TATA CONSULTANCY SERVICES

Building on belief

Secure but wary, confident but not complacent

TCS Risk & Cybersecurity Study:
Banking & Financial Services Report

Secure but wary, confident but not complacent

When inveterate criminal Willie Sutton was asked why he robbed banks, he replied, “Because that’s where the money is.”

Financial services firms have decades of experience guarding access to their customers’ money and personal identifiable information. But in today’s highly connected, dynamic digital world the stakes are even higher. Preventing security breaches is essential to avoiding financial harm and reputational damage over the short- and long-term.

As the TCS Risk & Cybersecurity Study reveals, banks and other financial services firms are keenly aware of the accelerating cat and mouse challenges of keeping the bad guys out of their networks, systems and applications, Many, particularly the more financially successful firms, have adopted extremely sophisticated cybersecurity measures to safeguard their data and processes.

Secure but wary, confident but not complacent

Yet even at leading banks and financial services (BFS) firms, CISOs and CROs may receive pushback from their C-suite peers or struggle to engage their boards. These tensions and challenges are captured in the results of a recent TCS survey, as well as in interviews with security executives working at banks, financial institutions, and in other industries. Two distinct groups emerged from the research. **Pacesetters**, whose companies reported higher than industry averages for both revenue growth and profit growth between 2017 and 2021 (21% of BFS firms surveyed), and **Followers**, who reported lower than average revenue and profit growth during that period (58% of BFS firms surveyed). Here's what we found:

1. With longer experience, banks and other financial services firms may be more confident than other industries about avoiding the worst outcomes of cyberattacks. But they're also more realistic about their capabilities.

2. Knowing their cash operations are a prime target for cybercriminals, BFS cyber executives continue to shore up their systems' defenses. CROs are especially focused on their firms' investing and payment services.

3. More than three-quarters of CISOs and over half of CROs at BFS firms got budget increases in the last cycle. Only a minority of CROs in other industries saw increases.

4. CISOs and CROs have allies in their corporate boards, who are among the most focused in business. But a majority of BFS C-suites remain at best reactive or even disengaged on issues of cyber risk and security.

5. The top financial firms compete for cyber talent across industries; as a result, their CISOs and CROs have experienced greater challenges in recruiting than have other BFS firms. They enjoy a sizable advantage, however, in retaining those same employees.

6. The industry's attitudes toward the cyber risks or advantages of cloud platforms are evenly divided, but the more successful BFS firms are more likely to be overtly cloud-friendly.

The TCS Risk & Cybersecurity Study of more than 306 chief information security officers (CISOs) and 301 chief risk officers (CROs) was conducted in 2022 via survey and in-depth interviews amid an unprecedented upsurge in increasingly sophisticated cyberattacks from criminals, sovereign states, and other bad actors exploiting global sociopolitical and economic tensions. The survey respondents were drawn from North American, European, and UK-headquartered companies in four industries — banking and financial services, manufacturing, utilities, and media and information services — facing an unprecedented range of cyber threats and increased risks, whether to business data, customer data, operations, trade secrets, or supply chains.

In this report, we examine the greatest security risks banks and financial services firms face, explore how effectively these 79 CISOs and 75 CROs are creating security strategies, and offer suggestions for improvement based on our work in the financial services sector worldwide.

I Risks, threats & targets

Banks and other financial services firms may be more confident than other industries about avoiding the worst outcomes of cyberattacks…but they're not taking their security capabilities for granted.

Complacency is not an option

"I think we know that we are in a good place relative to market leading practice, defensive practice. We absolutely know we have improvement opportunities, and we are comfortable that we are improving in line with the sort of threat, the speed of which the threat grows. So we're proud of where we are, but very far away from happy or complacent. We recognize we're in an arms race."

— CISO of a large European merchant bank

Top threats

BFS risk and cybersecurity executives are most concerned about malicious damage inflicted by attackers (see Figure 1). This ranking may reflect how well those executives recognize the potential scope for damage from insider threats, given the highly sensitive nature of the customer data the BFS industry must guard.

When considering the tactics cybercriminals are beginning to employ with more frequency against a variety of industries, BFS CISOs are most concerned about the attacks that leverage artificial intelligence and machine learning (see Figure 2), whether that's an attack on the bank's own use of artificial intelligence and machine learning or a sophisticated incursion of an AI/ML-driven virus or other exploit.

Types of cyberattacks ranked by concern level for CISOs & CROs	Banking & financial services *n = 154*	Other industries *n = 453*	BFS Pacesetters *n = 33*	BFS Followers *n = 90*
Malicious damage (including both digital and physical damage)	1	2	3	1
Data theft	2	1	1	2
Ransomware	3	3	2	3

Figure 1

Tactics which most concern CISOs when thinking about cybersecurity between now & 2025	Banking & financial services *n = 79*	Other industries *n = 227*
Attacks leveraging AI/machine learning	1	2
Advanced social engineering attacks (watering hole, pretexting, whaling, etc.)	2	1
Open-source exploitation	3	4
Crime-as-a-Service	4	3
Over-the-air (wireless chip) exploits	5	6
Chatbots	6	8
Web cache poisoning	7	5
Botnets	8	7

Figure 2

Risks, threats & targets

BFS CISOs and CROs express less confidence than their peers in other industries about handling actual external threats and internal risks (see Figure 3). Only a scant 30% of overall BFS respondents (30%) — and less than a third of BFS Pacesetters — say their ability to handle external and internal risks and threats is “well in hand” compared to their competitors. This difference between the harsh ratings some BFS executives give their abilities compared to those of other industries may reflect BFS’s longer experience with cyberattacks and their appreciation of the difficulty of identifying and thwarting them.

Ability to handle external threat & internal risks compared to competitors

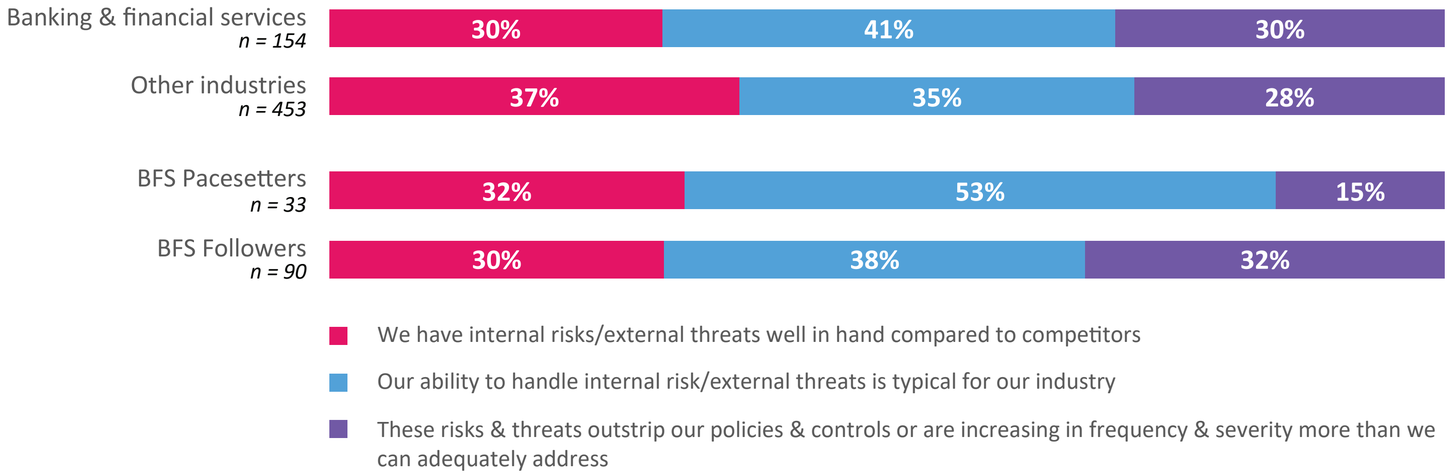

Figure 3

Risks, threats & targets

Comparing CISOs and CROs for diverging views to their firms' capabilities against external threats and internal risks (see Figure 4):

- BFS CROs feel more confident about their companies' ability to at least address internal risks, compared to their CISO colleagues views
- BFS CISOs are more likely to feel their capabilities for external threats are on par with the rest of the industry
- BFS CROs are more likely (compared to BFS CISOs) to be pessimistic about the company's abilities in the face of exogenous threats, whereas BFS CISOs would be more likely to feel the firm is more vulnerable against internal risks.

Inside jobs

> "Here's the bigger insider threat: the disgruntled worker. His girlfriend just got laid off. His boss is being a jerk and yelled at him. And so, on the one night he's going to finish up his shift late in the data center, and he's supposed to turn on a bunch of scripts, he just says, 'Forget that. I don't care.' And that's the night they get hit."

— CISO of US financial services firm

Ability to handle external & internal threats

BFS CISOs vs BFS CROs

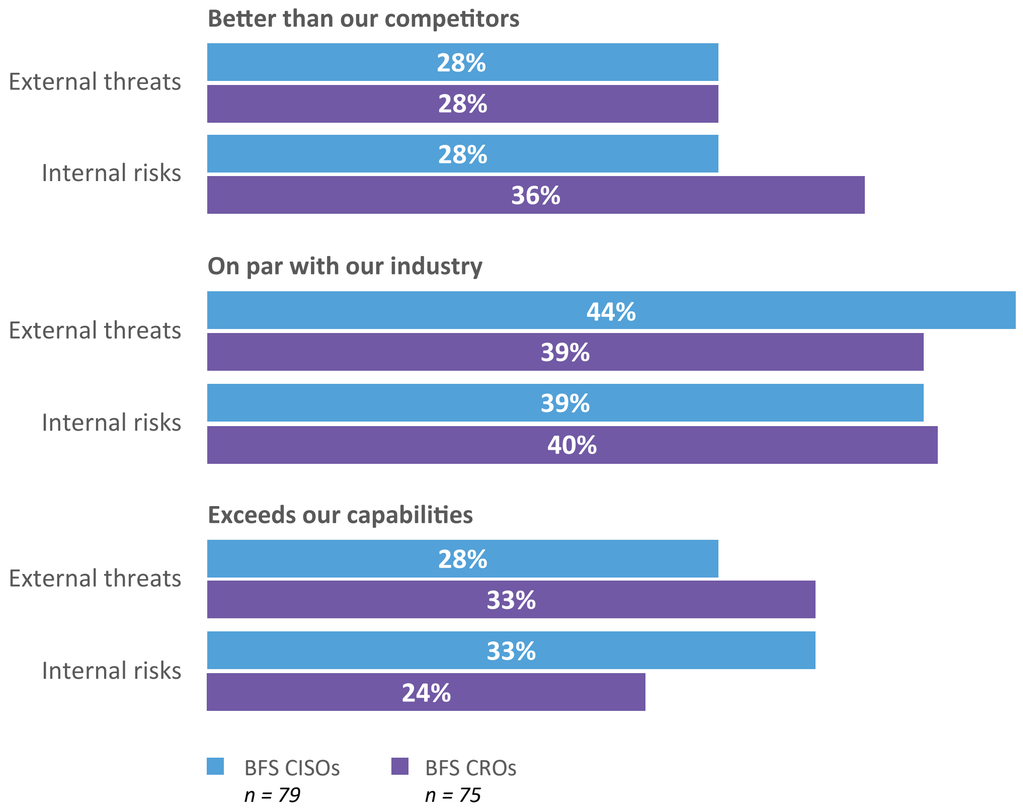

Figure 4

Risks, threats & targets

When asked to assess the cyber technology they are leveraging in their enterprise, more than half of BFS CISOs (53%) say their technology can't defend their organizations against today's most sophisticated threats, while the remaining 47% think their advanced technologies are effectively defending their organizations against such attacks (see Figure 5). Perhaps more alarming, 35% of BFS CISOs — six percentage points higher than across other industries — describe their abilities as sufficient only to deal with common threats such as signature-based malware and denial of service attacks.

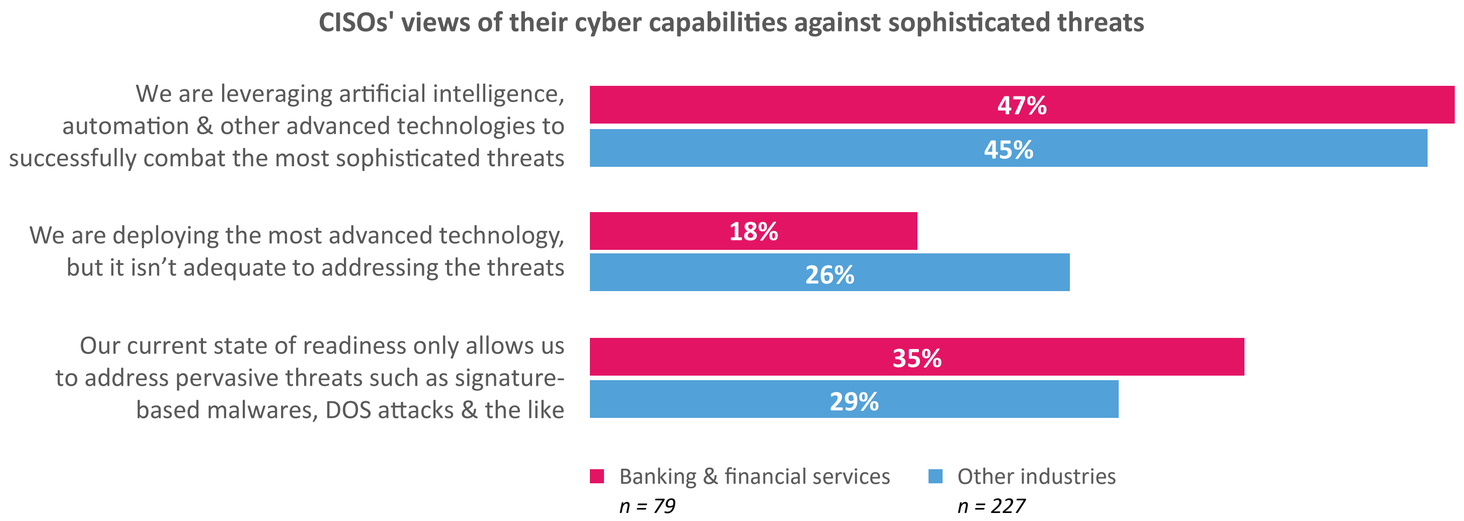

Figure 5

Risks, threats & targets

Nevertheless, compared to other industries, BFS security executives are more confident overall about avoiding the repercussions of a major cyber incident in the next three years (see Figure 6). Nearly 75% of BFS Pacesetters express some level of confidence their organizations can avoid a damaging incident.

A disconnect persists, however, between how CISOs regard their firms' chances against a cyber incident and how the CROs see it: three quarters of BFS CROs are somewhat or very confident their enterprise can avoid a major financial or reputational loss as the result of a cyber incident. Only 57% of BFS CISOs are as optimistic.

These differences across the industry are certainly worth a discussion within an individual bank or financial services firm, first between the CISO and CRO, and then among the board of directors. Particularly important to map would be how the company's cybersecurity capabilities and risk mitigation practices match up against:

- External threats, including the more advanced AI/ML-enabled tactics on the horizon
- Internal risks, whether intentional threats or inadvertent actions
- Executives' confidence in avoiding major financial or reputational loss as a result of a cyber incident

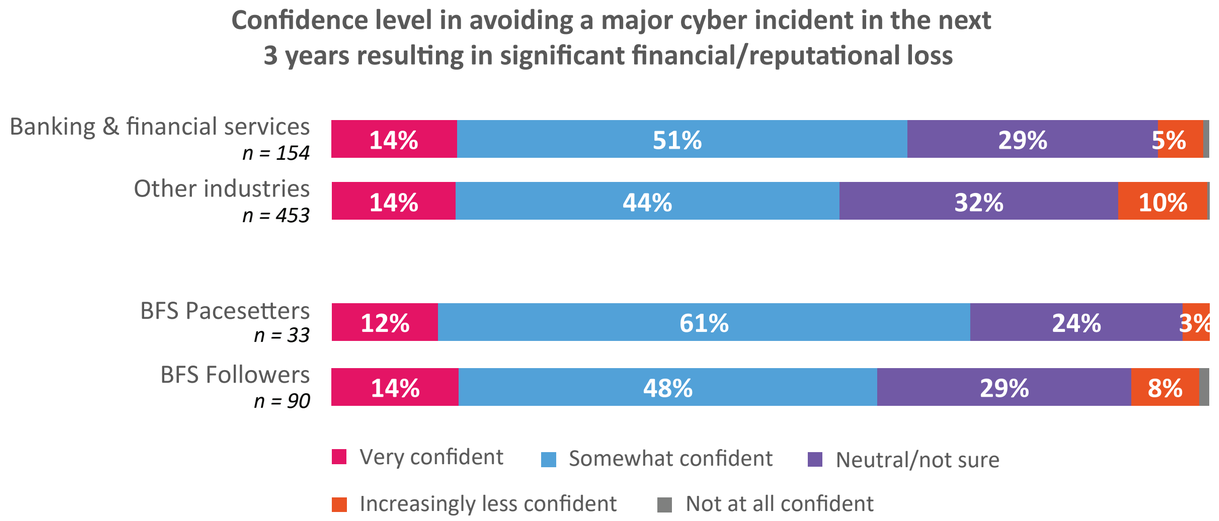

Figure 6

Ever-changing threat vectors

"The thing that worries me about cyber is what it meant six months ago could be very different from today. And what worries me is how quickly it's changing and how little we know: 'Where's the next attack going to come from? What's it going to look like?' It's changing all the time."

— US-based enterprise risk manager

Risks, threats & targets

Top targets

BFS cyber executives naturally expect their firms' operations related to cash and finance to be most at risk from cyberattacks — more than their customer databases and sales or e-commerce platforms, and ahead of other industries' concern for the cash and financial operations. (See Figure 7.) Given the nature of the business — money — this is not surprising.

Digging deeper, as part of their cyber risk mitigation initiatives, BFS CROs intend to focus on their firms' investment banking and payment services functions (see Figure 8), followed by asset and wealth management departments. Distributed ledger and other cryptocurrency-related functions and activities ranked fourth.

Corporate functions where CISOs & CROs expect to see the greatest number of cyber attacks between now & 2025	Banking & financial services *n = 154*	Other industries *n = 453*	BFS Pacesetters *n = 33*	BFS Followers *n = 90*
Finance	1	2	1	1
Customer databases	2	1	2	2
Sales/ecommerce	3	5	3	3
R&D	4	3	4	4
Marketing	5	8	5	5
Legal	6	9	6	7
Human resources	7	6	7	6
Ecosystem partners	7	10	7	8
Distribution/supply chain	9	7	9	9
Manufacturing plants/production/procurement	10	4	10	10

Figure 7

Cyber risk and security priorities for BFS CROs	*n = 75*
Investment banking	1
Payment services	1
Asset/wealth management	3
Distributed ledger/cryptocurrency	4
Corporate banking	5
Retail banking	6
Mortgage	7
Forex services	8
Lending/loans	8

Figure 8

Note: question was only asked of CROs in the banking & financial services industry

I Cyber priorities

Corporate processes continue to become more digitized, and devices ever more aware, with embedded sensors and monitoring. Digital advances also are making better security tools available to CISOs – and giving cyber criminals more sophisticated attack strategies. This digital dichotomy is driving increases in many CISO budgets (see Figure 9). BFS CISOs and CROs have been more likely than their peers in other industries to see budget increases.

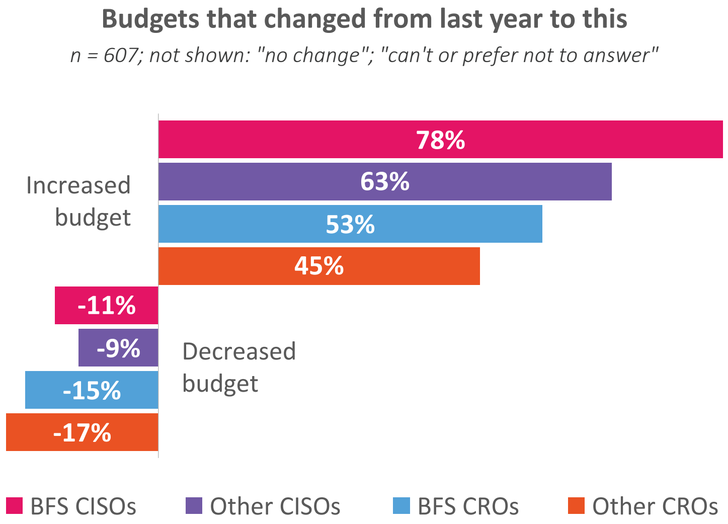

Figure 9

BFS CISOs' top budget drivers	BFS CROs' top budget drivers
1 Increasing digitization of our products	1 Customers
2 New cybersecurity capabilities and services that meet our needs	2 Investors
3 Emerging technology risks generally for our industry or processes	3 C-suite

Cyber priorities

Within those budgets, BFS CISOs say they are prioritizing emerging tech, such as decentralized identity and 5G security, and identity management more than CISOs in other industries (see Figure 10). (They also include data protection and privacy and cloud security management among their budget priorities.)

Closing identity loopholes

> But here is the biggest area: identity. Almost all the attacks that we find that are actually getting in, including ransomware attacks, it's usually through some kind of identity credentials that have been compromised or used inappropriately. I want to understand who's in my network, what they're doing, and why they're doing it.
>
> *— US-based financial services CISO*

When BFS CROs — who must assess risks across a wide range of domains — are asked to prioritize choices among possible cyber risk mitigation efforts, they list identifying the critical operations of their core business lines as a higher priority than it is for other industries' CROs (see Figure 11). They also put a greater emphasis on recovery and continuity planning. By contrast, other industries are more focused on understanding concentration risk, but CROs in banking (where the concept was first derived) already fully understand its importance, are better versed at mitigating it, and therefore rank it only fourth out of eight urgent cyber priorities.

Budget priorities for CISOs between now and 2025	Banking & financial services *n = 79*	Other industries *n = 227*
Emerging security technologies (e.g., decentralized identity, 5G security, etc.)	1	3
Data protection and privacy	2	1
Cloud security management	3	2
Identity management	3	6
Threat management (including ransomware protection)	5	4
Vulnerability remediation automation	6	8
Governance, risk and compliance	7	7
Managed detection and response	8	4
Advisory consulting	9	10
Operating technology (OT) security		9

Figure 10

Most important to cyber resiliency between now and 2025, according to CROs	Banking & financial services *n = 75*	Other industries *n = 226*
Identification of critical operations/core business lines	1	3
Integration of cyber and business strategies	2	2
Plans for business continuity/disaster recovery	3	6
Understanding concentration risk	4	1
Identification and clear ownership of digital assets	5	4
Partnerships with industry groups, government agencies	6	7
Fostering an organizational culture of resiliency	6	8
Measurements of resilience	8	5

Figure 11

Cyber priorities

BFS CISOs say their top priority for their firms' cyber risk and security roadmap between now and 2025 is embedding security into the foundations of all software development, whether through DevSecOps practices or other secured software development methods (see Figure 12).

As important as it is, CISO influence over how an organization and its vendors develop vehicles for increased revenue and reduced costs likely will require significant board and C-Suite support to overcome line-of-business opposition to security's involvement in software development.

Priorities for BFS CISOs' cyber risk and security roadmap between now and 2025	*n = 79*
Secured software development/DevSecOps	1
Infrastructure/cloud security	2
Sensitive data discovery & protection	3
Security architecture & governance	3
Governance, risk & compliance (GRC) implementation	5
Vulnerability management	6
Open banking security	7
Access control for employees, customers & partners	8
Customer consent management	9
Compliance to privacy laws	10

Figure 12

Note: question was only asked of CISOs in the banking & financial services industry

Top cyber risk & security priorities arising out of banks' & financial firms' board-level discussions

1. Improving visibility of cyber risks & ensuring compliance to regulatory & industry requirements
2. Increasing cybersecurity maturity of our company relative to industry peers & adopting emerging models like zero trust
3. Ensuring cyber risks are holistically managed & mitigated across our company & its larger ecosystem

Cyber priorities

With a relatively longer history of defending against cyberattacks as well as a more established role for CROs, BFS firms are more likely than other industries to be proactive at almost all levels when it comes to cyber risk and security.

BFS company boards are more likely to be discussing cyber risk and security at every meeting: 45% versus 38% in other industries. And a majority of BFS Pacesetter boards cover cyber at every board meeting — the only industry we surveyed where this is the case, even for Pacesetters (see Figure 13).

Frequency of board level discussions on cyber risk & security issues

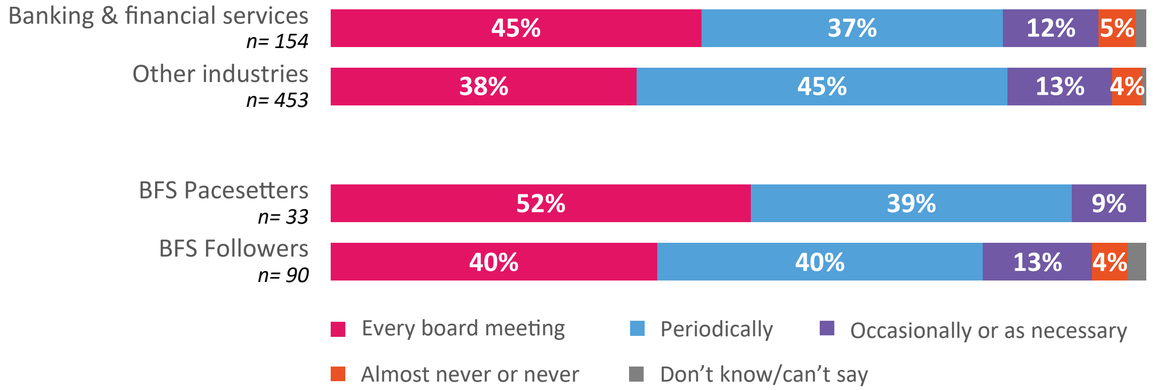

Figure 13

Frequency of BFS board engagement with cyber issues, by type of ownership

not shown: "Don't know/can't say" about board discussion frequency

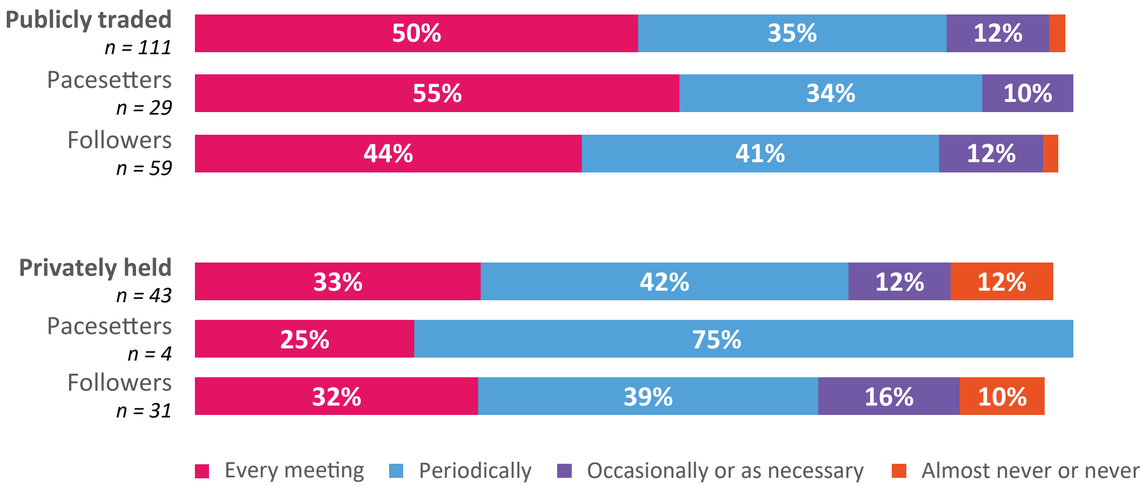

Figure 14

The distinction, however, seems to driven more by the type of BFS firm rather than any financial success or struggle (see Figure 14). Publicly traded companies have to answer to shareholders and, often, government regulations and securities exchange rules that don’t pertain to privately held firms — and a board’s fiduciary responsibilities increasingly overtly include cyber risk mitigation.

Cyber priorities

While the line-of-business executives and C-suite officers of banks and financial firms are slightly more proactive than those in other industries in addressing cybersecurity issues, a majority are still reactive or disengaged (see Figure 15). A plurality of BFS Pacesetters is more likely to have proactive, rather than reactive or disengaged, C-level leaders.

Tech and business still on different pages

> "I think most organizations have now got a separation between the security team and the technology team, so there's a delineation of accountability there. And the technology teams are increasingly incentivized by being secure. So that's step one. I think what we haven't got to yet is where business execs, the money makers, feel that same accountability. They absolutely still feel like, 'Well, cyber is his problem. If we get a cyber breach, then he screwed up."

— UK-based banking CISO

Attention given to cyber risk & security issues by line-of-businses leaders & C-suite executives

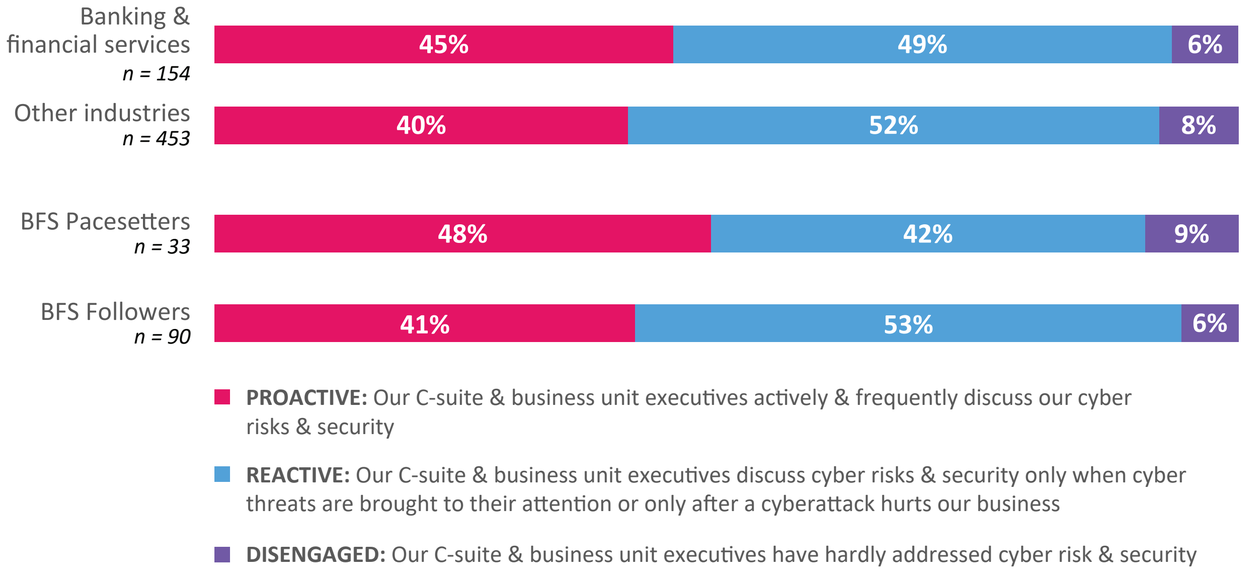

Figure 15

Cyber priorities

CROs in the BFS industry are more likely to report to the CFO than their counterparts in other industries are, demonstrating the role's origins in that department and within the finance industry (see Figure 16). Following similar corporate trends, the majority of BFS CISOs report to the CIO. Looking across both roles, however, BFS Pacesetters' cyber executives are much more likely to report to the CEO or COO than are those at BFS Followers — 45% vs 27%, respectively.

While collaboration between CISOs and CROs takes place more frequently in BFS than in other industries, CISOs and CROs at Follower firms are the most likely to collaborate more frequently (see Figure 17). This is in contrast to the study's larger findings where, across all industries, Pacesetter firms' CISOs and CROs were the most likely to collaborate more frequently.

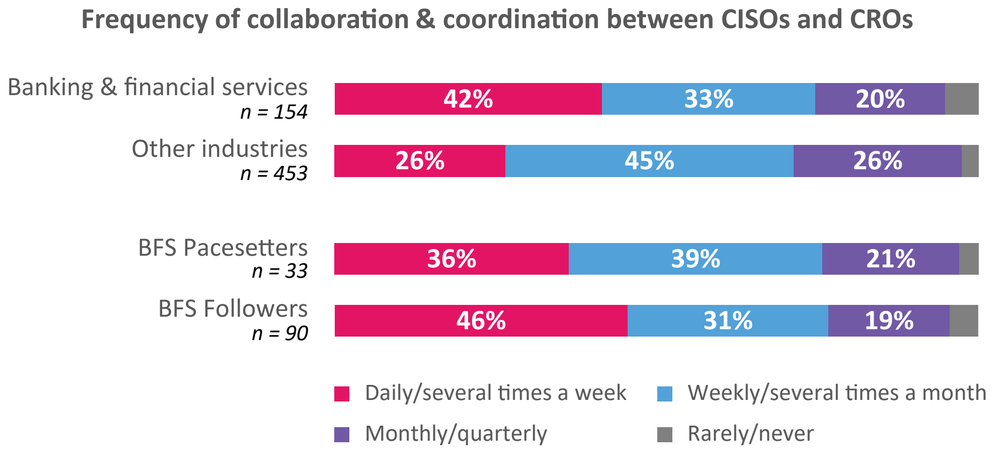

Figure 17

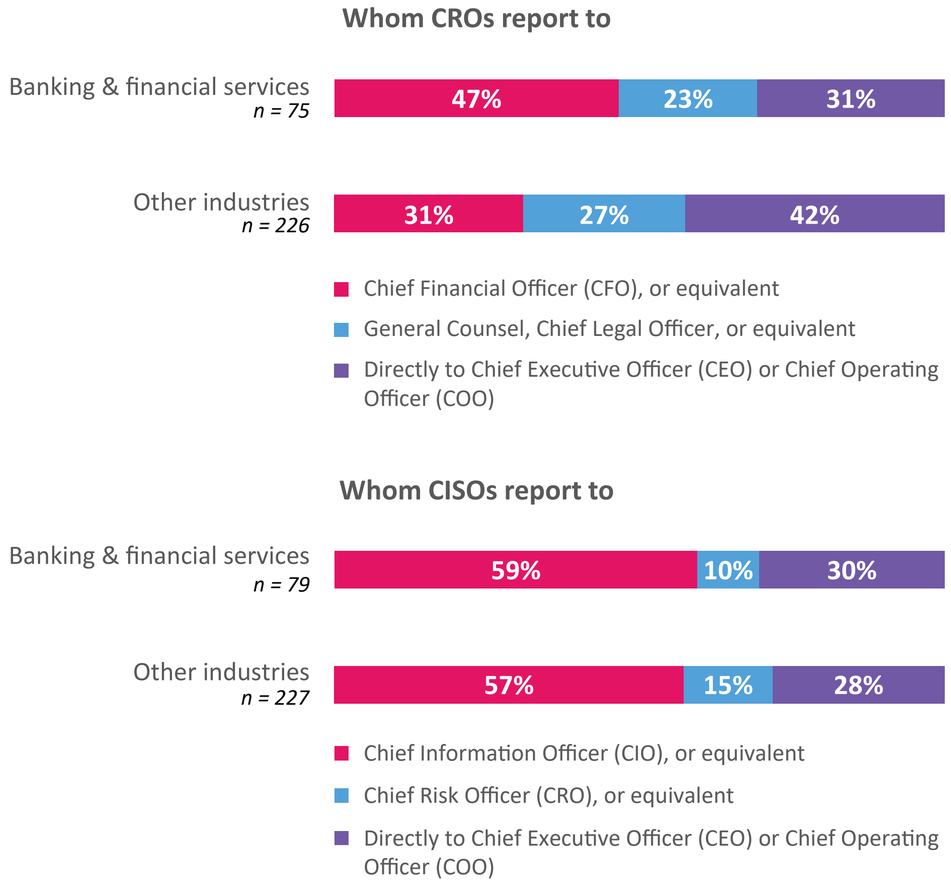

Figure 16

Recruiting & retention

The competition for talent with cyber skills is tougher in BFS than in most other industries. But some companies – the financially successful ones, the cloud-friendly ones – have found some advantages.

As in other industries, finding and keeping professionals with the right skill sets is the number one challenge to implementing and supporting BFS cyber security initiatives (see Figure 18).

Reliance on legacy IT systems is slightly more of an issue than it is for other industries. For Pacesetters, however, legacy IT is no longer a problem…but demonstrating a return on their investments in cybersecurity is.

The greatest challenges to cybersecurity & risk mitigation initiatives, according to CROs & CISOs	Banking & financial services *n = 154*	Other industries *n = 453*	BFS Pacesetters *n = 33*	BFS Followers *n = 90*
Skill sets to manage, engineer & support cybersecurity technology	1	1	2	1
Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.)	2	2	7	6
Reliance on legacy IT systems	3	4	8	2
Assessing cyber risks & quantifying relevant costs	4	2		5
Difficulty in mandating that our current vendors adopt advanced technologies & policies	5	11	4	3
Accumulated complexity of our own business processes & operations	6	4	10	4
Lack of collaboration across enterprise units (business, IT & security)	7	7	11	7
Lack of diversity (including of thought & experience) in staff assessing cyber risks & threats	8	8	4	8
Difficulty in demonstrating return on cybersecurity investments	9	6	1	9
Budget constraints	10	9	6	10
Competing interests for the board or senior leadership	11	10	11	11
Outdated, siloed & non-integrated security tools	12	12	8	12

Figure 18

Recruiting & retention

The competition for cyber talent has been greater in BFS than in other industries: 49% of BFS firms say they've had problems recruiting and 45% report difficulties in retention vs. 42% and 41% for other industries, respectively (see Figure 19). Pacesetters have found recruiting competition more intense than Follower firms report. This may be because the larger firms are trying to draw top talent yet have been less open to continuing remote working situations. Yet once cyber risk and security professionals are hired, BFS Pacesetter executives report far more retention success than BFS Follower CISOs and CROs.

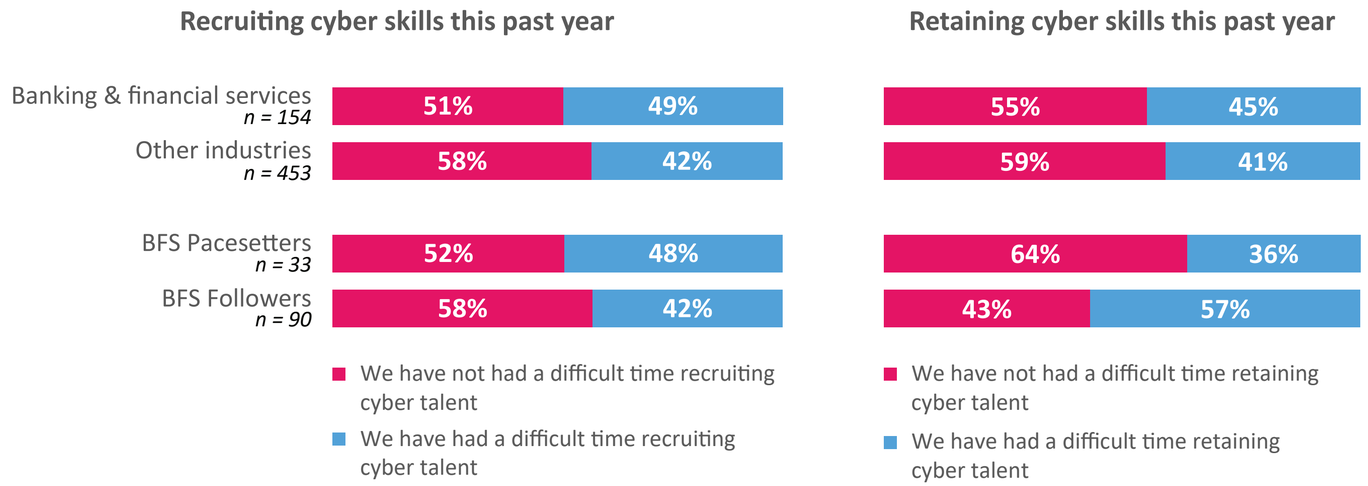

Figure 19

Strong talent is hard to find and keep

> This is unprecedented staff turnover that we haven't seen before. People are leaving. It's also difficult to backfill the position. The reasons seem to be several factors, one being: post-COVID, other firms, particularly non-financial firms are okay to allow people to work permanently remote. Whereas Wall Street firms are so keen on folks coming in at least two, three days a week. I think the nuance there is: if you're a cybersecurity expert, you're kind of industry-agnostic to a large extent. So a good cyber expert could just jump around and go from media to finance to something else.

— Enterprise risk manager, US financial firm

Recruiting & retention

In addition to such perennial factors as pay, reputation, and flexibility, another key for recruiting and retaining top cyber talent is the opportunity to work with the industry's latest and most sophisticated solutions. And, increasingly, those solutions are either designed to secure environments that include cloud platforms or they are cloud-based solutions themselves (or both). Companies with leadership that is more positive toward cloud environments for business have an advantage when it comes to recruiting and retaining their best workers (see Figure 20). Across all industries in our study, it was a five-point advantage; in BFS, cloud-friendly firms enjoy a 10-point advantage over the competition in recruiting and retention.

Cloud-friendly BFS firms have had less difficulty recruiting & retaining talent with cyber risk & security skills

n = 143; not included: can't come to agreement on cloud platforms

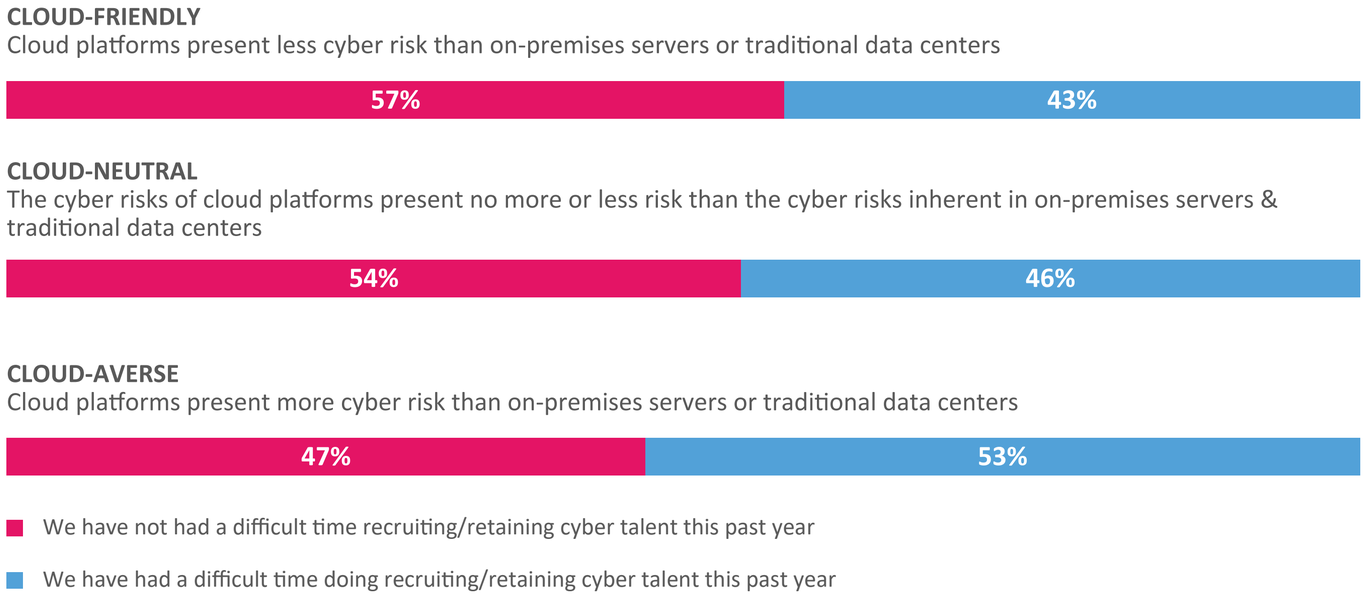

Figure 20

I Debating cloud security

The banking and financial services industry is evenly split in its attitudes about the security of cloud platforms. Yet almost twice as many BFS Pacesetters say cloud is the more secure choice compared to those who say cloud is riskier than traditional, on-premises server infrastructures (see Figure 21).

In addition to enjoying an advantage in recruiting and retaining top talent with cyber skills (see Figure 20 earlier), cloud-friendly BFS firms are also more likely than cloud-neutral and cloud-averse BFS firms to say they have external threats and internal risks well in hand compared to their competitors.

Attitudes toward cyber risk & security of cloud platforms

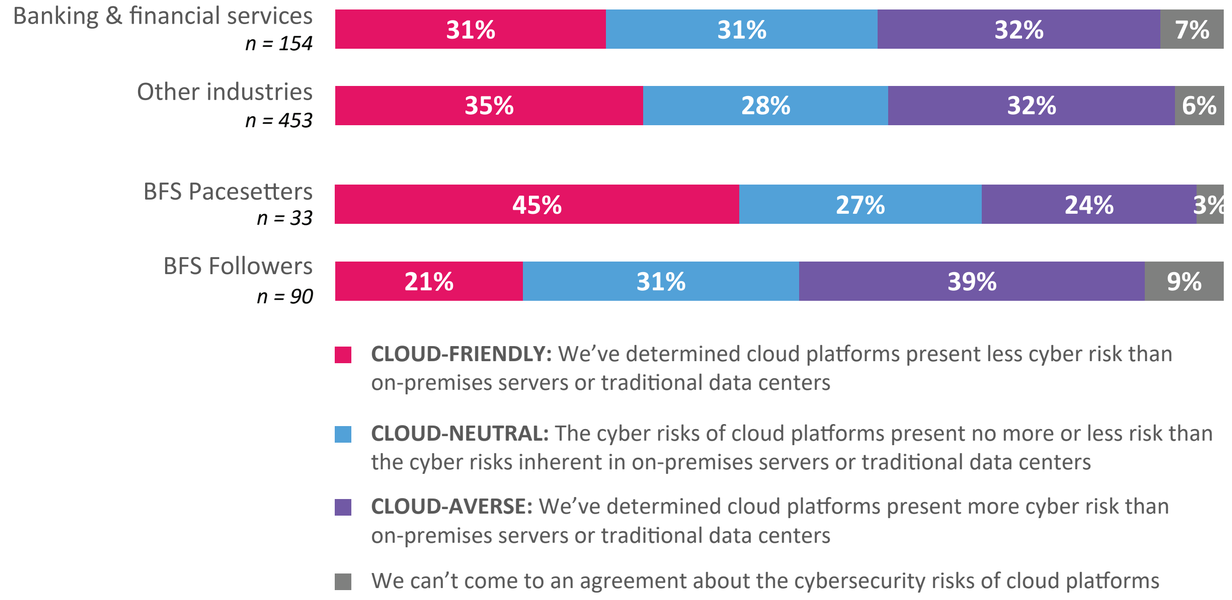

Figure 21

Protecting money means protecting data

Banking and finance have always been, by definition, a digital business

Because of their running start, banks and other financial services appear to be more confident than other industries about avoiding the worst outcomes of cyberattacks. But given ongoing advances in AI and machine learning, BFS CISOs and CROs are rightly concerned that these advanced tools in the hands of bad actors can more easily exploit cybersecurity vulnerabilities as quickly as they are identified and plugged.

And it's not just bad actors outside BFS's four walls operating from countries via the dark web where IP addresses can be easily disguised if not entirely masked. The threat from within financial institutions looms just as large and can be equally undetectable if proper security procedures and protocols are not instituted and monitored. For this reason alone, CISOs and CROs need to deepen their coordination to stay ahead of the ever-widening threat vector.

Greater collaboration between the risk and information security disciplines within the bank and across the entire C-suite (up to and including the board) is therefore non-negotiable. As is finding, keeping, and upskilling top-notch cybersecurity talent. Doing business via cloud platforms offers the opportunity to offer budding cybersecurity experts a growth path up the IT chain of command. However, focusing the skills lens purely on cybersecurity experts from within BFS may be overly restrictive. In our view, a domain expert in cutting-edge cybersecurity strategies and tactics can come from any industry sector. This transitive property of cyber skills is, after all, why the competition for top talent is so fierce.

Recommendations

To keep their cybersecurity house in order, BFS firms will need to build on the strong collaboration that already exists between CISOs and CROs. This means these leaders must not only understand cybersecurity best practices but make clear that to guard against debilitating breaches, everyone in the company, including the board and other C-suite officers, must remain vigilant. Here's how we suggest CISOs and CROs move forward.

1 **Focus on attack surface management.** The goal: data protection. The key here is to leverage a zero trust architecture. Perimeterless security improves the probability that the effects of cyber intrusions remain contained to smaller areas. We also recommend applying a minimum-security baseline at the end point, data center, and cloud environment to harden the core IT infrastructure.

2 **Incorporate cybersecurity by design and by default.** Design all IT infrastructure and its use to incorporate cybersecurity by default, without exceptions. Batten hatches with robust identity and access management systems. In concert with deploying a zero trust architecture, advanced identity and access management (IAM) systems provide defense against threats from outside and inside your organization. Be sure to leverage existing IAM investments and rapidly onboard critical assets. This not only improves your risk profile but also helps to demonstrate a return on cybersecurity investments.

3 **Inculcate cyber resiliency across an agile organization.** As attacks increase in sophistication and adversaries become better organized, assume the worst: your enterprise, like nearly every other, is likely to be targeted or to experience a security breach. Therefore, focus on resiliency – i.e., how quickly and effectively your organization can bounce back, with all systems, applications, and networks online and supporting the business. To do this you will need to automate key elements of your cybersecurity infrastructure, from security detection, design, and deployment, through monitoring and responding to security breaches across the enterprise. Intelligent automation will help your team to identify incidents earlier and to respond and recover completely. Organizations that have thoroughly adopted agile methods of development and operations are more likely to be able to respond more quickly and efficiently to vulnerabilities or attacks, and thus have a built-in advantage for cyber resiliency.

Recommendations

4 **Take ownership.** Not only should the business heads of a company be involved in its cybersecurity and risk policy framing and implementation, ownership of cybersecurity should lie in the hands of enterprise's top management and across the C-suite. Regularly scheduled meetings with top management and domain experts should be used to assess and review the cyber maturity level of the organization.

5 **Understand supplier and open-source software vulnerabilities.** In today's interconnected world, securing your developed code base, as well as hardening your networks and operating systems, is not enough. You need to continuously test, monitor, identify issues and create remediation routines for open-source frameworks and components, which is why deploying DevSecOps is critical. Software Composition Analysis (SCA) for open-source and third-party software is an integral part of a DevSecOps pipeline. Ensuring and enforcing security for supplier, third- and even fourth-party ecosystems should become a major consideration in managing any existing or proposed relationships, especially involving mergers and acquisitions. In fact, as financial institutions continue to become reliant on third parties for providing them with many IT- and non-IT-related services that could allow exposure to risk concentration and cyber threats, banks and financial services firms need to establish third-party risk management teams that focus on the cyber maturity of the third parties they deal with.

6 **Use automation as a lever to upskill your team.** As you automate more and more routine security tasks and remediation, you can move team members to more constructive and valuable tasks. Remember, these team members already understand your threat vector, as well as those systems, applications, and networks that could be impacted in the event of a breach. As more and more Level 1 and 2 security tasks become automated, your team can more fully enable advanced cloud capabilities across the enterprise. This will not only ensure first-class protection for your firm, but it will also help you to attract and retain top cybersecurity talent, who usually prefer to work on cutting-edge platforms.

7 **Audit and manage assets.** Regular audits will identify the gaps in cybersecurity implementation. Establish policies to measure the performance of the infrastructure and its use in line with solid zero trust security principles, and advance legacy systems with outdated security to the head of the list for replacement.

When the banking and financial services industry sneezes, the global economy catches a cold.

Banks and financial services firms — which have always engaged with organizations in every other industry — have long understood: we're all in this together. Disruptions of transactional services and breaches of banks' or bank customers' data can hinder payrolls, supplier payments, and consumer and investor trust.

Many BFS firms are at the forefront of cybersecurity defense, impatient for governments and other industries to catch up. And, as our study shows, BFS leaders as a whole have a more cautious, realistic appraisal of their defenses and exposures than cyber executives in other industries.

The business community will continue to watch how BFS firms mitigate their risks and will, eventually, follow suit. However, the banking and financial services industry will remain an attractive target for cyber terrorists and digital thieves, and thus has no choice but to continue to level up its defenses and practices in the face of an approaching tsunami of cyberattacks.

TATA CONSULTANCY SERVICES

Building on belief

Executive champions

Santha Subramoni
Head, Cyber Security Practice, TCS

Margareta Petrovic
Managing Partner, Risk & Cyber Strategy, TCS

Contributors

Samir Malaviya
Head, Cyber Security - USA, TCS

Ravi Yadav
Head, Cyber Security - Banking,
Financial Services & Insurance, TCS

Raghu Mahadev
Head, Risk & Regulatory Technology Solutions, TCS

Vijayaraghavan Venkatraman
Head, BFSI Risk Management & Regulatory Compliance, TCS

Aju Vasudevan Nair
Chief Technology Officer, BFSI Cybersecurity, TCS

For the most up-to-date content and news, download the 'TCS Perspectives' app for your iOS and Android device.

Download on the App Store

ANDROID APP ON Google play

Get more insights

If you would like to have more information on the TCS Risk & Cybersecurity Study, please visit on.tcs.com/risk-cybersecurity

For more information or any feedback, email the TCS Thought Leadership Institute at TL.Institute@tcs.com

About the Thought Leadership Institute

Since 2009, the TCS Thought Leadership Institute has initiated conversations by and for executives to advance the purpose-driven enterprise. Through primary research, we deliver forward-looking and practical insights around key business issues to help organizations achieve long-term, sustainable growth. For more information, visit tcs.com/insights/globalstudies

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 55 years. Its consulting-led, cognitive powered, portfolio of business, technology and engineering services and solutions is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 614,000 of the world's best-trained consultants in 55 countries. The company generated consolidated revenues of US $27.9 billion in the fiscal year ended March 31, 2023 and is listed on the BSE and the NSE in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit **www.tcs.com** and follow TCS news **@TCS**.