The CISO Outlook 2026

Authentic intelligence in the age of AI

Finding the right balance: AI opportunities and risk

In recent years, artificial intelligence (AI) has become an inescapable force impacting information management and cybersecurity. And while AI represents a real opportunity to manage cyber threats at scale, it also enables criminals and other bad actors to develop increasingly sophisticated methods of attack.

From managing suppliers to monitoring threats, the list of AI-related issues that chief information security officers (CISOs) need to address is growing exponentially.

To inform our latest report, CSC commissioned independent research with CISOs and other senior C-level executives worldwide to understand how they manage more traditional cyber threats, such as domain name system (DNS) outages, as well as how they navigate the balance between AI as an opportunity and a risk.

"AI plays an important part in managing cyber risks, but cybercriminals are also using AI to launch dangerous and widespread threats," notes Ihab Shraim, chief technology officer of CSC's Digital Brand Services.

"The average time for an attacker to get into a network—and then take over other accounts—is decreasing to a point where many organizations do not have the opportunity to detect them. As such, it makes more sense than ever to work with the right partner that can help mitigate the rising tide of threats."

> *AI plays an important part in managing cyber risks, but cybercriminals are also using AI to launch dangerous and widespread threats.*
>
> **Ihab Shraim**
> Chief Technology Officer of CSC's Digital Brand Services

OUR EXPERTS

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

Mark Flegg
Global Director, Security Services, CSC

Walt Fry
Global Domain Product Manager, CSC

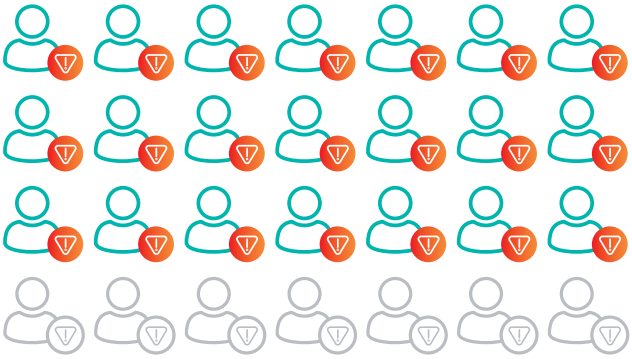
Key findings

We surveyed 300 senior executives—including CISOs, chief technology officers (CTOs), chief information officers (CIOs) and heads of cybersecurity—in Q1 2026 and found that:

The level of cybersecurity threats is critical

72%

of respondents say the level of threats was either **"critical"** or **"very critical"** in 2025



The top three threats in 2025 were ranked as:

1. Domain and DNS hijacking and subdomain takeover attacks
2. Cybersquatting, including typosquatting and online counterfeits
3. Ransomware and malware

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

1. Social media impersonation and defamation
2. Domain and DNS hijacking and subdomain takeover attacks
3. Distributed denial of service (DDoS) attacks
4. Cybersquatting
5. Employee and executive impersonation, including deepfakes, which were named as the fifth biggest area of risk

AI-related risks are also on the rise

The vast majority of respondents (98%) expressed concern about the risks of giving third-party AI-based systems and solutions access to company data, with 41% saying they are “very concerned.”

Very concerned **41%**

Somewhat concerned **57%**

Not concerned at all **1%**

Unsure about level of concern **1%**

AI-powered domain generation algorithms (DGAs) pose a threat to organizations, according to 86% of respondents.

But AI also presents a significant opportunity

73% say AI is more of an opportunity than a risk for cybersecurity. A further 10% say it's a "strong and clear opportunity."

16% say it's equally an opportunity and a risk.

Almost three-quarters **(72%)** say AI-driven automation plays a protective role with DNS and similar attacks, but requires oversight or careful management.

Risk controls for supply chain firms and partners are inconsistent:

More than two-thirds **(70%)** of respondents say their firms cascade risk controls to "key" suppliers only.

A further **14%** cascade controls to "very few" suppliers.

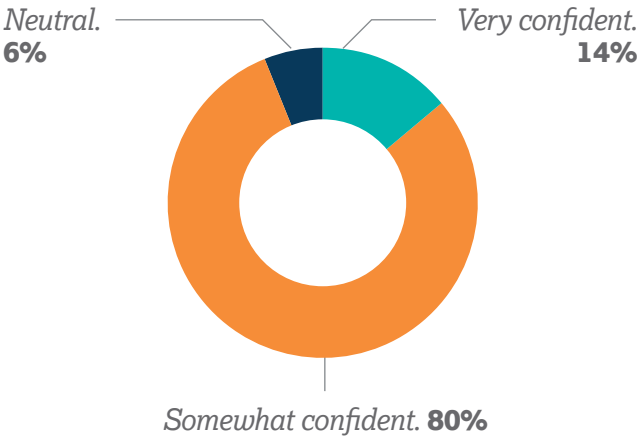
Just **15%** apply their own organization's risk controls to all suppliers.

Eight in 10 **(79%)** express concern that the increase of AI tool use by suppliers and partners poses a cybersecurity risk to their organization.

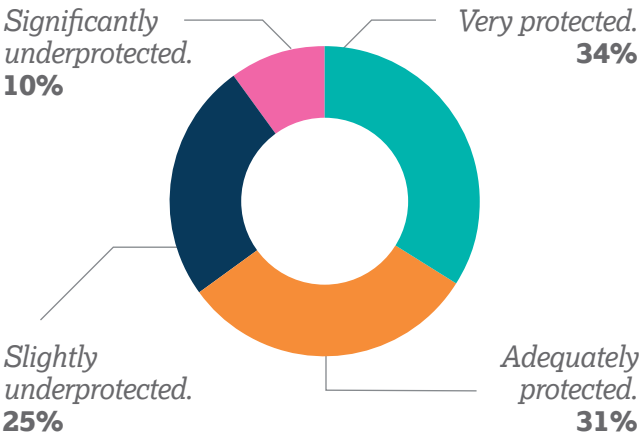
Many organizations remain vulnerable:

Only **14%** of respondents say they are "very confident" in their company's ability to mitigate domain attacks.

One in 10 **(10%)** believe major companies are "significantly" underprotected against DNS outages; another quarter **(25%)** say that they are "slightly" underprotected.



Just over a third **(34%)** believe they are "very" protected.



Escalating AI threats in a world of cyber risks

Cybersecurity threats continue to increase both in volume and complexity. The majority of respondents (72%) in this year's survey say the level of cybersecurity threats faced by their organization in 2025 was either "critical" or "very critical."

The top three threats they identified in 2025 are:

1. Domain and DNS hijacking and subdomain takeover attacks
2. Cybersquatting, including typosquatting and online counterfeits
3. Ransomware and malware

Compared to 2024 where the top three threats were:

1. Cybersquatting, including typosquatting and online counterfeits
2. Domain and DNS hijacking and subdomain takeover attacks
3. DDoS attacks

Looking ahead, respondents expect social media impersonation and defamation will pose the greatest cybersecurity threat over the next three years, ahead of domain and DNS hijacking and subdomain takeover attacks and cybersquatting. This represents a rise of four places from last year's survey when social media impersonation and defamation ranked fifth.

Employee and executive impersonation, including deepfakes, was named as the fifth biggest area of risk.

"Social media is constantly increasing as a means of information exchange, because organizations need to be where their customers are," says Walt Fry, global domain product manager, CSC. "The problem is that people are way more casual about using a social media site than they are when using a website. They are not questioning what it is they are dealing with."

Social media is constantly increasing as a means of information exchange, because organizations need to be where their customers are. The problem is that people are way more casual about using a social media site than they are when using a website. They are not questioning what it is they are dealing with.

Walt Fry
Global Domain Product Manager, CSC

"Identity theft can be seen as the new frontier for security," adds Mark Flegg, global director, Security Services, CSC. "That includes the rise of deepfake attacks, where people have lost money because criminals have impersonated a CEO to trick employees into divulging financial information or transferring funds."

Respondents expect threats to escalate further this year, with 75% saying they will see slightly more incidents and 14% expecting a significant increase. Notably, none of our respondents expect fewer incidents than in 2025.

While AI is driving intense activity across all industry sectors, it has also transformed information security.

Cybercriminals now use AI-based techniques across the full spectrum of cyberattacks, from identifying and targeting endpoints on the Internet of Things (IoT) to creating deepfakes of senior executives. Threat actors also use AI to scale phishing campaigns, including those launched with the help of domain generation algorithms (DGAs).

"AI-powered DGAs scale up the process of generating potential sources that look valid enough to launch phishing attacks," Walt says. "So, you need a monitoring solution that is going to match that type of scale."

THE RISKS ARE REAL: UNCOVERING A PHISHING EMPIRE

In 2025, a cybersecurity intelligence and advisory group exposed a phishing and brand impersonation scheme that had operated for more than three years on Google Cloud and Cloudflare platforms.[1]

It found that a large-scale, cloud-hosted infrastructure could hijack abandoned or expired domains, then pair them with cloned websites of multiple global brands. The scheme used a tactic called "hidden cloaking" to make it harder for the original brand to discover that their content appeared on a fake site.

The scheme put users at risk by exposing them to fake sites and created user confusion and eroded trust. But it also created regulatory and legal liability for the original brands. As stated in the research: "This suggests a failure to monitor and raises serious questions about due diligence, data protection, and customer safety."

Failing to identify risks presented by brand impersonation schemes could result in substantial exposure to General Data Protection Regulation (GDPR) law and Securities and Exchange Commission (SEC) disclosure requirements, highlighting the urgent need for organizations to use services that help them identify when criminals hijack old domain names.

"This scheme is a stark example of what can happen when trusted brands neglect the need to monitor the use of expired domains," says Walt. "It was running at scale for years, resulting in examples of large brands' own web content being displayed alongside nefarious betting sites."

Managing risks in a fast-moving cyber environment

The increasing complexity of cybersecurity threats means that CISO strategies for risks, such as DNS outages and domain attacks, need to evolve.

One in 10 respondents say they believe major businesses and organizations are "significantly underprotected" against DNS outages, while a further quarter say they are "slightly underprotected." Just over a third (34%) believe they are "very protected."

Only 14% of respondents say they are very confident in their company's ability to mitigate domain attacks. This reflects an improvement on last year's findings, when just 7% were confident.

Organizations face three challenges when mitigating domain attacks. For one, DNS incidents often originate from large cloud-hosting platforms, as seen in recent outages involving Cloudflare and AWS, rather than internal systems. Building in redundancy with systems purpose-built for DNS can increase resilience and reduce risk.

Second, organizations often fail to keep investment in security aligned with the pace of IT growth.

"Organizations put preventative measures in place to guard against DDoS attacks but then fail to carry out regular reviews on their evolving systems," explains Mark. "In the meantime, they have probably scaled up their systems and created a new set of risks. Protection is not one and done: Organizations need to make continuous investments in protection capabilities."

The third challenge organizations face involves domain name management. Many organizations now establish multidisciplinary teams with representatives from IT, security, legal, and marketing to stay ahead of potential risks, including those introduced by seasonal campaigns. Alternatively, organizations can choose to use a .BRAND top-level domain (TLD), certified by the Internet for Assigned Names and Numbers (ICANN). Due to exclusive ownership of the .BRAND TLD and the domain infrastructure, this approach reduces the risk of cyberattacks, like phishing and domain hijacking.

Of course, AI-related risks can also stem from a lack of internal governance. In fact, the vast majority of respondents (98%) are concerned about the risks of giving third-party AI-based systems, including large language models (LLMs), access to company data.

Organizations put preventative measures in place to guard against DDoS attacks but then fail to carry out regular reviews on their evolving systems.

Mark Flegg
Global Director, Security Services, CSC

To manage internal AI-related risks, many organizations put clear governance frameworks and risk controls in place to prevent the use of unauthorized LLMs and limit the exposure of sensitive corporate data. Another approach involves selecting LLMs tailored to the organization's specific business needs.

"It's vital to teach your workforce to use LLMs responsibly," says Ihab. "In the same way that you limit the use of Dropbox for file sharing, you shouldn't be uploading customer data to Google Bard or OpenAI."

At the same time, AI can help counter cybersecurity threats by helping security teams identify patterns in attacks and predict where they may occur next.

Fifty-seven percent of respondents say they use AI-based monitoring and enforcement solutions, while 44% use AI-based solutions for threat detection and fraud prevention. Both figures increased from last year, when 50% used AI-based monitoring and enforcement and 36% used AI for threat detection and fraud.

"AI is playing an increasingly positive role in managing threats internally," states Ihab.

"If your company isn't looking into it, then you will fall behind. This is an actual revolution, and we haven't had such a big disruption in the industry in the past 40 years, except for the invention of the internet. People were worried about changes then, too, just as they are concerned about change now."

"In the past, a company could build a solution to spot patterns in attacks as part of their monitoring activities," adds Walt. "But now the data involved keeps getting larger, and it's harder to model those patterns. AI can help to find some of those connections, so it's a big factor in helping to mitigate the threats because you can recognize potential threats much more quickly."

> *AI is playing an increasingly positive role in managing threats internally. If your company isn't looking into it, then you will fall behind. This is an actual revolution.*
>
> **Ihab Shraim**
> Chief Technology Officer of
> CSC's Digital Brand Services

Threats introduced by supply chains and partners

The interconnectedness of global organizations today means that security perimeters now extend into supply chains and corporate partnerships. As AI-enabled cyberattacks grow, incursions into corporate systems, including DDoS attacks via partners, may become more difficult to manage.

Eight in 10 (79%) say they are "concerned" or "very concerned" that suppliers' and partners' AI tool use poses a cybersecurity risk to their organization.

Yet almost three-quarters (70%) of respondents say their organizations apply risk controls only to key suppliers. A further 14% cascade controls to a very few suppliers, while just 15% apply the same controls across all suppliers.

"Inconsistent management of third-party threat controls introduces huge risks," asserts Ihab. "The only way to control it is to do a security audit. You've got to have a program for your third-party partners, including how you investigate or audit their use of AI."

Meanwhile, 63% say they expect risks relating to third-party risk management (TPRM) to increase slightly over the next 12 months, while 22% say they will rise significantly.

"It should be common practice to carry out an annual risk analysis to check the threat profile faced by all of your assets, including data," advises Mark. "As part of that, organizations should have ongoing conversations with their software partners to check they are using the right security tools."

In relation to the Network and Information Security (NIS2) directive, respondents say that their biggest concern about implementing it is ensuring compliance among external partners.

It should be common practice to carry out an annual risk analysis to check the threat profile faced by all of your assets, including data.

Mark Flegg
Global Director, Security Services, CSC

"There's that old adage that your team is only as strong as its weakest link," adds Mark. "Everyone uses third parties left, right, and center. But who's watching what they do? How do you know that they can't be compromised or breached, and what impact that will have on you? More security checks and questionnaires should be mandatory."

Organizations are right to be concerned about security threats relating to supply chains and partners. A consistent, proactive, and well-planned audit and regular checks should be in place, along with the use of trusted outsourced partners and cybersecurity specialists, to avoid critical data loss and exposure to critical risks.

Identity management essentials

A top challenge CISOs face today is identity management. You've got to have that deployed across the organization. Implement zero trust, which assumes all network traffic is hostile and requires strict, continuous authentication for every device and every user.

This relies on having the right tools in place properly integrated–not just purchased but fully configured. Use an intelligent, modern security operation center (SOC) to monitor the infrastructure, and take action when needed.

On top of that, you need a patch management program, penetration testing, and business continuity plans, all of which have to be audited against a security policy governed by ISO 27001/2, which is used by all of the large financial institutions, as well as by CSC.

And then you need a partner like us that can detect domain and DNS attacks and take action to take them down.

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

The rising tide of regulation

CISOs and senior information and technology executives have long had to manage regulations governing everything from data hosting and privacy to payment security. More recently, regulations such as the NIS2 directive have emerged to meet the needs of an increasingly digitized world.

New sets of AI regulation and guidance—including the European Union's (EU) AI Act, the National Institute of Standards and Technology's (NIST) AI Risk Management Framework (AI RMF), and the Organisation for Economic Co-operation and Development's (OECD) AI Principles—are emerging to provide stronger governance guardrails for users and system builders. This will likely add to the compliance workload for CISOs and their teams.[2,3]

In terms of current regulatory requirements, GDPR (first adopted in 2016) remains the most challenging to implement, according to CISOs surveyed for this report.

"GDPR is highly detailed and can apply to all of your operations if your customers reside in the EU, even though your HQ is based in the U.S.," explains Walt.

GDPR was followed by ISO/IEC 27001/2, the world's best-known standard for information security management systems; Cybersecurity Maturity Model Certification (CMMC); the NIS2 Directive; and the Payment Card Industry Data Security Standard. This marks a shift from last year's report, when CISOs saw NIS2 as the most challenging regulation to implement, closely followed by GDPR.

Lawmakers designed NIS2 regulation penalties to enforce high cybersecurity standards, with fines of up to 10 million euro or 2% of global turnover, as well as provisions that hold management personally liable.

Only 15% of respondents say they are fully compliant with all NIS2 requirements, with 72% saying they are largely compliant.

NIS2 is a very good framework: It has essential guidelines for cybersecurity, risk mitigation, and controls. AI is going to be significant with respect to governance, security, and regulations. I expect it to be built into frameworks like NIS2 in the near future.

Mark Flegg
Global Director, Security Services, CSC

This represents an improvement from last year's findings, when 9% said they were fully compliant and 63% said they were largely compliant. Our respondents identify ensuring compliance among external partners (67%) and lack of staff or budget (51%) as the biggest challenges when implementing NIS2.

"NIS2 is still fairly new, and adoption is not going to happen overnight. It has taken a while for companies and operational teams to digest the information needed," points out Ihab. "But NIS2 is a very good framework: It has essential guidelines for cybersecurity, risk mitigation, and controls. AI is going to be significant with respect to governance, security, controls, and regulations. I expect it to be built into frameworks like NIS2 in the near future."

As reliance on AI systems continues to grow, organizations must comply with evolving regulatory requirements for usage guidelines, as well as work with partners that adhere to the highest standards of governance.

Are you prepared for the EU AI Act?

The EU AI Act, or Regulation (EU) 2024/1689 of the European Parliament and of the Council, provides rules on AI as well as updated EU guidelines. Introduced on August 1, 2024, the regulation takes a risk-based approach, classifying AI systems into four categories based on their potential impact.[4]

- Minimal risk: Most AI systems, such as spam filters and AI-enabled video games, face no mandatory requirements, though companies may choose voluntary codes of conduct.
- Specific transparency risk: Systems like chatbots must clearly inform users that they are interacting with a machine, and certain AI-generated content must be labelled as such.
- High risk: Applications, such as AI-based medical software or recruitment tools, must comply with strict requirements, including risk-mitigation systems.
- Unacceptable risk: AI systems that enable "social scoring" by governments or companies are considered a threat to fundamental rights and are banned.

Most provisions of the AI Act's rules will start applying on August 2, 2026. However, the ban on unacceptable-risk systems will take place earlier, six months after the regulation enters into force, while the rules for general-purpose AI models will apply after 12 months.

Outsourcing for proactive protection

Given the increasing scope and sophistication of cyber threats, organizations of any size may find it difficult to protect every part of their digital infrastructure. Even the largest cloud service providers have experienced outages in recent years.

As cyber threats evolve and bad actors increasingly use AI to scale attacks, vulnerabilities at the DNS level remain one of the most significant risks.

"Perhaps the top challenge for a CISO right now is keeping abreast of everything: The world has gone mad for AI, so that's top of mind for them, and I'm sure that's consuming an awful lot of their time," says Mark. "But there are still fundamental building blocks like DNS, which is now considered critical infrastructure, that are not always carefully managed. Working with an outsourcing partner plugs that gap."

When asked about how they manage threats across their digital assets and attack surface, 62% of respondents say they use a trusted DNS provider with robust security.

However, an effective partner can proactively monitor and detect domain and DNS attacks, as well as provide brand and fraud protection.

A consumer-grade domain registrar isn't likely to monitor all channels, including social media, search engines, online marketplaces, and mobile apps, for malicious activity.

Responding to threats is as important as identifying them. The right partner will deal with the incident before it turns into a problem, not simply flag the risk.

"If you call the fire service, you want them to go to the fire itself and extinguish it," says Ihab. "You don't want them to take their trucks on the highway with their sirens blaring, then turn up and say it's not their job to put the fire out. In that same vein, you want an outsourcing partner that can proactively identify a DNS attack and stop it."

Perhaps the top challenge for a CISO right now is keeping abreast of everything: The world has gone mad for AI, so that's top of mind for them, and I'm sure that's consuming an awful lot of their time.

Mark Flegg
Global Director, Security Services, CSC

Facing the future with confidence

In the future, when we look back at the mid-2020s, we may see it as a time when we were still learning about the full implications of widespread AI adoption. Despite this uncertainty, organizations in 2026 still face strong pressure to adopt AI, whether to support day-to-day operations or manage cybersecurity threats.

Over the next few years, frameworks such as NIS2, NIST, and ISO/IEC 27001/2 will evolve, granting greater clarity on how we can safely apply AI.

As CISOs and their teams navigate this new era, many are adopting AI tools to address increasingly complex threats. While confidence in mitigating domain attacks has improved, the findings highlight persistent gaps.

These gaps include how organizations inconsistently manage risk across supply chains and software vendors. At the same time, attacks on SaaS software are increasing, with specific vulnerabilities exploited across multiple organizations, underscoring the need for visibility into emerging threat patterns.

In response, organizations are increasingly turning to trusted partners to support monitoring, detection, and mitigation across their digital footprint. Combining strong governance frameworks with internal capabilities and external expertise is becoming central to managing cyber risks at scale.

Organizations that take this approach will be better positioned to defend against increasingly complex domain-based threats, including those emerging through social media. They will also be better prepared as stronger AI-related governance frameworks continue to take shape.

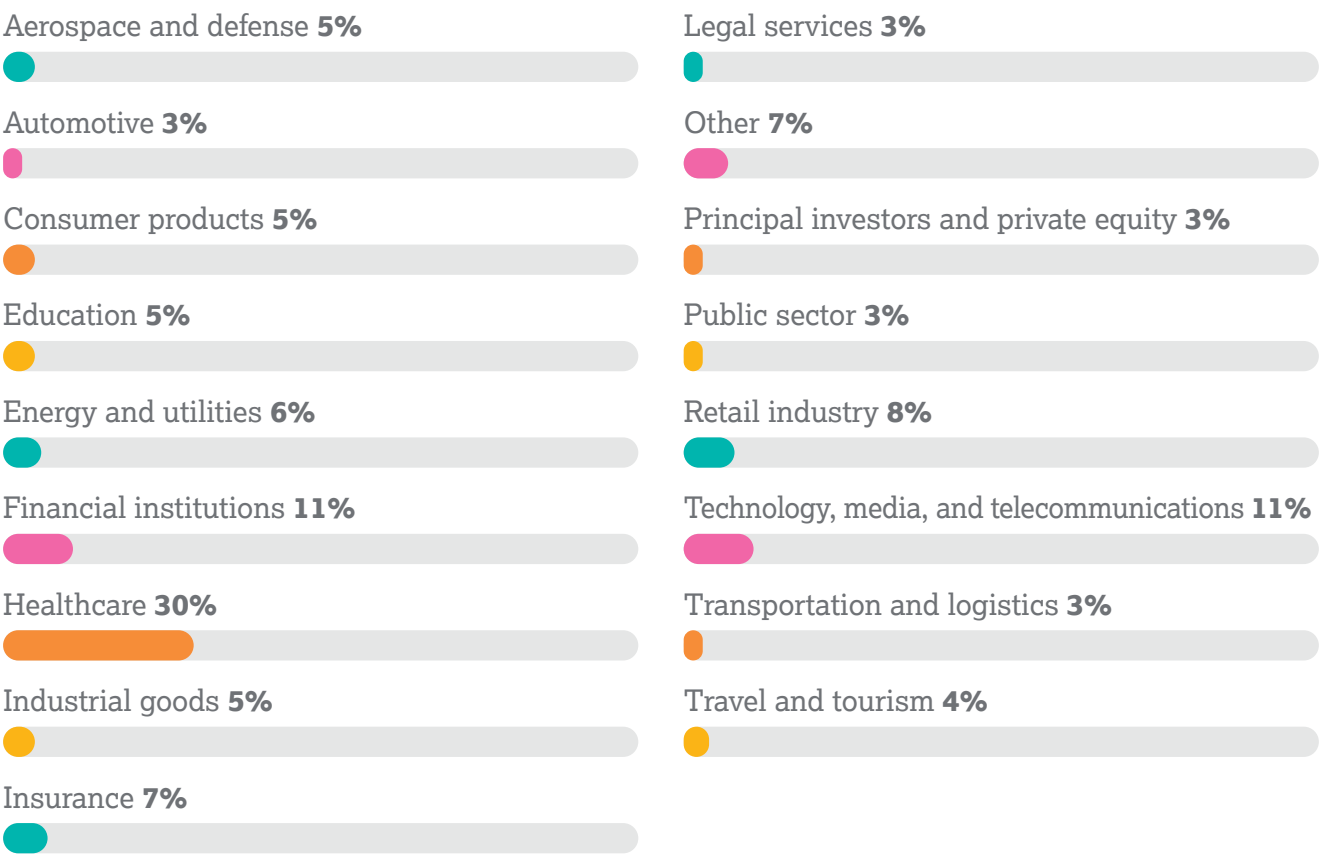
"The advancement of AI means attacks are getting harder to detect and block. On the upside, CISOs can turn to a rapidly developing set of AI tools themselves to take on the proliferation of threats. It's all about finding that balance," concludes Ihab.

The advancement of AI means attacks are getting harder to detect and block. On the upside, CISOs can turn to a rapidly developing set of AI tools themselves to take on the proliferation of threats. It's all about finding that balance.

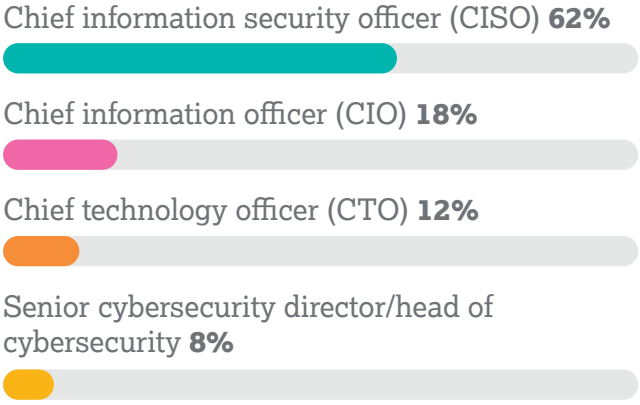
Ihab Shraim
Chief Technology Officer of CSC's Digital Brand Services

Overview

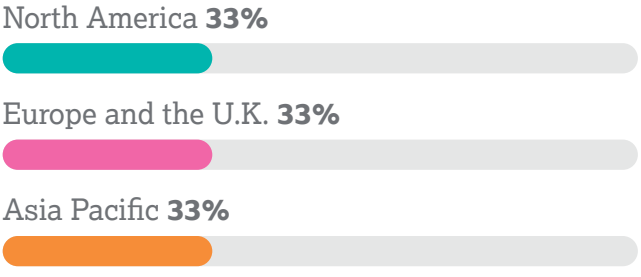
Percentages of companies by vertical sector



Job title of respondents



Headquarters of companies by region



Let's talk

800-927-9800 | cscglobal.com

Or scan the QR code

CSC—your trusted partner in private markets and real assets

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.

We are the business behind business®. Visit **cscdbs.com**.

This document is provided by CSC for information purposes only and does not constitute an offer, invitation, or inducement to contract. The information herein does not constitute legal, tax, regulatory, accounting, or other professional advice and therefore one should seek appropriate professional advice before considering a transaction as described in this document. No liability is accepted whatsoever for any direct or consequential loss arising from the use of this document.

1: "The Cloak and the Dagger: How Google and Cloudflare Missed a Global Phishing Empire," Medium, September 2, 2025, https://reporter.deepspecter.com/the-cloak-and-the-dagger-how-google-and-cloudflare-missed-a-global-phishing-empire-ed7176ebf82f

2: "AI Risk Management Framework," National Institute of Standards and Technology, accessed May 6, 2026, https://www.nist.gov/itl/ai-risk-management-framework

3: "OECD AI Principles Overview," OECD.AI Policy Observatory, accessed May 6, 2026, https://oecd.ai/en/ai-principles

4: "European Artificial Intelligence Act Comes into Force," European Commission, July 31, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123

Copyright ©2026 Corporation Service Company. All rights reserved.

DBS052026