CSC

We are the business behind business®

The CISO Outlook 2025

Navigating evolving domain-based threats in an era of AI and tightening regulation

Driven in part by the rapid rise of artificial intelligence (AI), the variety and intensity of cybersecurity threats to organizations continue to expand.

Today's bad actors have access to increasingly sophisticated methods—including deepfakes and domain generation algorithms (DGAs)—posing a growing challenge for businesses to anticipate and defend against. At the same time, chief information security officers (CISOs) and their teams must continue to guard against more established security threats such as distributed denial of service (DDoS) attacks. Such incidents still put companies at risk, despite measures and efforts over the years to curb their impact.

In Q1 2025, CSC commissioned independent research among CISOs, chief information officers (CIOs), and other senior IT professionals to understand more about their current concerns. We set out to understand evolving cyber threats, the current state of IT security budgets, how cybersecurity professionals are coping with tightening and evolving levels of regulation, and how teams are using security policies and technology to keep organizations safe.

Our study found almost three quarters (70%) of respondents believe that security threats will increase in the year ahead; almost all (98%) predict an increase in the next three years. Almost nine in 10 (87%) believe that DGAs powered by AI pose a threat.

There's no doubt that CISOs will continue to be challenged by security threats. Our job is to keep developing better ways to control both residual risks and newer threat vectors.

OUR EXPERTS

Ihab Shraim
Chief Technology Officer, CSC's Digital Brand Services

Nina Hrichak
Vice President of EMEA Account Management, CSC's Digital Brand Services

Mark Flegg
Senior Director of Technology, Security Products and Services, CSC's Digital Brand Services

Mark Eggleston
CSC Chief Information Security Officer

What CISOs are saying: A snapshot

We surveyed 300 CISOs, CIOs, and heads of IT in Q1 2025 and found that cybersecurity threats are material risks that are becoming more challenging.

67%

of respondents said cybersecurity threats were either critical or significant in 2024.

70%

expect an increase in threats in 2025.

98%

believe risks will rise over the next three years.

Domain and DNS threats will dominate the threat landscape

The top three security threats in 2024 were cited as:

1. Cybersquatting
2. Domain and domain name system (DNS) hijacking
3. DDoS attacks

4. *Ransomware and malware*
5. *Social media cyber attacks and defamation*
6. *Phishing and social engineering*
7. *Other*

The top three expected threats over the next three years are:

1. Cybersquatting
2. Domain and DNS hijacking
3. Ransomware and malware

4. *DDoS attacks*
5. *Social media cyber attacks and defamation*
6. *Phishing and social engineering*
7. *Other*

The adoption of outsourcing services for cybersecurity is widespread but inconsistent

Almost half our respondents said they mainly use in-house systems, processes, and staff, but outsource to specialists to a limited degree.

Just under a fifth (18%) in-source exclusively.

Almost a third (30%) outsource to specialists but also use in-house resources.

AI will have a significant impact on cybersecurity

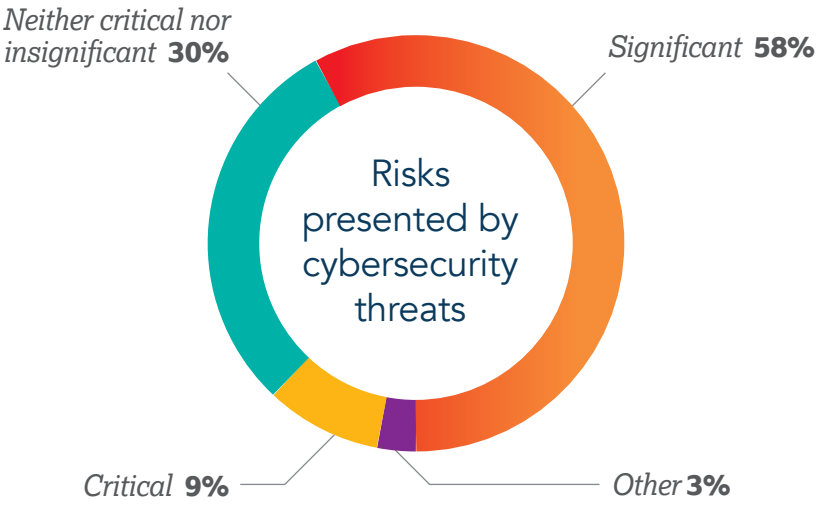
Almost nine in 10 (87%) believe that DGAs powered by AI pose a threat.

The vast majority (97%) said they're concerned about giving AI-based third-party systems access to company data.

Cyber threats are evolving—and only getting more complex

CISOs face a rising tide of ever-more sophisticated cyber threats. Worse, they predict the level of security challenges they face is only set to intensify.

Almost one in 10 (9%) of our respondents said the risks presented by cybersecurity threats were "critical" in 2024. Three fifths (58%) rated them as significant, meaning that two thirds (67%) thought risks were material. A further 30% said that risks were neither critical nor insignificant.



"CISOs have needed to deal with huge periods of transition, so it's understandable they feel the risks are so serious," says Mark Flegg, senior director of Technology, Security Products and Services, CSC's Digital Brand Services.

"As organizations began moving core systems away from in-house, on-premise infrastructure to the cloud, they opened up their IT environments to new threats. A perfect example is subdomain hijacking, or subdomain takeover, which wasn't as much of a concern 20 years ago—when firms ran their own data centers and rarely handed over IP address space or DNS control to third parties. Now IT systems are more easily penetrated, and we have bad actors looking for any opportunity to find gaps in the armor."

The risks presented by cyber threats will worsen in the months and years ahead, said our respondents. Almost three quarters (70%) expect an increase in 2025, with 5% saying the rise will be "significant;" 98% expect an increase over the next three years, with two thirds (66%) saying this will also be significant.

The rise of powerful AI-based capabilities means some domain-related threats are becoming more potent. For example, cybercriminals can use AI to scan for abandoned or misconfigured subdomains at remarkable scale, enabling subdomain takeovers.

Meanwhile a big challenge for CISOs is that most of the threats they have always faced are still causing problems, while the list of new potential attacks and methods continues to grow in both volume and complexity.

Cyber threats are growing more sophisticated, often combining multiple techniques to improve their chances of success. Many begin with some form of social engineering, sometimes paired with a tactic like lookalike domains, such as typosquatting, to increase credibility. These attacks serve as enablers, laying the groundwork for future threats.

Other examples include DNS tunneling to bypass security measures and transmit malware across a network, or compromising a third-party supplier's system and building on that access to steal data from a business.

> *"What we're seeing is that attacks such as ransomware don't happen in isolation, and that bad actors can then go on to steal information in hybrid or blended attacks, which could turn out to be truly devastating."*

Mark Eggleston
CSC Chief Information Security Officer

Domain-related threats dominate CISOs' concerns.

The top three security threats last year were named by respondents as cybersquatting, domain and DNS hijacking, and DDoS attacks.

Only 22% said they have the "right tools" in place. It's clear that CISOs feel they could do more to counter domain-based threats—and the need to strengthen resources is becoming more critical.

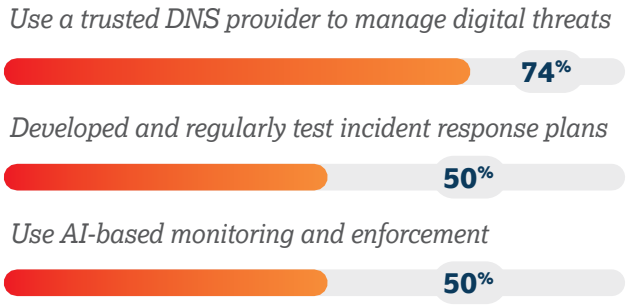
76% Three-quarters said they were "somewhat confident" about their company's ability to mitigate domain attacks; just 7% said they were "very confident."

99% In addition, almost all (99%) admit they're either somewhat or very concerned that their domain registrars were not following Know Your Customer (KYC) policies to verify the identity of clients and suppliers.

59% Nearly three fifths (59%) said when their firm detects domain-linked cyber threats, they have tools and processes in place to mitigate them, but it's a complex and time-consuming process to take threats down.

Three-quarters of respondents to our CISO Outlook 2025 use a trusted DNS provider to manage digital threats targeting their attack surface and digital assets.

50% have developed and regularly test incident response plans, and 50% use an AI-based monitoring and enforcement solution.



"The human element is still behind the biggest security risks, and the weakest link in any company is the lack of education within teams. DNS hijacking and subdomain takeovers are risks that some people are only now becoming aware of."

Nina Hrichak
Vice President of EMEA Account Management, CSC's Digital Brand Services

AI is playing a role in combating cyber threats—but its widespread use is still a cause for concern

There's no doubt AI is creating value for organizations globally. The CISOs and other senior leaders we spoke with said the biggest return on investment (ROI) in AI integration is process automation, followed by internal education and data analysis:

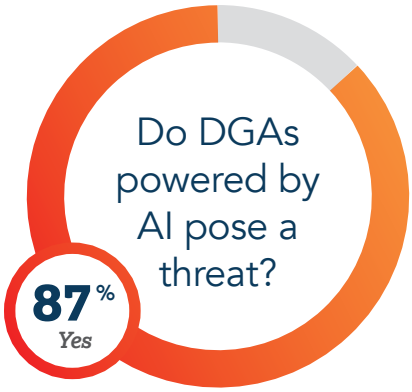
1. PROCESS AUTOMATION
2. INTERNAL EDUCATION AND STAFF TRAINING
3. CYBERSECURITY
4. FRAUD DETECTION
5. DATA ANALYSIS
6. QUERY RESPONSE

However, AI is clearly viewed as a double-edged sword in the security world, not least because it introduces the threat of employees and vendors uploading sensitive data to large language models (LLMs) like ChatGPT, as well as cyber criminals using AI to enhance tools such as DGAs.

"AI can be used for good because it helps us conduct research more quickly, so for example, it's a great way to conduct background work, though no one should be handing off GenAI materials without a human validating it because of the risk of error," explains Mark E. "However, it's also important to recognize that AI can be used for generating new threats such as deepfakes used for phishing."

Our respondents were almost unanimous in their concern over the risks of giving third-party AI-based systems access to company data.

The majority (87%) said that DGAs powered by AI pose a threat to their organization. Threat actors can generate large volumes of new domains that infringe on IP, sell counterfeit items, or support phishing schemes. The potential combination of keywords used in domains is almost endless.



The use of AI is also helping criminals build and launch complete campaigns—with persuasive messaging, fake websites, and automation tools—to attack organizations, warns Ihab.

"There are various platforms built with AI that enable bad actors to launch targeted campaigns against specific verticals, such as financial services," says Ihab. "These kits are designed to be comprehensive, making attacks more convincing. The misspellings and poor grammar we used to see are largely gone, as AI can produce highly accurate, polished messaging."

Organizations need to have a clear governance policy on who is accessing which LLMs within the organization and what information they're sharing. This includes being aware of the growing threat of Shadow AI, which is the unsanctioned use of AI tools or applications by employees or vendors.

EXPERT VIEW FROM IHAB SHRAIM, CHIEF TECHNOLOGY OFFICER, CSC'S DIGITAL BRAND SERVICES

Why domain-related threats are a growing challenge

"DNS and domain-related infrastructure are soft targets for cybercriminals, who use specific threat vectors like DNS hijacking or domain spoofing to exploit exposed systems.

"Bad actors conduct extensive reconnaissance—scanning everything from social media to job boards—to identify potential vulnerabilities, including disgruntled insiders who may be susceptible to phishing.

"They focus on the assets organizations must keep publicly accessible, such as DNS, websites, or email gateways, making it easier to launch precise attacks like cybersquatting or DNS cache poisoning.

"We're already seeing high volumes of these attacks, and we expect them to grow drastically in 2025, as more off-the-shelf tools and attack kits become widely available."

Ihab Shraim's top five measures to establish an AI governance policy

1. **Establish a clear AI policy.**
The top priority for any organization adopting AI is to create a formal policy that's communicated across the business.

2. **Set explicit data sharing rules.**
Clearly define what types of data employees can and cannot input into LLMs to minimize the risk of exposure.

3. **Use isolated environments for testing.**
When testing with AI models, run them in secure, private environments managed by the organization—rather than the cloud—to maintain control and reduce risk.

4. **Define specific use cases.**
AI models should be built with clear objectives, such as automating a particular function, to prevent unintended data contamination.

5. **Validate AI outputs.**
No one using AI should assume that AI-generated data is universally accurate—human oversight remains essential.

"You can contaminate a whole segment of the internet with false data as information gets repeated and reinforced across interconnected AI models," says Ihab. "Looking into the future, it will become even more challenging for technologists to carry out foundational checks on the data being used."

Ihab Shraim
Chief Technology Officer, CSC's Digital Brand Services

Focus on **Shadow AI**

In one way, Shadow AI can be seen as the latest in a long line of security threats that CISOs face when end users bypass IT governance, similar to when employees first adopted tools like Dropbox or brought their own mobile devices into the workplace without oversight.

In another, it's far more complex and insidious. Because many AI tools are cloud based and externally hosted, bad actors can exploit them to uncover vulnerabilities or misuse data unintentionally used by employees. The risks include data breaches and compliance failures if sensitive company or customer information is exposed through unauthorized use.

The answer to the problem of Shadow AI, says Mark E., is to use software agents that track all the LLMs used across an organization. "It means we can see who is uploading and downloading information from AI tools, and we can block the ones that are too risky. You then apply a zero-trust framework, validating users and enforcing control, to ensure everyone is following the organization's AI governance policy."

IT security budgets may not be keeping up with the growing cyber threat landscape.

Although cybersecurity is identified as a top business priority by large organizations, it can still be difficult to secure the budgets needed to protect against the growing range of threats and the huge data sets that organizations must manage.

"The problem is that there's no glossy return on investment from spending on cybersecurity," says Mark F.

"It's like buying insurance—everyone hates paying for it, but when it's time to file a claim, that policy is the best thing since sliced bread. Budget-conscious businesses still question whether the cost of protection is really justified."

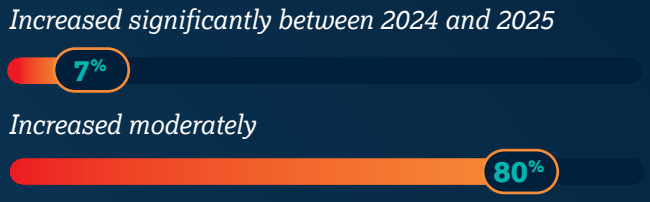
"You always have to plan for a higher budget year over year," adds Mark F. "The threats you've already been managing don't just disappear—so you still need funding for those, plus anything new that's emerged. CISOs have spent a lot of time building firewalls, pulling up the drawbridge to the castle—now they're finding that people are building tunnels beneath the moat."

One reason for the disconnect between the boardroom's cybersecurity priorities and funding is that decisions about domain security risks aren't always made by those who best understand their potential impact.

CISOs are taking steps to reconcile this discrepancy by discussing the real-world impact that domain-related threats can have, and many are engaging with senior colleagues to ensure threats are better understood.

Overall budget for cybersecurity and related information security and management.

Only 7% of respondents said their overall budget for cybersecurity and related information security and management had increased significantly between 2024 and 2025, while the majority (80%) said their budget had increased moderately.



Who is responsible for deciding cybersecurity allocations?

Allocations are most likely to be decided by the chief risk officer (CRO) or risk management teams (23%), CFO or finance team (21%), or by the CISO or IT team (18%).

The top five topics that CISOs discuss with other divisions relating to digital risks are ranked as follows:

1. REPUTATION AND FINANCIAL LOSS
2. CYBERSECURITY AND DATA PROTECTION
3. STRATEGIC PLANNING AND BUSINESS GOALS
4. BUDGETING AND RESOURCE ALLOCATION
5. COMPLIANCE AND RISK MANAGEMENT

It's good to see CISOs focusing on reputation and financial risk over compliance, which is usually the easiest part of your cybersecurity strategy," says **Mark E.** *"Most CISOs know how to handle compliance, but the reputation hit is the thing that keeps us up at night."*

Why budgets for domain security are sometimes overlooked

"Many companies still look at domain names as purely a trademark budget line and this thinking needs to shift towards security," says *Nina*.

"There are two things to bear in mind when it comes to a company's domain portfolio," she observes. "First, it's relatively cheap to register domain names. Second, in many jurisdictions, there are few to no rules associated with registration. This makes securing your brand through domain registrations extremely important—not only in core markets but also in high-risk domain extensions.

"This is why larger security budgets should be set aside for domain security. In companies where CISOs lack visibility of how digital assets are managed—and where responsibility sits with someone with less focus on security—critical, cost-effective measures such as registry locks can get overlooked.

"There is no one-size-fits-all approach. Companies can take a defensive strategy by registering broadly, or adopt a leaner style by monitoring for infringement and taking action when needed."

NIS2 compliance remains **a work in progress for many organizations**

Regulatory compliance is a constant challenge for CISOs. Non-compliance with initiatives such as The Network and Information Security Directive 2 (NIS2) and General Data Protection Regulation (GDPR) attract hefty fines and the risk of reputation damage.

Despite that, companies may have put NIS2 on the backburner in the belief that it doesn't apply to them, or because different European Union (EU) countries had been slow to roll out their regional variance of the new law.

This delay could explain why respondents ranked the following regulatory frameworks based on the level of difficulty they present in addressing specific cybersecurity and information security risks:

1. NIS2 ***(Europe)***

2. GDPR ***(Europe)***

3. Cybersecurity Maturity Model Certification ***(U.S.)***

4. International Organization for Standardization, International Electrotechnical Commission (ISO/IEC) 27001/2 ***(Global)***

5. Payment Card Industry Data Security Standard ***(U.S.)***

6. Critical Infrastructure Protection (CIP) Standards ***(U.S.)***

7. The Digital Operational Resilience Act (DORA) ***(Europe)***

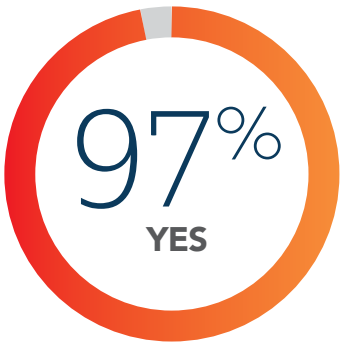
"Some countries will follow the directive verbatim, and others will adapt as they see fit," says ***Mark F.*** *"At the moment, all we can do is find the commonalities between the different ways in which countries have implemented NIS2 so far."*

Only 9% say their organization is fully compliant with NIS2. The biggest challenges are seen as ensuring compliance among external partners (cited by 73%) and difficulty in understanding and implementing the complex regulations correctly (64%).

This echoes findings earlier in this report, that respondents have concerns about partners not completing KYC checks with suppliers and other third parties, a practice that could impact the safety of an organization's supply chain.

"In our opinion, the reason NIS2 is number one is because it's the most time-critical one to deal with at the moment," says Nina. "We're going through similar processes as we did with GDPR, where everyone knows they need to do something, but they're not completely sure where to start. Meanwhile, ISO/IEC 27001/2 has been around for much longer, and it's a very intense process to get the certification."

Are you expecting an increase in the volume of security audits and regulatory and compliance requirements their firm will face over the next three years?



Preparing for increased security audits

Mark E. notes that the increase in regulatory requirements companies now face is partly due to jurisdictions showing the same tendency with AI regulation they previously did with data privacy laws, which is favoring the development of their own frameworks.

*"The way to manage it is to map all the data relating to regulation, whether it's privacy, AI, or other, to one control framework," **Mark E.** says. "It means when CISOs go to audit something, they can certify against all the standards; if they 'audit once and certify many' it really decreases the effort required.*

"CISOs need to make sure they have an effective governance, risk, and compliance program and that it applies all these requirements to one common framework—and that they're using automation to audit and maintain control."

Strategic outsourcing helps CISOs manage complexity at scale

Most CISOs and the organizations they work for recognize the value of outsourcing when detecting, managing, and preventing cyber attacks.

48%

said they mainly use in-house systems, processes, and staff

30%

mainly outsource to specialists

Keep everything in house

18%

Outsource everything

4%

The reality is that most IT and cybersecurity teams can't specialize in everything. Outsourcing helps fill critical gaps, especially in areas that require constant monitoring, deep expertise, or scale beyond internal capacity.

One example of where external partners can provide real value is in detecting and responding to third-party domain registrations. New domains are registered constantly—and with relative ease—making it nearly impossible for internal teams alone to keep up. Spikes in registrations often occur in response to real-world events, product launches, or public announcements, and tracking these patterns can reveal emerging threats or market signals beyond traditional brand monitoring. An experienced vendor can provide automated monitoring to scan at scale and identify trends that offer broader business intelligence, not just potential infringements.

However, automated monitoring is just the start. Human experts are essential for interpreting results and guiding decisions—such as whether to register a domain defensively or initiate a takedown. Not every organization has staff with deep visibility into domain activity or the surrounding context, so having a partner with their finger on the pulse adds critical insight and agility.

> *"An experienced partner can hold your hand through the evolutions of different cybersecurity risks. What we're seeing today doesn't mean that we're going to see the same trends in a couple of months' time. There may be something new that's coming up, and you just simply must be ahead of the game."*
>
> **Nina Hrichak**
> *Vice President of EMEA Account Management, CSC's Digital Brand Services*

More from our experts

Partnering for simplicity:
Managing domains and DNS security in one place

When considering working with an outsourcing partner for domain and DNS security, it's important to establish a strategy depending on the industry an organization works with, the way in which their digital asset portfolio is structured, their budget, and their risk tolerance, says ***Nina***.

"That includes choosing the right provider—singular—not providers, because having many different points of contact can introduce risk. Organizations should streamline their strategy to make sure that if something's on fire, they know who to reach out to, and don't have 10 different providers—especially in an intense situation.

"There's also the aspect of building a trusted partnership and knowing the provider will adopt the same approach as the company does internally.

"And going back to the evolution of the industry and the threat vectors emerging, companies constantly have to rethink strategy because there's no business that's just going to stand still, where the domain and trademark portfolio don't change.

"At the same time, companies have to keep up with what's happening in the industry, and this is another area where a trusted provider can really help."

What does a multi-layered, compliant security program look like?

CSC is well placed to help enterprises in the domain security ecosystem. This is because we provide multi-layered security—a cybersecurity approach that employs multiple security measures across different layers, including domains. We protect against threats including DDoS attacks, domain spoofing, online brand abuse, and phishing.

"Without domain security, your security posture is incomplete," ***Ihab*** explains. "Monitoring is important, but it can't stand alone. Without a global enforcement mechanism, you're just notifying the enterprise there's a problem, but not having the ability to mitigate that problem."

When domains are compromised, criminals can redirect website visitors to phishing sites, impersonate brands to sell counterfeit goods, and take down websites and business-critical operations that then compromise customer trust and company reputation.

Mark F. emphasizes that domains and DNS form the foundation of a business's online presence. "Think of your organization as a house built out of playing cards. The bottom row represents your domains and your DNS, supporting everything you do online. If I take that bottom layer of cards out, everything you've built above it collapses. There goes your website, your email, and if you're using voiceover IP, there go your phones. CISOs need to ask themselves, 'What's our Plan B?' for if and when that happens."

In other words, enterprises must treat domain security as an integral, elementary part of their overall security strategy, because when that part fails, the entire structure is at risk.

Conclusion

CISOs are responsible for one of the toughest jobs in business—keeping their organizations' data safe and complying with ever more complex regulation. Cyber threats are increasing in volume and sophistication, including in the realm of domain and DNS attacks.

AI has valuable applications in security, but it's also enabling a new wave of sophisticated methods designed to wreak havoc on organizations lacking adequate protection.

Despite these challenges, our first CISO Outlook report found that IT security budgets are only increasing modestly year over year for most CISOs. This may reflect gaps in understanding within the broader C-suite regarding where today's most significant organization threats truly lie.

Ensuring staff and partners are consistently aligned with governance programs is particularly important, says Nina.

"You just need one person in your team to click on the wrong email and give out the wrong data, and the same goes for your partners," Nina says. "You just need one partner that drops the ball on something, and it could lead to very big problems."

Staying agile in a fast-moving threat landscape is equally important—particularly when it comes to evolving risks tied to domains and digital infrastructure.

With this context, we encourage CISOs to:

- Adopt a well-structured, multi-layered security strategy that incorporates the right mix of tools, processes, and skills knowledge
- Establish a GRC program with a particular focus on user monitoring, employee education, and supplier data security practices
- Partner with a trusted and forward-thinking provider who can ease the burden on internal teams and enhance overall resilience

To learn how CSC can help your organization remain one step ahead in domain management and cybersecurity, visit cscdbs.com.

"There's a reason we're forced to change our passwords frequently, because the longer it's out there, the more chance somebody has of cracking it," concludes **Mark F.** *"It's the same with any breach or hijack that happens, or any fake website. The longer it's out in the wild, the more impact it's going to have. It's not an easy thing to manage, but you've got to be ahead of the curve."*

Overview of our **survey respondents**

Industry segments

- **19%** *Financial institutions*
- **18%** *Healthcare and insurance*
- **17%** *Retail industry and consumer products*
- **16%** *Technology, media, and telecommunications*
- **11%** *Industrial goods, energy, and utilities*
- **20%** *All others*

Job title of respondents

- *Chief information security officer* — **60%**
- *Chief information officer* — **13%**
- *Senior cybersecurity director and head of cybersecurity* — **11%**
- *Chief technology officer* — **8%**
- *Head of IT (or equivalent)* — **8%**

Headquarters of companies by region

33%
Europe

33%
North America

33%
Asia Pacific

Let's talk 1 800 927 9800 | cscdbs.com

About CSC

CSC is the trusted security and threat intelligence provider of choice for the Forbes Global 2000 and the 100 Best Global Brands (Interbrand®) with focus areas in domain security and management, along with digital brand and fraud protection. As global companies make significant investments in their security posture, our DomainSec℠ platform can help them understand cybersecurity oversights that exist and help them secure their online digital assets and brands. By leveraging CSC's proprietary technology, companies can solidify their security posture to protect against cyber threat vectors targeting their online assets and brand reputation, helping them avoid devastating revenue loss. CSC also provides online brand protection—the combination of online brand monitoring and enforcement activities—with a multidimensional view of various threats outside the firewall targeting specific domains. Fraud protection services that combat phishing in the early stages of attack round out our solutions. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are—and we accomplish that by employing experts in every business we serve.

DBS06272025