REPORT

The 2025 Cyber Threat Landscape Report:

Cyber Risks, Opportunities, & Resilience

COPYRIGHT © 2025 VIKINGCLOUD, INC. OR ITS AFFILIATES.

VIKINGCLOUD®
BUSINESS UNINTERRUPTED.

Executive Summary

The cybersecurity battlefield has fundamentally shifted.

The frequency and severity of cyberattacks continues to rise—and while AI used by bad actors is a primary driving force of the influx of attacks, new research shows it's not the only emerging threat vector that companies are scrambling to address.

Insider threats are a persistent risk and a notable source behind the incidents companies faced this past year. Additionally, escalating geopolitical tensions are creating an environment ripe for nation-state attacks. In fact, nearly 80% of cybersecurity leaders are concerned or extremely concerned they could be targeted—directly or indirectly—by a nation-state cyberattack in the next 12 months.

Several forces are compounding to create a new cyber threat landscape for organizations to navigate—one where traditional defense measures are proving inadequate against increasingly sophisticated threats.

VikingCloud set out to understand how cybersecurity leaders and their companies are responding to these challenges. The 2025 Cyber Threat Landscape Report, based on a survey of 200 cybersecurity leaders (directors and above) across the United States, the United Kingdom, and Ireland, uncovers that companies are starting to shift their strategies to keep up with savvy cybercriminals, but these steps may not be enough.

This report reveals how AI is intensifying cyber threats while also emerging as a critical line of defense. It uncovers why nearly half of security leaders hide attacks from their own organizations, and how the businesses most confident in their defenses may, in fact, be the most at risk. Most importantly, it outlines the five strategic shifts that separate resilient organizations from those destined for the next headline.

VikingCloud surveyed over

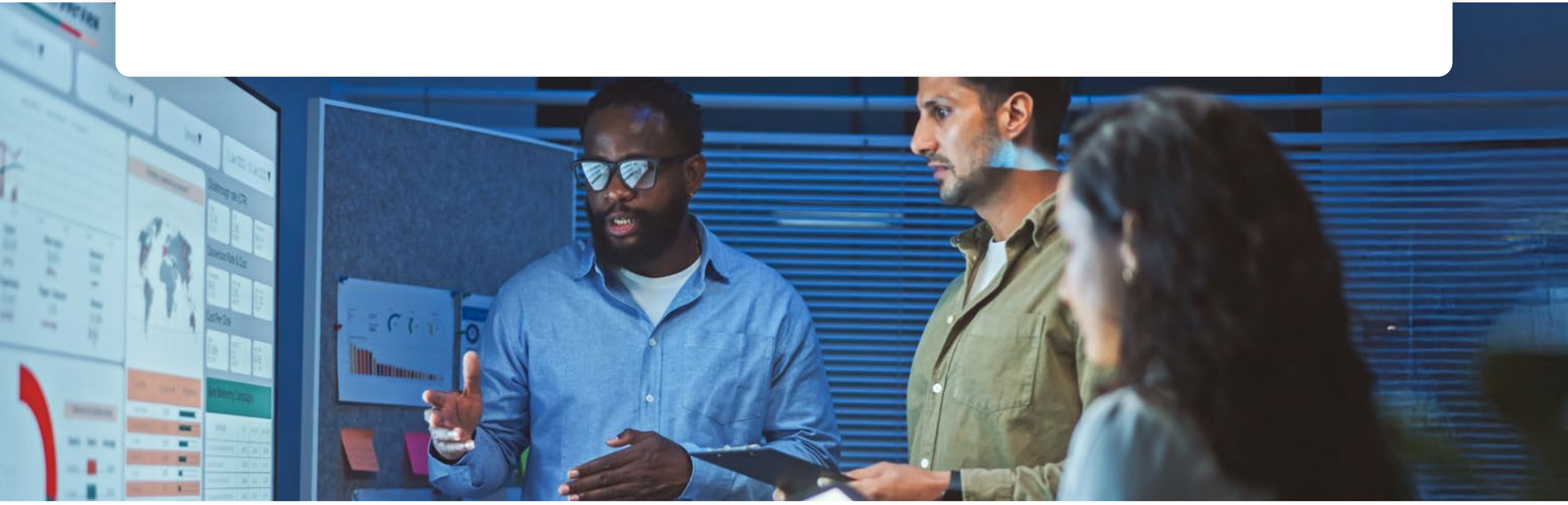
200 cybersecurity leaders

(directors and above) across the **United States, the United Kingdom, and Ireland**.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

Nation-State Attacks Are a Top Concern

Nearly **80%** of cybersecurity leaders are concerned or extremely concerned they could be targeted—directly or indirectly—**by a nation-state cyberattack in the next 12 months.**



Geopolitical tensions are high, and cyberwarfare is becoming more prevalent. Nation-state hackers—cybercriminals backed or directed by foreign governments—are impacting a wider range of organizations today, as companies of all sizes and in all industries can be affected by nation-state attacks that ripple through software supply chains. Nation-state cyberattacks are typically more advanced, persistent, and well-funded than those carried out by independent hackers or criminal groups and can cause significant operational disruption and financial loss.

These hackers typically focus on long-term access, IP theft, and espionage, and they typically infiltrate by exploiting third-party software vulnerabilities. **Many are leveraging AI to scale their attacks**. Most businesses' standard security practices and tools aren't built to detect or defend against these advanced threats. And as the U.S. federal government pulls back on cybersecurity oversight, companies are facing these threats with fewer resources, reduced guidance, and less warning.

In fact, 76% believe that recent or proposed cuts to U.S. federal cybersecurity programs, such as the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and others, could increase their organization's cyber risk.

It's important for all businesses to **invest in proactive defense measures**, but especially smaller or mid-sized firms, which are becoming prime targets for nation-state actors and are at increased risk of getting caught in the crossfire.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

Rising Cyberattacks Are Fueled by AI and Insiders

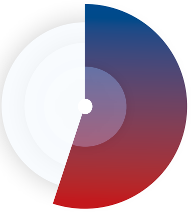
Cybersecurity leaders say the frequency (71%) and severity (61%) of cyberattacks have increased in the past year. 59% say their companies were hit with at least one successful cyberattack in the past 12 months. Over half (52%) lost more than 5% of their total revenue as a result.

This year's report shows a clear shift: more cybersecurity leaders say the frequency and severity of attacks are growing, underscoring the escalating threat environment.

In 2025, **71% report rising attack frequency and 61% cite increasing severity**—compared to 46% and 41% respectively in 2024.

For a company with an annual revenue of $500M, that's at least $25 million in financial impact from a single attack. For a smaller business with $5 million in revenue, that would mean at least $250K in losses. In fact, these types of damaging cyberattacks can cause some businesses to close their doors. According to a VikingCloud survey earlier this year, **55% of small and medium-sized businesses (SMBs) would go out of business from cyberattack impacts of less than $50,000**.

Two primary drivers of the influx of cyberattacks were AI and insider threats.



58%

of those attacked in the past year suspected AI was used.

36%

said over a quarter of their team's cybersecurity incidents in the last year were caused by insiders, either accidental or malicious.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

Cyberattacks Are Underreported—Which Leaves C-Suites in the Dark

71% of cybersecurity leaders would consider **not reporting a cybersecurity incident.**

Underreporting cyberattacks is surprisingly common and a big risk because it hides the true scale of attacks and the company's exposure, leading to false confidence in defenses.

Nearly half (48%) of cyber leaders didn't report a material cybersecurity incident to their broader executive leadership or board of directors in the past year. 86% of these leaders failed to report multiple breaches. 22% opted to hide 5 or more incidents.

The top 2 reasons why cybersecurity teams would consider not reporting an incident: (1) the perception that the broader leadership team or the board would react punitively vs. constructively to the incident (40%) and (2) concerns about the financial and reputational impact on the company if the incident became public or led to regulatory action (44%).

More Reasons Leadership Is Kept in the Dark

41% Belief that the incident could be contained internally without formal disclosure.

37% Lack of clear internal reporting protocols or a "safe" channel where incidents can be reported without fear of immediate blame.

37% Uncertainty about what constitutes a "reportable" incident.

34% Pressure from other departments or senior management to keep incidents quiet.

32% A sense of personal responsibility or shame for the incident, even if it was beyond control.

C-suites and board directors need a full picture of their company's cyber risk to make informed decisions. A strong cybersecurity defense requires creating a company security culture that provides a safe space for reporting all incidents. It's up to cyber and broader executive leadership to create those clear reporting protocols and establish a culture of continuous learning and improvement.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

Cybersecurity Teams Still Can't Keep Up with AI-Driven Attacks

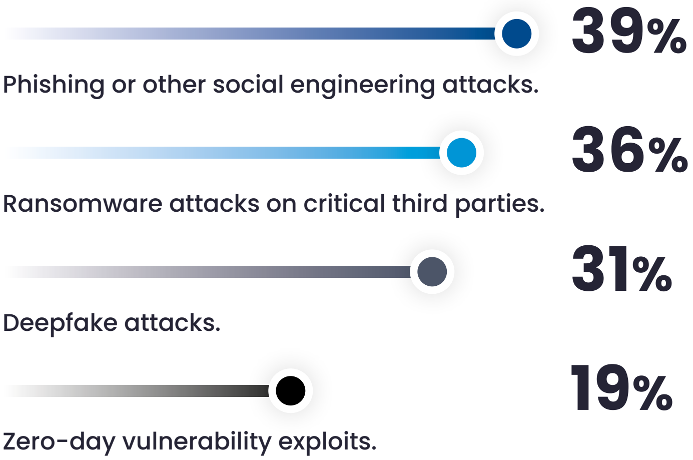
AI-driven attacks are still evolving faster than most teams can keep up.

68% of companies are only moderately or somewhat confident in their organization's ability to **detect and defend against AI-driven threats in real time**.

Cybersecurity leaders say their top 3 challenges are that (1) AI is creating new attack points (53%), (2) the tech behind cyberattacks is more sophisticated than the tech their teams have access to (36%), and (3) modern cybercriminals are more advanced than their internal teams (36%).

When asked broadly about which cyberattacks they're least prepared for, ransomware attacks on their business (46%) topped the list—up from 28% last year. This is a growing preparedness gap, likely due to hackers' greater attack sophistication with AI and the rise of ransomware as a service (RaaS), which lowers the barrier to entry and increases attack volume.

Other attacks cybersecurity leaders say they're least prepared for (which are all becoming more sophisticated with AI) include:



Notably, deepfakes are a rising concern—with an over **6x increase YoY** in organizations reporting they are **unprepared for these AI-based attacks**.

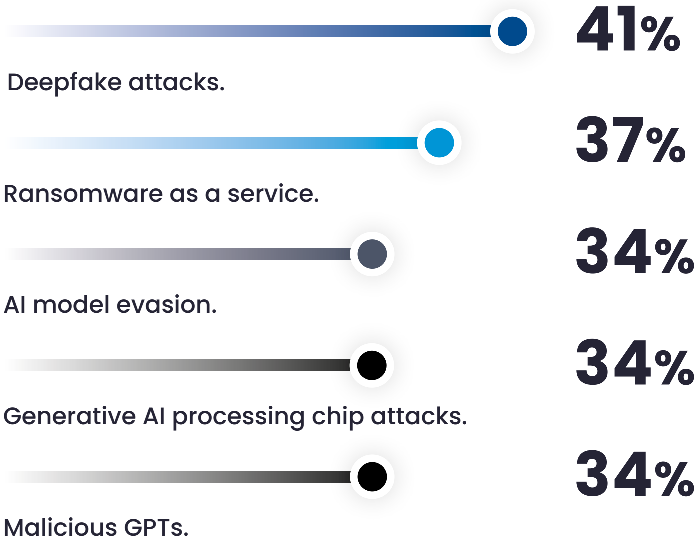
Copyright © 2025 VikingCloud, Inc. or its affiliates.

Leadership Teams Are Waking Up to the Dangers of AI Threats

Generative or agentic AI-driven phishing attacks (51%) are leadership teams' top concern when it comes to new cyberattack techniques. Last year, only 22% of respondents said that their leadership teams were concerned about generative AI phishing attacks.

This suggests that more leadership teams recognize the perils of AI-driven attack methods, especially as agentic AI becomes more ubiquitous and makes bad actors even more dangerous, efficient, and relentless than generative AI alone. Generative AI model prompt hacking (45%) and AI-vishing (voice deepfake) attacks (43%) are the other two most concerning modern threats.

Leadership teams are also specifically concerned about the following attack methods:



> "Phishing has become a top concern, not just because it's more convincing, but because it's faster, more scalable, and increasingly autonomous. With agentic AI, attackers no longer need deep technical expertise or to constantly oversee their attack campaigns.
>
> It takes much less skill and effort to launch sophisticated campaigns that evade traditional security defenses. AI is fundamentally reshaping the threat landscape in ways that organizations are just starting to grasp."

Kevin Pierce
VikingCloud
Chief Operating Officer

Copyright © 2025 VikingCloud, Inc. or its affiliates.

How Organizations Are Responding to Today's Threat Landscape

In the past 12 months, cybersecurity leaders say their organizations have increased security and awareness training (51%) and improved network security (47%) to proactively address cyber threats. 33% have allocated additional budget to their cyber program, a stark increase from the 7% who said they were increasing their budgets last year.

Evolving Defenses:
Comparing 2024 and 2025 Cyber Priorities

- Additional budget allocation **(7% → 33%)**.
- Security and awareness training **(35% → 51%)**.
- Hiring of cyber talent **(12% → 25%)**.
- Securing the software development lifecycle **(17% → 26%)**.

With 36% of cybersecurity leaders reporting over a quarter of their incidents being caused by insiders—whether accidental or malicious—organizations are recognizing that their employees serve as the first and last line of defense against sophisticated cyber threats.

Training is now the top way organizations are responding to an influx of threats, with 51% saying they've increased general security and awareness training—a 46% increase compared with those who said they were doing this in 2024.

36% of cyber leaders say over a quarter of cyber incidents start inside the organization—proof that **people, not just technology, are the frontline of defense.**

Copyright © 2025 VikingCloud, Inc. or its affiliates.

The focus on AI-specific training is particularly telling. 43% have provided training on both generative AI and agentic AI cybersecurity risks, while 40% have provided training on either generative AI (23%) or agentic AI (17%). As cybercriminals leverage AI to create more convincing phishing attempts and sophisticated social engineering attacks, organizations are racing to educate their workforce about these evolving threats.

This investment in human-centered defense acknowledges a hard truth: the most advanced security systems can be undone by a single employee clicking the wrong link or falling victim to an AI-generated deepfake. By prioritizing training, organizations are building their most scalable and sustainable cyber defense.

Nearly 5x as many cyber leaders are allocating additional budget to cyber programs compared to last year.

Only 16% report insufficient budget to hire additional staff (compared to 31% last year). Just 13% don't have enough budget to invest in new tech (compared to 35% last year).

Confidence in incident response times is on the rise, which could be a result of the steps companies are taking. In 2024, 65% of cyber leaders said it would take over 3 days to recognize and initiate a response to cyberattacks they feel least prepared for. Today, 65% say it would take less than 3 days.

The takeaway is clear: AI is changing the threat landscape—and companies are starting to evolve their strategies and defenses alongside. These changes are only going so far, and the evolution is seemingly slow, given nearly 60% still suffered an attack this past year.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

AI as an Asset: A Tool to Ease Bandwidth and Skills Constraints

96% of organizations surveyed are using AI to automate routine tasks in a way that **saves their cyber team meaningful time.**

Automation enables security teams to reallocate more time to high-value initiatives such as:

44% Advanced threat hunting.

43% Upskilling in advanced cyber domains such as cloud security, incident response playbook design, or secure development training (DevSecOps).

38% Employee security awareness training and culture building.

36% Prioritizing strategic risk management and compliance initiatives

35% Developing custom security solutions and automation scripts.

Many see AI as a powerful force to help cybersecurity teams stay ahead of the rapidly evolving threat landscape.

45% Automating incident detection and response workflows.

45% Automating threat detection and hunting.

34% Generating and analyzing security content (logs, alerts, reports).

31% Automating identity and access controls aligned with zero trust.

30% Increasing the scale and speed of security patching.

29% Reducing alert fatigue through smarter threat triage.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

Reliance on Outsourced Defenses Climbs

Year-over-year data shows that many businesses are turning to managed security service providers (MSSPs) to help close gaps in their defenses. Today, 66% of organizations rely on MSSPs in some capacity to augment internal defenses—up 2x from 2024.

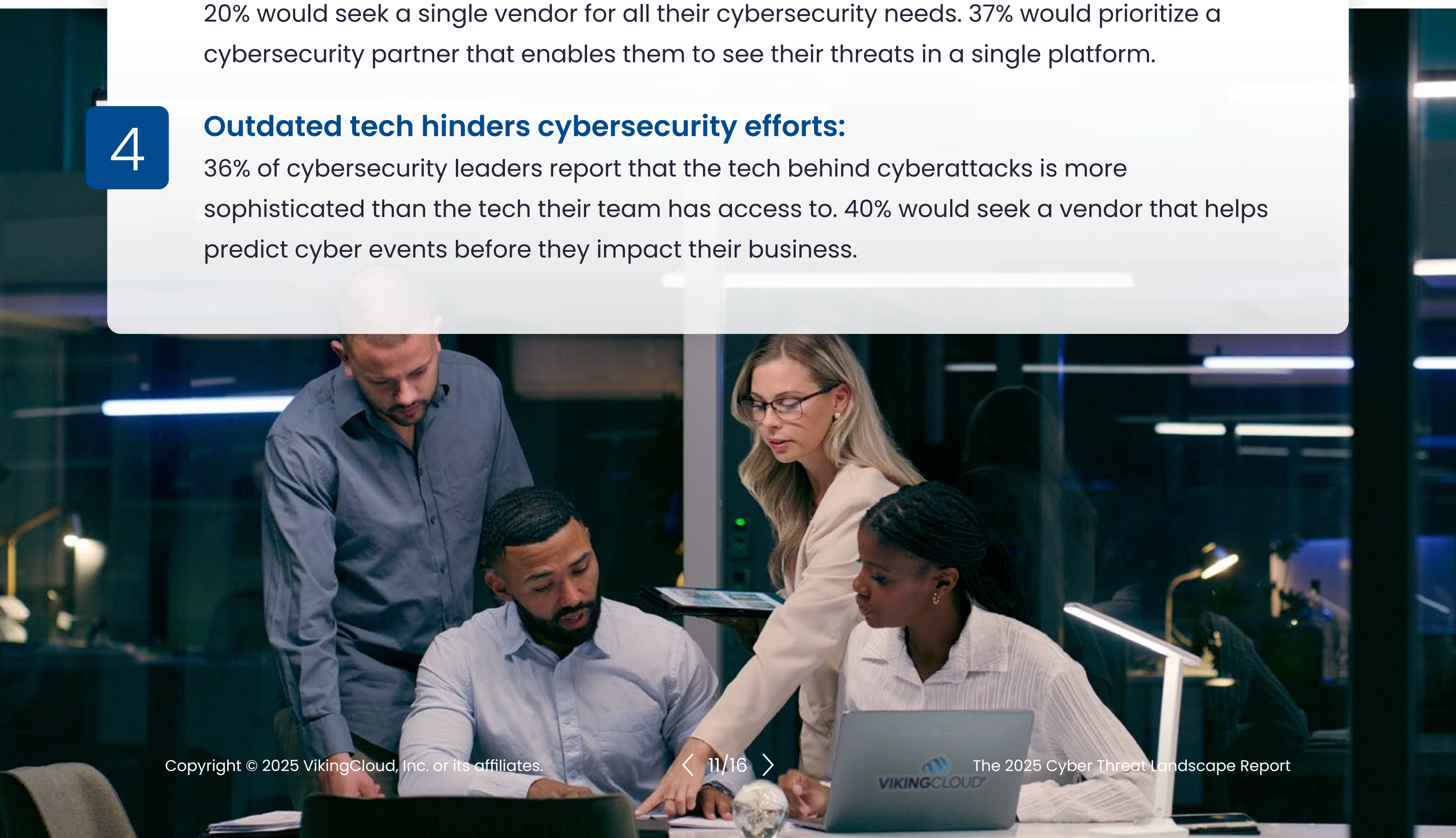
MSSP support can help cybersecurity teams solve several key challenges and evolve their defenses for today's threat landscape faster.

1 **Evolving defenses for the age of AI:**
36% of cybersecurity leaders still admit that modern cybercriminals are more advanced than their internal teams. 41% say they would prioritize a cybersecurity partner that offers GenAI and agentic AI solutions that are cost-effective and easy to use.

2 **A lack of qualified talent:**
Nearly a third (31%) still lack access to qualified talent, up from last year (19%). 31% would prioritize a partner that augments the skills of their internal team. 39% say the same for tech that helps alleviate the impacts of the cybersecurity talent shortage.

3 **Vendor overload creates complexity:**
1 in 5 say they work with too many cybersecurity vendors, which is challenging to manage. 20% would seek a single vendor for all their cybersecurity needs. 37% would prioritize a cybersecurity partner that enables them to see their threats in a single platform.

4 **Outdated tech hinders cybersecurity efforts:**
36% of cybersecurity leaders report that the tech behind cyberattacks is more sophisticated than the tech their team has access to. 40% would seek a vendor that helps predict cyber events before they impact their business.



Copyright © 2025 VikingCloud, Inc. or its affiliates.

Over the next 12 months, cyber leaders are also prioritizing cybersecurity partners that:

38%

Help manage both cybersecurity and PCI/ payment card compliance risks.

37%

Are customized to their company's unique digital environment.

35%

Limit alert fatigue by providing customized insights on threats most dangerous to their business.

35%

Offer technology backed by great customer service.

MSSPs offer more than just outsourced cybersecurity technology and services—they provide strategic guidance to help businesses grow safely and free up internal teams to be more productive.

The Bigger You Are, the Harder You're Hit

Multi-Location Businesses Face Amplified Cyber Risk

Size brings scale—and exposure. A staggering 86% of respondents say they operate multi-location businesses, and that complexity is compounding their cybersecurity risk.

29%

cite the complexity of their digital environment as a top challenge in defending against cyberattacks.

34%

report that 25% or more of their incidents stem from insiders—a risk that grows with more people, sites, and endpoints.

53%

say AI is creating new attack points faster than their teams can secure them.

Translation: More locations = more users, devices, vendors, and variables—all widening the attack surface and increasing the chance of accidental or malicious internal exposure. Even with increased budgets and AI tooling, internal teams are struggling to keep pace.

33%
cite a cybersecurity talent shortage.

Only 24%
are very confident in detecting real-time AI-driven attacks.

19%
are overwhelmed by managing too many vendors.

That's why 66% of organizations now augment internal security teams with MSSPs—to gain scale, consolidate tools, and regain control across sprawling, distributed environments.

Closing Insights

Elevate Your Cyber Defenses for the AI Era.
VikingCloud's 2025 Threat Landscape Report offers
5 key takeaways for cyber leaders.

Companies that prioritize these strategies are better positioned to go from reacting to AI-driven threats to leading with AI-powered cyber resilience.

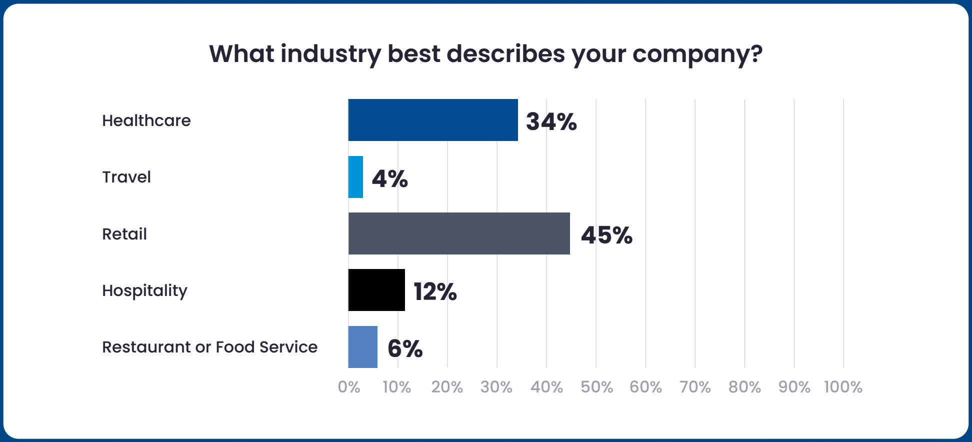
1. Recognize how geopolitical events impact cybersecurity—and prepare now to be ready for these types of attacks.
2. Adopt advanced generative and agentic AI tools to boost your defenses and keep pace with modern cybercriminals.
3. Assess your company's security culture and how that impacts incident reporting.
4. Automate what you can to save your team time—and upskill your cybersecurity workforce.
5. Consider outsourcing all or part of your cyber defense to an MSSP to help you keep up.

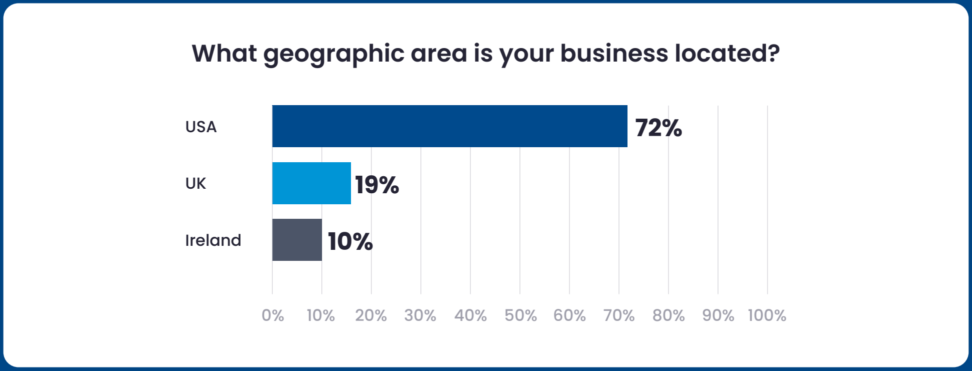
Copyright © 2025 VikingCloud, Inc. or its affiliates.

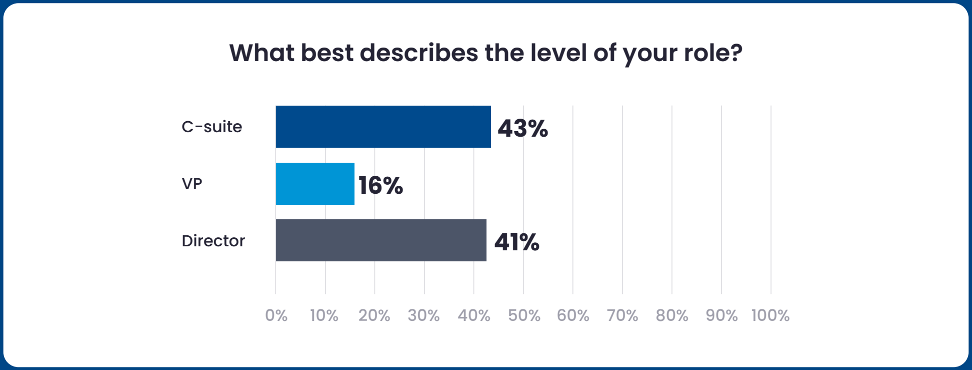
About this Study

These findings are based on a VikingCloud July 2025 online quantitative survey of **200 cybersecurity leaders** at companies in the **United States, the United Kingdom, and Ireland**, managed by an independent market research agency.

Survey respondents work at companies in hospitality, retail, travel, healthcare, and restaurant or food service. All respondents have director-level titles and above, with 43% in C-suite roles.







Copyright © 2025 VikingCloud, Inc. or its affiliates.

About VikingCloud

VikingCloud is the **leading Predict-to-Prevent cybersecurity and compliance company**, offering businesses a single, integrated solution to make informed, predictive, and cost-effective risk mitigation decisions—faster. **Powered by the Asgard Platform®**, the industry's largest repository of anonymized cybersecurity and compliance event data, we continuously monitor and analyze over 6+ billion online events every day.

VikingCloud is the one-stop partner trusted by 4+ million businesses to provide the predictive intelligence and competitive edge they need to stay one step ahead of cybersecurity and compliance disruptions to their business. Our 1,000 dedicated cybersecurity and compliance expert advisors understand that it's not just about technology. It's about transacting business and delivering an exceptional customer experience every day, without fail.

That's the measurable value we deliver.
And that's what we call, Business Uninterrupted.

6+ billion
analyze over 6+ billion online events every day.

4+ million
trusted by 4+ million businesses.

1,000
1,000 dedicated cybersecurity and compliance expert advisors.

Copyright © 2025 VikingCloud, Inc. or its affiliates.

For more information, visit:
vikingcloud.com

Follow us: in
linkedin.com/company/vikingcloud

COPYRIGHT © 2025 VIKINGCLOUD, INC. OR ITS AFFILIATES.

VIKINGCLOUD®
BUSINESS **UNINTERRUPTED.**