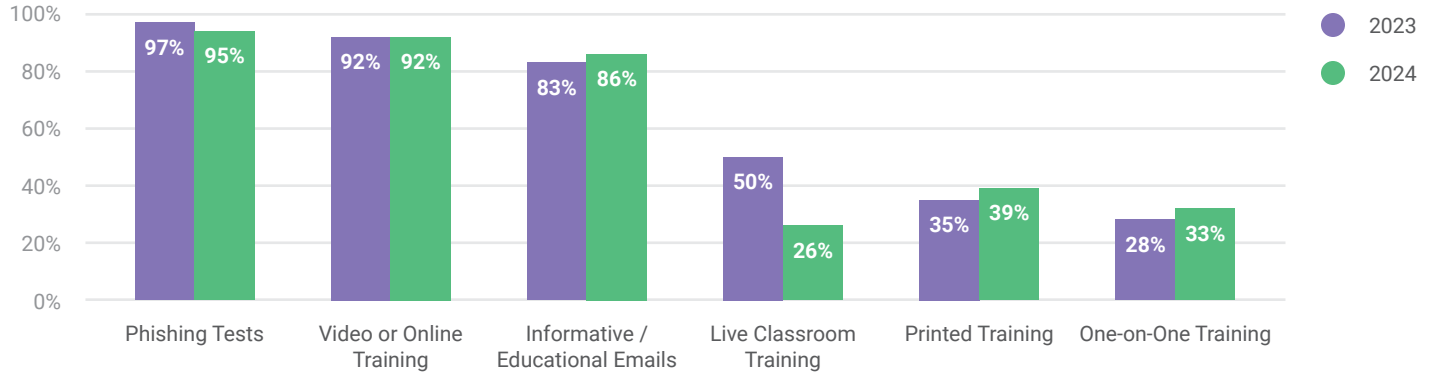
TRAINING HOURS COMPARED WITH TRAINING EFFECTIVENESS



Observation: Phishing Tests and Video Top the Training Types

Simulated phishing emails and video training remain the two most common forms of training. The use of phishing tests has slightly decreased to 95%, while video or online training has remained consistent at 92%. Informative and educational emails have seen an increase, possibly due to their effective combination with phishing tests.

SECURITY AWARENESS TRAINING ACTIVITIES



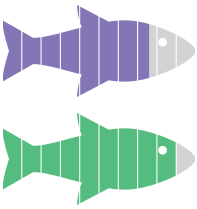
This graph shows a significant change in the "Live Classroom Training" answer from 2023 to 2024. This is likely due to a change in how the question was presented in the survey and is not indicative of a change in training activities.

Diving Further

Almost all financial institutions are now conducting phishing testing as part of their cybersecurity awareness training, going from 88% of institutions in 2019 to 95% of institutions in 2024.

There is also a trend toward conducting phishing testing more frequently. In 2024, more than 60% of financial institutions report they conduct phishing tests monthly or more frequent. This is likely due to having easy and affordable products, such as Tandem Phishing, to conduct the testing, combined with the value perceived from this type of training.

CONDUCTING PHISHING TESTS

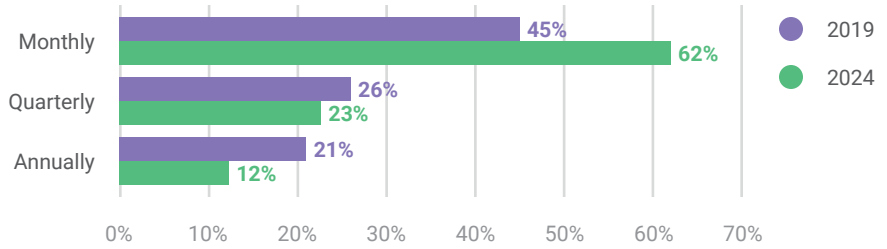


88% (2019)

95% (2024)

Shown on 50% to 100% scale with 5% intervals.

FREQUENCY OF CONDUCTING PHISHING TESTS



Commentary

Increasing the frequency of security awareness training you administer throughout the year can positively impact employees' awareness and skill in cybersecurity. Try creating a schedule at the beginning of the year to help you to strategically plan and spread these activities out over time.

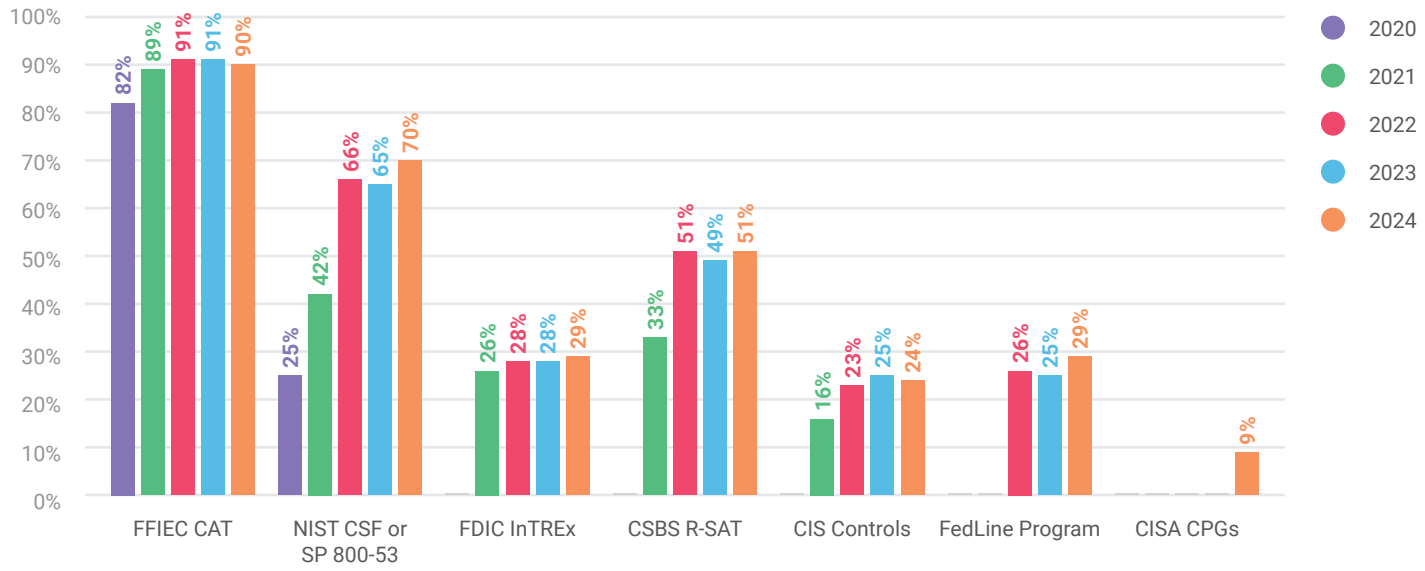
Regular phishing tests reinforce good habits by keeping cybersecurity top of mind, while video and online training offer engaging and easily digestible content that simplifies complex concepts. By combining these methods, you ensure that employees remain attentive to social engineering attempts, contributing to a more secure workplace environment.

Cybersecurity Tools & Frameworks

Observation: CAT and NIST Lead in Framework Use

The FFIEC Cybersecurity Assessment Tool (CAT) continues to be the most used framework with 90% of respondents stating use of the framework. The use of NIST frameworks continues to grow with 70% of respondents using a NIST framework in 2024 compared to 65% in 2023.

ADOPTION OF CYBERSECURITY FRAMEWORKS AND TOOLS



Diving Further

While the CISA Cybersecurity Performance Goals (CPGs) are relatively new, they have seen noticeable adoption in the financial sector (9%) since their release in October 2022.

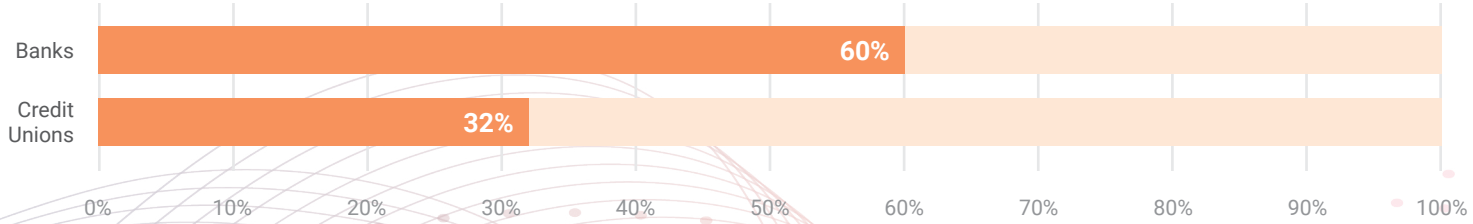
The Ransomware Self-Assessment Tool (R-SAT) has also seen wide industry adoption with 60% of banks and 32% of credit unions reporting use.

9%

NEW TREND

Financial institutions who use the CISA Cybersecurity Performance Goals.

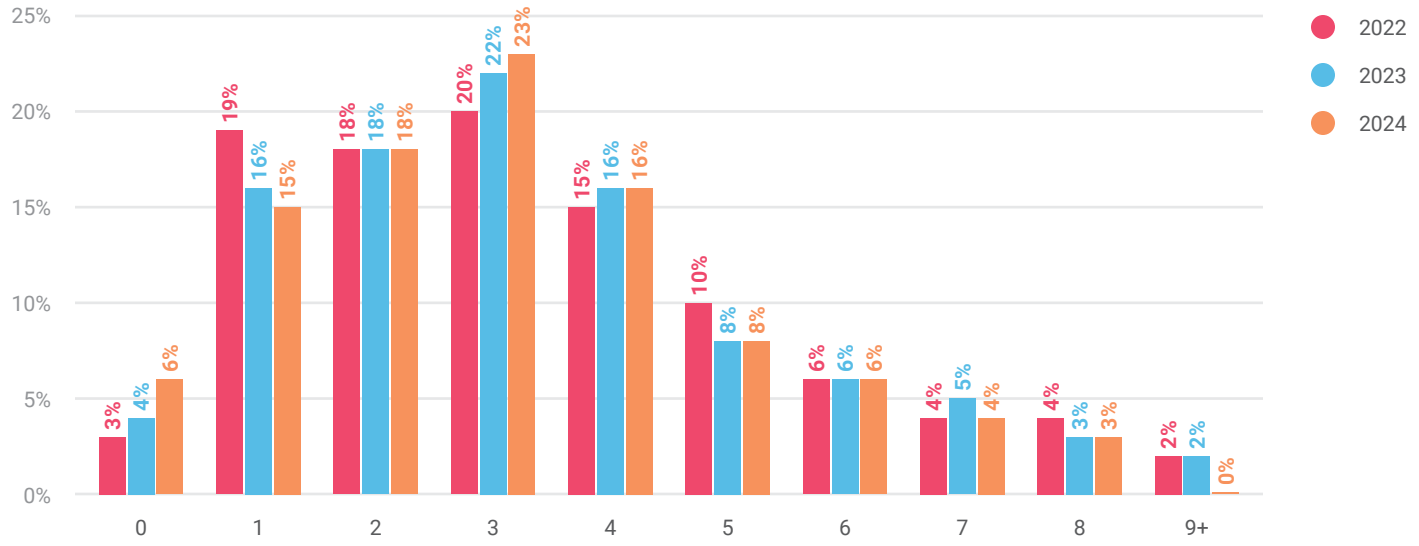
R-SAT ADOPTION BY TYPE



Diving Further

Of the 15 possible answer options, 66% of survey participants reported using one to four cybersecurity assessment tools and frameworks. While this number has decreased slightly since 2022, the reason appears to be due to people using more frameworks, with 28% now reporting use of five or more.

NUMBER OF ADOPTED CYBERSECURITY FRAMEWORKS AND TOOLS



Commentary

On August 29, 2024, the FFIEC announced the sunset of the Cybersecurity Assessment Tool (CAT) effective August 31, 2025. For the last 10 years, the CAT has been the go-to cybersecurity controls framework for community financial institutions, speculatively due to the tool's use in federal banking agency examination programs.

Now, the data shows that other tools are gaining traction, with the FFIEC giving a nod of encouragement to several different frameworks. This aligns with the positive trend showing increased adoption of frameworks like the NIST Cybersecurity Framework (CSF), NIST SP 800-53 Controls, CISA Cybersecurity Performance Goals (CPGs), and CSBS Ransomware Self-Assessment Tool (R-SAT).

That said, not everyone is saying goodbye to the CAT. While banks will likely begin to explore other risk-focused frameworks, the NCUA has announced their continued support of the ACET for credit unions, offering a familiar and trusted option for the industry.

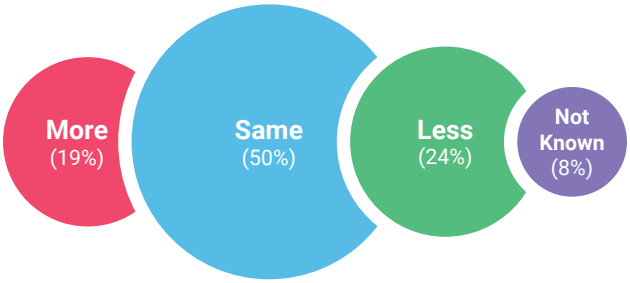
Learn more about the FFIEC CAT sunset and stay updated with Tandem's future plans: Tandem.App/News/Tandem-Statement-on-FFIEC-CAT-Sunset.

Incident Response

Observation: Number of Cyber-Attacks Increase for Some Institutions

The overall number of cyber incidents for financial institutions appears to be holding steady from last year with 50% reporting no increase nor decrease, 24% said fewer, and 19% said more. This appears to be a balance for the industry as a whole.

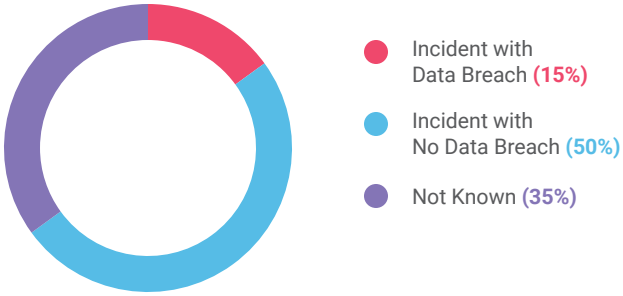
VOLUME OF CYBER INCIDENTS COMPARED TO LAST YEAR



Observation: 85% of Cyber Incidents do not Indicate a Data Breach

Of the 238 respondents, only 15% of financial institutions said they had a cyber incident that resulted in a confirmed data breach. However, 35% reported not knowing whether a data breach occurred.

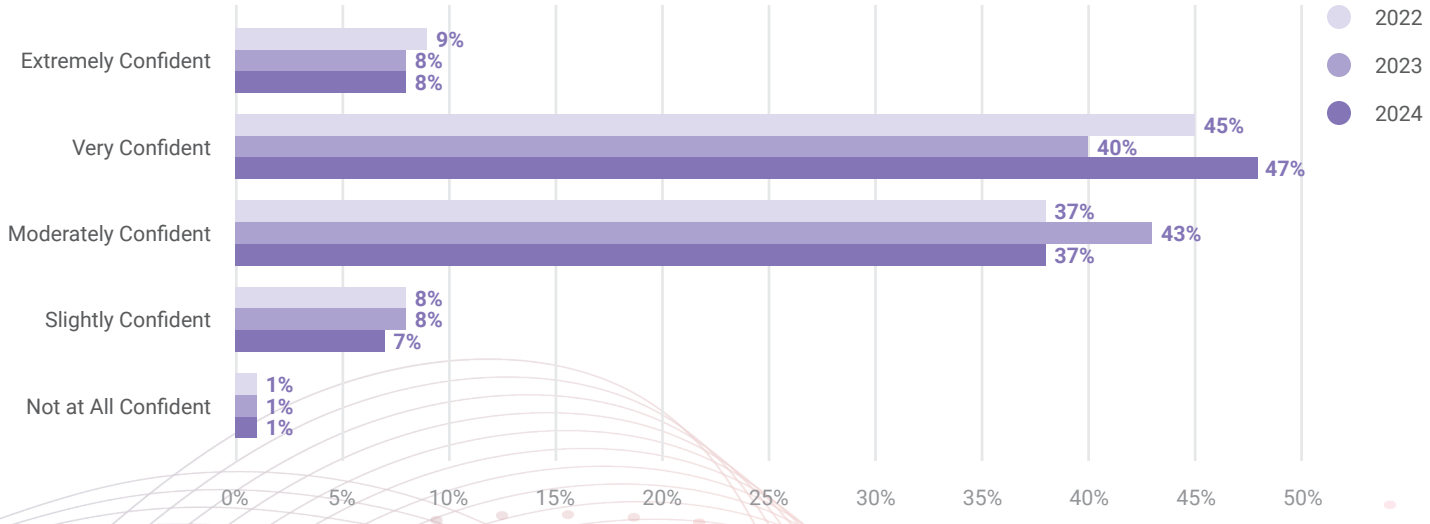
INSTITUTIONS WHO EXPERIENCED A DATA LOSS OR BREACH



Diving Further

A little over half of institutions have confidence in their monitoring and detection systems, with 55% of institutions claiming they are extremely confident or very confident in their ability to detect an incident as it is happening.

CONFIDENCE IN DETECTING AN INCIDENT OCCURRING

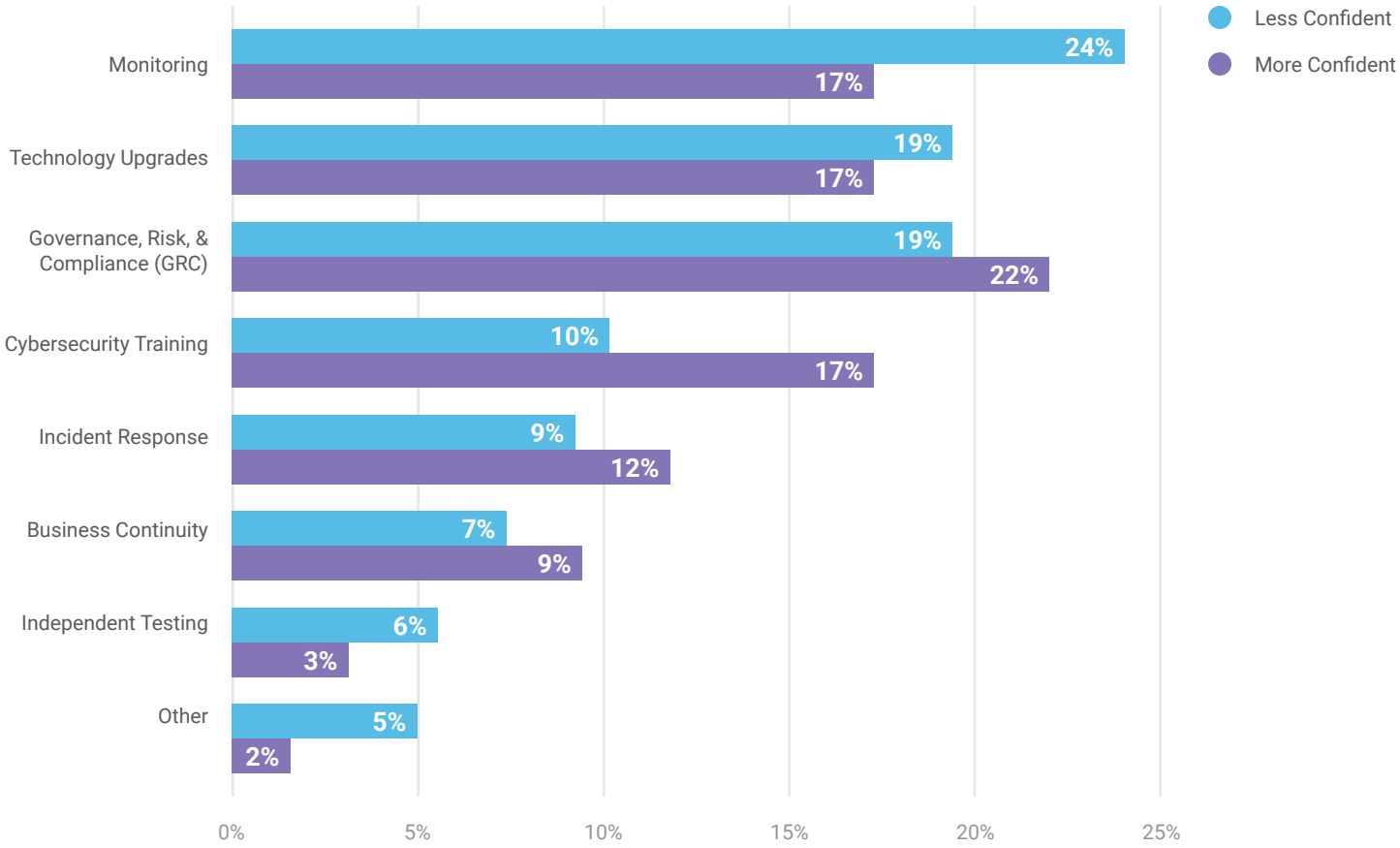


Diving Further

There is a correlation between participants' confidence in detecting incidents and the areas where they would choose to invest additional cybersecurity resources, if available.

Those who are less confident in their ability to detect incidents as they occur (i.e., "Moderately," "Slightly," or "Not at all") are more likely to invest in monitoring and technology upgrades. On the other side, those who are more confident (i.e., "Extremely" or "Very") are more likely to invest in GRC, cybersecurity training, and incident response.

CONFIDENCE IN INCIDENT DETECTION COMPARED TO WANTED RESOURCES



Commentary

While cyber-attacks are happening more frequently across the globe, financial institutions are doing well to prevent, detect, and respond to incidents. While resources are still needed and systems can always be improved, it's encouraging to see a majority of institutions are moderately to extremely confident in their ability to detect an incident. This success could be thanks to heightened emphasis on cybersecurity practices in the financial sector.

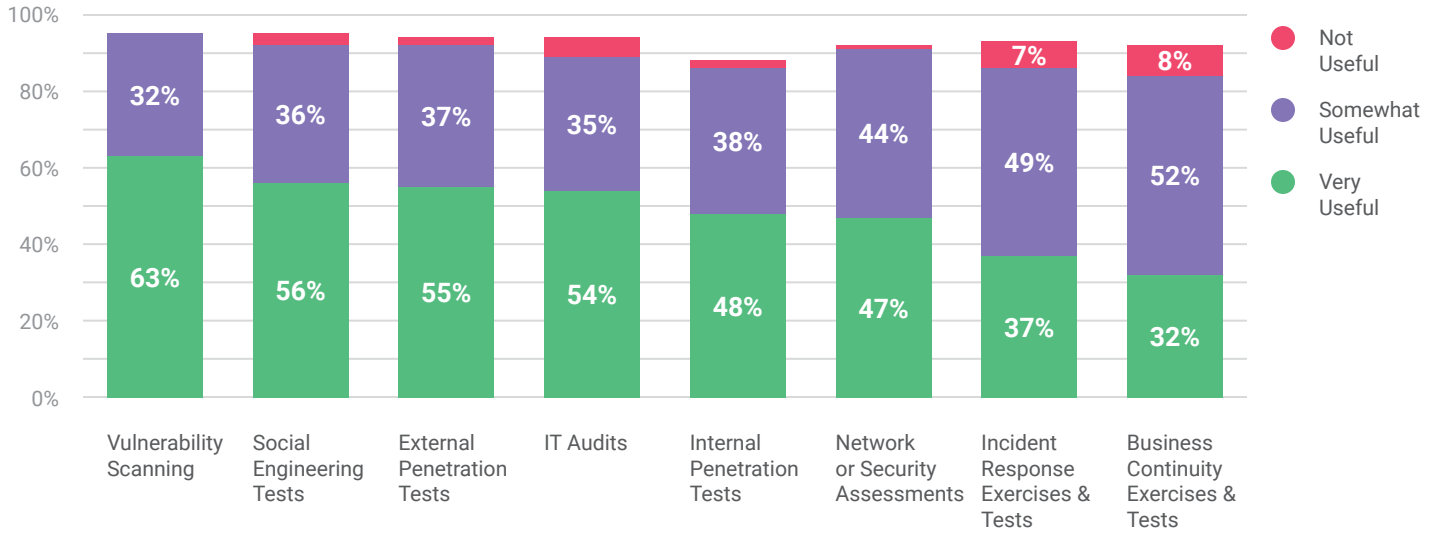
It is also encouraging to see trends showing that institutions are aware of their current posture and their next steps. Institutions who lack the ability to quickly detect incidents recognize the importance of improving monitoring first, while institutions who are confident in detection are focused more on incident prevention (i.e., training) and response.

Assurance & Testing

Observation: Institutions Favor Technical Tests and Audits

Financial institutions found most testing and assurance activities useful with 63% of participants finding vulnerability scanning to be the most useful security practice. Incident response and business continuity plan tests and exercises, such as tabletop tests, are perceived to be less useful.

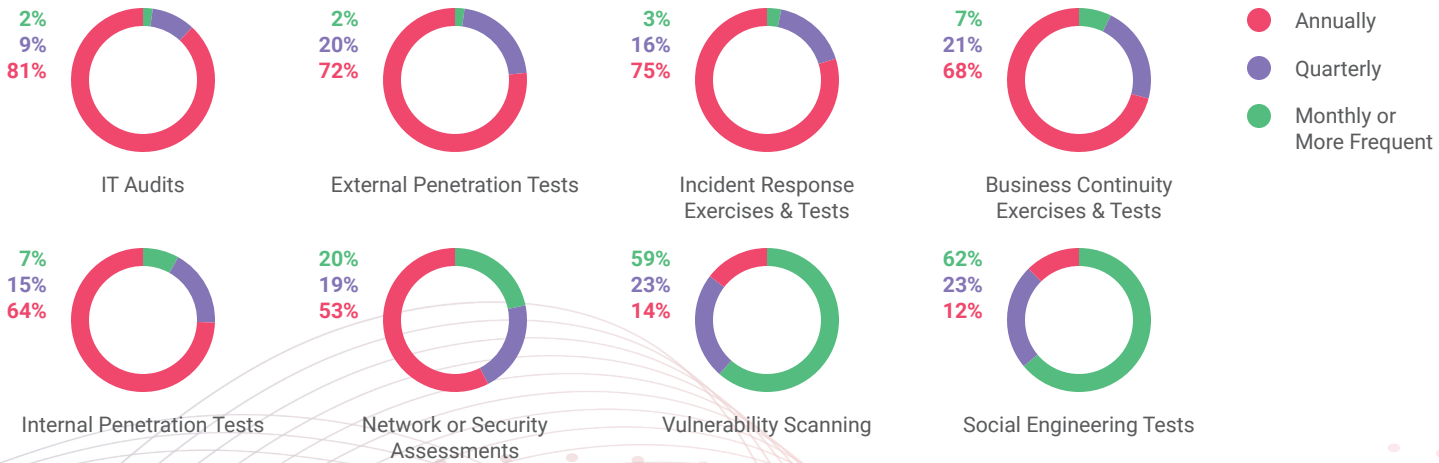
USEFULNESS OF TESTS AND AUDITS



Diving Further

The frequency of testing may play into the perceived value of tests as the two most useful tests are also the two types of tests performed most frequently by institutions (vulnerability scanning and social engineering tests). Alternatively, these tests may be conducted more frequently because of their perceived value and affordability.

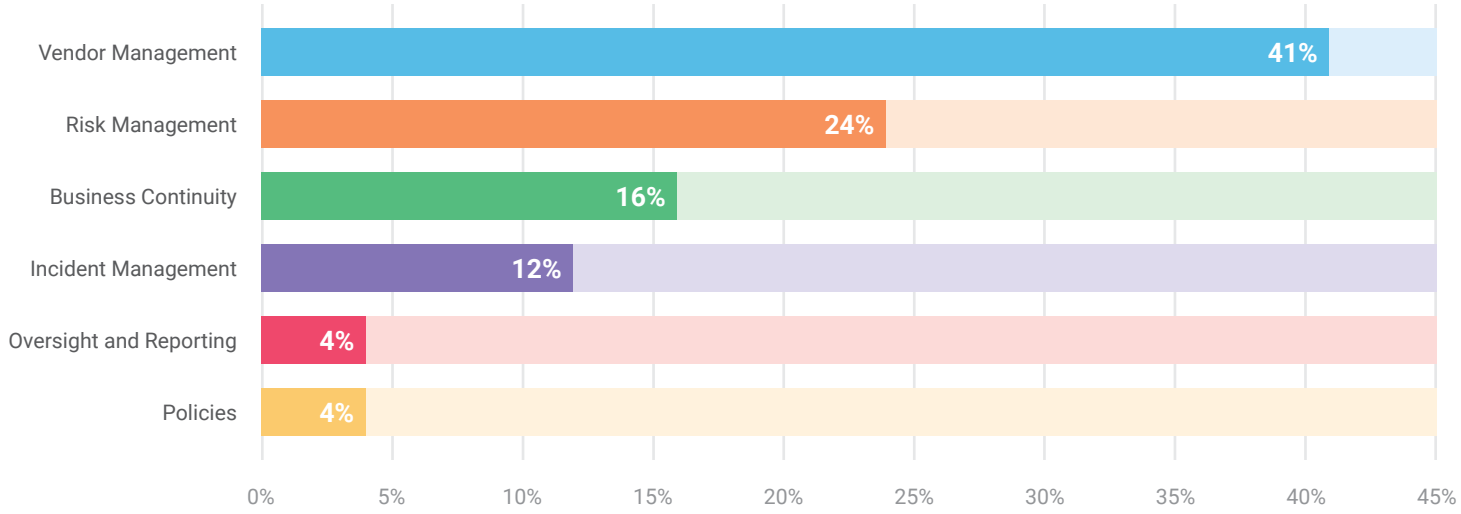
FREQUENCY OF ASSURANCE AND TESTING ACTIVITIES



Observation: Examiners are Focused on Third-Party Risk

When asked what examiners focused on during the most recent examination, 41% of participants cited vendor management (third-party risk) as a focus area.

FOCUS AREAS FROM RECENT EXAMS



Commentary

In light of recent high-profile third-party incidents, it is not surprising to see vendor management as the top area of interest for examiners. While bad actors continue to exploit third-party (and fourth-party) relationships as a way to gain access to an institution's data or network, it is important for financial institutions to ensure their vendor management programs are in tip-top shape.

Independent reviews are an important element of an effective third-party risk management program. To that end, we encourage financial institutions to:

- Include the institution's own vendor management practices in the scope of assurance and testing activities (e.g., audits, security assessments, exercises and tests, etc.).
- Ensure vendors have independent reviews performed on their own security environment through effective due diligence, contract negotiations, and ongoing monitoring.

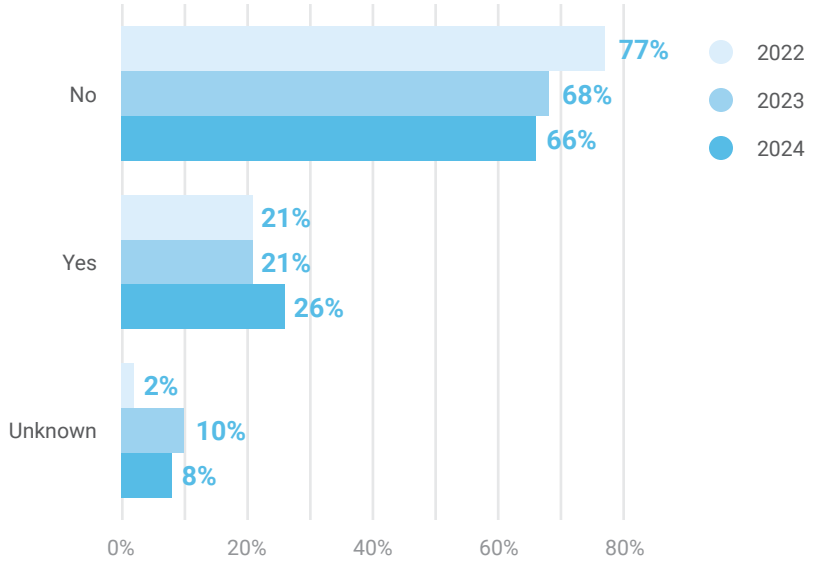
Learn more about third-party risk management with this free resource: Tandem.App/Vendor-Management-Workbook.

Vendor Management

Observation: Incidents Caused by Third-Party Vendors Increased

While most financial institutions did not report a major incident caused by a third-party vendor within the last year, 26% did have customer data lost or exposed due to a vendor incident, which is up slightly from the past two years. Additionally, 8% of respondents reported not knowing whether their data was breached as a result of a third-party incident.

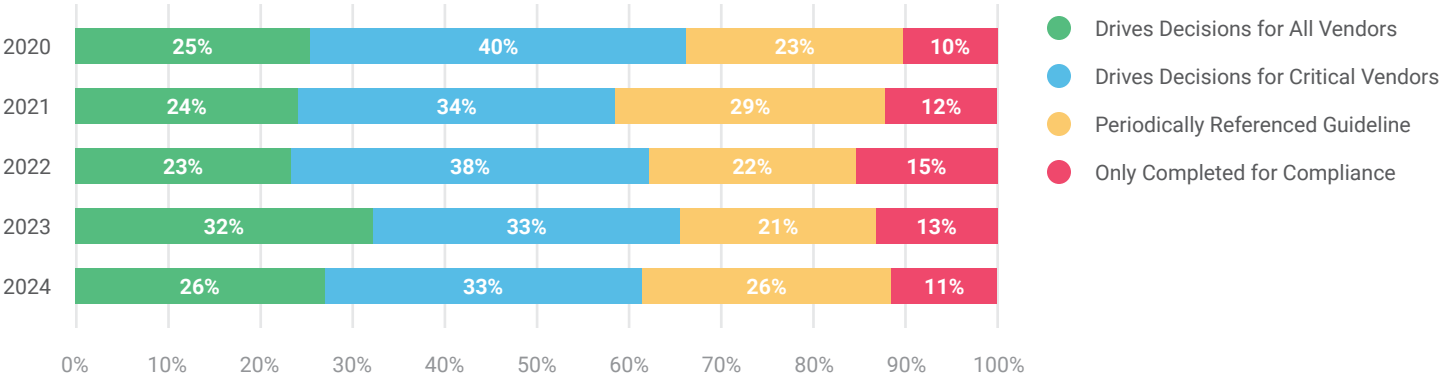
DATA BREACHES CAUSED BY VENDOR INCIDENTS



Diving Further

Twenty-six percent (26%) of institutions say their vendor management program is a driving decision factor for managing all vendors, and one-third (33%) use their vendor management program only when making decisions for critical vendors.

INSTITUTION PERSPECTIVE ON THE VENDOR MANAGEMENT PROGRAM



Commentary

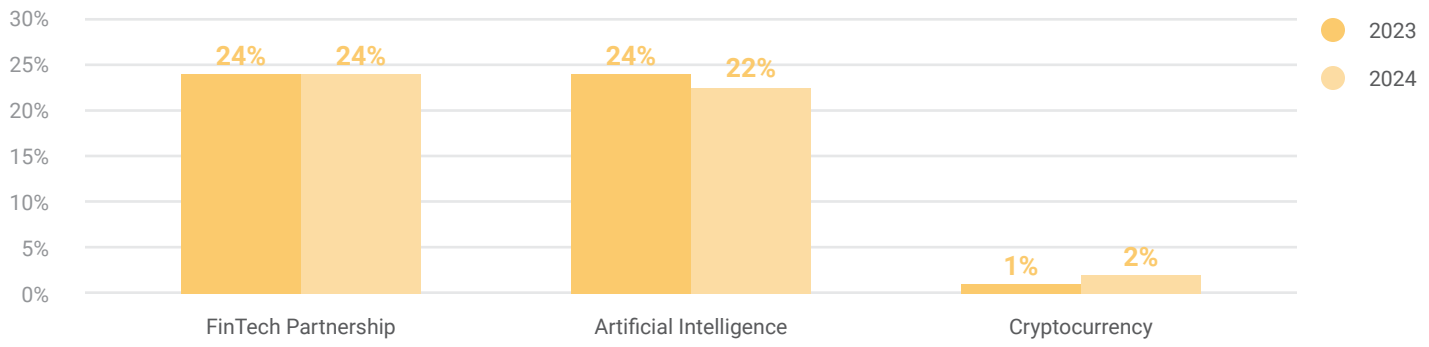
Financial institutions use their vendor management program across a scale of dependence, from using it solely for compliance purposes, to using it to drive decisions for all vendors. Across the past four years there has been no significant pattern of change about the way the program is viewed. Instead, there has been a steady distribution of about 25% using it for all vendors, 35% for critical vendors, 25% for periodical reference, and less than 15% for compliance only. This could simply reflect different styles of work and management, or it could reflect how well a program has been developed.

Emerging Technologies

Observation: Cautious Adoption of Emerging Technologies

While there is a slight change in financial institutions' perspective on emerging technologies, the adoption of artificial intelligence (AI), cryptocurrency, and fintech partnerships has stayed relatively the same from last year.

INSTITUTION ADOPTION OF EMERGING TECHNOLOGIES



Results include institutions who are currently using or actively researching the emerging technology.

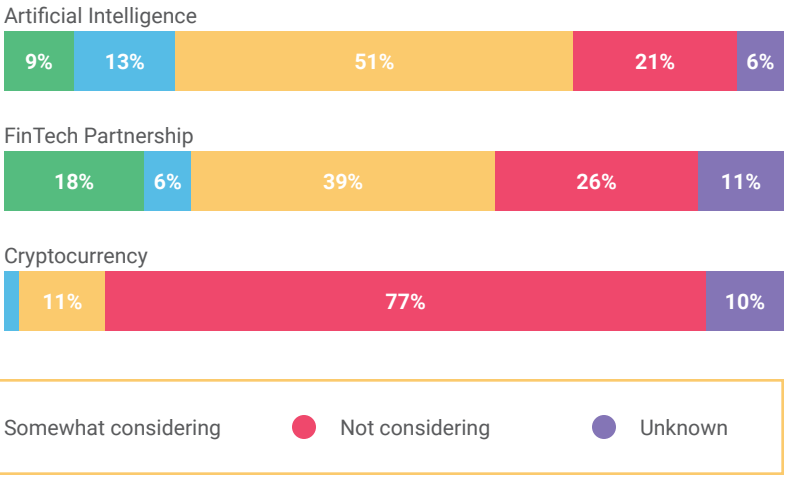
Diving Further

Institutions appear to be open to the idea of using AI technologies with 64% saying they are evaluating the benefits and risks.

Institutions seem more split on fintechs with 18% who have already adopted a fintech partnership, contrasting the 26% who are not interested.

An overwhelming majority of institutions are not pursuing cryptocurrencies with 77% saying they are not interested at all.

INTEREST IN EMERGING TECHNOLOGIES



Commentary

Balancing the need to mitigate risk while simultaneously maintaining a competitive edge with technology is not a new struggle to the financial institution industry. While there is no way to predict the future on which technologies to adopt, decision makers can set their organization's risk appetite and set strong vendor management practices to help guide their decisions when working with novel third-party technologies.

About the Authors

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

ALYSSA PUGH, CISM, CRISC
GRC Content Manager

Alyssa is a content creator with a passion for helping people navigate the challenges of governance, risk management, and compliance (GRC). With more than ten years of experience, Alyssa currently serves as the GRC Content Manager for Tandem, where she participates in the development of content and educational resources. In addition to her passion for technology, Alyssa is also a wife, graphic designer, and video game enthusiast.

BRIAN WHIPPLE
Marketing Manager

Brian has over ten 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 four children on their small farm.

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.

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.

SAVANNAH RICHARDSON, ITRF
Software Specialist

Savannah finds joy in education - striving to make information more accessible for teaching and sharing resources. She has a B.A. in Business Administration, an M.S. in Finance, and has earned the IT Risk Fundamentals ISACA certificate. Currently, Savannah works as a Software Specialist and is a part of the content team at Tandem. In her free time, Savannah collaborates with a dedicated group supporting small businesses through vendor markets, enjoys reading, and loves to travel.

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 a cybersecurity assessment using a streamlined framework. Report your growth 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 digital banking risk assessment. Offer education with expert-designed security awareness materials.

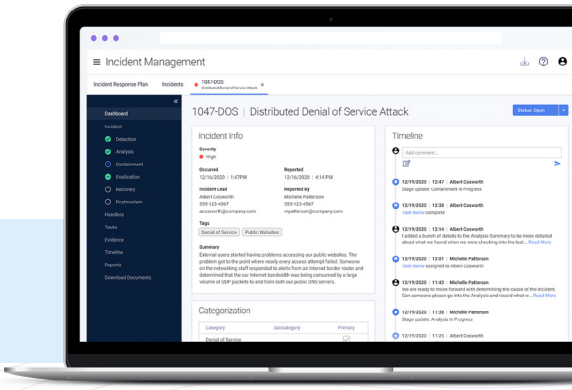
PHISHING
Teach your employees to recognize and avoid social engineering attacks by sending simulated phishing emails and enrolling users in training.

POLICIES
Create and maintain your policies in Tandem. Use our Information Security Policies set, tailored for you through a questionnaire.

RISK ASSESSMENT
Perform information security and asset-based risk assessments with our easy-to-follow format and available templates.

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

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



Tandem®

info@tandem.app
844-698-9800