The State of Cybersecurity in the Financial Institution Industry

2019 Survey Report

CoNetrix surveyed over 240 cybersecurity professionals working in the financial institution industry.

CoNetrix
A Family of Technology Companies

Contents

About This Report

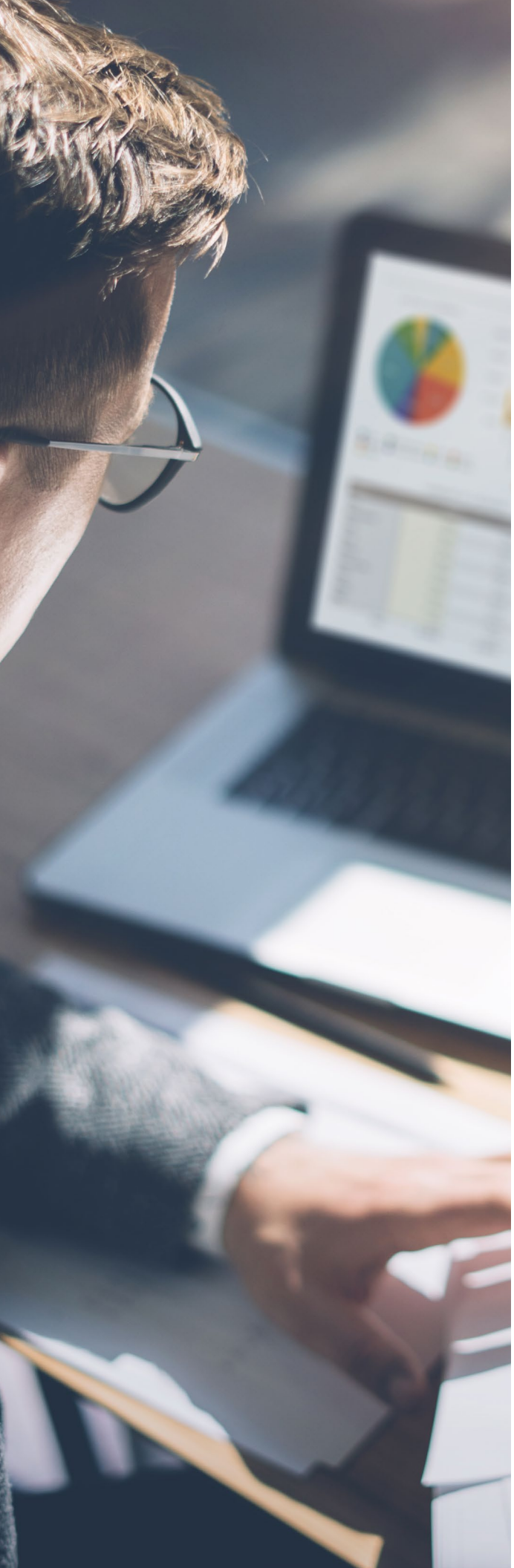
CoNetrix surveyed cybersecurity professionals working in the financial institution industry to discover:

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

The survey was conducted from November 1, 2018 to January 31, 2019 and generated 243 responses. All respondents are based in the United States.

Totals in this report may not equal 100%, due to participants not answering or not knowing the answer to specific questions. Percentages were rounded to the nearest whole number.

The survey was conducted by CoNetrix, LLC. For more information about CoNetrix, see page 20.



Demographics

Types of Institutions

Out of the 243 respondents who completed the survey, 82% of respondents worked for a bank at the time of the survey, 13% worked for a credit union, and the remaining worked for other financial institutions, such as mortgage companies or trust companies.

82% Banks

13% Credit Unions

4% Mortgage & Trust Companies

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

ISO Role Definition

For the survey, we defined cybersecurity as a subset of information security; therefore, the Cybersecurity Officer typically reports to an Information Security Officer, also known as the ISO. In this survey, we used ISO to represent Cybersecurity Officer. Results from surveyed institutions found:

74% have a designated Information Security Officer (ISO).

12% have an ISO department with multiple people.

12% have an ISO committee of individuals from various areas.

Asset Size of Institutions Surveyed

$0 - $100M	10%
$100M - $250M	21%
$250M - $500M	25%
$500M - $1B	21%
$1B - $10B	18%
> $10B	1%

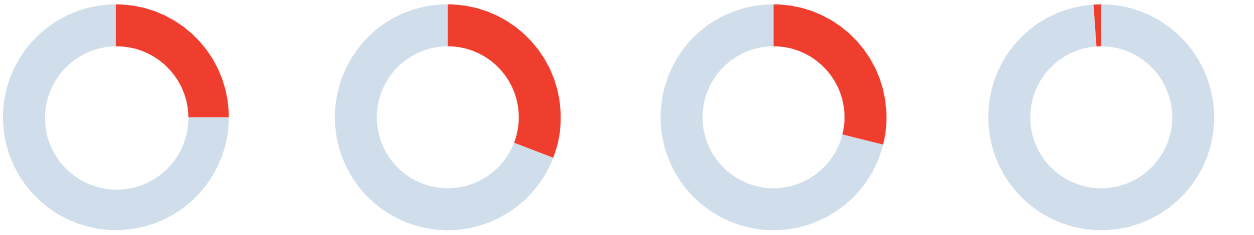
Board Oversight

The survey shows Board understanding and involvement in the financial institution's cybersecurity program is critical to the program's success. In addition, increased involvement from the Board ensures the program receives adequate funding and organization buy-in.

Frequency of Reporting

Significant Finding

The frequency with which cybersecurity reports were presented to the Board varied significantly with 25% of respondents saying they reported monthly, 31% quarterly, and 29% annually. Only 1% of respondents said they reported to the Board less than annually.



25% monthly **31% quarterly** **29% annually** **1% less than annually**

Diving Further

The frequency of reporting to the Board was not impacted by the existence of Board members with related experience.

Out of those who reported to the Board monthly, 44% were extremely confident or very confident in their Board's understanding of the institution's cybersecurity posture. Only 27% of those who reported annually felt the same level of confidence.

Lessons Learned

Currently, there is no standard within the industry defining the frequency an institution should report to the Board. According to the data, if the institution is looking to increase the level of confidence in the Board's understanding of the institution's cybersecurity posture, they should consider increasing the frequency with which they report to the Board.

Board Member Experience

Significant Finding

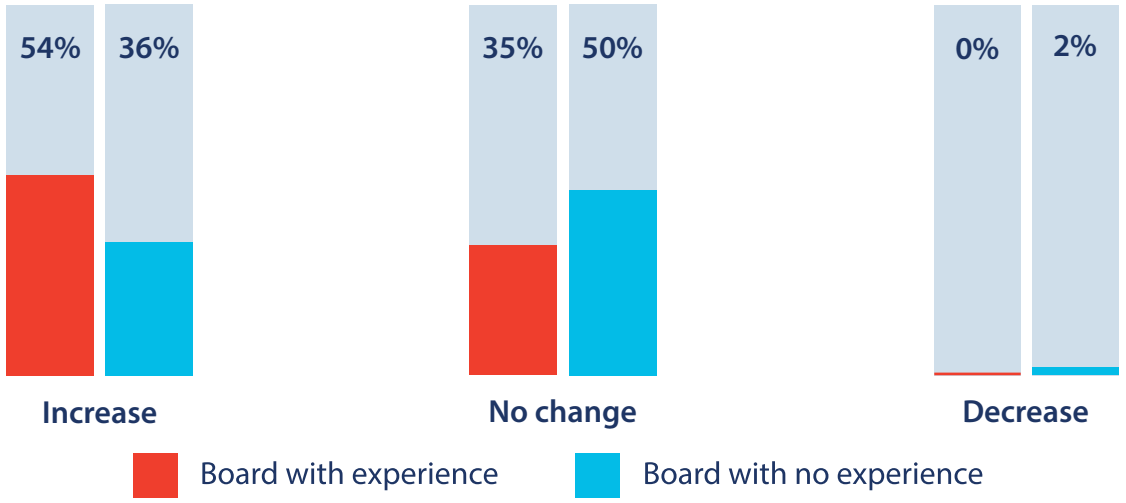
Findings show 61% of institutions do not have a Board member with professional cybersecurity or information technology (IT) experience.

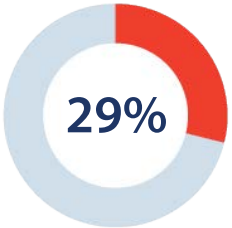
Diving Further

It is 22% more likely for the Board to set the institution's risk appetite statement if at least one of the Board members has professional experience in cybersecurity or IT.

From those who responded, 54% of institutions with a Board member who has relevant experience reported they plan to increase their cybersecurity budget in 2019. Conversely, when there is no Board member with relevant experience, only 36% of institutions plan to increase their budget in 2019. The data allows us to draw the conclusion: it is 18% more likely an institution's cybersecurity budget will increase in 2019 if the institution has a Board member with professional cybersecurity or IT experience.

Planned changes for 2019 cybersecurity budgets





Board members with cybersecurity or IT experience

Lessons Learned

With cybersecurity threats on the rise for financial institutions, we expected to find more financial institutions with a Board member having cybersecurity related experience. Only 29% of the total sample had a Board member with cybersecurity or IT experience, while 9% of the sample was unaware or unresponsive regarding Board member experience.

Adding a Board member with relevant experience will help drive key cybersecurity oversight controls such as development of a risk appetite statement and increases in the cybersecurity budget. According to the data, if an institution is looking to increase their security posture, they should consider adding a Board member with relevant experience.

ISO Management and Staffing

Staffing and managing employees in charge of the cybersecurity program is a common concern shared in the financial institution industry. The survey results give insight into how this role is being filled within institutions in the industry.

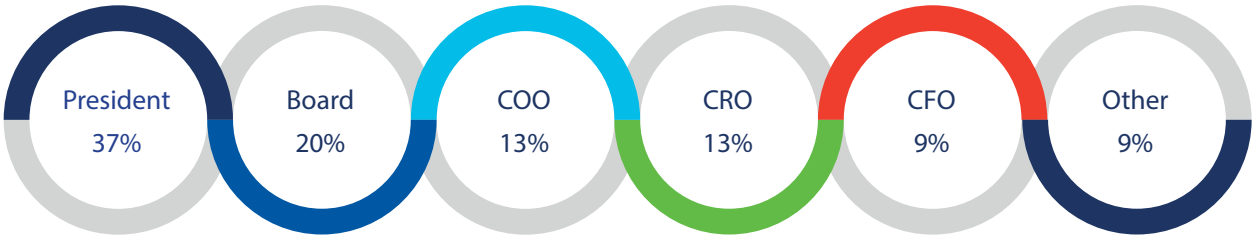
ISO Independence

Significant Finding

According to the data, 55% of ISOs are either the IT manager or report directly to the IT manager.

Diving Further

If the ISO does not report to the IT manager, the study shows the ISO reports to other members of the institution's senior management, including:



Lessons Learned

More than half of respondents state their ISO is either the institution's IT manager or reports directly to the IT manager. This a notable finding, since the FFIEC encourages independence between these two roles. According to the FFIEC IT Examination Handbook, Management booklet,

> "to ensure independence, the CISO should report directly to the board, a board committee, or senior management and not IT operations management."

Based on the FFIEC's expectations, it would be in the interest of each institution to ensure separation between the IT role and the cybersecurity role.

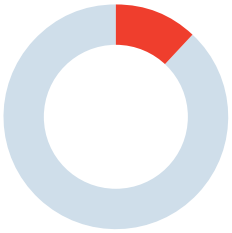
In-house vs. Third-party Management

Significant Finding

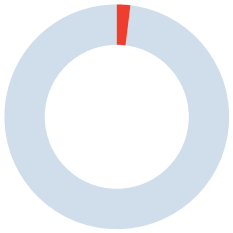
According to the data, 28% of respondents manage their cybersecurity program completely in-house, and 58% manage it in-house with support from third-parties. Another 12% of institutions said their program was managed by third-parties with support from inside the institution, and 2% outsourced their program completely.

28% completely in-house

58% support from third-parties



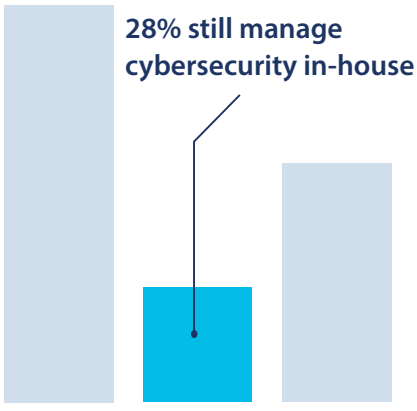
12% managed by third-parties



2% outsourced completely

Diving Further

Credit Unions are more likely to contract with a third-party provider to help manage their cybersecurity program (82%) compared to banks (71%). However, when looking exclusively at the sample of institutions that use a third-party provider, banks are more willing to give full control over to a third-party service provider.



Lessons Learned

While 28% of institutions are still managing their cybersecurity in-house, there is a growing trend in 2019 for institutions to turn to third-party service providers to partially or completely manage their cybersecurity programs. While the data shows that financial institutions are increasingly relying upon third-party service providers for management of the cybersecurity program, it is important for institutions to be mindful of the fact that the institution remains accountable for the program and its success.

Strategic Planning for Cybersecurity

Significant Finding

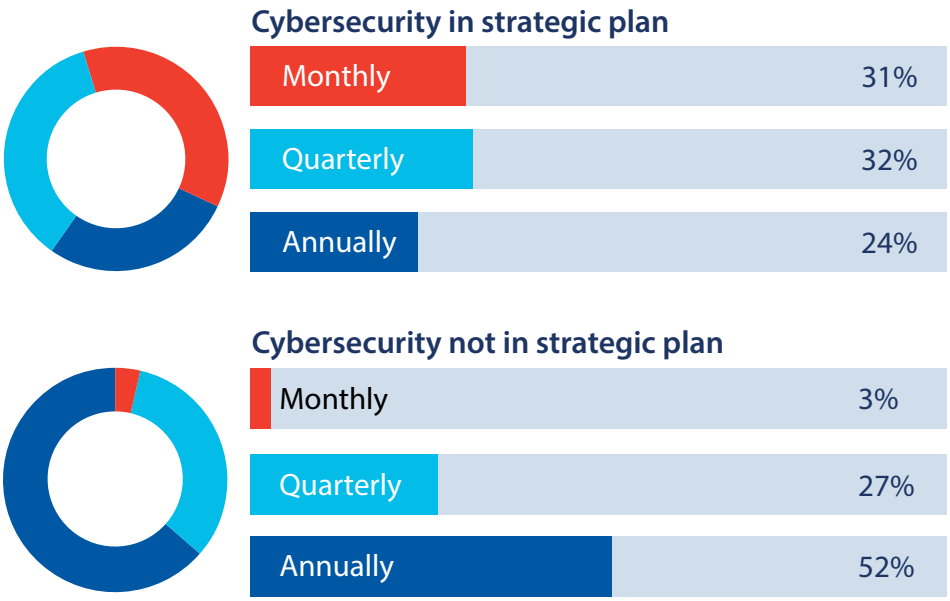
Of those who responded, 75% of institutions said cybersecurity is addressed in the institution's strategic plan.

Diving Further

Financial institutions who address cybersecurity in their strategic plan are likely to update their Board of Directors more frequently (monthly – 31%, quarterly – 32%, annually – 24%).

Conversely, institutions who do not address cybersecurity in their strategic plan are correlated with annual reports to the Board (monthly – 3%, quarterly – 27%, annually – 52%).

Frequency of reporting to the Board



Lessons Learned

The higher correlation between inclusion of cybersecurity in the strategic plan and frequent reports to the Board indicates the institution's Board members will be more aware of cybersecurity issues and the institution's cybersecurity posture.

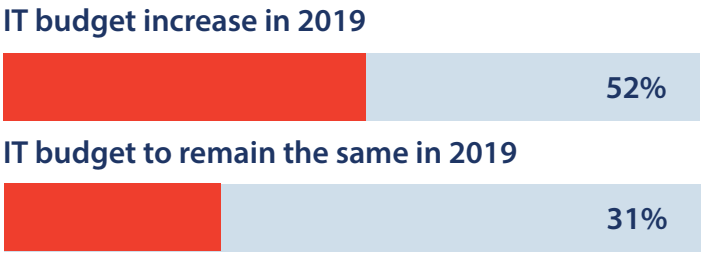
Budgeting

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

IT Budget for 2019

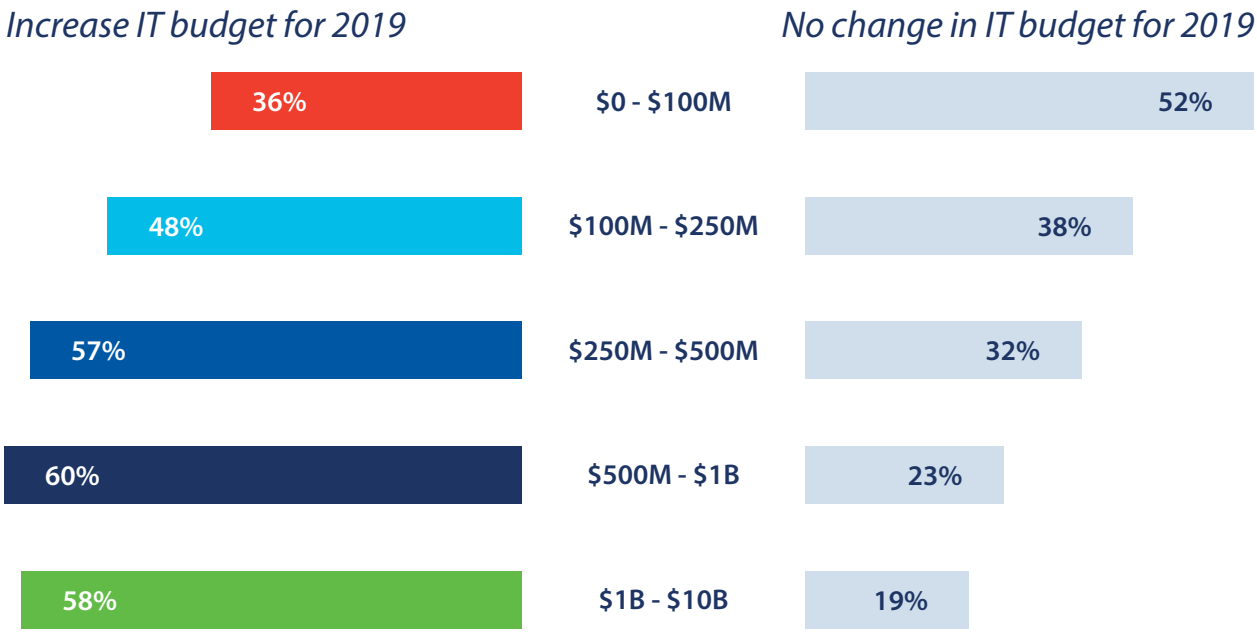
Significant Finding

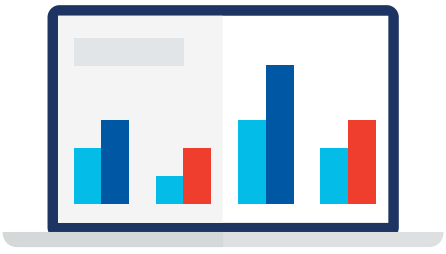
Roughly half (52%) of all respondents reported their IT budget for 2019 will exceed the allotted amount for 2018. Almost a third of respondents (31%) reported they will neither increase nor decrease their IT budget for 2019.



Diving Further

Institutions with a larger asset size are more likely to increase their IT budget in 2019.





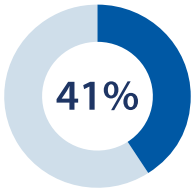
Lessons Learned

Budgets are continuing to increase in an effort to keep pace with advances in technology. Institutions under $100M in assets are likely investing in other assets for the institution. Once institutions reach $100M, there seems to be an increased focus in scaling up technology.

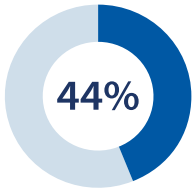
Cybersecurity Budget for 2019

Significant Finding

Findings show 41% of financial institutions will be increasing their cybersecurity budget in 2019; 44% will maintain the same budget.



Increase budget



Maintain same budget

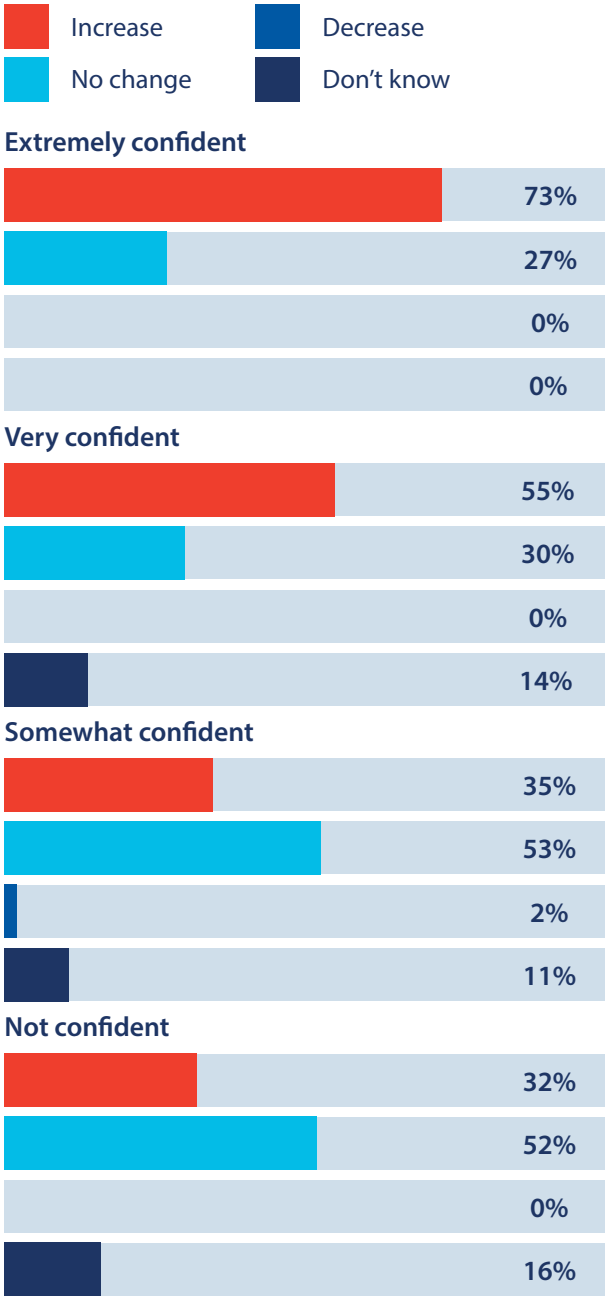
Diving Further

Institutions with a higher confidence in their Board's understanding of their cybersecurity posture results in a higher likelihood the budget will increase.

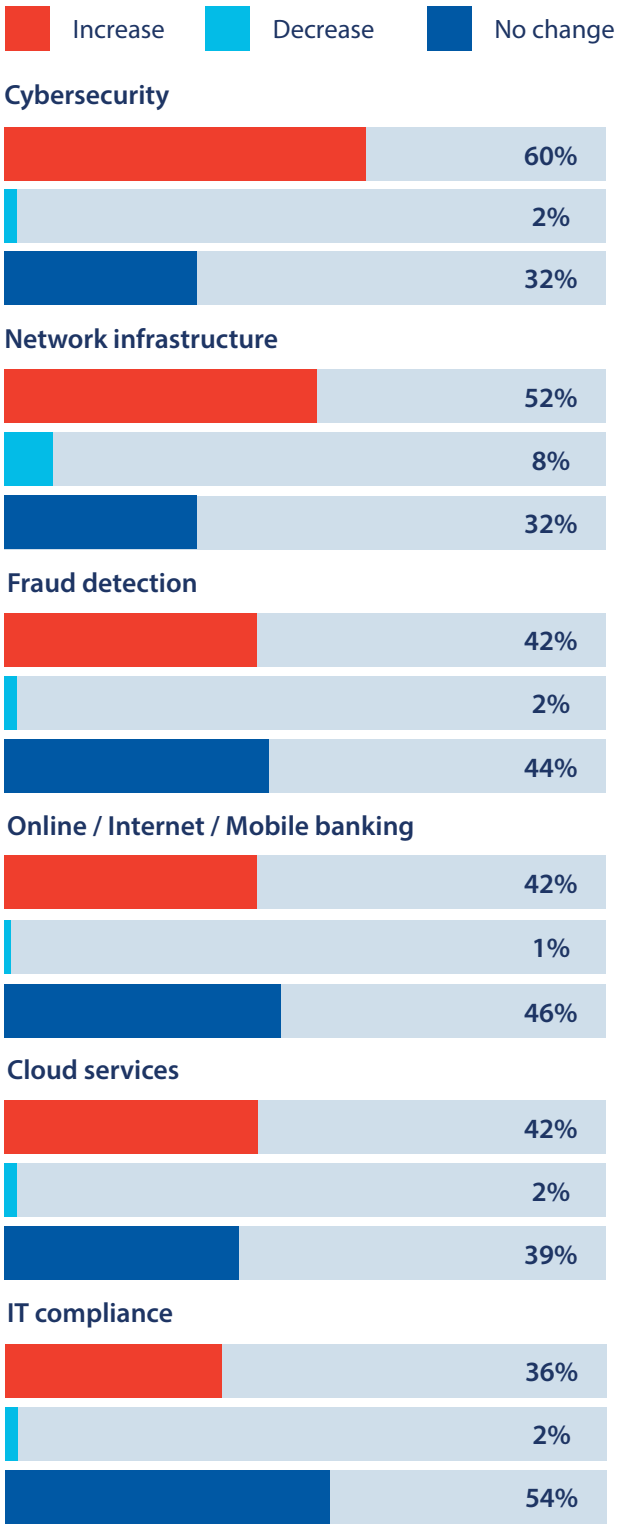
Lessons Learned

Like most institutions, budgets are allocated according to the priority set by the Board. If an institution wishes to increase their cybersecurity budget, the ISO should consider an effort to increase education for the Board of Directors.

Relation between planned cybersecurity budget changes and confidence in the Board.

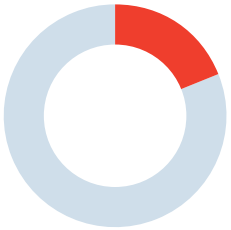


What kind of IT spending change do you expect to see at your institution over the next 12 months for each of the following areas?

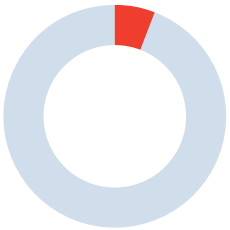


How is your cybersecurity budget allocated?

66% Shared budget with IT



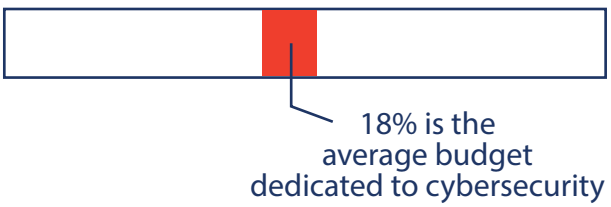
19% Shared budget with designated line item for cybersecurity



6% Dedicated budget for cybersecurity outside of the IT budget

>1% No money is spent on cybersecurity

From your institution's overall operations budget, what percentage is currently dedicated to cybersecurity?



Training

Proper training is considered to be an effective method for preventing incidents from occurring in a financial institution. The findings below give insight into how institutions are managing their training programs, and the impact the training makes.

Cybersecurity Awareness

Significant Finding

Most institutions (78%) believe their information security training directly reduces the risk of cybersecurity incidents.

Diving Further

The top three information security training activities used by financial institutions are phishing tests (88%), educational emails (77%), and video training (72%).

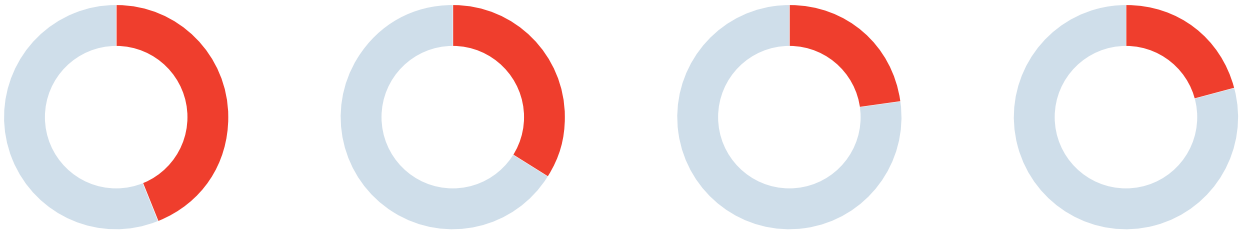
Training Activities

**Respondents were asked to choose all that apply*

On average, institution employees receive 6.8 hours of information security training per year.

For those institutions performing more than five hours of training, 53% feel their training is extremely or very effective. For those performing less than five hours, 44% feel their training is extremely or very effective.

When asked to choose an area of cybersecurity where their institution needs additional resources, the top choice (44%) was more resources for employee training.



44% Employee training

34% Network defense

23% Incident response planning

21% Infrastructure upgrades

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

Lessons Learned

Institutions are implementing various types of training for their employees in an effort to reduce risk. The use of different types of training and mediums has become a well adopted best practice in the industry. However, the data shows institutions desire better training programs.

Cybersecurity Tools & Frameworks

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

Use of the FFIEC CAT

Significant Finding

A large majority of institutions (80%) use the FFIEC Cybersecurity Assessment Tool as the primary method of evaluating the maturity of their cybersecurity program.

Why institutions use the FFIEC CAT

Diving Further

When asked why the organization used the FFIEC CAT, 45% of the participants "strongly agree" that they use the tool to meet regulatory requirements. Conversely, 20% of the participants "strongly agree" that they use the tool as a means to influence cybersecurity control decisions.

Lessons Learned

While the FFIEC CAT is widely adopted in the financial institution industry, the survey results show its prevalence is due to perceived regulatory expectations. However, in spite of its prevalence, financial institutions do not currently rely upon this tool as a method for supporting the institution's cybersecurity decisions.

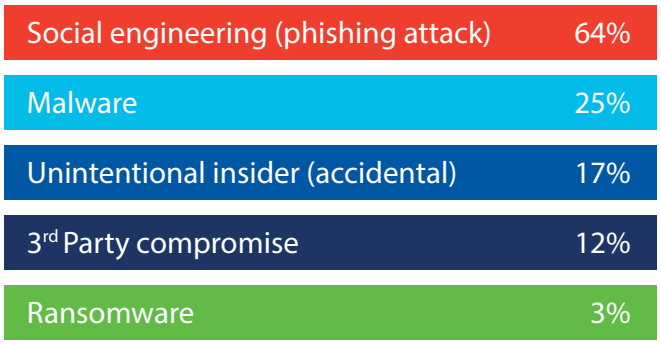
Incident Response

This section gives data on common information security incidents seen in financial institutions and gives insight into how those incidents are being managed by the parties responsible for cybersecurity.

Threats to Financial Institutions

Significant Finding

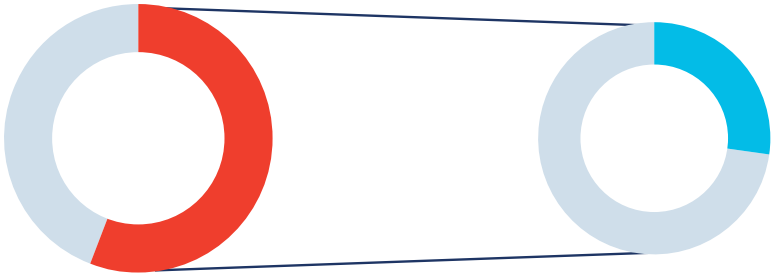
The top three security incidents experienced by institutions in 2018 were social engineering (phishing attacks), malware, and accidental security breach by an employee.



**Respondents were asked to choose all that apply*

Diving Further

Of the institutions who had an incident in 2018, an average of 56% reported to the Board of Directors when they had an incident. From this same group, 28% of institutions reported every single incident in 2018 to the Board.



56% reported to the Board when they had an incident

28% reported every incident in 2018 to the Board

Lessons Learned

According to the data, threats resulting from employee compromise remain a significant source of security breaches at a financial institution. However, institutions do not find these security incidents significant enough to report to the Board, as a little more than a quarter of respondents said they report all incidents to the Board. When the Board is not informed of the frequency or severity with which the institution experiences security incidents, it may be more difficult to acquire necessary resources to educate and prevent these threats from occurring in the future.

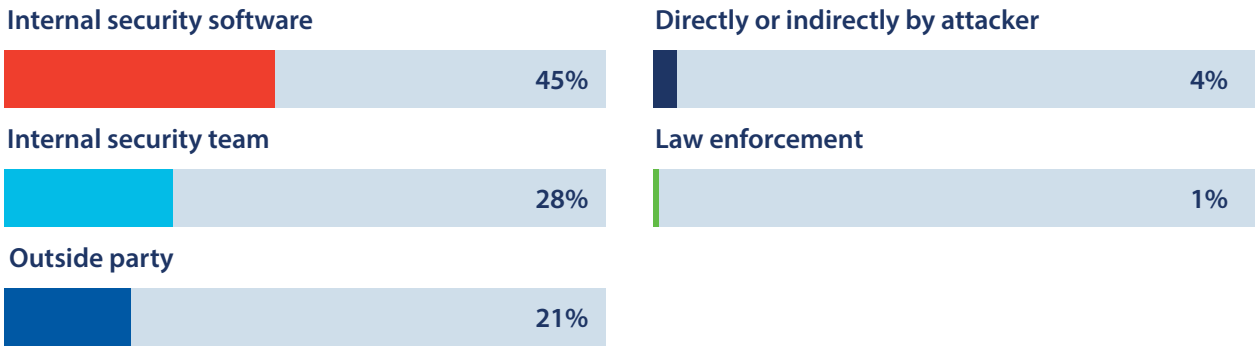
Incident Discovery

Significant Finding

According to the data, 63% of incidents were discovered in less than 24 hours, and 61% of respondents found their response to be effective following incident discovery.

Diving Further

The top ways institutions discover significant incidents occurring in their organization are through internal security software (IDS/IPS), internal security team (manual review of logs or anomalies), or an outside party (customer or vendor). Most institutions did not discover an incident directly from the attacker or through law enforcement.



Lessons Learned

According to the data, incidents were discovered via multiple methods, including almost equal discovery through both technical and administrative methods. This finding emphasizes the importance of a layered security program. If an institution is looking to improve discovery of incidents, they should consider improving use of technical tools, as well as improving employee education.

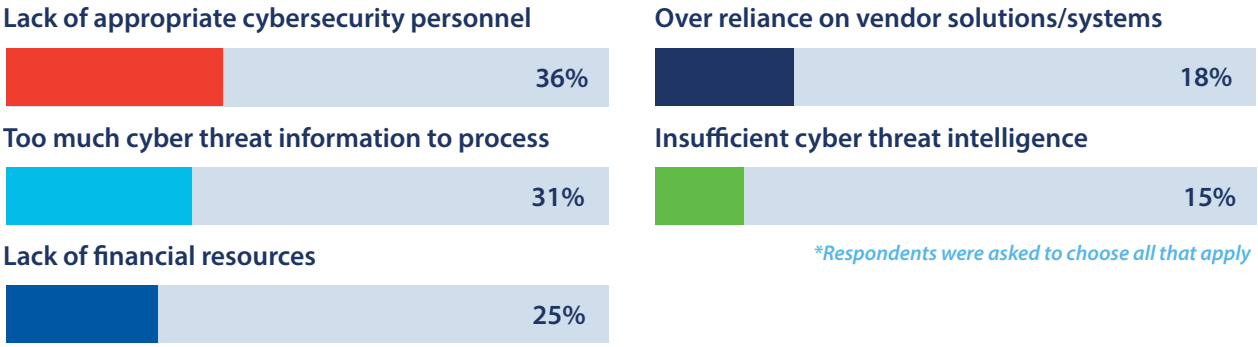
Evaluating the Response Plan

Significant Finding

Only 49% of respondents made changes to improve their incident response plan following an incident. When looking specifically at respondents who did not feel their incident response was very or extremely effective, only 43% said they made changes to their incident response plan.

Diving Further

The biggest barrier to mitigating and remediating cybersecurity incidents was a "lack of appropriate cybersecurity personnel" (36%). The second highest chosen was "too much cyber threat information to adequately process" (31%).



**Respondents were asked to choose all that apply*

Lessons Learned

Institutions are discovering threats quickly with the help of software and monitoring. While 61% feel they are responding correctly to incidents, there is room for improvement for many. However, when it comes to actually improving processes and systems, less than half of institutions actually take the time to improve. This inaction is largely due to personnel constraints. Institutions should consider what personnel requirements are needed to effectively manage cybersecurity.

Assurance and Testing

Implementing an adequate amount of internal cybersecurity tests is the key to being prepared for attackers. The data shows financial institutions are implementing many of the best practices known in the cybersecurity industry.

Frequency of Testing

Significant Finding

Overall, institutions plan on increasing most testing types in 2019. The testing activity institutions plan to increase the most is social engineering tests.

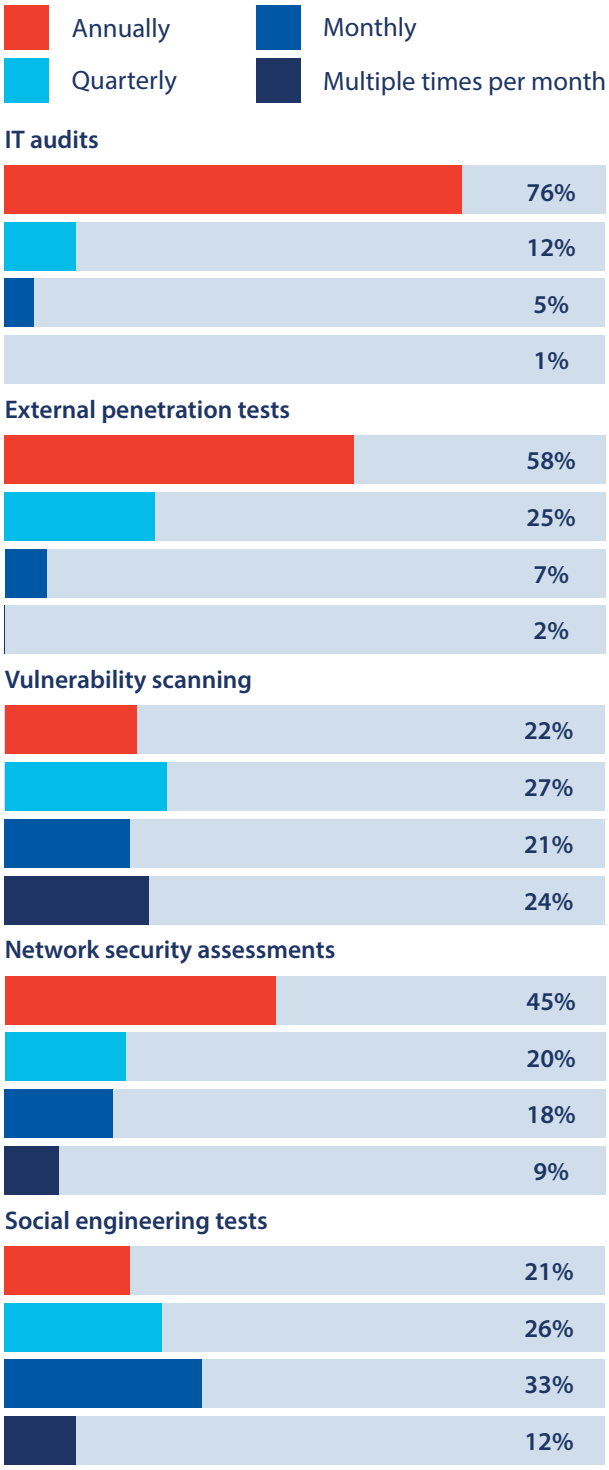
Diving Further

Institutions plan on performing vulnerability scans the most with 45% planning on performing scans one or more times per month. Institutions plan on doing incident response training and IT audits the least, with a large majority doing tests annually or less than annually.

Lessons Learned

Institutions are ambitiously trying to add more testing to their schedules. Not surprisingly, the testing activities that are expensive, time consuming, and generally outsourced are performed less frequently. Tests which are easier to implement are conducted at a higher frequency.

How frequently do you plan to conduct each of the following types of assurance and testing activities in 2019?



Testing Activities

Significant Finding

The most valued testing activities when trying to increase security posture are:

Vulnerability scans	70%
External penetration tests	64%
IT audits	64%
Network or security assessments	61%
Social engineering tests	60%

**Respondents were asked to choose all that apply*

Diving Further

Even though institutions feel external penetration tests and IT audits are highly valuable, institutions are increasing frequency of these services marginally in 2019.

Lessons Learned

External testing, scans, and audits provide the most value to institutions. According to the data, if an institution is looking to improve their security posture, they should consider ways to increase the frequency and variety in which their systems can be tested.

About CoNetrix

Who We Are

CoNetrix is a full service computer networking, security and compliance firm built on the principles of integrity, innovation, and initiative. CoNetrix has roots dating back to 1977, when it was founded in Lubbock, Texas. We now serve over 1,400 customers across the US, in all 50 states.

Who We Serve

We specifically serve financial institutions (banks, savings associations, credit unions, trust companies, etc.), as well as enterprises requiring a high level of security in their operations.

How We Serve

CoNetrix provides a variety of technology and security solutions including network consulting, security vulnerability testing, IT audits, risk management, compliance solutions, and managed services. Security is designed into all of our offerings, from our software to our consulting services.

Our employees are diligent in preserving the highest caliber of integrity, unassailable professional conduct, and personal conduct that is beyond reproach. Our entire business is based on trust that we will deliver on expectations, agreements, and promises.

Our Mission

The mission of CoNetrix is to provide an environment that inspires integrity, wisdom, ambition, and team spirit so each of the CoNetrix companies are equipped and enabled to solve challenging problems with the use of technology in innovative ways.

Aspire™ secure • reliable • cloud

CoNetrix Technology

Tandem™

CoNetrix Security

BOOST™ consulting

CoNetrix
A Family of Technology Companies

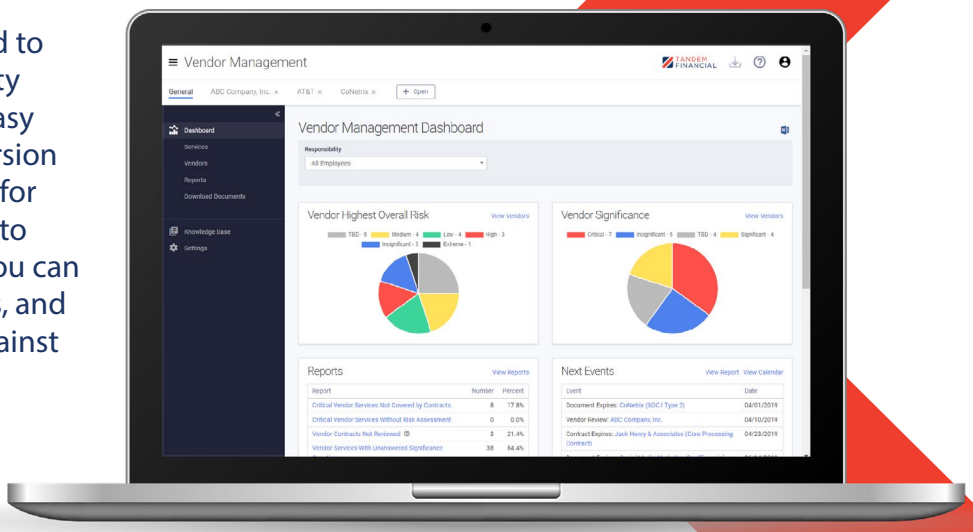
800-356-6568 | info@conetrix.com | conetrix.com

Benchmark your cybersecurity preparedness in Tandem

GET STARTED

The agencies agree: you need to benchmark your cybersecurity program. Tandem makes it easy for you with an electronic version of the FFIEC's CAT (and ACET for credit unions)! By upgrading to Tandem Cybersecurity Pro, you can copy assessments, see trends, and benchmark your maturity against similar institutions.

Make your life easier with Tandem.



CoNetrix is the creator of Tandem, a simple yet robust online platform for managing security and compliance. ISO support and other services are available through Boost Consulting, a division of CoNetrix Security. Additional Tandem modules include:

- *Vendor Management*
- *Business Continuity Planning*
- *Risk Assessments*
- *Information Security Policies*
- *Phishing*
- *Audit Management*