

THE SURVIVAL IMPERATIVE:

Cyber Resilience in
Financial Services in 2025



New research explores the state of cybersecurity across the financial sector, focusing on the risks that undermine investor confidence, the drag of legacy systems, and the resilience advantage of firms partnered with managed security experts.



*Insights aligned with Microsoft-
based infrastructure*



Table of Contents

Executive Summary	03
Investor Confidence is on the Line	04-05
Family Office Perspective	06
Attacks Are Routine and Pervasive	07-08
Infrastructure Challenges and The Cost of Standing Still	09
Recovery Blind Spots	10
Partnering for Cyber Resilience: The MSSP Difference	11
Looking Ahead: 2026 Financial Services IT Priorities	12
How to Increase Cyber Resilience and Protect Investor Trust	13
About Omega Systems	14
Survey Methodology	



88%

of financial executives say a successful cybersecurity attack would trigger withdrawals or AUM loss.



Executive Summary

Cyber-attacks strike at the core of financial services: client trust. A single breach can trigger investor withdrawals, erode assets under management, and send firms into crisis. Nearly nine in ten executives admit a successful attack would provoke client flight and investor panic.

In an industry built on confidence and trust, cybersecurity has become inseparable from business relationships and survival.

To better understand how financial firms are addressing cybersecurity pressures, Omega Systems surveyed more than 300 financial leaders across family offices, registered investment advisers (RIAs), wealth managers, hedge funds, private equity firms, and other investment management firms. The survey examined how the market is safeguarding investor trust, where weaknesses like outdated infrastructure and limited testing leave firms exposed, and how internal-only versus outsourced IT models influence cyber resilience.

The research reveals a sector under constant pressure. Ninety-three percent (93%) of firms experienced at least one cyber incident in the past year, and nearly one in five faced threats numbered in the dozens. While cybersecurity budgets are rising, complex technology and operational challenges continue to plague financial firms and risk leaving protections out of step with the scale of today’s threats.

This report unpacks where financial services firms are excelling, where they are exposed, and what must change to stay ahead of increasingly sophisticated attacks.

Investor Confidence is on the Line

Trust is currency in financial services. When trust is broken, clients don't wait for explanations. They move their money.

Eighty-eight percent (88%) of executives surveyed by Omega Systems acknowledged that a successful cybersecurity attack would trigger withdrawals, raise investor concern, or lead to direct loss of assets. That concern is even more pronounced among CFOs, with 94% saying they would expect client departures in the wake of a major incident.

The anticipated damage of a cyber-attack extends far beyond lost assets. Additional concerns include prolonged downtime that disrupts services, theft of sensitive client data, exposure to fraud, and reputational harm that lingers long after systems are restored.

Emerging threats such as deepfakes reinforce this vulnerability. Sixty-one percent (61%) of executives are concerned about impersonation campaigns targeting their firms. While most report having taken steps to prepare, the high level of concern suggests many remain uncertain whether those defenses are strong enough to withstand an actual attack.



Top 5 Negative Cyber-attack Impacts



***Investor Confidence is on the Line** continued*

That uncertainty extends inside organizations as well. While most leaders say they are confident employees could recognize an AI-driven phishing or social engineering threat, nearly a third admit they are not fully confident, and only 17% indicated that security awareness training will be a priority in the coming year.

In the absence of stronger readiness, almost nine in ten financial firms now carry cyber insurance coverage as a safety net.

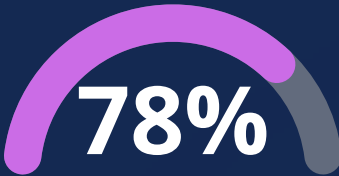
While cyber insurance is prudent, it has its limits. At best, it cushions financial losses — but it cannot prevent withdrawals or restore reputation once trust has been compromised.



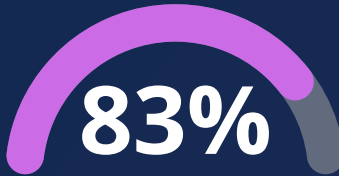
Despite pervasive threats across the industry, **only 17%** of financial executives indicated that security awareness training will be a priority in the coming year.

Family Office Perspective

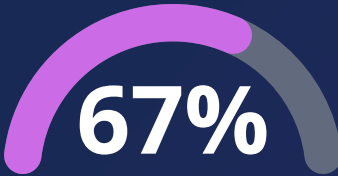
The research shows that family offices, which manage concentrated assets for high-net-worth clients, are consistently less prepared than their peers:



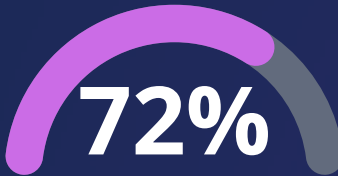
say a successful attack would trigger withdrawals or investor panic



are concerned about deepfakes or other impersonation threats



acknowledge reliance on legacy systems would likely hinder breach recovery



believe they are targeted more often because they manage high-net-worth assets

 Family offices surveyed:

showed **lower than average concern** for cybersecurity as a business challenge

admit the **least amount of confidence** that their employees can detect and prevent AI-powered cyber-attacks (60% compared to 69% average and 78% among RIAs)

demonstrated the **highest level of concern** about outdated infrastructure and their ability to recover from a data breach (67% compared to 50% average)

Attacks Are Routine and Pervasive

Leadership and IT concerns are not theoretical. Cyber incidents have become routine across financial services. Nearly all firms (93%) reported at least one known attack in the past year, and 18% faced more than 25.

When asked about the types of attacks they feel least prepared to recover from, leaders pointed to a wide range of threats.

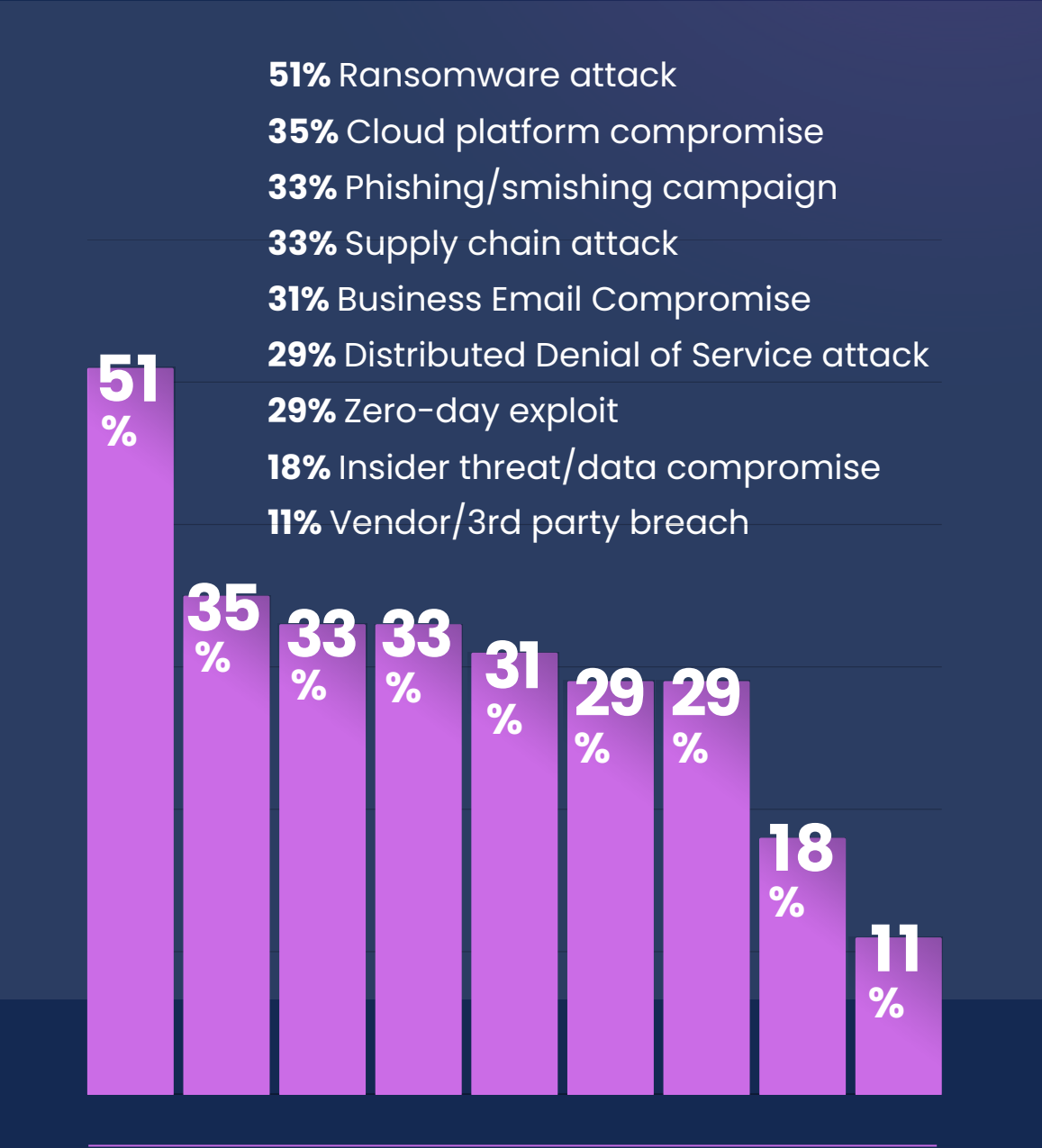
- Ransomware attack (51% say they are unprepared to recover effectively)
- Cloud platform compromise (35%)
- Phishing or smishing campaign (33%)
- Supply chain attack (33%)
- Business Email Compromise (31%)
- Distributed Denial of Service attack (29%)
- Zero-day exploit (29%)
- Insider threat or data compromise (18%)
- Vendor or third-party breach (11%)

The variety of attack types underscores that firms cannot focus on a single threat vector — resilience requires preparation on multiple fronts.

Response times are also troubling. More than a third of firms said it would take a week or longer to detect and contain a breach, and 6% admitted it could stretch into a month or longer. In a sector where capital and confidence can shift in hours — and money is expected to move instantly — failure to respond swiftly and effectively magnifies the impact.



Most alarming attack vectors



⚠️ **“More than one third** of firms say it would take a week or longer to contain a breach.”

Attacks Are Routine and Pervasive *continued*

Furthermore, cyber assessments and vulnerability testing reveal a clear divide in defense maturity. While some firms have adopted continuous or monthly assessments to strengthen resilience, 31% still rely on quarterly or less frequent reviews, which create extended windows of vulnerability that attackers can exploit.

The good news is most financial firms are not ignoring the problem.

In response to market volatility, 78% of firms increased cybersecurity spending in the past year, with firms in the \$101–500M range showing the greatest proclivity (88% increased spending in the last 12 months).

Among the sub-verticals, RIAs were least likely to increase security budgets (only 57% did), and, in fact, 11% of RIAs said they significantly *decreased* their IT spend last year.



Breach detection and containment:



“Capital and confidence can shift in hours and money is expected to move instantly — failure to respond swiftly and effectively magnifies the impact.”

Infrastructure Challenges and The Cost of Standing Still

The lack of technology modernization remains a challenge across the financial services sector. The fact that half of firms plan to prioritize cloud adoption in 2026 is telling: it highlights how many are likely still relying on outdated systems today, even though cloud migration offers stronger built-in security and resilience.

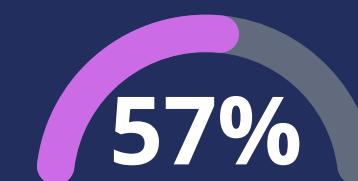
More than half (57%) are not monitoring threats in real time, which limits their ability to detect and contain attacks before they escalate.

Outsourcing is another area where most financial services firms lag. Sixty-five percent (65%) continue to manage IT and security entirely in-house. Only 16% are fully outsourcing IT and cybersecurity to an MSP/MSSP, and 17% use a co-managed model.

Family offices are the least likely to embrace a fully outsourced model, with only eight percent (8%) using an external provider for day-to-day cybersecurity management.



At a time when most financial firms believe they are targeted because they manage high-net-worth assets



are limiting their ability to detect and contain attacks before they escalate.



Family offices are the least likely to embrace IT outsourcing, with only eight percent (8%) using an external provider for day-to-day cybersecurity management.

Recovery Blind Spots

The ability to respond and recover quickly after a disruption is essential to limit financial, reputational, and regulatory fallout. Despite this, many executives acknowledge their firms carry significant weaknesses that could slow recovery, including:

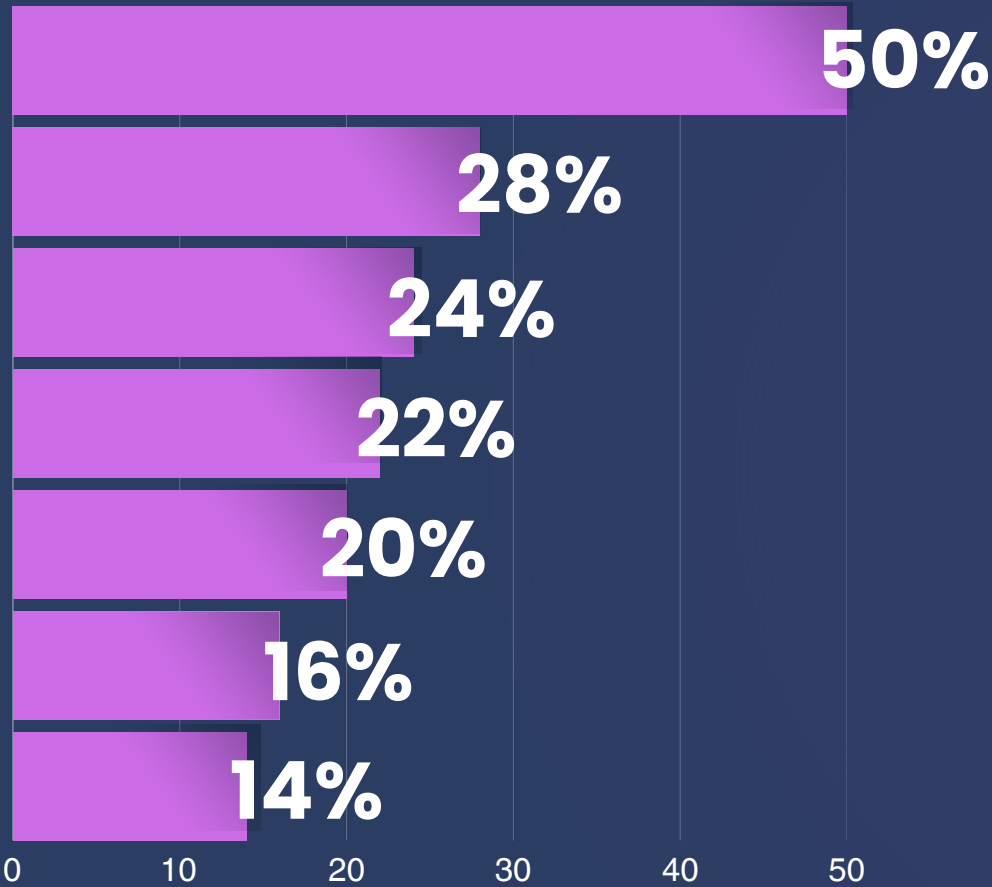
- Reliance on outdated or on-premises systems that slow recovery
- Lack of current backups or recovery capabilities
- Teams not trained on incident response processes
- No regular vulnerability assessments
- No effective incident response plan
- Lack of experienced IT or security staff
- No access to a SOC partner

When asked about their most pressing IT and security challenges for 2025, executives pointed to gaps in employee preparedness and expertise as major concerns. One in five (21%) cited a lack of employee security awareness as a significant challenge, while one in three (34%) said they lack the internal resources or expertise to manage complex IT and security controls.

The lack of modern systems, tested processes, cybersecurity partners and trained staff leaves firms vulnerable at the exact moment when clients and investors are most alert.



Slow recovery by significant weakness



- 50% Reliance on outdated or on-prem systems
- 28% Lack of current backups or recovery
- 24% No incident response training
- 22% No regular vulnerability assessments
- 20% No effective incident response plan
- 16% Lack of experienced IT or security staff
- 14% No access to a SOC partner



Partnering for Cyber Resilience: The MSSP Difference

The survey shows a clear divide between firms that rely on internal IT teams with shared resources and those that extend their capabilities with an MSSP (fully outsourced or co-managed).

Key differences include:

- **Threat exposure and readiness:** Internal shared-resource firms are 56% more likely to face 25+ attacks annually and are far less confident in spotting advanced threats — only 10% are “very confident” their teams can detect AI-driven attacks, compared with 30% of MSSP-supported firms.
- **Containment speed:** Internal shared-resource firms are more likely to face delays, with 25% requiring two to four weeks to contain a breach compared with just 16% of MSSP-supported firms.
- **Recovery posture:** MSSP-supported firms are more likely to report mature response capabilities (14% vs. 8% internal) and less likely to say they skip vulnerability assessments (20% vs. 30% internal).



↓ Bottom Line

MSSP-backed organizations deliver faster containment, stronger recovery posture, and greater readiness against evolving risks — advantages that directly safeguard capital and preserve client trust.

Looking Ahead: 2026 Financial Services IT Priorities

As the financial services industry looks ahead amidst continued economic uncertainty and a deeply complex cybersecurity threat landscape, operational priorities and budgets will need to shift to ensure firms can withstand repeated attacks and mitigate business and financial risk. **In 2026, firms plan to shore up defenses and invest or upgrade in IT and security** areas such as:

- Cloud adoption, migration and security (51%)
- Advanced threat detection and response, such as MDR, EDR, SOC (50%)
- IT infrastructure modernization (41%)
- Multi-factor authentication and identity access management controls (39%)
- Network and perimeter security (37%)
- Backup and disaster recovery solutions (36%)

Firms currently outsourcing IT and security or considering doing so in 2026 expect to look for partners that can deliver advanced threat protection capabilities, round-the-clock IT help desk support and deep knowledge of the financial services industry to support their ongoing operations and instill greater confidence in their risk management practices.

Security Investments In 2026



How to Increase Cyber Resilience and Protect Investor Trust

One theme runs through every finding: in financial services, cybersecurity is business security. A single breach can unravel years of client relationships, erode AUM overnight, and leave reputations permanently scarred.

The path forward requires urgency, investment and action:

- **Modernize infrastructure:** Retire legacy platforms that slow recovery and expose sensitive data.
- **Move from periodic testing to continuous monitoring:** Catch threats before they escalate.
- **Augment internal teams with trusted partners:** Ensure 24×7 expertise, faster detection, and proven response capabilities.

Cyber insurance can soften financial loss, but it cannot stop withdrawals, repair relationships or restore confidence. Only true cyber resilience can protect investor trust.



The message is clear:

the financial services market is under attack, and investor trust is on the line every day.

Modernization, vigilance, and partnership are no longer optional.

They are the new survival imperatives.



About Omega Systems

As a multi-award-winning MSP and MSSP, Omega Systems is passionate about delivering the security and compliance expertise today's businesses need alongside the responsive and reliable managed IT support they deserve. Omega's service-driven IT solutions portfolio includes 24x7 managed IT support, cybersecurity risk management, managed detection & response (MDR), backup and disaster recovery, multi-cloud connectivity, and much more. Omega Systems supports customers across the U.S. in key regulated industries such as financial services, healthcare, and professional services.



Survey Methodology

Findings are based on an Omega Systems survey conducted in August 2025 of more than 300 U.S. financial services executives, including CEOs, CIOs, CISOs, CFOs, COOs, and other senior leaders. Respondents represented firms operating in the financial services sector including family offices, RIAs, wealth management firms, hedge funds, private equity, and investment advisory firms, with assets under management (AUM) ranging from less than \$1 billion to more than \$10 billion.



Microsoft is a registered trademark of Microsoft Corporation. No sponsorship or affiliation implied.

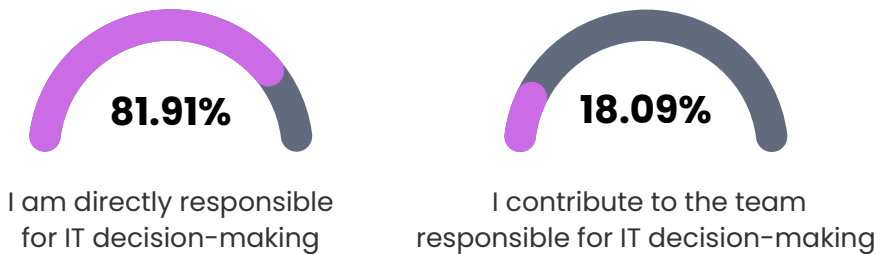
follow us: @omegasystemsMSP

learn more at www.omegasystemscorp.com

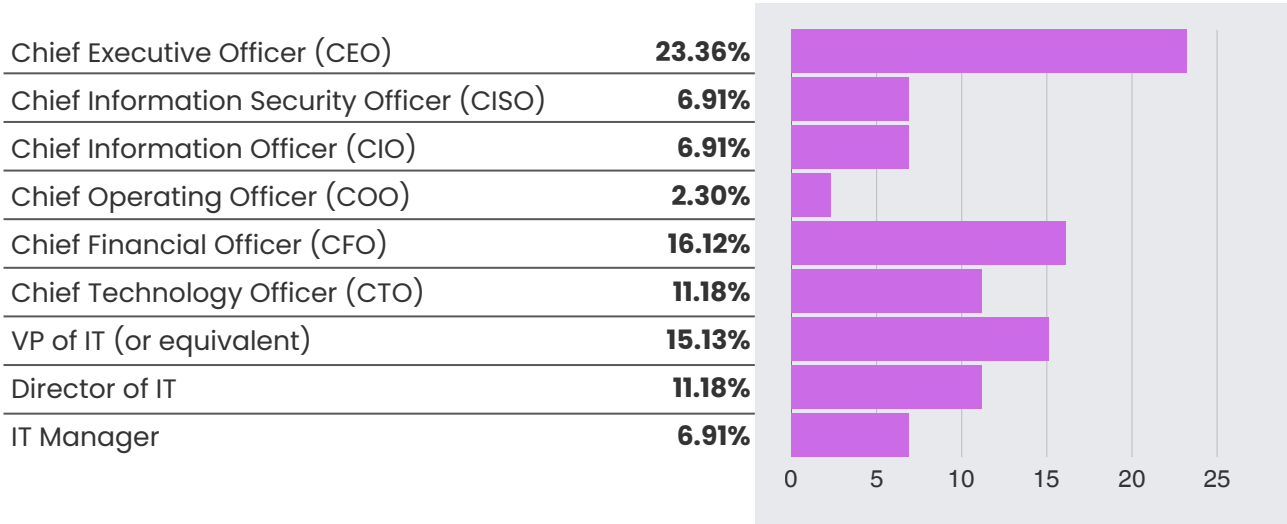
Appendix

Demographics

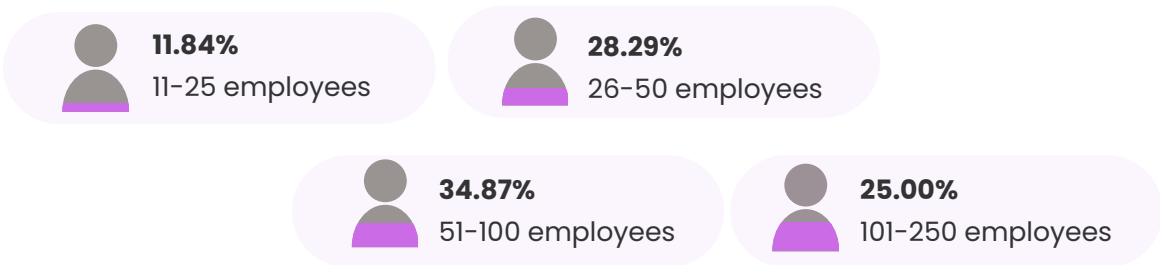
What is your role in IT decision-making?



What is your job title?

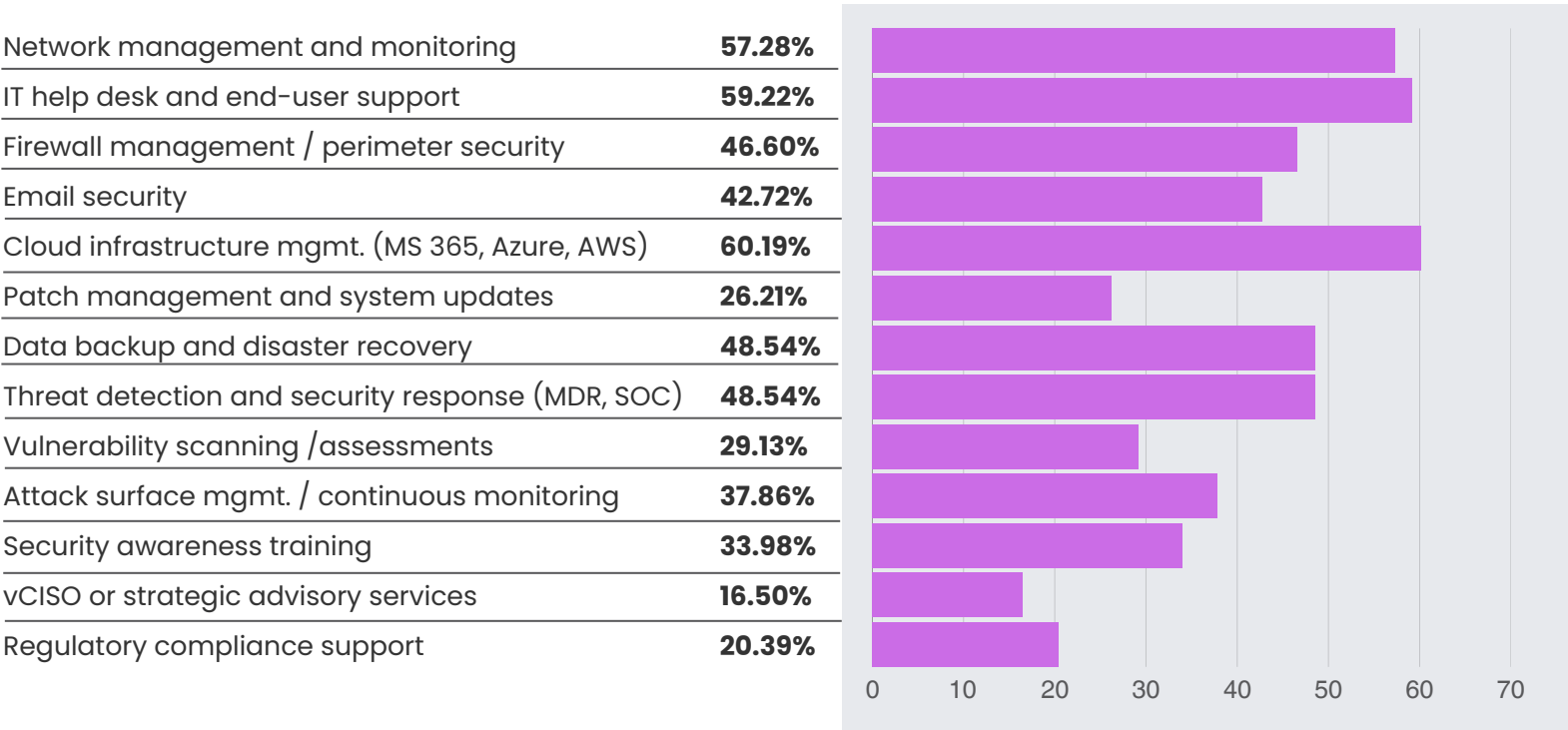


How many employees do you have?

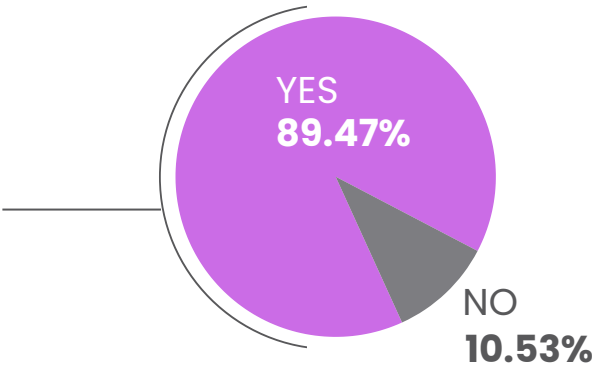


Outsourcing & Insurance Trends

Which of the following IT and security functions are currently fully or partially managed by an MSP or MSSP? *Select all that apply.*



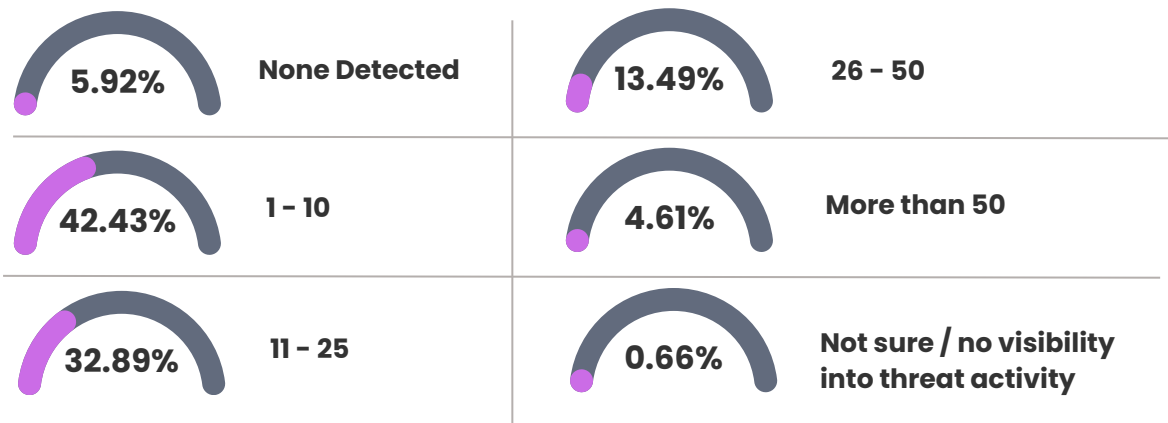
Does your firm carry cyber liability insurance?



Appendix continued

Cybersecurity Trends

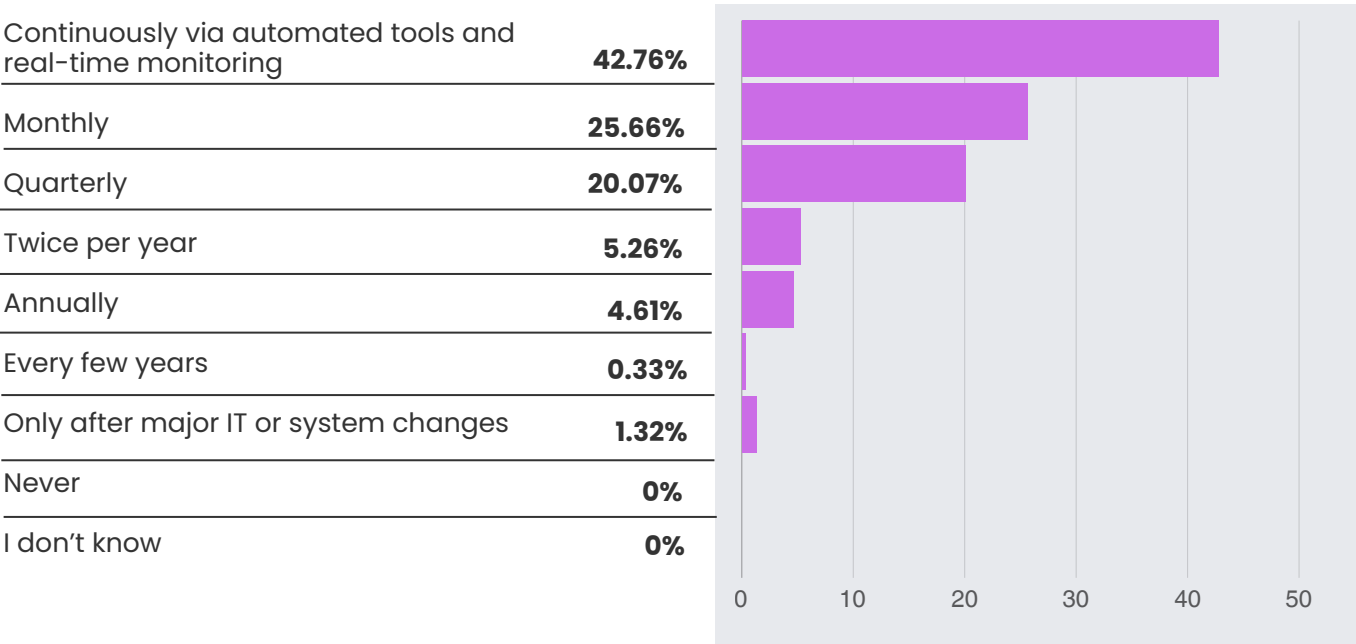
How many total cybersecurity threats did your firm detect or experience in the past 12 months? (Including phishing attempts, malware infection, unauthorized access attempts, etc.)



How has market volatility recently impacted your firm’s IT and cybersecurity spending in the past 12 months?



How often do you assess cybersecurity vulnerabilities across your networks and attack surface? (e.g. through vulnerability scans, penetration tests or IT risk assessments)



As you plan your 2026 IT and security budget, which areas are you most likely to invest in or upgrade?

