CYBERCRIME MAGAZINE

Q1 2026 | PAGE ONE FOR THE CYBERSECURITY INDUSTRY | CYBERCRIMEMAG.COM

2026 CISO REPORT

35,000 Chief Information Security Officers Employed Globally in 2026

MSPs and MSSPs, the force multiplier in security leadership, are positioned to provide SMBs with CISO services

SAUSALITO, CALIF. – Mar. 23, 2026

Cybersecurity Ventures predicts that cybercrime will cost the world $12.2 trillion USD annually by 2031, up from $6 trillion in 2021. As a result, every business in the world should have a chief information security officer or equivalent. For Fortune 500 and Global 2000 corporations, that means a full-time CISO, which nearly all large enterprises employ. Some midmarket companies employ CISOs while many others hire fractional (onsite) CISOs. Most small businesses lack a CISO, but a growing number of them are turning to virtual (remote) CISOs.

Sophos brings a groundbreaking solution to market - its "CISO Advantage"- a set of capabilities designed to scale the knowledge, judgment, and operating discipline of a world-class CISO to organizations with or without dedicated security leadership, combining agentic AI, integrated platforms, and trusted human expertise delivered in partnership with managed service providers (MSPs) and managed security service providers (MSSPs).

The consequence of not having a CISO or comparable resources is a gaping security hole leaving a business exposed to severe threats including cyberattacks and data breaches, leading to financial loss, missed opportunity, and reputational harm.

The 2026 CISO Report from Cybersecurity Ventures in partnership with Sophos examines the shortfall of CISO resources available to the world's businesses, and shares related facts, figures, predictions, and statistics in order to help close the gap.

Cybersecurity Ventures estimates that there are 35,000 CISOs employed worldwide in 2026, up minimally from 32,000 in 2023

WORLD'S FIRST CISO

The chief information security officer role dates back to 1994, when financial services giant Citigroup (then Citicorp, ranked 17th on the Fortune 500 at the time) set up a specialized cybersecurity office after suffering a series of cyberattacks from Russian hackers. Steve Katz was anointed the world's first CISO in 1995 and served in that position for six years, until 2001. Twenty years later, Katz, 78 at the time, visited Cybercrime Magazine's headquarters, just a few miles from his home, and told us his story. Katz passed away on Dec. 2, 2023, at 81.

FORTUNE 500 & GLOBAL 2000

Ed Amoroso is the world's second-ever CISO, serving in the position for AT&T from 1999 until 2016. He told Cybercrime Magazine that he learned of the title from Katz and then printed new business cards. From there, the CISO role grew steadily and by 2021, a quarter-century after the first CISO emerged, 100 percent of Fortune 500 companies and nearly all Global 2000 organizations employed a full-time CISO, up from 70 percent in 2018, according to Cybersecurity Ventures. Today, 40 percent of Fortune 500 companies have deputy CISO roles or equivalent security leadership positions.

CISO HEADCOUNT

Cybersecurity Ventures estimates that there are 35,000 chief information security officers employed worldwide in 2026, up minimally from 32,000 in 2023. There are approximately 359 million businesses in operation in the world today being serviced by those CISOs. Joe Levy, CEO at Sophos, told the World Economic Forum that's a 10,000:1 ratio and a massive challenge for global cybersecurity resilience. "Those are not good odds," says Levy. "This is a market failure. We haven't figured out how to address this gap. We have the potential to do that now."

Joe Levy, CEO at Sophos

U.S. ROLL CALL

Zippia estimated, based on its database of 30 million profiles and verified against Census Bureau data, that 7,523 chief security officers (an interchangeable term with CISOs) were "currently employed" in the U.S. as of 2021. The U.S. Bureau of Labor Statistics (BLS) projected a 6 percent growth rate for CISOs from 2021-2031 (cumulative), which aligns with the average for all U.S. occupations. Based on that data, we can estimate there are approximately 7,750 CISOs employed in the U.S. as of 2026. Nearly every state in the U.S. has its own CISO.

The challenge with the vCISO offerings in the market today is that human bandwidth doesn’t scale infinitely

FRACTIONAL & VIRTUAL

Raja Patel, President, Products and Marketing at Sophos

Some organizations hire “fractional” CISOs. These part-time officers work on-site, whereas “virtual” CISOs (vCISOs) provide on-call security strategy support, incident response leadership, governance, and more. These options are more affordable than a dedicated, full-time CISO. When we estimate how many CISOs are active, we should also remember that some security leaders may be working for multiple businesses simultaneously. A number of CISOs may be more akin to contractors than full-time employees and there may be far more security leaders on duty than estimates can provide. A qualified full-time CISO commands $250,000 to $400,000 a year, and most SMBs simply cannot afford this, according to a LinkedIn post by David D. Love, CISSP, CEH, and head of security operations at Verizon. The vCISO Fix: For $40,000 to $120,000 annually (a fraction of the cost), companies get access to a senior leader. It turns a fixed "payroll" cost into a flexible "operating" expense. “The challenge with the vCISO offerings in the market today is that human bandwidth doesn't scale infinitely,” says Raja Patel, President, Product & Marketing at Sophos.

FIELD POSITIONS

Field CISOs are typically sales and marketing enablement positions at security vendors. They do not own the responsibility to oversee internal security for their company. Oftentimes they will provide clients with advisory services in connection with a security vendor’s tools and platforms.The Field CISO role often involves public speaking, industry networking, and sharing insights on emerging threats and technologies. Some of the larger security vendors employ multiple Field CISOs. This distinction must be made clear to Boards to avoid hiring a "brand ambassador" when a "wartime general" is needed. Field CISO is a relatively new title that has emerged over the past several years and there is no accurate prediction or count on how many of them exist.

BOARDROOM PRESENCE

In a 2025 global study of the goals, priorities and strategies of chief information security officers (CISOs), security analytics and observability supplier Splunk and economic advisory firm Oxford Economics found that 82 percent of CISOs now report directly to CEOs, a dramatic increase from 47 percent in 2023. Most boards and CISOs

have established access – 95 percent of CISOs provide regular updates to the board, with 60 percent engaging with the full board, according to an IANS 2026 report. But their time is short – roughly 30 minutes – and for 35 percent of boards, the CISO's security updates are limited to committee discussions. Cybersecurity Ventures predicted that by 2025, 35 percent of Fortune 500 companies would have board members with cybersecurity experience, and by 2031 that will climb to 50 percent.

WOMEN IN CYBER

Women hold around 30 percent of cybersecurity jobs globally, but there is an even broader gender gap in relation to CISO roles. Research conducted by Cybersecurity Ventures shows that women held 17 percent of CISO positions at Fortune 500 organizations (as of our last count), and 12 percent of all CISOs are female, according to CareerExplorer. In privately held companies, female CISOs earn 83 percent of what male CISOs earn, closely mirroring the broader U.S. workforce trend reported by the Pew Research Center (82 percent). In publicly traded companies, the gender pay gap is notably smaller, with female CISOs earning 92.5 percent of their male CISO counterparts' salaries. ISC2, a leading nonprofit member organization for cybersecurity professionals, has published its latest research examining the perceptions of women in the cybersecurity industry; a key finding is that women (27 percent) were more likely than men (17 percent) to report having 'significant' knowledge of AI and machine learning. That may be an indicator of more women filling CISO roles in 2027 and beyond.

COMPENSATION

According to Glassdoor data, the median annual pay range for a CISO is $321,000, while Salary.com puts the figure at $385,000. Lower tier estimates, provided by Zippia, bottom out at $144,000. CSO reports that CISO pay at the largest U.S. enterprises is closer to $500,000, with some CISOs receiving 7-figure annual compensation packages, and a few even hauling in $5 million a year. Estimated equity values are driving significant increases in year-over-year compensation for CISOs, particularly in larger public companies. CISOs in publicly traded companies typically receive better compensation-related benefits, such as equity, insurance, and signing bonuses, according to the 2025 CISO Security Leadership Survey from Hitch Partners. CISOs in the technology and services sector earn the highest total compensation on average, largely driven by equity and long-term incentives, according to a survey by Heidrick & Struggles. The survey also states that CISOs in Europe earned less on average than their U.S. counterparts. U.S. Cities including San Francisco, New York, Seattle, and Washington, D.C. offer the highest salaries, according to an analysis of compensation data from publicly available job postings, salary benchmarks from trusted job sites and recruiter-reported ranges from cybersecurity hiring reports.

75 percent of security chiefs are interested in a job change, and one-third of them say that stress is adversely affecting their performance

BURNOUT & TURNOVER

“For a while now, the industry data has told us that the average tenure for a CISO is less than any other [C-suite] member,” according to Levy. CSO names frustration, stress, and increased liability as a few of the off-putting realities giving CISOs cold feet. More CISOs are dissatisfied with the role today than ever before, with studies indicating that 75 percent of security chiefs are interested in a job change. Surveys show that 99 percent of CISOs work extra hours every week, and 1 in 5 work an extra 25 hours per week, according to Help Net Security. ComputerWeekly reports that almost one-third of CISOs say stress is adversely affecting their performance. Dark Reading reports that average CISO tenure now hovers between 18 months and 26 months, according to multiple industry estimates, and the result is not just executive churn, but instability that ripples through security programs, teams, and risk posture. It doesn’t help that in several incidents over the past couple of years, CISOs have been held legally and personally responsible for the handling and reporting of breaches. A survey by Heidrick & Struggles found that nearly half of surveyed CISOs did not have an adequate internal successor in place.

CERTIFICATIONS

Alongside academic qualifications, most CISOs hold one or more certifications that validate their operational and strategic skills. Getting certified shows employers that a CISO has the necessary knowledge and skills to succeed and they can increase their chances of getting promoted and paid more, according to the SANS Institute, a provider of several CISO certifications. For aspiring professionals eyeing a move into a C-Suite position within the cybersecurity landscape, a CCISO certification from EC-Council could be a valuable addition to a CISSP, which was launched in 1994, and is the premier certification in the cybersecurity sector, administered by ISC2. How important are certifications to employers? CISSP appears in approximately 85-90 percent of CISO job descriptions, according to an analysis of Cyberseek postings and executive search requirements.

RECRUITING

Although CISOs have long cited challenges in hiring enough qualified security workers, they’re increasingly citing it as a roadblock to advancing their security

Sophos views managed service providers (MSPs) and managed security service providers (MSSPs) as the force multiplier in security leadership

agendas. The 2025 State of Cybersecurity Resilience from professional services firm Accenture found that 83 percent of IT executives identified their cyber talent shortage "as a major obstacle to achieving a strong security posture." CyberSeek reported that there are just over 1.3 million people employed in cybersecurity in the U.S. in 2025, but more than 500,000 positions remain unfilled. Worldwide, the cybersecurity workforce gap increased by 19 percent to nearly 4.8 million unfilled jobs between 2023 and 2024, according to ISC2. Cybersecurity Ventures predicts a more modest 3.5 million unfilled cybersecurity jobs globally as of 2024-2025, and the figure is being recalculated for 2026, taking numerous trends into consideration, including AI. No matter how you slice it, CISOs are faced with stiff competition for the security managers and practitioners who work under them, and that includes competition from cybercrime and ransomware gangs.

SMALL BUSINESS

The World Economic Forum (WEF) reports that 90 percent of all companies worldwide, or roughly 323 million of them, are small. Close to zero percent of these companies employ a dedicated security officer. Three out of five small-to-midsized businesses (SMBs) permanently shuttered their doors within six months of being hit by a data breach or hack, Cybercrime Magazine reported in its first annual cybercrime report six years ago. Recent statistics indicate that SMBs remain vulnerable: Four out of five small businesses were victims of a security or data breach in 2025, Tech Xplore reports; Numerous media outlets have reported that employees of small businesses experience 350 percent more social engineering attacks than those at larger enterprises, and that half of all SMBs say it took them 24 hours or more to recover from a cyberattack; More than three-quarters of small businesses say their breach cost them at least $250,000, according to the Identity Theft Resource Center, and an unprecedented 37 percent say they lost more than $500,000. "We need to provide the effective leadership of a CISO to the hundreds of millions of organizations that couldn't have even dreamed of having one previously," says Levy. "This is the biggest opportunity that exists in cybersecurity today."

MANAGED SERVICE PROVIDERS

Sophos views managed service providers (MSPs) and managed security service providers (MSSPs) as the force multiplier in security leadership. Just as managed detection and response (MDR) proved that security operations scale best through services, security leadership scales best through partners. Various industry estimates put the number of MSPs and MSSPs at tens of thousands globally. As per a 2025 KPMG Cybersecurity Survey, 53 percent of leaders cited a lack of qualified candidates as a high-impact challenge, prompting higher compensation (49 percent), more internal training (49 percent), and more reliance on external partners (25 percent), including Managed

There's an opportunity to create the next generation of MSPs and MSSPs through this hybrid model of humans and agents working together

Security Service Providers (MSSPs), to close critical gaps. These service providers already sit at the intersection of technology, operations, and trust. Sophos is providing MSPs and MSSPs with its CISO Advantage to extend their role into governance, compliance, and risk management, services that are desperately needed by underserved small to midsized businesses (SMBs). "There's an opportunity for us to create the next generation of MSPs and MSSPs through this hybrid model of humans and agents working together to be able to deal this strategy leadership to hundreds of millions of businesses that would otherwise not have access to it," says Levy.

Sophos CISO Advantage

SPENDING

Cybersecurity Ventures predicted that global spending on cybersecurity products and services would hit $454 billion annually (USD) in 2025, up from $260 billion in 2021. Today, nearly 15 percent of (corporate) cybersecurity spending comes from outside the chief information security office (CISO), and non-CISO cyber spending is expected to grow at a 24 percent CAGR over the next three years, according to a McKinsey study, which goes on to state that this has changed from a decade ago, when almost all cybersecurity spending came from the CISO organization. Going forward, as we trend towards a potential $1 trillion annual cybersecurity market by 2031, providers will need to increasingly cater to non-CISO customers, the McKinsey study posits, with most non-CISO cyber spending coming from buying centers responsible for cloud, product, network, and audit and compliance.

BUDGET

Frost & Sullivan reports that the average cybersecurity spend is 15.6 percent of the overall IT budget. However, there is significant geographic variation: Germany allocates the lowest percentage at just 9.5 percent of IT spend to cybersecurity; India is at the other end of the scale, investing about 24 percent; Energy companies invest around 11 percent; Banking, Financial Services, and Insurance (BFSI) and high-tech companies invest above average. Splunk's 2025 CISO report found that only 29 percent of respondents had an adequate budget, compared to 41 percent of boards who felt cybersecurity budgets were adequate. New research finds CISOs ready to work with bigger budgets. In a survey of 300 C-suite and senior security leaders, services and consulting firm KPMG found that 98 percent of their respondents confirmed they received budget increases over the previous 12 months heading into 2026.

Ransomware, the fastest growing type of cyber-crime, is 35 years old and it shows no signs of slowing down

CYBERINSURANCE

Cyberinsurance emerged in the late 1990s, according to TechTarget, initially as an offshoot of errors and omissions (E&O) insurance. It now covers cyberattacks, including data breaches, ransomware, and social engineering. Cybersecurity Ventures predicts that the global cyberinsurance market will reach $34 billion USD by 2031, up from $8.5 billion in 2021. Ransomware continues to vex insurers and policyholders, sources told Business Insurance. "There's no question that, from a pure loss perspective, ransomware is still number one," says Mike Colford, SVP, cyber product leader with Westfield Specialty, a prominent specialty insurance carrier. "We're trying to predict the future a little bit with AI and where it's going and where that could lead to gaps in coverage or potential claims, but ransomware hasn't gone anywhere." Most CISOs still see cyberinsurance as something you rely on after an incident, according to Fair Institute, a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and risk management. Jason Hart, a managing director at CFC, a specialist insurance provider and market leader in cyber, believes that cyberinsurance has become a critical tool for CISOs, and that it can be one of the best investments any business—and CISO—can make.

ARTIFICIAL INTELLIGENCE

When asked to identify their top areas of expertise to build or maintain, 57 percent of respondents to the Heidrick & Struggles 2025 Global Chief Information Security Officer Compensation Survey selected "artificial intelligence, machine learning, and data analytics." AI still ranks almost twice as high as the next most selected area. This focus is reinforced by the fact that 96 percent of respondents say they are already using AI to enhance their company's cybersecurity posture, signaling that AI-enabled defense is rapidly becoming a standard expectation rather than an emerging capability. Securing AI infrastructure is the biggest issue CISOs face, according to CSO based on data from ISACA. AI can be pricey, and Forrester analysts have a recommendation for CISOs: Funding AI security solely from the security budget guarantees tradeoffs that weaken core defenses. CISOs should push to embed AI security costs directly into enterprise AI investments, aligning funding with risk ownership and protecting foundational security programs.

RANSOMWARE

Ransomware, the fastest growing type of cybercrime, is 35 years old, it shows no signs of slowing down, and it's predicted to cost victims around $74 billion in 2026, and $275 billion annually by 2031, according to Cybersecurity Ventures, with a new attack every 2 seconds as perpetrators progressively refine their malware payloads and related extortion activities. According to the latest ransomware report by

Cybersecurity Ventures predicts that global damage costs resulting from software supply chain attacks will reach $138 billion by 2031

by Sophos, the average ransomware demand has now reached $1 million, while average recovery costs stand at $1.5 million, and CISOs have a 25 percent chance of their job surviving a successful ransomware attack. When the World Economic Forum (WEF) Global Cybersecurity Outlook 2025 Report asked CISOs "Which organizational risk concerns you the most?" 57 percent replied with ransomware, which was followed by supply chain disruption (22 percent), cyber enabled fraud (7 percent), and malicious insider (7 percent).

SUPPLY CHAIN ATTACKS

CISOs are being urged to shift attention from standalone threats and AI hype towards systemic cloud risk, as security leaders forecast a sharp rise in attacks on major cloud platforms and their supply chains through 2026. The 2025 Verizon Data Breach Report states that in 2025 alone, data breaches involving third-party software doubled, accounting for 30 percent of all breaches. Gartner projected that by the end of 2025, nearly 45 percent of companies were expected to have faced at least one software supply-chain incident. Cybersecurity Ventures predicted that global damage costs resulting from software supply chain attacks would reach $60 billion USD by 2025, and $138 billion by 2031. A World Economic Forum (WEF) report states that of large organizations, 54 percent identified supply chain challenges as the biggest barrier to achieving cyber resilience.

Q-DAY / Y2Q

Preparing for Q-Day is a critical priority for CISOs. Cybersecurity Ventures predicts that Q-Day will arrive on or around Jan. 1, 2031. That will be the day, also known as Y2Q, when cryptanalytically relevant quantum computers (CRQCs) will finally be able to decrypt the world's secrets. The threat isn't only that Y2Q will hasten the cracking of encrypted systems, but that cybercriminals and nation-states are already warehousing encrypted data with the expectation that they'll be able to crack it a few years down the track. This practice – known as harvest now, decrypt later, or HNDL – poses a clear and present danger to every organization relying on encryption to protect its data, and it's a key reason executives must move sooner rather than later to progress their post-quantum cryptography (PQC) transition. "Everything we know about cybersecurity – every lock secured by current encryption methods – could get blown wide open," says Theresa Payton, former CIO at The White House, warning that "our choice is a simple one: to await the devastation of the first cyberattack fueled by quantum decryption, or to build the defenses to stop it."

Phishing remains the most common form of cyber-crime faced by CISOs and their teams, with an incalculable number of spam emails sent daily

HUMAN RISK MANAGEMENT

Industry research indicates that 70 to 90 percent of breaches are the result of employees succumbing to social engineering, making skills-based errors, sharing sensitive data with shadow IT services, or through a compromise of a privileged user. If humans are cybersecurity's weakest link, then security awareness training may be a CISO's strongest weapon. Phishing remains the most common form of cybercrime, with an incalculable number of spam emails (in the billions) sent every day. Millions of smishing (SMS) and vishing (voice) attacks have been recorded over the past year. Social engineering attacks, including deepfakes, are targeting employees at companies of all sizes and types globally. In 2014, Gartner pegged the security awareness training market at $1 billion in revenue worldwide, a fraction of the estimated market size of $6 billion in 2025 and between $10 billion and $13 billion by 2030.

REGULATORY

According to Gartner, regulatory pressure and attack surface expansion will result in 45 percent of CISOs' remits expanding beyond cybersecurity by 2027. CSO reports that 21 percent of CISOs are pressured not to report compliance issues, and with increasing regulatory scrutiny and the rise of personal liability for security leaders – especially under regimes like the EU's General Data Protection Regulation (GDPR), SEC regulations, and critical infrastructure laws – CISOs must navigate a fine line when pressured to not raise flags about corporate issues. Other regulations, such as the Cyber Security and Resilience Act, DORA, and NIS2 are increasing the regulatory scrutiny. The upside for CISOs is that pay raises are tied in part to growing regulatory issues, though this also adds stress to the role.

INSIDER THREAT

In Jan. 2026, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published a new resource on "Assembling a Multi-Disciplinary Insider Threat Management Team." The guidance is intended to assist critical infrastructure stakeholders, which includes private sector entities across various sectors, with implementing an insider threat mitigation program that combines physical security, cybersecurity, personnel awareness, and community partnerships. Although framed for critical infrastructure, CISA's guidance is relevant to a broader range of organizations, including those outside of critical infrastructure sectors – a point echoed by Inside Privacy, a resource for updates on developments in data privacy and cybersecurity, edited by Covington. In 2025, organizations allocated an average of 19 percent of IT security budgets to insider risk management, up from 8.2 percent in 2023, according to Help Net Security. Many organizations view agentic AI as important for early insider risk detection, but only a small share classify AI agents as equivalent to human insiders.

The 2026 CISO Report is authored by the editors at Cybercrime Magazine and published in partnership with Sophos

ABOUT

Cybersecurity Ventures is the world's leading market-watcher, a trusted source for cybersecurity facts, figures, and statistics, and publisher of Cybercrime Magazine. We provide cyber economic market data, insights, and ground-breaking predictions to a global audience of CIOs and IT executives, CSOs and CISOs, information security practitioners, cybersecurity company founders and CEOs, venture capitalists, corporate investors, business and finance executives, HR professionals, and government cyber defense leaders.

Sophos is a cybersecurity leader defending 600,000 organizations globally with an AI-powered platform and expert-led services. It adapts to organizations at any stage of security maturity, combining machine learning, automation, and real-time threat intelligence with human expertise from Sophos X-Ops for 24/7 threat monitoring, detection, and response.

Sophos delivers industry-leading managed detection and response (MDR) and a broad portfolio of solutions, including endpoint, network, email, and cloud security, extended detection and response (XDR), identity threat detection and response (ITDR), and next-gen SIEM. Paired with expert advisory services, Sophos helps reduce risk, accelerate response, and outpace evolving cyber threats.

MEDIA CONTACTS

Editors at Cybercrime Magazine
info@cybersecurityventures.com

Sophos PR
press@sophos.com