The frequency and severity of cyberattacks are increasing—yet most businesses remain unprepared. Between a growing talent shortage, cyber alert fatigue, and new sophisticated attack methods, companies are more susceptible than ever.

VikingCloud set out to assess the readiness of nearly 170 businesses and their cybersecurity leadership across the United States, United Kingdom, and Ireland to overcome the influx of new cyber challenges. One of the key findings: Leaders are very confident in their defenses—and that false sense of security risks leading to a damaging breach.

VikingCloud’s 2024 Threat Landscape Report uncovers an alarming disconnect between perceived and actual cybersecurity readiness. While business leaders remain confident, the facts on the ground show that cyber criminals are advancing and innovating faster than their internal teams. This report details the most critical vulnerabilities, uncovers where teams are exposed today, and how technology—especially Artificial Intelligence (AI)—is helping them fight back.

A Distorted Reality: Overconfidence Amid Rising Attacks

The vast majority of companies surveyed—96%—are confident in their ability to detect and respond to cyberattacks in real time. It’s no surprise then that only 5% have allocated additional budget to their cyber programs in the past 12 months.

Yet, a significant number of companies also report being unprepared for today’s most pressing cyber risks, including:

- **49%** Ransomware Attacks Against Critical Third Parties
- **33%** Domain Name System (DNS) Attacks
- **40%** Phishing Attacks
- **32%** Ransomware Attacks

Our research revealed readiness differences by business vertical. For example, healthcare organizations are least prepared for DNS-related attacks — 46% — vs. 38% for hospitality companies.

Is a false sense of security leading to a lack of preparedness? In the case of third-party ransomware attacks, the cyber risk companies are least prepared for, only 17% have taken steps in the past 12 months to better secure their critical supply chain.
New cyberattack methods—especially those fueled by AI—are also keeping leaders up at night. The most worrying AI threats, according to the survey: Generative AI (GenAI) model prompt hacking (46%), Large Language Model (LLM) data poisoning (38%), ransomware as a service (37%), GenAI processing chip attacks (26%), Application Programming Interface (API) breaches (24%), and GenAI phishing (23%).

This disconnect shows a distorted reality that invites significant risk. Cyber leaders are confident in their overall cyber posture but note major holes in their cyber defenses when drilling down into specific vulnerabilities, threats, and attack methods.

The Rising Skills Gap: Cyber Leaders vs. Cyber Criminals

According to our surveyed companies, cyberattacks have increased in frequency (49%) and severity (43%) over the past 12 months.

However, not all verticals are experiencing the same threat levels. Hospitality companies reported even higher levels of frequency and severity—57% and 47% respectively; travel companies have reported lower levels—36% and 35% respectively.

One clear reason why: 55% of companies said modern cyber criminals are more advanced than their internal teams. 35% reported that the technology cyber criminals use is more sophisticated than the tech their team has access to. In fact, 53% of companies admit emerging AI attack methods create new attack points they are unprepared to defend against.

Many cyber teams are not trained for the emerging GenAI-fueled attacks. VikingCloud found that a third of companies still have not trained their team on GenAI-related cyber risks. This oversight, paired with ongoing challenges related to talent and resources, paints a bleak picture for resilience in the months to come.
Persistent Pain Points: A Talent Shortage, Limited Resources & More

Cyber teams are facing major strains, from a growing talent shortage to cyber alert fatigue, which increases vulnerability.

Only 10% of companies have increased cyber hiring in the past 12 months. The primary roadblock is the ongoing talent shortage, with the industry workforce gap standing at about four million workers currently, according to ISC2. Nearly 20% of companies say a lack of qualified talent is a key challenge to overcoming cyberattacks.

The challenges are also financial. 35% of companies don’t have enough budget to invest in new tech and 32% don’t have enough budget to hire more staff.

Making matters worse, most companies are dealing with a lot of false alerts, which distract and waste the scarce resources they have.

Our research found that:

- **33%** of companies were late to respond to cyberattacks because they were dealing with a false positive.
- **63%** of cyber teams spend 4 or more hours per week dealing with false positives (equating to 208 hours per year).
- **15%** of teams spend more than 7 hours per week or over 364 hours per year managing false positives.

Travel companies report being more prepared to deal with false positives, as only 21% were late to respond to a cyberattack. Hospitality companies are even less prepared: 43% were late to respond to a cyberattack because they were dealing with false positives.
The resource constraints also impact incident preparedness. Most companies rarely practice incident response, with 58% conducting drills only quarterly or annually.

⚠️ The Securities and Exchange Commission’s new disclosure rule has set the industry standard for incident response at four days. 68% of companies surveyed would not meet this benchmark currently.

It’s alarming to note that some teams are skipping disclosure altogether. **40% of cyber teams have intentionally not reported cyber incidents because they were worried about losing their jobs.**

The research notes that non-disclosure of cyber incidents is even higher for hospitality companies, with 54% stating they did not report a cyberattack. In contrast, “only” 30% of healthcare and 21% of travel companies did not report a cyberattack out of fear of expected consequences.

This research disclosure signifies a serious underreporting of cyber global breaches—which is alarming given the already record high levels of reported incidents in 2023, which is only expected to grow in 2024. This lack of transparency is also concerning because cyber leaders do not have the full picture of their own cyber posture. You can’t fix what you don’t know about; staying exposed means a successful attack can easily cascade into a breach that’s both more severe and expansive.

To learn from each cyber incident to uplevel future defenses requires full transparency into the actual risks facing the team.

**GenAI: A Weapon for Transformed Cyber Defense**

Technology has the potential to be an equalizer for cyber teams. For instance, 24% of respondents said GenAI has the potential to create more efficient incident response plans.

Tech also helps teams overcome workforce constraints. 63% of companies are looking to implement new tech that can help alleviate the impacts of the cyber talent shortage—which was rated as the most important factor for companies choosing a new solution. 41% say GenAI has the most potential to close the cybersecurity talent shortage and skills gap.
There are two ways cyber leaders can look at GenAI—as a threat or as a weapon. The reality is that it’s both—which makes it essential for businesses to aggressively implement the technology to beat criminals at their own game. The only other alternative is falling behind.

**Grow Confident in Your Cyber Defense**

The 2024 Threat Landscape Report offers 6 key takeaways for cyber leaders:

1. **Address** your team’s overconfidence in their cybersecurity posture.
2. **Assess** your organization’s actual preparedness for the myriad of new cyber risks emerging everyday.
3. **Invest** in GenAI tools to close the technological gap between your cyber team and criminals.
4. **Prioritize** technology that alleviates the cybersecurity talent shortage, lack of resources, and cyber alert fatigue.
5. **Develop** robust incident response plans to meet industry disclosure standards.
6. **Create** a culture where employees aren’t afraid to speak up, either before or after a cyber incident.

Companies that prioritize these strategies at the forefront of their approach are better positioned to respond to threats, limit disruption, and build resilience in this new era of cyber risk.
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.

Position your organization to better respond to threats, limit disruption, and build resilience in this new era of cyber risk. Visit vikingcloud.com today and check us out on LinkedIn at linkedin.com/company/vikingcloud.
**About this Study**

These findings are based on a VikingCloud April 2024 online quantitative survey of 168 cybersecurity professionals at companies in the United States, United Kingdom, and Ireland managed by an independent market research agency. Survey respondents work for companies in the healthcare, hospitality, travel, and retail industries; 77% of respondents have Director-level titles or above.

---

**What Geographic Area is Your Business Located?**

- **USA**: 58%
- **UK**: 21%
- **Ireland**: 21%

**What Best Describes the Level of Your Role?**

- **Manager**: 23%
- **Director**: 44%
- **VP**: 15%
- **C-Level**: 18%

**Who Oversees Your Company’s Cybersecurity Program?**

- **In-house cybersecurity team**: 60%
- **Outsourced managed security service provider (MSSP)**: 22%
- **Combined MSSP and in-house cybersecurity team**: 15%
- **We don't have a cybersecurity program**: 3%

**What was the Annual Revenue for Your Company Last Year?**

- **<1M**: 2%
- **1M-4.9M**: 30%
- **5M-9.9M**: 15%
- **10M-19.9M**: 17%
- **20M-99.9M**: 5%
- **>100M**: 5%