TATA CONSULTANCY SERVICES

Building on belief

Cyber confidence

TCS Risk & Cybersecurity Study
Master Report

What we're recommending

You'll find a lot of data, correlations, answers, insights, and examples in this report. But the most important thing to take away from it all is some idea of where to start and what to do to better equip your enterprise with a risk and cybersecurity strategy that can deliver on the implied promise of a business-aligned approach to the digital risks and threats of modern business. We recommend the following actions, which you can read more about on page 24.

- Chart a long-term strategy that aligns security technology and functions around both regulatory compliance and protecting the applications, data, and infrastructure most critical to the business.
- Take an integrated approach to governance and implementation of cybersecurity that makes it the responsibility of all functional and business units in the enterprise as well as third parties and vendors involved with relevant processes.
- Consider creating a board-level committee charged specifically with cyber risk and security.
- Focus on cyber resilience because even the best-guarded organization can become a victim of a malicious cyber breach.
- Embed security as a foundational layer in every aspect of the organization.
- Make supply chain and partner ecosystem security a higher priority.
- Leverage the cloud and cloud services to enhance your security profile. And maintain cybersecurity vigilance and regulatory compliance by weaving established cybersecurity frameworks into cloud adoption, including insight into third-party vendors' compliance with cybersecurity controls.
- Coordinate the cybersecurity and risk functions closely.

Contents

The keys to confidence

Despite years of investment in risk assessment and security tools, many chief information security officers and chief risk officers feel worried or even overwhelmed about their ability to meet current and emerging cyber threats.

Protecting their organizations from a rising tide of cyber threats requires advanced technology. But just as important, it requires engaged leadership and strategically aligned stakeholders if an organization is to fight off the most critical developing threats and recover quickly from attacks when they occur.

Those were among the top findings from a TCS study of more than 600 chief information security officers (CISOs) and chief risk officers (CROs) conducted early in 2022 amid an unprecedented upsurge in increasingly sophisticated cyberattacks from criminals, sovereign states, and other bad actors exploiting global socio-political and economic tensions. The survey respondents were drawn from North American, European, and UK-headquartered companies in four industries facing an unprecedented onslaught of cyber threats and increased risks, whether to business data, customer data, their operations, trade secrets, or their supply chains: banking and financial services, manufacturing, utilities, and media and information services.

Essential takeaways

- Companies where the board of directors and C-suite are proactive about its cyber strategy are more likely to see better-than-average revenue and profit growth and fewer problems recruiting and retaining advanced cyber skills.
- Financially successful companies are also more likely to regard cloud-based tools and platforms as more secure than on-premises data centers.
- While companies rightly see much promise for future revenues and productivity by participating in emerging digital ecosystems, most companies are too complacent about the risks and threats inherent in such exchanges of data.
- Recruiting and retaining top talent with the relevant skill sets to manage, engineer, and support cybersecurity technology is the number one challenge for cyber professionals today.

Our survey, along with in-depth interviews with business and security leaders, shows the importance of processes, collaboration, and awareness in aligning all stakeholders on the top-priority risks and the most effective remediation tactics. This coordination must extend from the board to C-level executives and business units down to functional organizations such as technology, finance, and legal. Our findings uncovered that, above all, such efforts require real collaboration between the CISO and CRO offices, as many of them have told us.

Our study found 30% of CISOs and CROs coordinate their efforts several times a week and even daily. Another 42% confer weekly or at least several times a month. Perhaps more telling, collaboration at least several times a week between CROs and CISOs is more likely to be found at the companies who lead their industry peers in revenue and profit growth; in our study, these are the companies we call "Pacesetters." Meanwhile, at a majority of the companies struggling to compete on such financial terms — "Followers" — coordination between the CISO team and the CRO function occurs no more often than "several times a month," at most. Yet even here among the Followers, more than a quarter of CROs and CISOs say they work together daily or several times a week.

Beyond top-down alignment of business and security strategies, Pacesetter companies seem to enjoy other advantages over their Follower peers. For example, they're experiencing less difficulty in recruiting or retaining top talent with cutting-edge cyber risk and security skills. And they're more likely to be leveraging cloud platforms because they've discovered cloud-based infrastructures to be as or more secure than on-premises servers and traditional data centers.

The study showed interesting correlations between the level of attention that corporate boards of directors give to cyber risk and security issues compared against other measures of success, including financial. Two out of five corporate boards cover risk and cybersecurity issues at every meeting, or at every meeting of a committee of the board. Other boards, however, only do so "periodically," "occasionally, as necessary," or even — in some cases — "almost never or never." Yet our findings reveal that the more successful a company has been in growing both revenue and profitability, the more often its board probably engages on cyber issues. Going forward, all corporate boards will need to focus attention on cyber risk and security, given the vulnerabilities of, threats against, and attacks on the emerging digital ecosystems of global business.

In short, our study showed that the challenges for CISOs and CROs are less about budgets and technology than they are about people-centric issues, such as board engagement, skills recruitment and retention, and confidence: confidence in the cloud, confidence in how integrated their cyber and business strategies are, and confidence in their ability to stay ahead of data thieves, digital terrorists, state-sponsored criminal outfits, and — the greatest threat of all — complacency.

Pacesetters & Followers

To unearth best practices and gain an insight to some of the thinking of industry-leading companies and the executives who work for them, we cross-tabulated many of our study findings against the financial success of these companies, dividing the 607 participating companies into "Pacesetters," "Followers," and "all others."

Pacesetters reported growth in both revenue and profit from 2017 to 2021 that was higher than the average reported by all respondents in the same industry or, for those with at least 30 respondents, the same subsector.

Followers, by contrast, reported lower than the same averages for both revenue and profit. For the companies that might have higher than average revenue growth, but lower than average profit increases — or vice versa — they fell into the "all others" camp. This way we can compare what financially successful companies do and how their executives approach business and technology issues, and how that contrasts with the actions and attitudes of the companies struggling to compete in their industry.

Security & the enterprise

As businesses struggle to protect themselves against a growing scale and variety of cyber threats, the TCS Thought Leadership Institute conducted this study to understand:

What are board of directors and C-suite levels of engagement in preparing for and protecting companies from attacks and incursions by malicious actors?

We found two out of five boards include cyber risk and security on their agendas at every meeting, but almost one in five boards are mostly disengaged from the topic. Given the increasing regulations and reporting requirements around privacy and security, especially for exchange-listed corporations, companies with publicly traded shares are more likely to have boards that focus on risk and cybersecurity at every meeting. (See Figure 1.) CISOs and CROs reported similar — if slightly less proactive — engagement from their fellow C-suite executives.

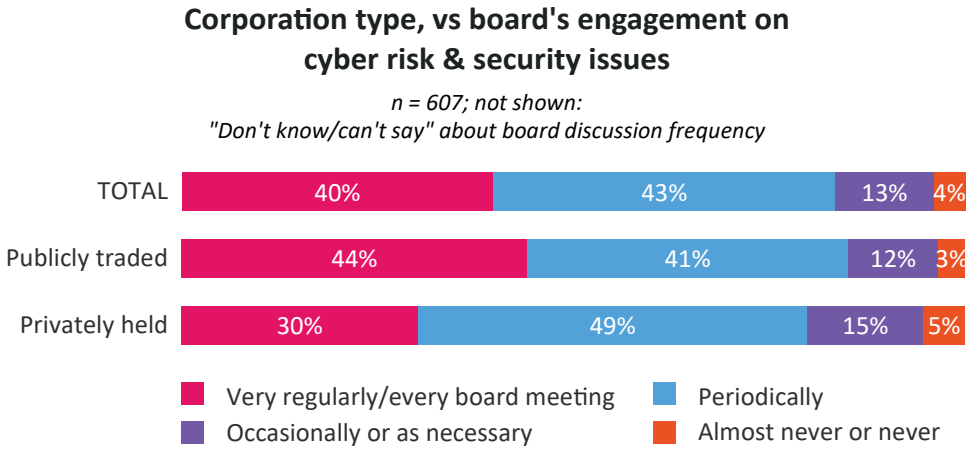


Figure 1

How strong is CISO and CRO confidence in their cybersecurity capabilities?

Only six in ten CISOs and CROs have any confidence their firms can avoid a major cyber incident in the next three years. Another three in ten are “neutral/not sure” and one in 10 “increasingly less confident.” We found confidence was higher where the board is more involved in cyber risk and security.

Significantly, about 30% of CISOs said they can only address the most pervasive kinds of threats, such as signature-based malware or denial of service attacks. This leaves them vulnerable to more advanced and serious threats such as ransomware, web application hacking, insider and privilege misuse, and targeted intrusions.

What are the top priorities for cyber defense and business resiliency?

Cyber risk and security strategists say their board of directors most commonly charges them to: 1) improve visibility of cyber risks and ensure compliance to regulatory and industry requirements; 2) increase the company's cybersecurity maturity and adopt emerging models such as "zero trust"; and 3) ensure cyber risks are holistically managed and mitigated across their companies and partners (see Figure 2).

Cyber risk & security priorities arising out of board-level discussions *n = 587; not included: "There have been no cyber risk or security priorities arising out of board discussions" (3%)*	**Rank**
Improving visibility of cyber risks & ensuring compliance to regulatory & industry requirements	1
Increasing cybersecurity maturity of our company relative to industry peers & adopting emerging models like "zero trust"	2
Ensuring cyber risks are holistically managed & mitigated across our company & its larger ecosystem	3
Creating & adopting a comprehensive cybersecurity governance model	4
Focusing on ecosystem risks & collaboration for oversight, monitoring & mitigation of those risks	5
Creating a "resilience-by-design" culture & adopting such standards & controls	6

Figure 2

The low priority given specifically to focusing on the risks inherent in a company's (otherwise advantageous) participation in digital ecosystems (#5) contrasts with findings in the TCS 2021 Global Leadership Study,[1] which found that:

- 45% of companies today include digital ecosystems in their strategic planning; and
- Executives expect, on average, nearly half of their revenue to come from new industry ecosystems by 2025.

Yet in this study focused on risk and cybersecurity executives, only 15% of respondents said focusing on these risks and collaborating with other ecosystem partners to identify, monitor, and mitigate them was the top priority for their board. This disconnect — between the high priority of digital ecosystems in conducting global business and the lack of attention paid to the risks accompanying those ecosystems — also showed up elsewhere in our study.

[1]TCS 2021 Global Leadership Study: www.tcs.com/perspectives/ceo

What are the threats on which CISOs and CROs are focused and the challenges they face?

CISOs and CROs agree that data theft is both the most likely and the most potentially damaging threat facing them today, followed by malicious damage (whether physical or digital), and ransomware. The top three challenges in fighting these threats were finding skilled security staff, changing work environments (such as work from home and bring-your-own-device), and assessing cyber risks and quantifying their costs. And more than half of CISOs say their cyber tech is inadequate to the more advanced threats (see Figure 3).

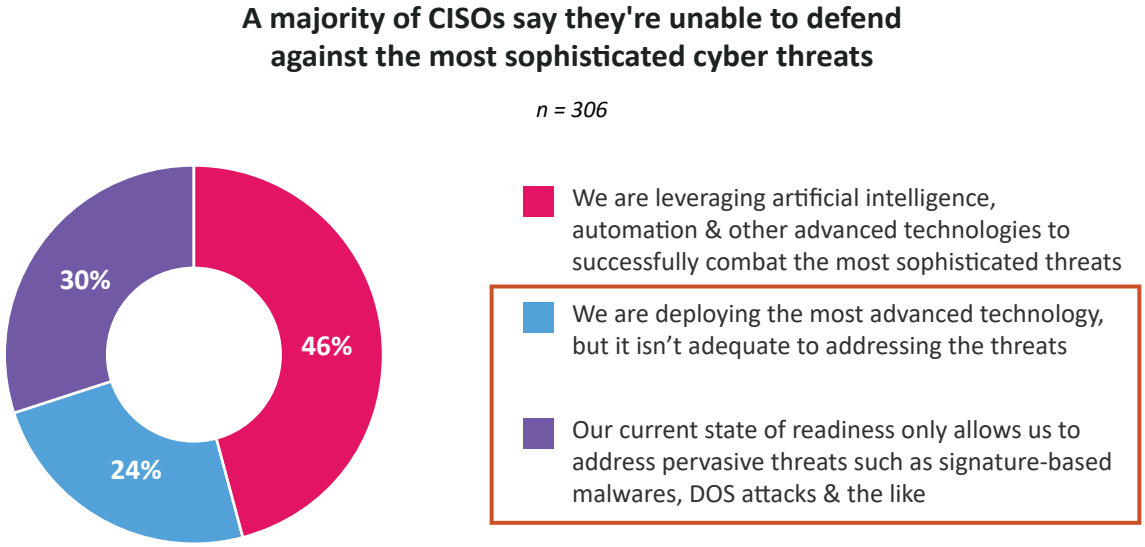


Figure 3

Cyber executives' top 3 challenges

1. Skill sets to manage, engineer, and support cybersecurity technology
2. Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.)
3. Assessing cyber risks and quantifying relevant costs

What impact has pervasive migration to cloud platforms had on their security posture?

Back in 2018, a survey of CIOs conducted by industry analyst firm IDG Communications found that "nearly 60 percent believe apps that touch critical data and systems must remain on-premises for security reasons."[2] A threshold seems to have been crossed, with now more than 60% of surveyed CISOs and CROs saying their companies have decided that the security of cloud platforms is at least as secure as — and over a third believe even more secure than — on-premises servers or traditional data centers (see Figure 4). And the more successful a company is, the more likely they are to regard the cloud as the more secure option.

Most companies find cloud platforms as or more secure compared to on-premises infrastructures

n = 607

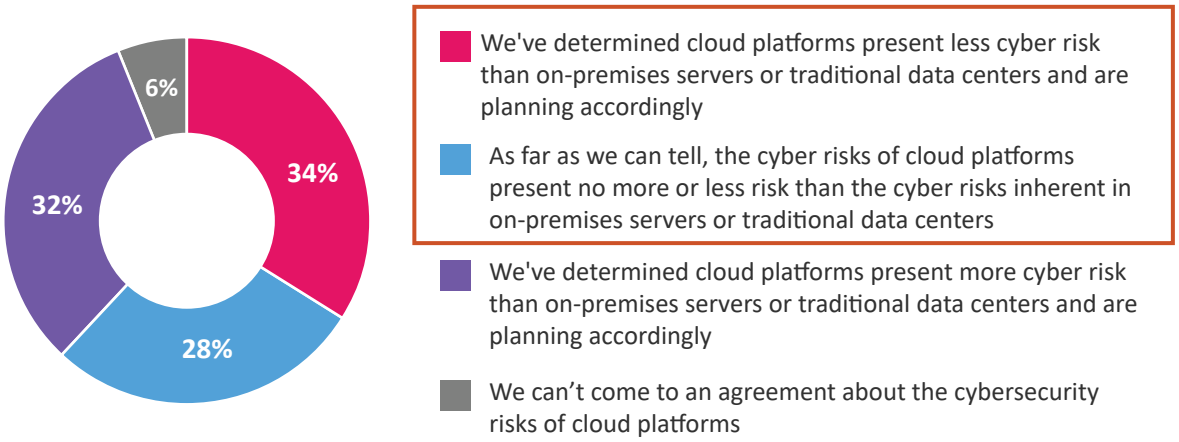


Figure 4

[2]Enterprise CIO, "Why CIOs say the cloud isn't replacing on-premises systems," January 23, 2018: www.enterprise-cio.com/news/2018/jan/23/why-cios-say-cloud-isnt-replacing-premises-systems/

Top threats & priorities

Data theft, more sophisticated hacker tactics, and the lack of skills to combat them will be the primary concerns for cyber risk and security strategists in the near term. CISOs are most concerned with criminal incursions based on methods of deception that, psychologically, people are likely to fall prey to. These methods are known as "social engineering" attacks, which includes such techniques as creating "watering holes" (hole, pretexting, whaling, etc.), attacks leveraging AI/machine learning, and open-source exploitation. (See Figure 5.) Defending against these will require robust identity management for bots as well as people, leveraging high-quality security-as-a-service offerings, and the use of AI-aided tools to proactively detect and fight attacks.

Tactics which most concern CISOs when thinking about cybersecurity between now & 2025 *n = 306*	**Rank**
Advanced social engineering attacks (watering hole, pretexting, whaling, etc.)	1
Attacks leveraging AI/machine learning	2
Open-source exploitation	3
Crime-as-a-Service	4
Over-the-air (wireless chip) exploits	5
Web cache poisoning	6
Botnets	7
Chatbots	8

Figure 5

When asked which areas of the company CISOs and CROs expect to see the greatest number of cyberattacks, finance, customer databases, and research and development, were regarded as the top three. Similarly, in our own work with organizations, we also found that cyber criminals are most likely to target processes that can generate them cash (such as payments and receipts), customers' personal financial data, and a corporation's intellectual property.

These same top three corporate functions (in the same ranking order) were validated by the TCS 2021 Global Leadership Study[3] of corporate strategy leaders, operations vice presidents, and chief operating officers.

Corporate functions where CISOs & CROs expect to see the greatest number of cyberattacks between now & 2025 *n = 607*	**Rank**
Finance	1
Customer databases	2
R&D	3
Sales/ecommerce	4
Marketing	5
Manufacturing plants/production/procurement	6
Human resources	7
Legal	8
Distribution/supply chain	9
Ecosystem partners	10

Figure 6

Similar to the findings regarding board priorities (see Figure 2 earlier), the lack of concern for the digital ecosystem and its related domain, the distribution and supply chain — ranked tenth and ninth, respectively — is a cause for concern. Digital ecosystems may not yet warrant one of the top positions, and many respondents may only be worrying about what happens to their ecosystem partners insofar as it eventually affects the other nine. It may signal a lack of regard for threats they don't feel they have as much direct control over compared to the functions and offices they deal with regularly in their own companies. But given the interconnected nature of global business today, for only 15% of CISOs and 18% of CROs — or 16% of the total sample — to name the digital ecosystem as a concern among likely targets suggests a blind spot in corporate cyber risk and security strategy today.

Prioritizing threats involves both the likelihood of a successful attack and its impact. The two biggest threats facing one US financial services firm, its CRO told us, are a loss of data and an attack that disrupted the business. "The first one is more likely but potentially less impact," he says. "The second is less likely because of some of the controls we have. But if it does happen, it's going to have significant reputational damage and potential financial impact."

[3]TCS 2021 Global Leadership Study: www.tcs.com/perspectives/ceo

Tools, challenges & plans

To fight data theft, data protection and privacy tools are the primary defenses CISOs intend to deploy. Those are followed by cloud security management, and the emerging suite of more advanced defenses such as decentralized identity and 5G security solutions.

The more financially successful companies are also placing a premium on identity management, ranking it second in importance. Less successful companies ranked it seventh. (See Figure 7).

Where CISOs expect to prioritize their information security budget between now & 2025 *n = 306*	**Rank**	**Pacesetters**	**Followers**
Data protection & privacy	1	1	2
Cloud security management	2	3	1
Emerging security technologies (such as decentralized identity, 5G security, etc.)	3	6	4
Threat management (including ransomware protection)	4	5	3
Identity management	5	2	7
Managed detection & response	6	4	5
Governance, risk & compliance	7	8	6
Vulnerability remediation automation	8	7	7
Advisory consulting	9	9	10
Operating technology (OT) security	10	10	9

Figure 7

The challenges to implementing cybersecurity and risk mitigation tend to be more tactical than technical: a lack of skilled personnel, a changing work environment, and difficulty in assessing security risks and quantifying their costs are considered the biggest obstacles to improving security by CISOs and CROs (see Figure 8).

The greatest challenges to cybersecurity & risk mitigation initiatives according to CROs & CISOs *n = 607*	**Rank**
Skill sets to manage, engineer & support cybersecurity technology	1
Workforce changes/requirements (e.g., work from home, bring-your-own-device, etc.)	2
Assessing cyber risks & quantifying relevant costs	3
Reliance on legacy IT systems	4
Accumulated complexity of our own business processes & operations	5
Difficulty in demonstrating return on cybersecurity investments	6
Lack of collaboration across enterprise units (business, IT & security)	7
Lack of diversity (including of thought & experience) in staff assessing cyber risks & threats	8
Difficulty in mandating that our current vendors adopt advanced technologies & policies	9
Budget constraints	10
Competing interests for the board or senior leadership	11
Outdated, siloed & non-integrated security tools	12

Figure 8

Cyber leadership & alignment

Across banking and financial services, utilities, and media and information services, CISOs consistently ranked enhancing security governance and risk management (e.g., assessing the security posture of the company, defining controls and standards, etc.) as their top priority; in manufacturing, CISOs ranked it third, tied with acquiring or developing security talent, which also ranked third among all respondents (see Figure 9).

The US National Institute of Standards and Technology defines cyber resiliency as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.” For CROs, this means understanding their highest concentrations of risk, whether in information assets, suppliers, geographies, or other such elements; integrating the company’s cyber and business strategies; and identifying the most critical, but often little known, operations that support their core business (see Figure 10).

CISO work priorities *n = 306*	Rank
Enhancing security governance & risk management	1
Establishing a more robust cybersecurity strategy	2
Security talent acquisition & development	3
Strengthening enterprise-wide cyber hygiene	4
Enterprise-wide employee awareness & training	5
Implementing models like "zero trust"/perimeterless security	6
Executive/board mandates on cybersecurity risks	7
Regulatory or industry compliance mandates	8
Managing ecosystem & supply chain risks	9
Outsourcing our security operations	10

Figure 9

CRO cyber resiliency priorities *n = 301*	Rank
Understanding concentration risk	1
Integration of cyber & business strategies	2
Identification of critical operations for core business lines	3
Identification & clear ownership of digital assets	4
Plans for business continuity/disaster recovery	5
Measurements of resilience	6
Partnerships with industry groups, government agencies	7
Fostering an organizational culture of resiliency	8

Figure 10

One encouraging sign is that CISOs and CROs largely share top priorities. They include security governance, risk concentration and management, and the integration of cyber and business strategies.

As well as having similar priorities, CISOs and CROs believe they are successfully coordinating their work. In fact, over half (51%) say they confer with their counterparts at least weekly; 1 out of 8 do so daily. And the more financially successful the company, the more likely CISOs and CROs are to collaborate frequently (see Figure 11).

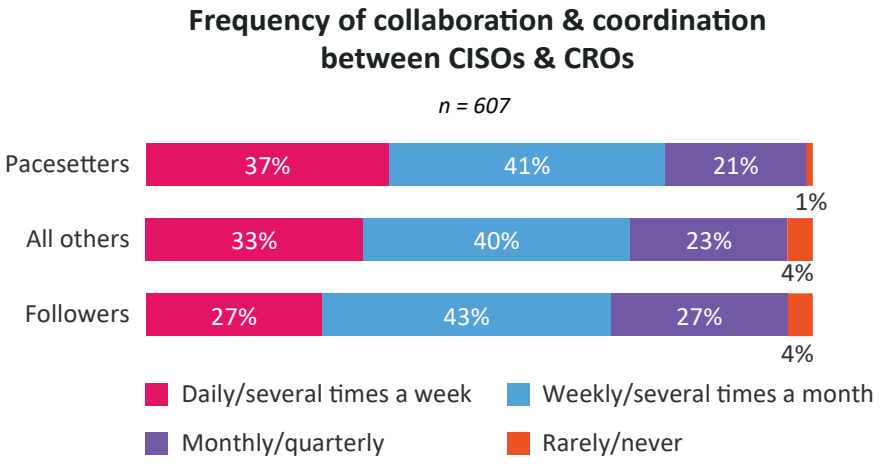


Figure 11

The CISO at a UK-based financial services firm told us he meets daily with his CRO counterpart, who he sees as an "absolutely critical stakeholder." He envisions himself as the first line of cybersecurity defense, with the CRO "the second line." Over time, he sees these two "lines of defense" overlapping, resulting in more and closer collaboration.

One example of such collaboration is data privacy, which requires tight integration between the data protection technology and processes executed by the CISO and the legal and regulatory understanding of the CRO. The CRO staff oversees "the collection of data, the fair processing of it, the sort of information governance aspect of it. I make sure that the custodian and owner are really doing their job in terms of access rights, that data loss prevention is working and tuned around the kind of data that we're most worried about," says the CISO.

The two teams meet monthly to discuss issues such as the business' data needs and any security events in a combination of objective reports and "a collaborative discussion-based aspect," he says.

"I would push the board and the CISO to say, 'Maybe [the defense against a current threat] needs higher spend to solve the problems now,' because who knows what we'll be tackling 12 months from now."

—CRO, US-based financial services firm

Sometimes the issue is not collaboration between CISOs and CROs but among CISOs in various business units. At one large US utility holding company, the CRO wanted help consolidating cybersecurity functions across its main organization and operating companies. A third-party review found the CISO of each holding company was operating independently not just of the corporate CISO's team, but from the CISOs in other business units. This lack of coordination resulted in duplicate spending for common projects, an inability to adopt lessons learned, inadequate security and risk mitigation training for employees, widespread non-compliance with control measures, and, ultimately, a cyber breach. Consolidating CISO governance helped in the short term, but the company still faces challenges in funding additional projects, training and awareness, and in making the organizational changes required to improve alignment among CISOs.

"I meet with my CISO all the time — two or three times a week at least," says the CRO of a US-based financial services firm. For each current or potential threat, they assess "is the risk going from green to amber to red? And if it's red, what sort of actions do we need to take and how are we progressing on the actions?"

They also review their response to successful or "near miss" attacks, with the CRO doing a root cause analysis of the failure and lessons learned for sharing with the corporate board and risk committee. He sees his role as "independently kicking the tires and testing and challenging" the security technology and processes suggested by the CISO to assure they fit the company's acceptable levels of risk.

In some cases, he says, he will lobby for more and faster security spending to counter fast-changing threats. "I would push the board and the CISO to say, 'Maybe [the defense against a current threat] needs higher spend to solve the problems now,' because who knows what we'll be tackling 12 months from now," he says.

Board & business unit engagement

As the ultimate decision makers and allocators of budget, boards of directors play an essential role in ensuring a proper focus on security. Our survey found mixed results about their engagement in security. Although 40% of boards discuss cyber risk and security issues very regularly, at every meeting or every meeting of a committee of the board, another 43% do so with some regularity, but only periodically, rather than proactively. And 1 in 6 boards address security occasionally or even never (See Figure 12).

In the last 12 months, how often has your company's board of directors (or a committee of the board) discussed cyber risk & security issues as an agenda item or in depth?

n = 607

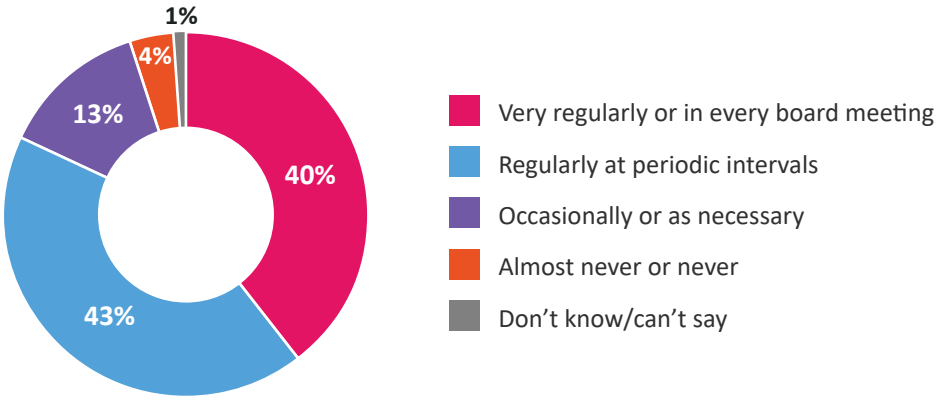


Figure 12

The CISO at a UK-based financial services firm says he briefs his board on security issues more frequently and longer than in years past, as more tech-savvy members join the board and members who sit on other boards bring their experience of security breaches at those firms.

In communicating with the board, he uses "a very formal, fact-based objective set of measures that turn the words in a risk appetite statement into numbers that can be measured by technical people," such as the IT organization's success at patching applications or limiting successful phishing attacks. "Then we hold people accountable for achieving those targets in public. And generally, that drives the behaviors we need," he explained.

He also combines "theoretical paper-based, KPI (key performance indicator)-driven mathematical analyses of risk with a description of 'here's what happened the last time we paid someone to hack us.' And that brings it to life … [and] gets the heart rate moving."

The CRO for a US financial services firm has seen his board's awareness of cyber threats increase dramatically. "They're extremely engaged on that topic. Five or seven years ago, it was a conversation on 'What does it really mean? Is this really our problem? Can this happen here?' Today, the conversation is, 'Of course, it can happen here.'"

Our research also showed Pacesetter firms' boards are the most engaged on the issues of cyber risk and security (see Figure 13).

In the last 12 months, how often has your company's board of directors (or a committee of the board) discussed cyber risk & security issues as an agenda item or in depth?

n = 607

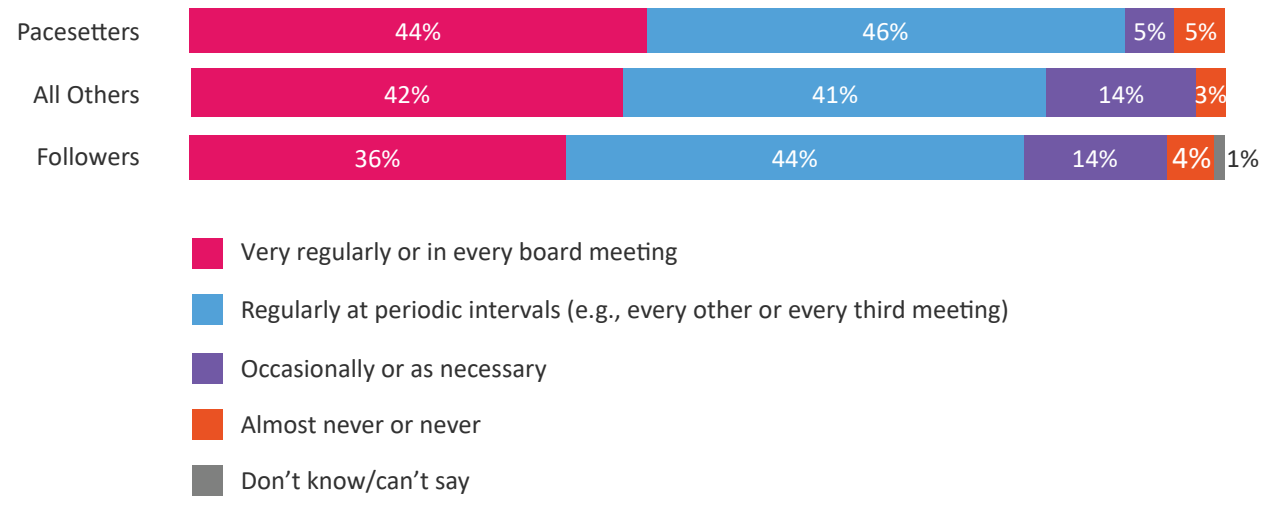


Figure 13

However, C-level executives and business unit leaders often put less of a priority on security, with one in five only engaging with cybersecurity after a breach or other attack has materially affected the business, our study found. Another third only address cybersecurity issues when it's brought to their attention, respondents noted.

How much attention is given to cyber risks & security issues by your firm's business unit leaders & its C-level executives?

n = 607

Figure 14

This disconnect between the board and C-level executives "is a really, really hot point," said the CISO at a UK-based financial services firm. "I don't know any CISO that's fully overcome it." Misalignment is often caused by a security team that wants to ensure every business function is secure and business unit heads that want to bring new products or business models to market quickly. When compromises must be made between security and speed, he added, how much of that decision "belongs to the CEO? How much of it belongs to the CTO? How much of it belongs to me?"

That can also lead to friction between CIOs and CISOs, the CISO for a US-based financial services firm says. CIOs, he noted, "want fast delivery, cheap delivery, low-operating cost from a technology perspective. They do want to have good security, but that comes second to having fast delivery, low cost, and quick implementation. So, the reality is the CIO and the CISO often find themselves at loggerheads."

The CISO at a US-based media firm told us he's seen increased attention to security from business unit heads after they've gone through tabletop security exercises and seen their counterparts in other organizations suffer security breaches.

Cloud platform security

As the hyperscale cloud providers — Amazon Web Services, Microsoft Azure, Google Cloud Platform, Alibaba AliCloud, and others — have improved their security and as more companies in every industry have moved their applications and data to the public cloud, businesses are becoming more comfortable with the security that cloud platforms offer. A majority of CISOs and CROs we surveyed (62%) said their companies now believe cloud platforms offer as good as or better security than on-premises servers and traditional data centers (see Figure 4 earlier). Yet about one-third of respondents — especially those who told us they were most concerned with data protection over data privacy — still believe the cloud is riskier than on-premises systems.

The trend, however, is clear: major cloud providers' business depends on securing their customer's operations and they have the resources to boost the security of their services. As the IT industry moves to more cloud-based infrastructures, whether in whole or as hybrid arrangements with more traditional data centers, cloud platforms and cloud-based services will increasingly provide as good as or better security than in-house data centers. That seems to be reflected in our study data by the fact that the more successful a company is (see Figure 15) and the more confident its executives feel about its posture toward both internal cyber risks and external hacker threats (see Figure 16), the more likely the company is to trust its data and processes to the cloud.

Enterprise attitudes toward cloud platforms

n = 607

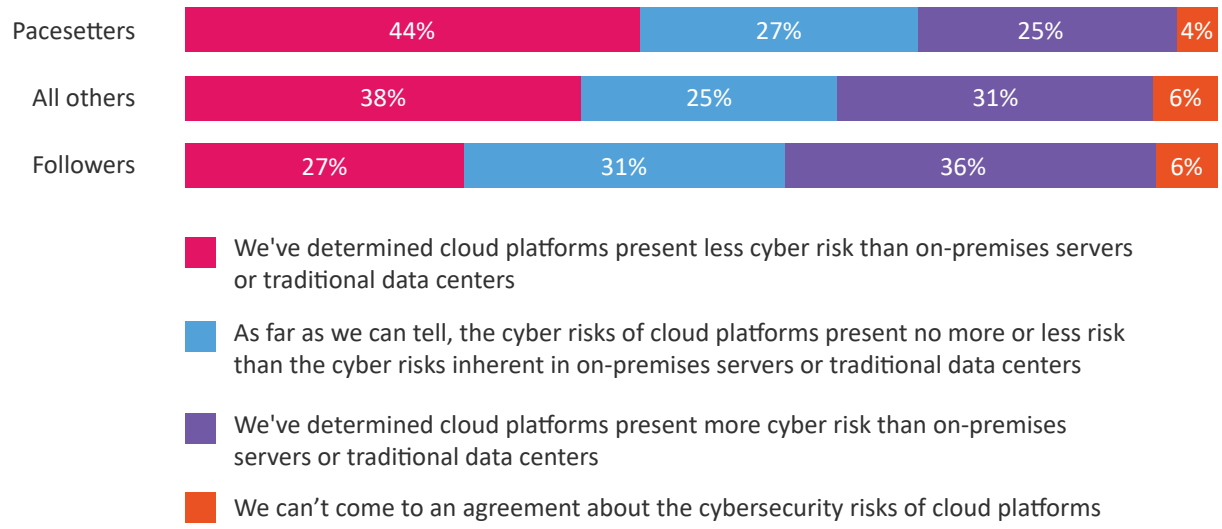


Figure 15

Perceptions of external/internal risks & threats, vs enterprise attitudes toward cloud platforms

n = 607
not shown: can't come to an agreement about cybersecurity risk of cloud platforms

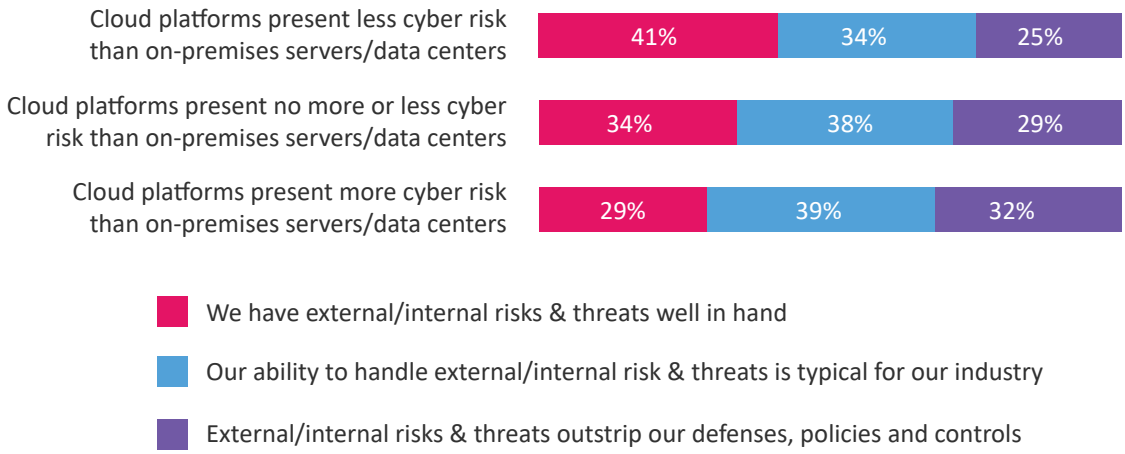


Figure 16

Companies choosing to host their data on-premises may often be limited to older security solutions and tactics rather than the state-of-the-art cybersecurity available in cloud platforms — a risky position as cyber defense develops further and faster into an arms race.

Even organizations that, for regulatory and other reasons, choose to keep some applications and data in-house can use cloud-based security services to leverage the latest security technology and tactics. This assumes, however, that they identify and prioritize protection of their most critical data and computing resources with the most current capabilities, such as encryption on the fly and zero-trust security, regardless of where their data is stored.

One risk is not the applications that move to the cloud, but those older vulnerable applications that never make it as planned, said the CISO for a US-based financial services company. Known vulnerabilities in the legacy system aren't always fixed, he explained, because that work would be thrown away when "application XYZ [migrates] to the cloud in six months." A year and a half later, the same app is still running on legacy, on-premises hardware with the same vulnerabilities. "That situation happens 1,000 times a day across corporate America and the world. And it's a challenge because those are the exact applications and entry points that are getting hit by the bad guys."

Finally, the CISO for the UK-based financial services firm noted that any application or database on the cloud must be correctly configured if it is to be secure. "[We] see so many cloud breaches that are a result of misconfigurations. And those misconfigurations are not necessarily because people didn't understand the technical [aspects]. They just haven't thought about what they needed properly. And that requires in-house knowledge."

Investment & skills

Keeping abreast of the most advanced tactics of cyber criminals is less cost-related and more about spending the available budget wisely. In fact, our study found that budget constraints rank low — tenth out of 12 choices — on the list of obstacles to effective cybersecurity and risk mitigation initiatives (see Figure 8 earlier). And only 8% of respondents cite it as the primary obstacle. Difficulty in demonstrating a return on the investment in cyber risk and security capabilities ranks only sixth. Similarly, the continued use of outdated, siloed, and non-integrated security tools — often a budget-related issue, when it arises — is also not generally a major obstacle, ranking last.

In fact, two-thirds (67%) of CISOs and nearly half (47%) of CROs saw a budget increase last year (see Figure 17). Of those that saw an increase, CISO departments averaged an estimated[4] 18% budget increase over the previous year; CRO departments averaged an estimated 13% budget increase. (The average estimated decrease for each was around 10%.)

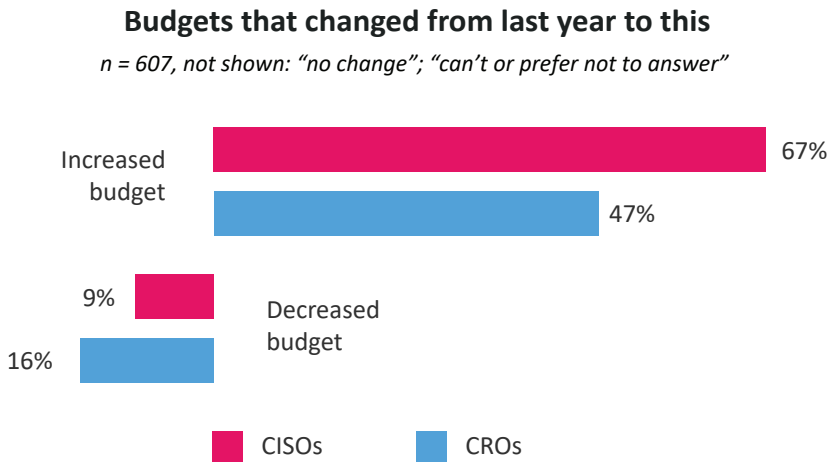


Figure 17

Paying for the right capabilities is less of a problem than finding and keeping the right skills to make the best use of those capabilities. A lack of security skills was cited as a top challenge for most respondents. And indeed, more than 4 in 10 respondents said they had difficulty this past year either recruiting top talent with cyber risk and security skills, difficulty retaining talent with those skills, or both (see Figure 18). While this has been an issue across the IT industry in the last couple of years, cybersecurity skills are especially in demand. One estimate[5] for the US labor market says that cybersecurity roles will sit unfilled 21% longer than do other IT jobs.

[4]Estimates based on average of reported range midpoints.
[5]CyberSeek, April 2022: www.cyberseek.org

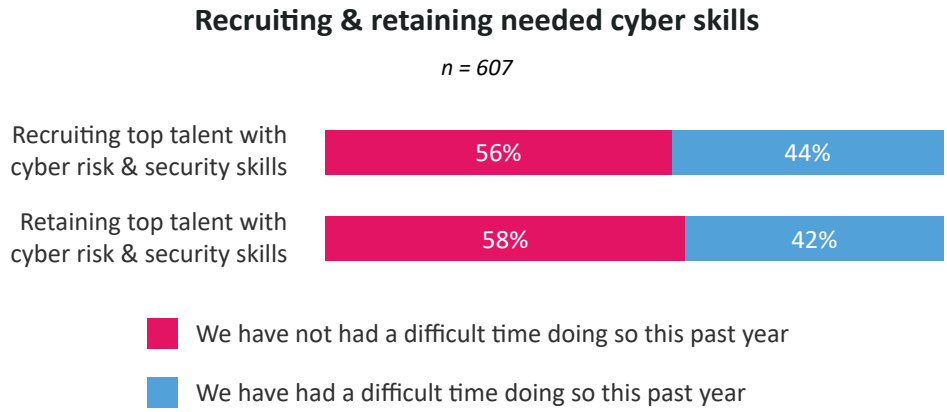


Figure 18

While there is no single solution to the staffing challenge, our report shows that the more frequently the board engages in risk and cybersecurity (see Figure 19), the more proactively the C-suite engages on it (see Figure 20), and the more open to cloud computing the company is (see Figure 21), the more successful the company is in finding and holding onto their top talent with cyber risk and security skills.

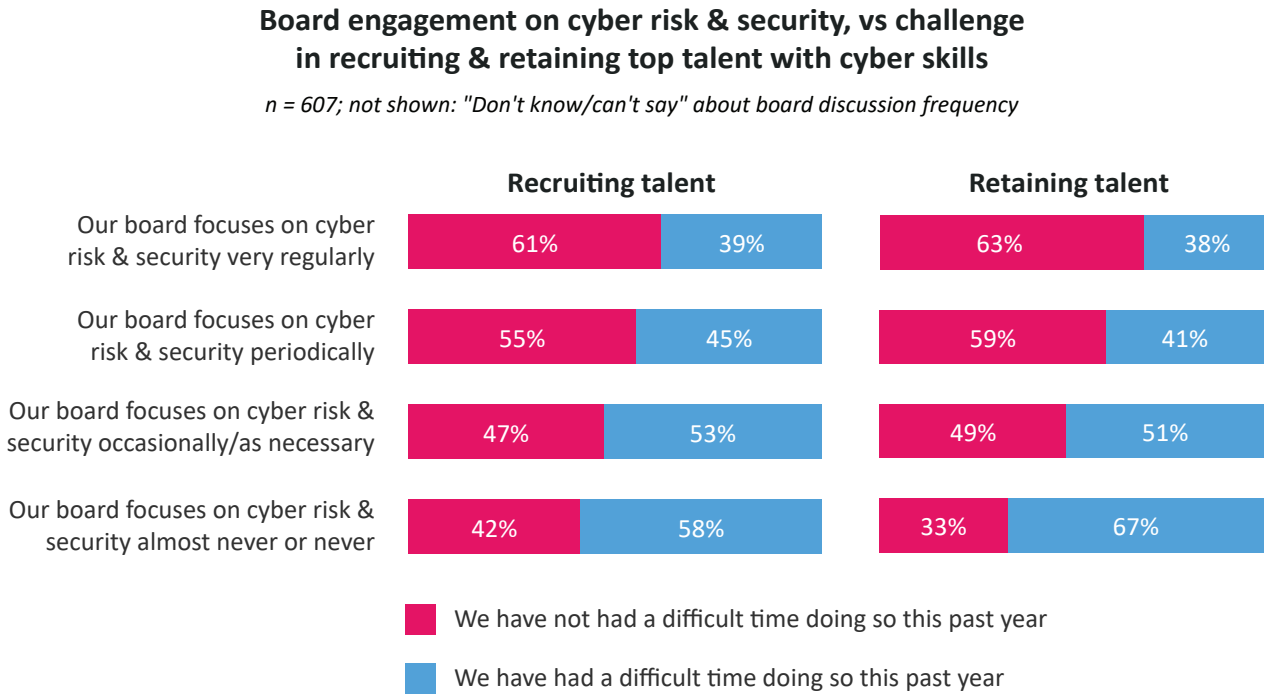


Figure 19

C-suite & business unit engagement on cyber risk & security, vs challenge in recruiting & retaining top talent with cyber skills

n = 607; combined "recruiting" & "retention" answers

Figure 20

Embrace of cloud platforms, vs challenge in recruiting & retaining top talent with cyber skills

n = 607; combined "recruiting" & "retention" answers;
not shown: "We can't come to an agreement on cloud"

Figure 21

Our recommendations

The findings from this study and TCS' work with companies worldwide suggest some recommendations as best practices for enterprises today.

Chart a long-term strategy that aligns security technology and functions around both regulatory compliance and protecting the applications, data, and infrastructure most critical to the business.

Educate top management about the damage security breaches can cause through financial loss, damage to company and brand reputation, and the loss of company data. Supplement statistics and hypothetical scenarios with real-world examples and the results of penetration tests.

Take an integrated approach to governance and implementation of cybersecurity that makes it the responsibility of all functional and business units in the enterprise as well as third parties and vendors involved with relevant processes.

Build on the knowledge and experience of staff in business lines to identify and implement steps needed to bring cybersecurity controls in line with time-tested security frameworks and keep the enterprise operating without interruption.

> The CISO at a US-based media firm told us he's seen increased attention to security from business unit heads after they've gone through tabletop security exercises and seen their counterparts in other organizations suffer security breaches.

For example, after a data breach a global biotech firm realized the need for increased focus by senior managers and increased collaboration among business units. Multiple assessments by external vendors showed the need to increase responsibility of multiple business units for cybersecurity functions, as well as to increase collaboration among them and sharpen the focus by senior management on the responsibilities of groups including IT, information security, enterprise risk management, HR, finance, legal, and compliance. The increased focus by the board led to annual assessments and a notable improvement in how well the company aligned its spending to reducing cyber risk.

Consider creating a board-level committee charged specifically with cyber risk and security.

This takes pressure off audit committees that often have far too many other responsibilities to give regular and sustained attention to rapidly evolving cyber threats. In addition to strong business operations

backgrounds, the members of this new Cyber Risk and Security committee should have a strong familiarity with the enterprise IT landscape either as providers, practitioners, or customers of advanced technology. At the very least, update the board regularly and frequently on cyber risks and mitigation efforts. When updating the full board, each C-suite and business unit should include the cyber risk and security implications of any planned activities, indicating their alignment with corporate-wide cybersecurity initiatives and strategy.

Attention to security from regulators and even investors is driving increased board engagement on the issues of cyber risk and security. Following the invasion of Ukraine, for example, the US Department of Homeland Security advised boards of directors to improve their internal oversight and coordination of cybersecurity activities.[6] Among its recommendations were that CISOs be empowered to act across the organization and that boards and senior managers participate in tests of cyber response plans, focusing their enterprises on resiliency and understanding their companies' plans for worst-case scenarios.

Less than two weeks later, the US Securities and Exchange Commission proposed new rules[7] requiring publicly traded companies to provide more information about their security posture in regulatory filings. These include disclosure about the board's oversight of cybersecurity risk, management's role in assessing and managing such risk, management's cybersecurity expertise, its role in implementing cybersecurity policies, procedures, and strategies, and whether and what expertise board members have in cybersecurity.

Focus on cyber resilience because even the best-guarded organization can become a victim of a malicious cyber breach.

A serious effort to enhance cyber resilience should include establishing a program dedicated to this important goal and led by an individual whose ideal background would be a combination of both information technology and business experience. This person would be explicitly supported by senior leadership and work in partnership with business executives, with authority to examine current cyber processes, systems, and data in the various IT and business units and advocate resiliency improvements. He or she would function as the cyber resiliency champion for the organization and should drive fortification of core business processes in order to build resilience against cyber threats.

The CROs we polled said their top resiliency priorities are understanding where risk is most concentrated, integrating their cyber defense and business strategies, and identifying the critical operations in core lines of business.

Because it's so difficult to accurately predict the likelihood of a successful attack, "I've been advising our executive team and the board that we need to focus on the impact" and how to alleviate it, says the CISO at a US water utility.

"We sit down with our business owners and the folks that run the operations and say, `What would your worst day look like?'" and then they identify the types of cyberattacks that could cause them. The team then gives the board examples, such as: "A major ransomware event can cost up to two weeks downturn on our operations. This is the amount of [bottled] water we would have to deliver when our system is not available, and this is the impact to our customer." For each critical business process, he then works with the business owners to understand what it would take to meet its recovery time objective — that is, the target period it takes to restore a business service.

---

[6]Cybersecurity & Infrastructure Security Agency, memo to members of the National Association of Corporate Directors, February 25, 2022: www.nacdonline.org/files/CISANote.pdf

[7]Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 23, 2022: www.federalregister.gov/documents/2022/03/23/2022-05480/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

Embed security as a foundational layer in every aspect of the organization.

From initial planning to end-of-life cycle, boardrooms to far-flung third-party partners, security must be embedded within every aspect of an organization, or the enterprise will, by definition, remain unsecured. Treat security measures as a critical element of design and operations at the foundational layer, and deeply embed it within the company culture.

One example is extending more advanced security methods such as multifactor authentication that combines a user's identity, a device they have (such as a smartphone), and something they know, such as a password, to even consumer-facing applications, where appropriate.

Another example of "built-in" security is security and privacy controls that move with data as it is transferred across internal and external security boundaries, using encryption, hashing, aggregation, and other best practices.

Business today runs on data, and development and maintenance of the code that uses that data should have cybersecurity integrated into the life cycle of all IT projects. Commonly referred to as "DevSecOps" (for "development, security, and operations"), such environments integrate security end-to-end in the life cycle of digital work, rather than "bolting it on" after the fact. Automating the inclusion of application security as part of a normal Agile development framework makes the product, service, or process more likely to be successful and to receive buy-in from stakeholders.

Make supply chain and partner ecosystem security a higher priority.

Maintain open, regular channels of communication and collaboration about security with partners, suppliers, vendors, and distributors. Boards of directors, CISOs, and CROs — across several measures — are not yet focusing as strongly as they should on the ecosystem risks or on collaboration for oversight, monitoring, and mitigation of those risks. For example, enterprise software today leverages huge libraries of APIs (application programming interfaces), which passes data from one application to another, often — although certainly not exclusively — using internet protocols. Besides interconnectivity, one benefit of APIs is that, if designed securely, they can allow two applications to interact without revealing the inner workings of either application. However, these connections can be exploited if security corners were cut or ignored in the development of the API. In fact, in our study, CISOs cited "open-source exploitation" as the third most alarming threat they expect to face more of between now and 2025. (See Figure 5 earlier.)

Despite this concern by CISOs for the points where the digital ecosystem is glued together, they also rated "ecosystem partners" last in their list of cyber target concerns. And of priorities arising out of board-level discussions, "focusing on ecosystem risks and collaboration for oversight, monitoring, and mitigation of those risks" was cited as the top priority by only 14% of respondents. CISOs also ranked "managing ecosystem and supply chain risks" as next to last (out of 10) when asked about their own departmental priorities.

But visibility between organizations is necessary for the leaders of service providers, suppliers, and distribution partners to maintain a higher level of security for major endeavors that involve many players. Ransomware and other hacker threats are increasingly relying on the open door often provided by unsecured systems run by contractors, vendors, and suppliers.

The CISO at a US-based financial services firm sees vendors, including those who serve his primary vendors, as his second-highest threat vector "just because we don't have as much visibility" into vendors with whom

they may not have a close relationship. To learn more, he asks them to complete security questionnaires, audit their security practices, and test their security practices in a controlled setting.

The CISO of the US-based media company told us his company includes security requirements in its contracts with any vendor that can access its network or hosts critical information or services. Among the requirements, he noted, are that they have someone in charge of security, "implemented policies and practices that help secure the environment, and that they notify us within 24 to 48 hours if there's an incident." Resistance from vendors to such language is declining, he explained, as regulators begin pressuring all companies to divulge more of their security practices.

One Europe-based manufacturer requires vendors accessing their systems to use multifactor authentication, dedicated VPN tunneling, and establishes tight limits to the information they can see. "We actually put together standard contractor clauses to make sure everyone is signing up on the same level of security that we are willing to support and also opening up to audit from a third party," the company's CISO told us.

Leverage the cloud and cloud services to enhance your security profile.

Cloud-positive organizations seem to have a slight advantage in retaining and recruiting talent with cyber skills, compared to those companies who think on-premises or traditional data center security is preferable to what's available via the cloud (see Figure 21 earlier). This makes sense, since more and more computer science and business graduates today assume a cloud-based environment and marketplace as the rule, rather than the exception. Additionally, our study data shows that organizations that see cloud platforms' security capabilities as an improvement over on-premises infrastructures are likely to be more successful in terms of revenue and profit (see Figure 15 earlier).

As your firm modernizes or replaces applications with cloud-based platforms, maintain cybersecurity vigilance and regulatory compliance by weaving established cybersecurity frameworks into cloud adoption, including insight into third-party vendors' compliance with cybersecurity controls. In the event of a breach, this would establish evidence for demonstrating compliance, from both a maturity and assurance perspective.

Integrating on-premises and cloud security is not easy, the CISO for a US-based manufacturing firm told us. It requires the right level of oversight into which users are accessing which systems, either on-premises or in the cloud, and what they are doing with the data on both platforms. "All of those monitoring tools will have to be integrated with your strategy," and the security operations team must ensure any potential breaches are correctly investigated, he says.

Coordinate the cybersecurity and risk functions closely.

CISOs and CROs should coordinate at least weekly to ensure the company's strategic interests, its approach to risk, and its cybersecurity initiatives are aligned and evolve as technologies and business needs change. Our study found that frequent collaboration between the CISO and CRO offices correlates with corporate financial success (see Figure 11 earlier).

Such collaboration can also help a company determine when overly strict security measures might negatively impact the business. For example, while the CRO might want robust authentication for every user of every application to meet the requirements of a security framework, the CISO might seek an exemption for an

e-commerce web site to avoid presenting potential customers with an off-putting authentication requirement before they can enter a storefront and make a purchase.

At a US-based media firm, the CISO and a vice president filling the CRO role run joint continuity planning exercises for events such as security breaches or natural disasters. The CISO draws on the risk unit's rigorous processes and connections to key stakeholders to encourage adoption of cybersecurity capabilities. Since two other companies in their industry suffered cyberattacks, the CISO office and risk unit are working even more closely to understand and mitigate the impact of an event on the business.

> The CISO at a UK-based financial services firm told us he meets daily with his CRO counterpart, who he sees as an "absolutely critical stakeholder." He envisions himself as the first line of cybersecurity defense, with the CRO "the second line." Over time, he sees these two "lines of defense" overlapping, resulting in more and closer collaboration.

CISOs and CROs at publicly traded companies will also need to bring investor relations into their discussions as investors pay more attention to cyber risk and security as part of an increased focus on environmental, social, and governance (ESG) issues, says the CISO for a UK-based financial services firm. The CISO and CRO can help investor relations, along with senior management and the board, understand the damage successful cyberattacks can do to a company's share price, market share, and reputation.

Confidence in the face of certain attack

As the CROs and CISOs of large companies realize, the question of cyberattacks is no longer "if" but "where" and "how." Most large enterprises today are already dedicating sizable headcount and operating budgets to identifying risks, defending the company against threats, and mitigating the effects of the attacks that are already occurring. Companies in every industry, government bodies, and non-governmental organizations are all experiencing an unprecedented level of attacks from freelance hackers, state-sponsored cyber terrorists, and criminal consortia-for-hire. It's an arms race that requires staying one step ahead of malefactors just to continue doing business in today's increasingly interconnected digital ecosystem.

Yet, as this first-ever TCS study of enterprise risk and cybersecurity professionals shows, there is good news. For one thing, funding for cybersecurity and risk mitigation initiatives isn't generally a problem (see Figure 8 earlier). For another, taking all other factors into consideration, 60% of cyber risk and security executives feel some confidence their company will be able to avoid a major cyber event that results in significant financial loss or reputational damage (see Figure 22). They know they'll be attacked, but they are either cautiously confident or (for 14%) even very confident they will weather the onslaught.

CISO & CRO confidence in their company's ability to avoid a major cyber incident in the next 3 years resulting in significant financial or reputational loss

n = 607

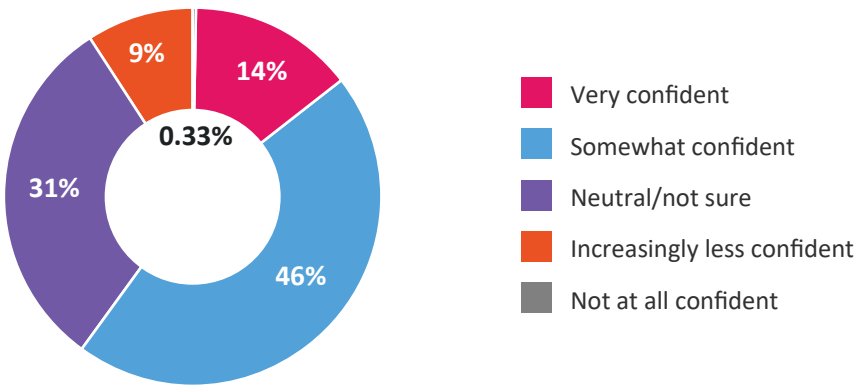


Figure 22

Companies that have already adopted or adapted several of the recommendations in this report enjoy even greater confidence in their ability to withstand the worst effects of a cyberattack. For example, companies where the board takes a proactive approach to cyber risk and security and where the CISOs and CROs collaborate and coordinate frequently are both more likely to have cyber risk and security executives with a degree of confidence greater than cyber executives at companies where the board is less engaged and where coordination is more perfunctory or an after-thought (see Figure 23).

Confidence in avoiding a major cyber incident resulting in financial loss or reputational damage between now & 2025

n = 607; not shown: "Don't know/can't say" on board discussion frequency

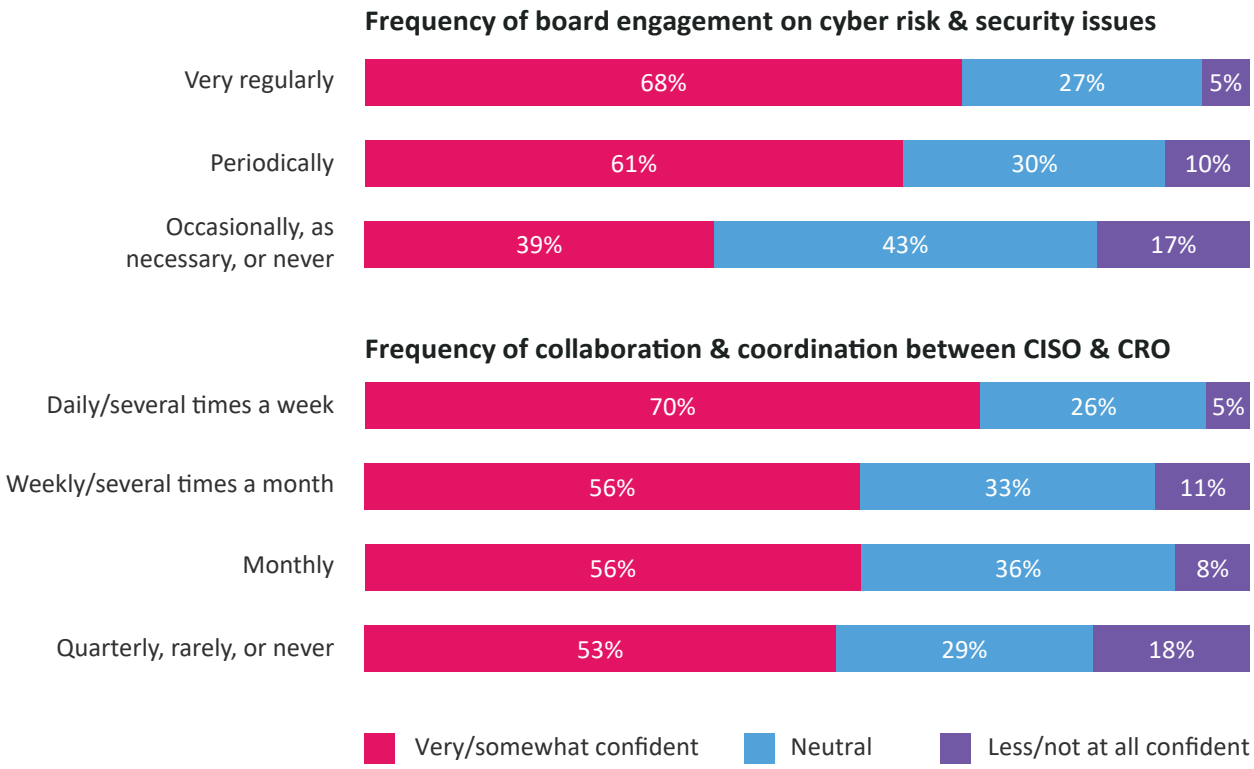


Figure 23

However, too many businesses still feel they cannot adequately protect themselves against today's threats, much less emerging dangers such as AI-aided attacks. While boards are increasingly focused on cyber risk and security, C-suites and lines of business are still mostly only focusing on the issue when it's brought to their attention; 18% of C-suites only focus on it after the organization has already been attacked (see Figure 14 earlier). A lack of security skills is a constant and difficult to meet challenge, which further complicates the challenge (see Figure 8 earlier).

Our study and work with enterprises show a path forward: Looking beyond technology to improved collaboration and security and data protection processes. Establishing formal mechanisms for collaboration to ensure all stakeholders agree on the data and applications that most need protection and coordinate the purchase and use of tools to protect them, with a complete accounting of the myriad software solutions different departments and businesses have deployed. Secure, advanced processes that leverage automation for data migration, protection, access control, and training can mitigate many of the most common risks.

To meet emerging risks, we recommend businesses require leadership across the organization to align its security spending and efforts on the most critical risks, ensuring that all stakeholders have the information they need to identify and assess risks and can work together to improve cyber resilience.

Companies can help fill the skills gap by using external service providers for harder-to-staff work, such as 24/7 network monitoring, while growing talent internally by giving them exposure to not only the technical but the business aspects of cybersecurity. Expand your pool of talent by seeking out more diverse recruits, and don't underestimate the importance of a high-quality workplace in retaining that talent.

Cyber security will always be an ongoing arms race between defenders who must protect every system and database all the time against all threats, and attackers who only need to find one vulnerability to steal data, bring down systems, or hold data for ransom. No CIO, CISO, or CRO can guarantee their organization will never be hacked.

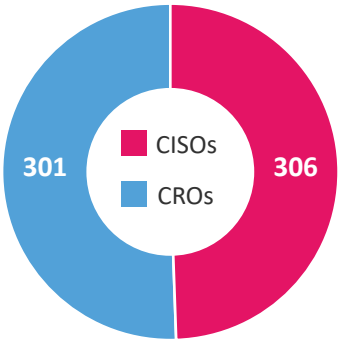
However, the most successful organizations can secure the most critical assets with the best use of their available funds by:

- Gaining high-level support for coordinated dynamic cybersecurity measures focused on the applications and data most critical to the business;
- Investing the time and effort required to align all stakeholders with those priorities;
- Leveraging the cloud, and cloud-based security services, to tap the most current defenses against ever-changing threats;
- Building and testing resiliency plans so you can recover the most important parts of your business if an attack succeeds; and
- Becoming a preferred employer to attract and develop internal talent for the security functions you need to do in-house, while leveraging outside providers for work requiring industry-leading expertise.

Methodology

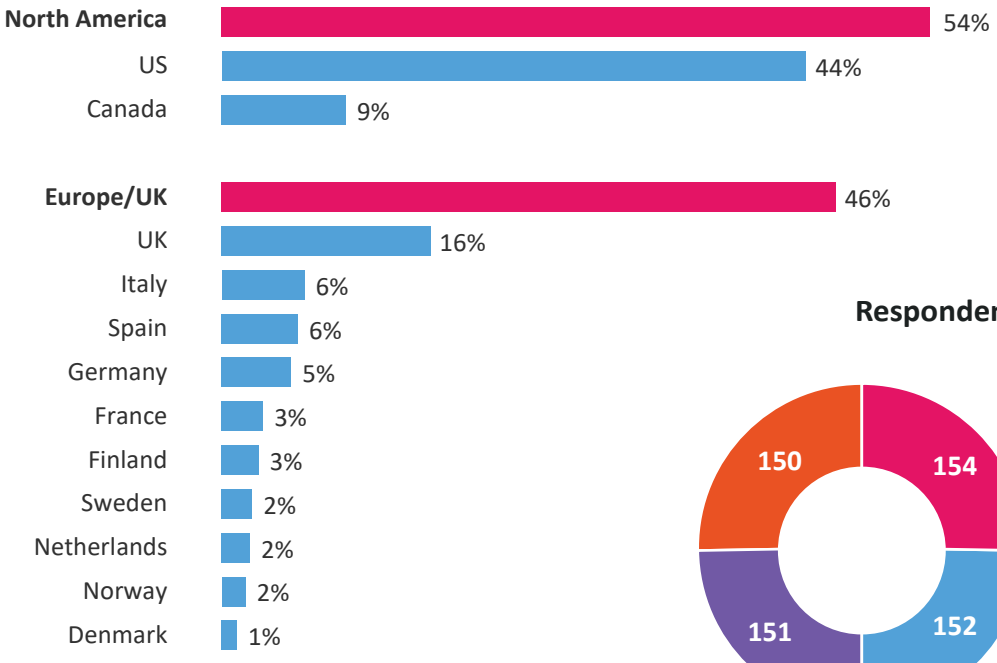
We surveyed 607 security professionals, split between chief information security officers (CISOs) and chief risk officers (CROs) in North America and Europe between February 15 and March 21, 2022. Respondents represented the banking and financial services, utilities, media and information services, and manufacturing industries, given the increasing number of cyberattacks being experienced by these industries in particular. Approximately half of respondents were CISOs and half CROs. This report is based on their responses and on in-depth interviews with other CISOs and CROs in the geographies and industries represented in our survey.

Respondents by role

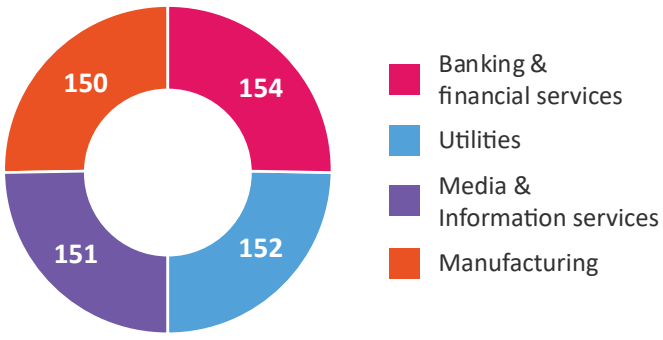


Respondents by region & country

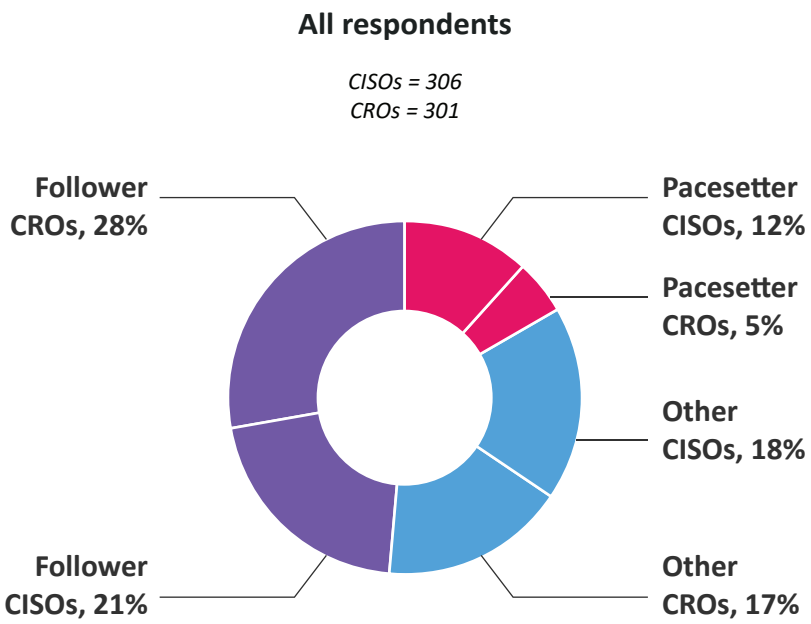
n = 607



Respondents by industry



As part of the analysis, the most successful companies — those who had both revenue and net profit changes from 2017 to 2021 that were higher than the average of all the companies surveyed in their industry (or, if at least 30 companies existed for a subsector, in their subsector) — were deemed "Pacesetters." Those whose revenue and net profit growth were both lower than the industry or subsector average were, for comparison purposes, considered "Followers."



Percentages in charts may not add up to 100% due to rounding

Executive champions

Santha Subramoni
Global Head, Cyber Security Services, TCS

Margareta Petrovic
Managing Partner, Risk & Cyber Strategy, TCS

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

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 TCS Thought Leadership Institute at TL.Institute@tcs.com

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 50 years. TCS offers a consulting-led, cognitive powered, integrated portfolio of business, technology and engineering services and solutions. This 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 592,000 of the world's best-trained consultants in 46 countries. The company generated consolidated revenues of US $25.7 billion in the fiscal year ended March 31, 2022 and is listed on the BSE (formerly Bombay Stock Exchange) and the NSE (National Stock Exchange) 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 us at www.tcs.com.

Visit **www.tcs.com** and follow TCS news **@TCS_News**.