2023 Cyber Risk Benchmarking Report: How Financial Institutions Play Defense and Offense

Financial institutions (FIs) operate in an environment of constant change, and therefore constant risk. Expanded digital offerings, upgraded technology at existing branches or opening new branches are all reasons to celebrate change, but if FIs aren't careful, these advancements open the door open to even more risk. Cyber criminals are always on the watch, seeking out weaknesses that enable them to penetrate your defenses. Banks and credit unions need to measure the implications that changes have on risk in whens, not ifs – because financial loss, business continuity, reputation and community trust are at stake.

While it's impossible to completely eliminate cyber risk, we do have good news to share. Leading FIs have proven that a more proactive approach improves their ability to avoid and mitigate risk, staying ahead of threat actors. They effectively address cyber risk from two positions:

Defense – establish a foundation that protects against current threats and prevents them from gaining a foothold.

Offense – proactively identify new threats as they arise and develop responses to them, better mitigating and avoiding risk.

Read on to discover top insights from this year's Cyber Risk Benchmarking Report.

DEFENSESTORM
THE BEST OFFENSE.

Table of Contents

Introduction

The dynamic nature of cyber risk means that there is more to consider than just cybersecurity. To safeguard sensitive information, enable business continuity, support financial performance, and ensure community trust, an effective cyber risk program must address five key areas:

01 Business Implications

The strategies put in place to support the growth and profitability of your institution create constant change and can have short and long-term ramifications for cyber risk. Similar to how you manage other risks, they are best addressed proactively before an issue arises.

02 Assessing Risk

Continuous assessment of risks is essential to the success of a cyber program. FIs can't manage the risks they don't know about. They cannot apply the proper system of controls if they haven't properly assessed identified risks. And they can't ensure the risks are being properly managed if they aren't monitoring the level of risk and the effectiveness of controls on an ongoing basis.

03 Monitoring and Governance

Proper oversight enables the proactive identification of internal and external threats in a manner that allows for timely response and remediation. Ongoing monitoring for adherence to internal policy and process, industry control frameworks and regulatory requirements is an essential piece of a FI's cybersecurity program.

04 Threat Management

How well an FI is positioned to predict, prevent, and respond to ever-evolving threats is critical. Effective cybersecurity is a function of technology, talent, culture, training, testing and oversight. A well-positioned institution defends itself with timely and effective reactions, while also employing a strong offensive front against new and emerging threats to better manage risk.

05 Fraud Practices

As fraudsters advance their tactics, you must also advance your techniques for detection and prevention. A strong offense includes systems and technologies that monitor against cyber fraud attack vectors. An offensive stance paired with defensive strategies, such as transaction monitoring, protects FIs and their customers or members from fraud.

Based on their responses, participants were grouped into four maturity levels to benchmark their progress in addressing cyber risk:

STARTING 20%
Below-average FIs, still mapping out their cyber risk defenses and offenses, with potential for significant growth

DEVELOPING 53%
Average FIs, with some defensive and offensive capabilities in place, but still refining their strategy

OPTIMIZING 24%
Above-average FIs, with established defensive and offensive capabilities, and minor fine-tuning still required

LEADING 3%
Top FIs, with well-established best practices and significant defensive and offensive capabilities

Only **1 in 4 respondents** were considered above average in their efforts to build a cyber risk strategy, leaving plenty of room for improvement. Research shows the more mature an FI, the greater the likelihood it has adopted a more offensive stance to help ward off cyber risk.

This whitepaper takes a closer look at several defense and offense techniques, the breakdown of where respondents scored on each and what their answers mean for the state of cyber risk for FIs. In general, we saw that while FIs know there's work to be done, most are taking proactive steps to become stronger in both defense and offense.

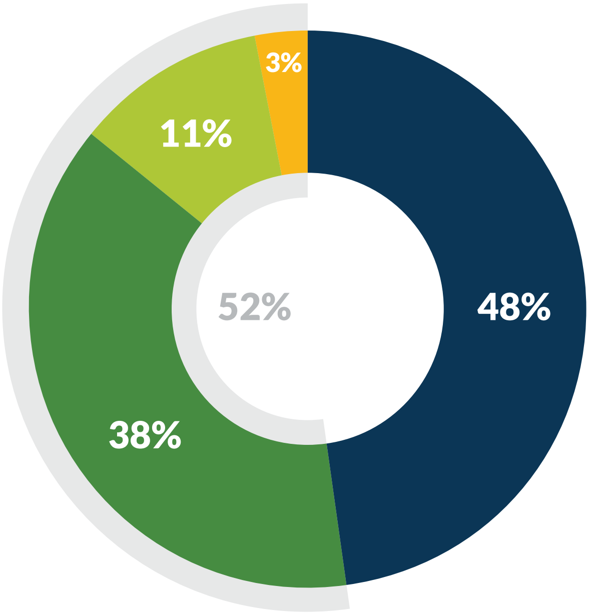
DEFENSE:
How Secure is Your Vault?

A strong cyber risk defense is crucial for financial institutions to protect sensitive client data and confidential business information. When data that includes Nonpublic Personal Information (NPI) falls in the wrong hands, the result can be disastrous to FIs and their customers alike. A data breach resulting from a cyberattack can result in significant monetary losses and threaten strategic objectives; additionally, reputations and business continuity are put at significant risk.

A sound cyber risk defensive strategy – a blend of planning, practice and pivoting the game plan to resist the opponent – can give FIs peace of mind by protecting financial networks and the information contained within. Such a program effectively detects risky events and potential threats and responds using a well-designed cyber risk playbook. It prevents the attacker from a successful compromise.

Reinforcements needed

Defending networks is an ongoing process, but one that can be better implemented and managed. More than half of the respondents (**52%**) admitted designing and implementing a program that adequately manages risk is difficult and indicated their program needs a lot of work.



Do you feel like you are adequately managing information security and cyber risks?

- 🟦 Yes, we have an excellent program and do a good job staying on top of new and emerging risks
- 🟩 Mostly, we have a solid program but staying on top of new and emerging risks is difficult
- 🟩 Somewhat, but recognize that our program needs some work
- 🟨 Not even close, our program needs a lot of work

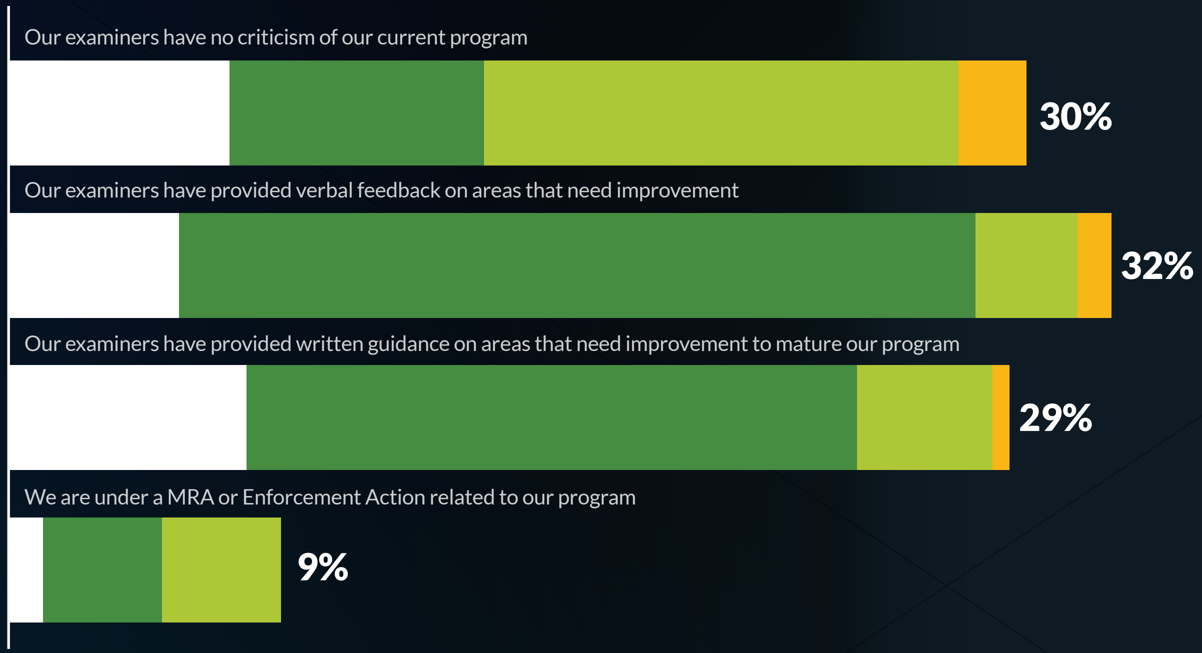
Examiners tend to agree. **70%** of respondents said they had some sort of examiner criticism during their most recent exam. This indicates cyber and operational risk are an ongoing supervisory priority and area of focus. **8%** are under a matter requiring attention (MRA) or enforcement action, while another **29%** have received written criticisms and recommendations for improvement within the exam report. Regulatory findings cause headaches across the maturity spectrum – even above average FIs struggle to get to the other side of an exam without criticism or recommendations, with **nearly 1 in 3** respondents noting they've received written guidance or are under an MRA or enforcement action.

Unfortunately, respondents are often working on borrowed time to make these recommended adjustments, since attacks are now a matter of *when*, not *if*. And information security departments that run lean face an even greater challenge keeping up.

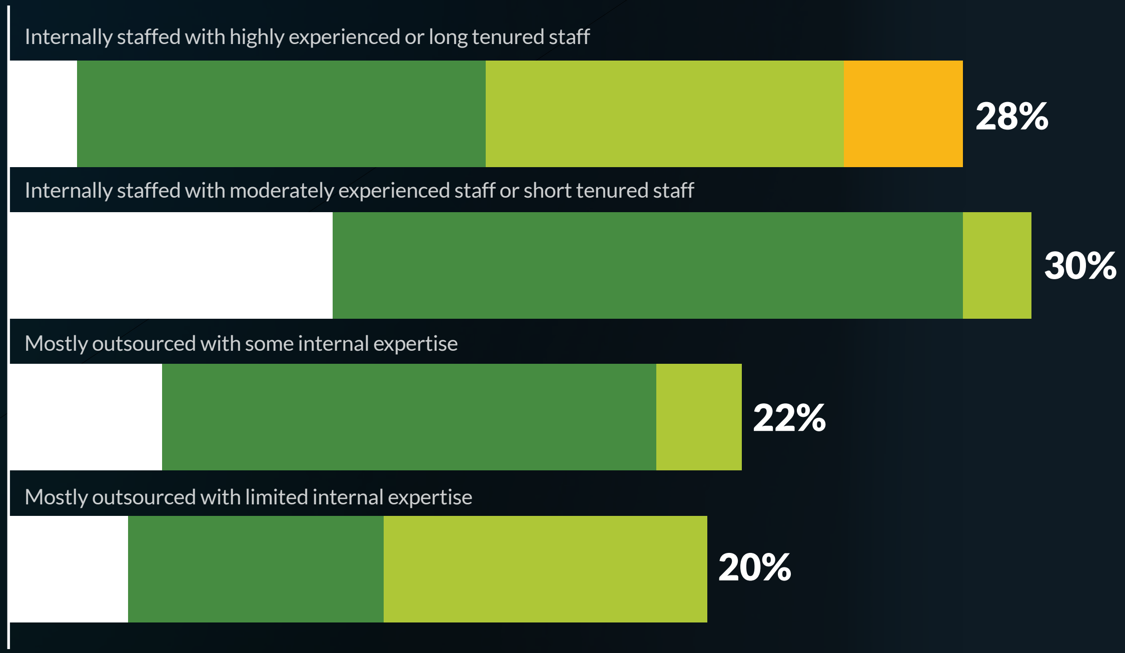
Although adding in-house security experts is worth evaluating – given the value of having internal experts who fully understand the unique configuration of your institution – it can also be quite expensive. Almost half of respondents said they rely on outside talent to supplement their team, and **even 1 in 3** FIs scoring above average mostly outsource their information security talent.

STARTING DEVELOPING OPTIMIZING LEADING

Select the most accurate statement:



Which best describes your cybersecurity talent?



Building a digital fortress

Organizations don't have to defend their FIs alone. New technologies such as security information and event management (SIEM), intrusion detection systems/intrusion prevention systems (IDS/IPS) and endpoint detection and response (EDR) solutions give FIs avenues to better defend against coming attacks.

Still, more than half of survey respondents are unable to get the full benefit from adopting these solutions. Whether they lack the talent to implement and use technology, focus their budget elsewhere or keep an "if it's not broken, don't fix it" mindset, they remain at risk for significant damage from a cyberattack by sticking with outdated or manual solutions.

Utilization is an issue with existing technology, with **57%** of respondents admitting they could benefit from additional or better technology. They use their existing technology only to a moderate or limited degree, or if at all, indicating issues with functionality, usability and ability to address the key issues.

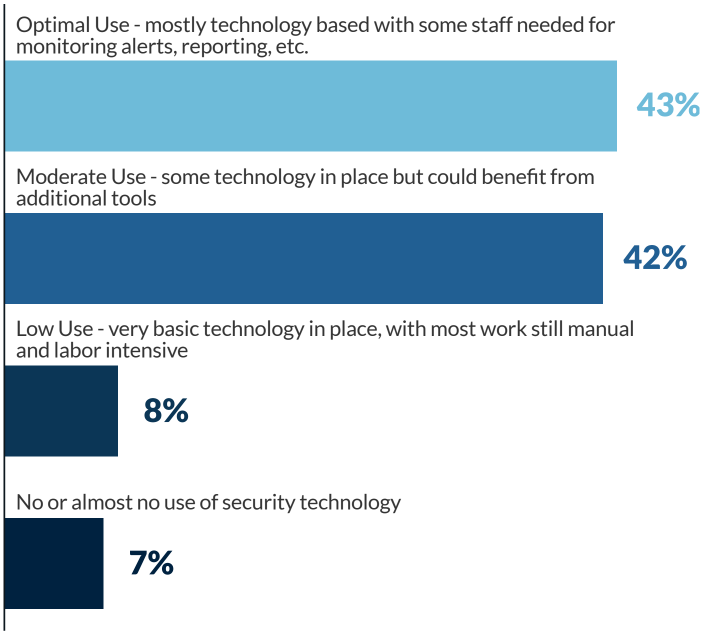
An equal number of FIs acknowledge they struggle to master key metric monitoring and reporting around information security – challenges that could be addressed with better technology. When FIs fail to monitor performance and risk metrics, they can neither gauge the success of their defenses nor employ their offensive strategy in a timely manner. That's concerning, especially when **nearly 1 in 5** FIs report no access to real-time cyber risk data.

This lack of automation in cyber risk technologies suggests a continued reliance on manual strategies for governance and compliance activities. This translates to time, and time is money. By leveraging integrations and automating activities, FIs can effectively govern their programs while saving time for critical talent.

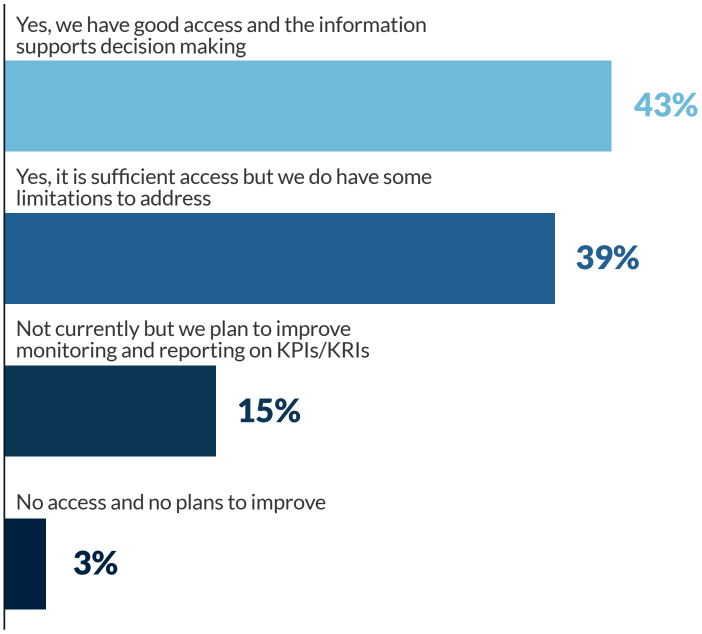
The time to improve governance and compliance with automation is now. Two-thirds (**67%**) of respondents say they are working on doing so or understand they should. However, nearly **23%** have automated less than half of their workflows or have few (or no) automated workflows, indicating there is plenty of work to be done.

In sum, a strong cyber risk program relies on a solid, resilient defense. Far from reactive, however, shoring up defenses requires FIs to create a viable cyber risk management plan that can respond effectively and quickly when an attack occurs. A robust mix of internal expertise, outside allies and advanced technology can help make a strong cyber risk program even more resilient.

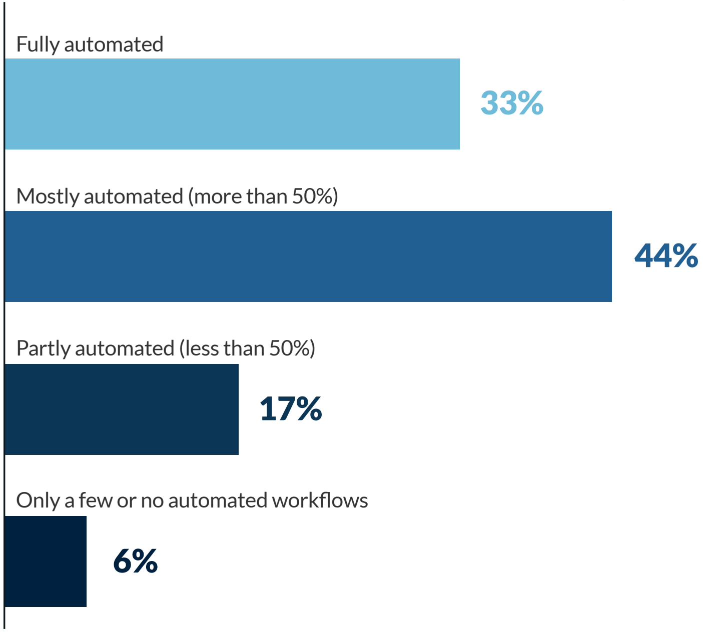
To what extent do you use technology such as SIEM, IDS/IPS, EDR,etc?



Do you have comprehensive access to real-time data, KPIs, and KRIs related to your security programs?



To what extent are governance and compliance activities automated?



OFFENSE: Stay One Step Ahead

For many financial institutions, it can seem like cyber threats are evolving at an exasperating pace. Threat actors never sleep, finding new vulnerabilities every day, making it an ongoing struggle to keep up with the increase in threats. As we noted in the last section, that's why FIs need to have a robust defense framework in place.

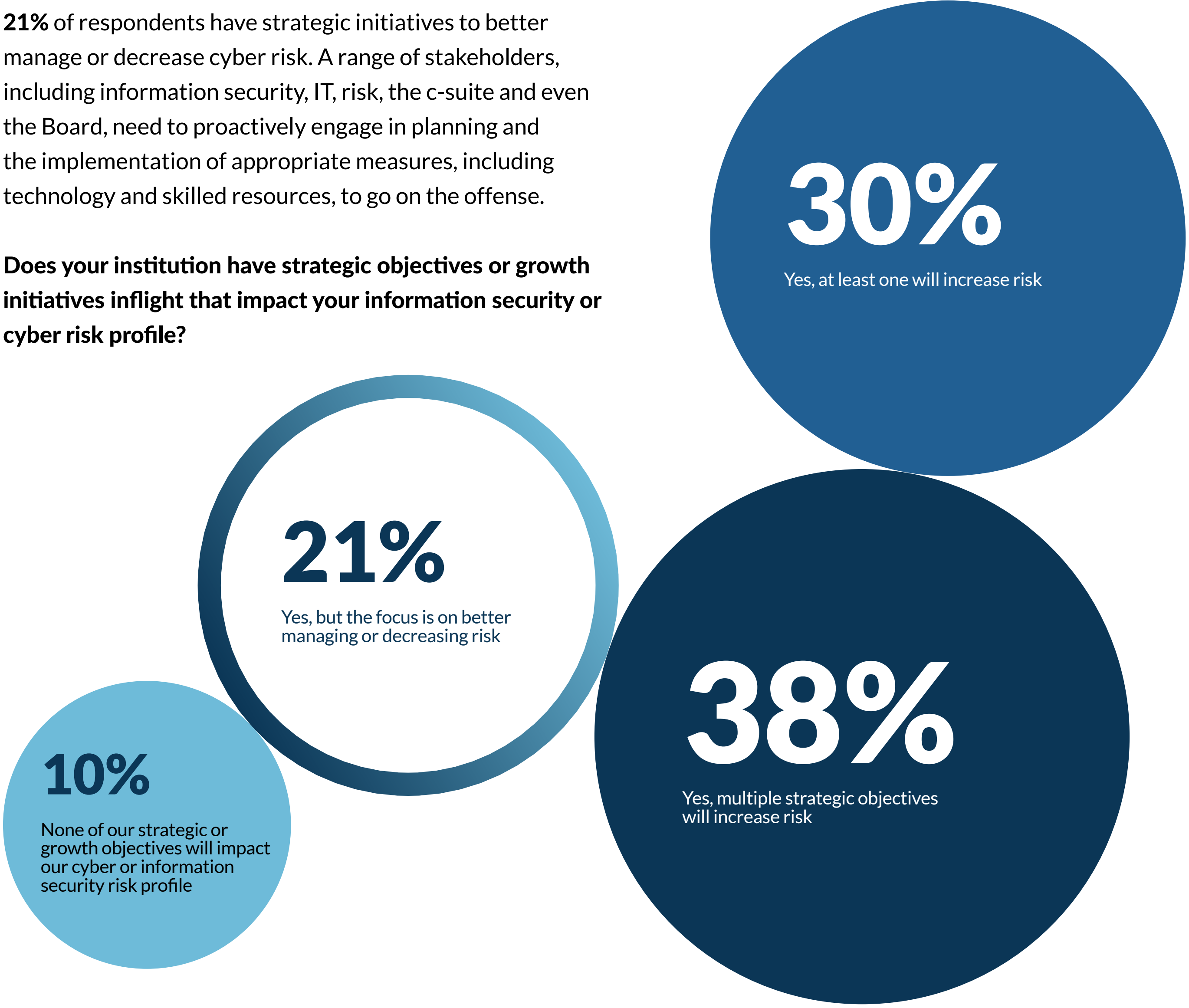
A strong offense enables a financial institution to pivot and address cybercrime by identifying new and emerging threats promptly. With today's detection and compliance technologies, FIs can gain an upper hand on criminals – using artificial intelligence-driven tools that continually monitor the threat landscape, helping them continuously strengthen their offensive strategy. Taking this proactive approach to cybercrime will become more important as banking services become increasingly interconnected, adding to an FIs potential attack surfaces. Manual monitoring and defense of every surface doesn't scale.

Understanding – and mitigating – risk

Financial institutions, like any business, are always changing. On a yearly basis, they typically have multiple strategic or growth initiatives in flight. They must ensure these strategies are analyzed for the implications they have for cyber risk. Growing your internet presence does bring new business, but it also elicits new threats. Identifying and proactively solving for these newly introduced risks set up the FI up for success in achieving its strategic objectives.

More than two-thirds of survey respondents acknowledge having strategic initiatives that will increase security or cyber risk. Acknowledgement isn't enough, however. Only **21%** of respondents have strategic initiatives to better manage or decrease cyber risk. A range of stakeholders, including information security, IT, risk, the c-suite and even the Board, need to proactively engage in planning and the implementation of appropriate measures, including technology and skilled resources, to go on the offense.

Does your institution have strategic objectives or growth initiatives inflight that impact your information security or cyber risk profile?

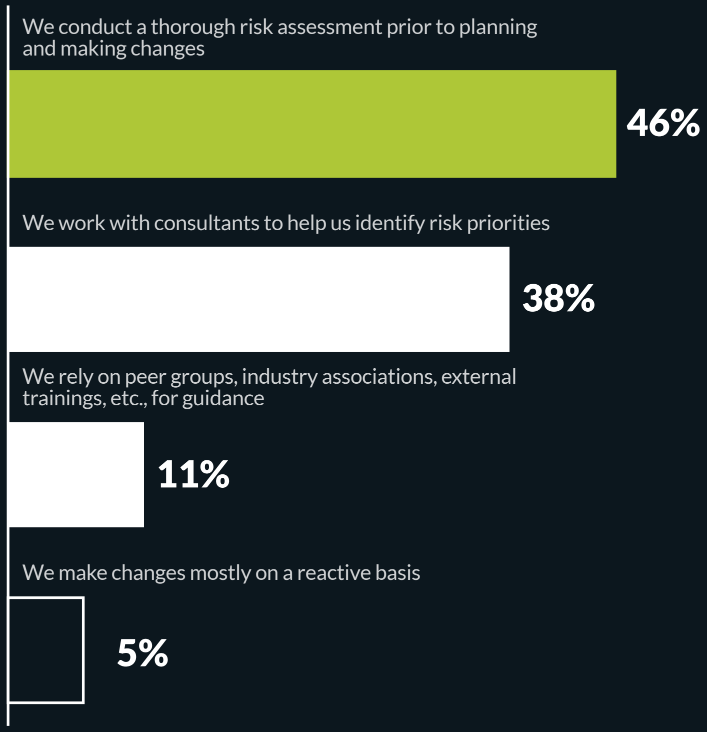


A successful offense requires detailed planning, design and execution of the cyber risk playbook, which is continuously reviewed and tested. FIs can leverage internal or external resources to assist in updating their offensive playbook. About **46%** of respondents conduct thorough in-house risk assessments ahead of planning and updating their program, while about **49%** leverage external resources such as consultants and peer groups.

Overall, offensive planning is strong with all but **5%** taking a proactive approach to advance their playbook.

These findings are in line with respondents' broader views of their offensive stance to identify and mitigate risk through systems of controls. While **about 1 in 3** say they're extremely confident in their ability to manage risk, the rest (**64%**) could benefit from better risk identification and control design processes.

Which best describes your process for planning and implementing improvements to your program?



36%

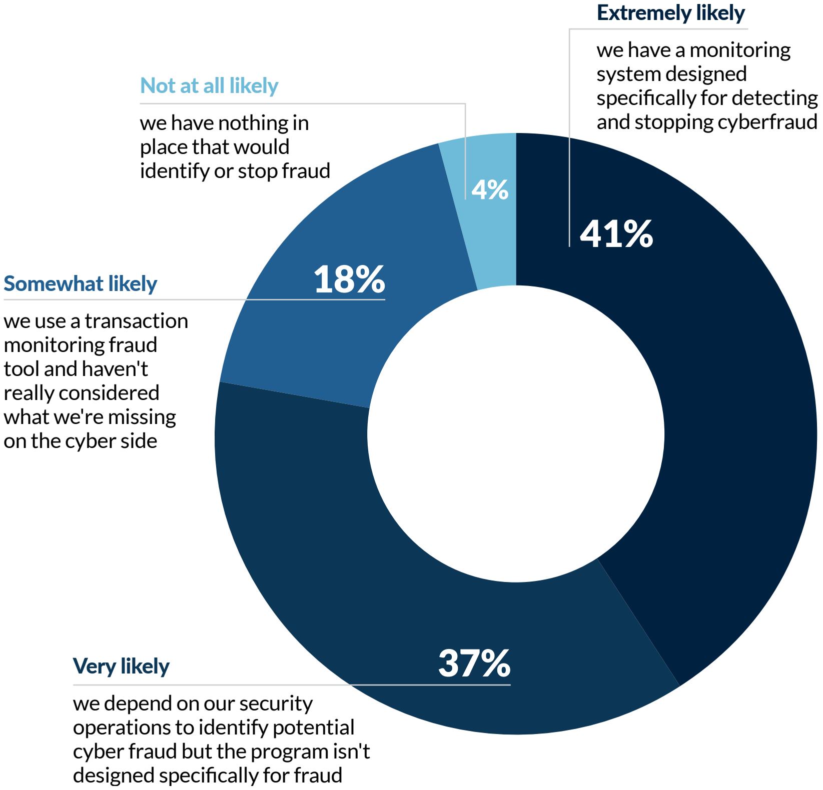
are extremely confident in their ability to identify risk and design controls to effectively mitigate those risks - they have robust risk assessments and strong systems of controls

Confronting fraud

It is important for FIs to employ both processes to detect cyber risk threats as well as cyber fraud threats. In a digital-first world, cybercriminals are getting better at impersonating consumers, gaining access to client accounts and escaping without a trace. Cyber fraud is a significant risk with serious impacts to an FIs bottom line and reputation. As a result, it deserves serious consideration when developing the offense component of a cyber risk program.

It's concerning, then, that **1 in 3** respondents said they depend on their cyber risk tools to detect cyber fraud despite not being designed or calibrated for fraud monitoring. Even more concerning, **almost 1 in 5** only use reactive transaction monitoring tools, meaning they don't proactively monitor against cyber fraud threats. Combining traditional transaction monitoring tools with solutions specific to cyber fraud can position FIs to successfully detect and prevent fraud before money goes out the door.

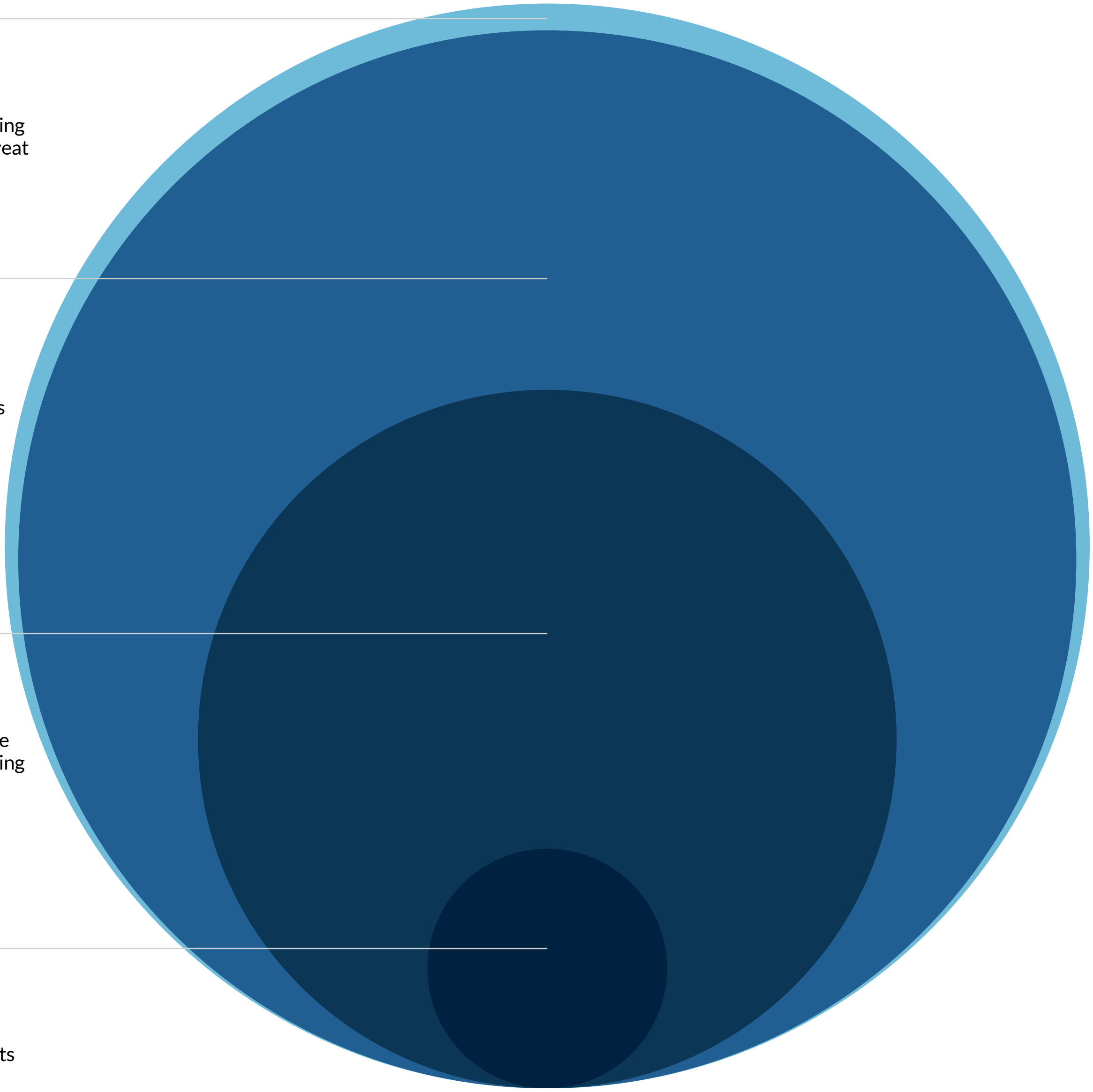
How likely are you to stop cyberfraud?



FIs consider themselves well-positioned to learn about new and emerging cyber fraud threats, but that comes with a few asterisks. Even those who say they're very confident they can keep up with fraud (**40%**), also say they leverage external resources to do so. **1 in 5** struggle to address cyber fraud and often find themselves reacting to fraud rather than proactively neutralizing it.

In sum, FIs must take a proactive approach to protect themselves against both security and fraud threats. An effective offense includes technology, tools and talent that enable timely identification of new and emerging risks so that FIs can be nimble and pivot to effectively counter each unique threat.

How confident are you in your ability to stay informed on new and emerging cyber fraud threats?



41%
Very confident
we do better than most at staying informed but recognize the threat landscape changes quickly

39%
Extremely confident
we have internal expertise and we leverage external resources

17%
Somewhat confident
Staying up to date is a challenge and we often find ourselves being reactive instead of proactive

2%
Not at all confident
We're well behind on our efforts to stay on top of cyber fraud

In Closing

The fight against cyber risk will never be done, but there is a clear and compelling path forward for financial institutions. Holding the line requires them to deploy a two-fold defense and offense strategy. A strong defense helps to mitigate risks and prevent attackers from gaining a foothold, while a proactive offense, focused on what's coming next, delivers intelligence on evolving threats and prepares accordingly.

The respondents to this Cyber Risk Benchmarking Survey delivered mixed messages. Banks and credit unions are aware of evolving threats and are taking steps to address fraud and cybercrime – but most also believe they should do more. **57%** said they could better utilize technology in their cyber defenses, **67%** said they needed to improve (or initiate) automating their governance activities, and **1 in 3** are monitoring fraud using tools not designed for that purpose.

Perhaps these mixed messages themselves reflect a landscape that's changing rapidly; Or is it uncertainty about what to invest in next? What constitutes the optimal mix of technology and talent to deploy in the fight?

Whatever the case, it's clear there's plenty of room for improvement.