2023

Cyber Risk Confidence Index

CRITICALSTART®

Key Findings

66% of U.S.-based cybersecurity decision-makers are **not highly confident that their current strategies for evaluating and mitigating major cyber risks are effective**.

67% of organizations **have been breached in the past two years**, despite having traditional threat-based detect and respond security solutions in place.

61% of respondents claim their organization's **cybersecurity investments and risk reduction priorities are not highly aligned**.

51% of companies are **failing to run full and comprehensive cybersecurity assessments and risk evaluations more frequently than once every six months**.

83% of security leaders say their firm **prioritizes the cost of security over the risk of a breach**.

63% of organizations **cannot fully quantify the return on investment (ROI) for their cybersecurity initiatives** or the risk reduction impact they make.

73% of security leaders **feel their cybersecurity team needs more resources**.

46% of organizations **have only one dedicated person responsible for managing and reducing cyber risk**. **10%** do not have anyone dedicated solely to cyber risk reduction.

69% of security leaders **say that unknown organizational cyber risk is a top concern**.

82% of respondents **expect security vendors to leverage AI technology** to enhance their cyber risk capabilities in the next 12 months.

Risk vs. Reality:
Understanding Cyber Risk Confidence

Organizations today face the often-insurmountable challenge of aligning their cyber protection measures with the level of risk they are willing to accept, balancing the need to mitigate threats against the financial and operational realities of implementing robust cybersecurity measures.

They do so against the backdrop of greater cyber risk, more sophisticated cybercriminal tactics, techniques, and procedures (TTPs), and under resourced security teams. Experts predict that the cost of cybercrime will hit **$8 trillion in 2023** and will grow to **$10.5 trillion by 2025**.[1] Cybercrime has become a lucrative industry that incentivizes malicious actors to constantly find ways to circumvent prevention measures and avoid detection. As a result, security professionals are scrambling to stay ahead of attackers and avoid a breach that disrupts business operations.

Critical Start's study examines the current level of confidence IT security leaders have in their existing risk evaluation and mitigation strategies and solutions and how that aligns to their organization's appetite for cyber risk. The Cyber Risk Confidence Index is illustrative of the perceptions organizations have of the efficacy of their current cybersecurity infrastructure. The study also reveals the greatest challenges security leaders face in today's threat environment and examines ways organizations feel they can best overcome those challenges.

Methodology

Via online survey, Censuswide sampled 501 IT decision makers (18+) in cybersecurity (VP+) within businesses with 2,500-25,000 employees in the U.S., between June 27, 2023 - July 3, 2023. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

Cyber Risk Confidence Index:
The Cyber Risk Confidence Index has been calculated focusing on respondents' perceptions of the success of their cybersecurity infrastructure. We have avoided basing the scoring on breaches detected as that maybe a sign of a successful defense, whereas perception gives us a better indication on the overall health of the security. The scoring is based on positive scores, so all answers give a positive score, but the more positive the view the higher the value added to the score. The groupings have been banded relatively between respondents. The most positive grouped in the highest score with four groups in total, which gives us a relative view of responses and good bases sizes to analyze.

Little Confidence in **Current Cyber Risk Strategies**

66% of U.S.-based cybersecurity decision-makers are not highly confident that their current strategies for evaluating and mitigating major cyber risks are effective. That number grows to 78% for the largest organizations surveyed – those with 20,000 to 25,000 employees.

The lack of confidence might come as a surprise to many, but it is well placed considering the following results of our research:

67% of organizations surveyed **have experienced a cyber breach requiring attention** in the past two years despite having implemented traditional threat-based detect and respond security measures. Even with the expanse of technology and cybersecurity solutions on the market today, attackers are still successful.

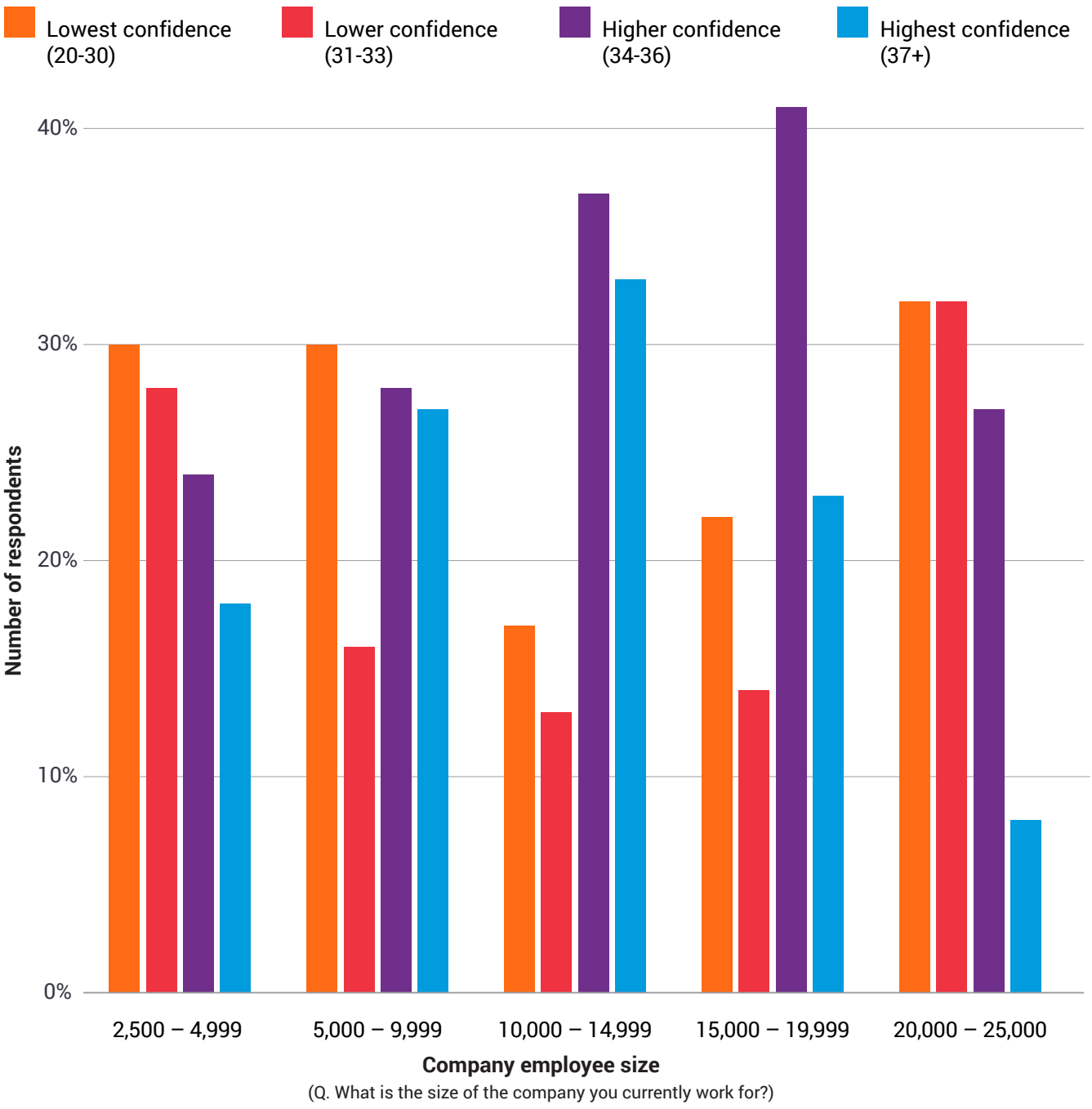
83% of organizations **prioritize the cost of security over the risk of a breach**. Current economic headwinds have put IT budgets under greater scrutiny, and cybersecurity could be taking a hit as a result.

61% of respondents claim their organization's **cybersecurity investment and quantifiable risk reduction priorities are not fully aligned**, while 90% say that obtaining that alignment is at least somewhat of a priority.

51% of firms are **failing to conduct a full and comprehensive cybersecurity assessment** and risk evaluation even once every six months, despite the number of cyber breaches. With a highly dynamic and volatile threat landscape, a more frequent way to understand organizational risk is needed to successfully defend against attack.

46% of organizations **cite challenges with the evolving and sophisticated threat landscape** as being a significant barrier to effectively managing cyber risk. 44.5% also identify a lack of resources as being a top challenge.

Cyber Risk Confidence Index
by Company Size



(Q. What is the size of the company you currently work for?)

IT Leaders Hungry for **More Balanced Risk Appetite**

While measures can be taken to manage risk, it is impossible to eliminate it completely.

A risk appetite refers to the amount of risk an organization is willing to accept after controls have been put into place.

It's essentially asking how comfortable the organization is with the amount of risk they are accepting with their current solutions and strategy.

Striking the right balance between investment and risk appetite is not easy, yet a high degree of imbalance leaves businesses vulnerable to attack.

A staggering **83%** of respondents surveyed believe their organization currently prioritizes the cost of security over the risk of a breach. The problem is most prevalent at mid-sized organizations, with **88%** of respondents based at firms with 15,000 to 19,999 employees agreeing that cost is the priority, with **86%** prioritizing cost where the workforce is between 10,000 and 14,999.

To sufficiently fund risk reduction measures, security leaders are often required to demonstrate both effectiveness and ROI, yet **63%** of organizations say they cannot fully quantify ROI for their cybersecurity initiatives or the risk reduction impact they make. Accessing and analyzing the data security leaders need to demonstrate ROI and inform security investment decisions is painful.

Complicating the issue further is that cybersecurity is often a part of the business that is the least understood. This leads to friction between security teams, business leaders, and the board. Even where risk is known, organizations wrestle with small staffs already over capacity, broad multi-domain security expertise requirements, and limited budgets. As a result, organizations are playing security investment roulette and are guessing where to place their security bets.

Cyber Risk
Often on One Expert's Shoulders

For many years, cybersecurity has been plagued by a substantial shortage of skilled talent. At the end of 2022, there was an estimated cybersecurity workforce gap of **3.4 million worldwide**[2]. Adding insult to injury, burnout has now begun to infiltrate the security leadership ranks with little being done to address it. According to Gartner®, "by 2025, nearly half of cybersecurity leaders will change jobs, **25%** for different roles entirely due to multiple work-related stressors."[3]

It likely comes as no surprise that **73%** of security leaders in our study feel their cybersecurity team needs more resources. While **90%** of respondents say their organization has dedicated resources responsible for managing and reducing cyber risk, in almost half of situations (**46%**) this consists of just one person. This is more often the case at companies with between 15,000 and 19,999 employees (**50%**).

Companies with the highest level of confidence, according to our Cyber Risk Confidence Index, are the most likely to have only one person overseeing risk (**58%**). The opposite is true in organizations with a cyber risk team of more than one person in place. These companies are most likely to have the lowest confidence in their cyber risk management operations (**49%**).

Alarmingly, this could be a case of unknown variables. An overburdened security team of one likely has neither the time nor the resources to perform the manual, non-evidence based, limited scope assessments currently available today. Those that are confident in the effectiveness of their existing solutions could be operating with a false sense of security. This can be especially troubling for smaller businesses, as our research found that **75%** of companies with 2,500 to 4,999 employees experienced a cyber breach in the last two years and were about **10%** more likely to have experienced a breach than organizations with a larger workforce of 20,000 to 25,000 (**64%**).

58%

of companies with the highest level of confidence are the most likely to have only one person overseeing risk.

Cybersecurity Assessments
Too Infrequent

Considering the astronomical cost of cybercrime and its potential to severely disrupt the act of doing business, many organizations immediately look toward more security people and more security tools as the best way to fend off cybercriminals. But with such a shortfall of skilled security talent, more people are hard to come by. Having more tools solves all problems…until it doesn't. Big enterprises currently have an average of **76** security tools,[4] yet a majority of security leaders now agree that monitoring and addressing expected controls failure and risk will likely have a bigger impact on their security posture than buying additional tools providing more controls.[5]

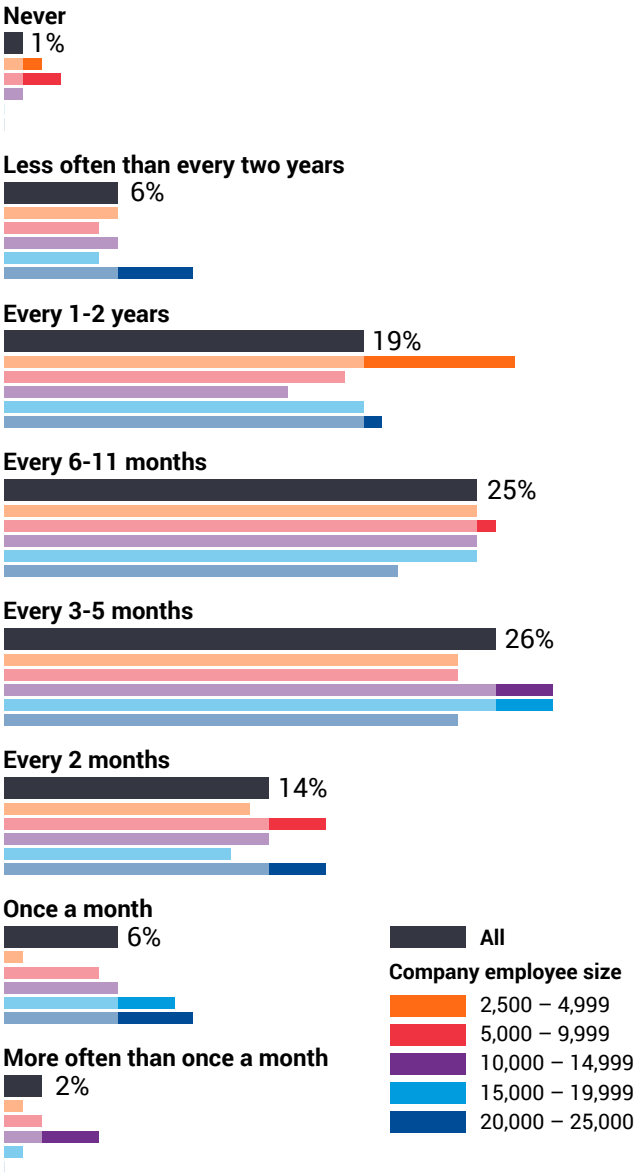
Our research findings indicate that **51%** of firms are failing to conduct a full and comprehensive cybersecurity assessment and risk evaluation more frequently than once every six months. That number jumps up to **60%** for smaller businesses of 2,500 to 4,999 employees.

Respondents whose organizations have the lowest confidence as revealed by the Cyber Risk Index carry out tests less frequently, at **2.80** times annually. Those with the highest confidence do so the most often, **4.49** times per year.

To have true confidence that cyber risk levels are at accepted and expected levels, organizations must have a way to understand risk more frequently, if not at all times. This is critical amid a highly dynamic threat environment and constant changes to organizations' security posture.

"by 2026, organizations prioritizing their security investments based on a continuous exposure management program will be three times less likely to suffer from a breach."
Gartner [6]

How often, if ever, do you conduct full and comprehensive cybersecurity assessments and risk evaluations across your environment?



Moreover, Gartner expects "the number of security service providers that provide cybersecurity validation assessments to test their service efficacy and their client's security posture will grow from less than **10%** in 2023 to over **50%** by 2026."[7]

Expansive Threat Landscape
Key Concern for IT Leaders

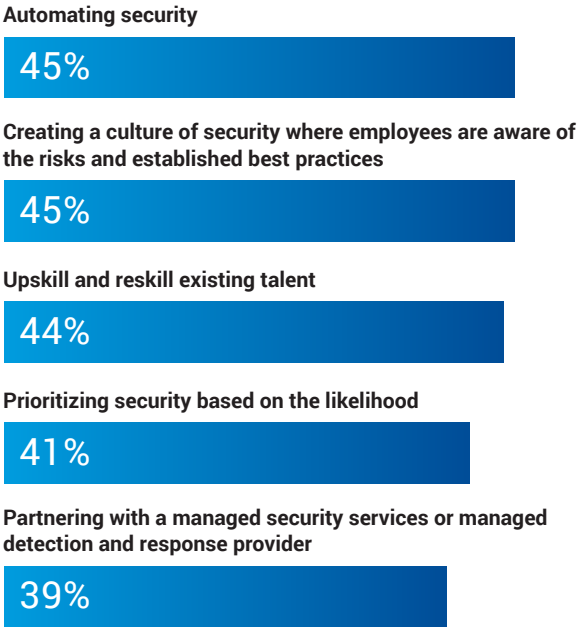
Cybersecurity leaders today face a growing list of challenges to securing their organizations. The increasing sophistication of an evolving threat landscape is the challenge respondents cited most frequently (**46%**). A similar level of concern is ascribed to the lack of resources at IT and cybersecurity leaders' disposal (**45%**). **38%** of companies directly cite budgetary pressures as a problem. Additionally, **37%** say lack of expertise at their business is hampering efforts to provide effective cyber risk management services.

Finally, the lack of risk assessments is also deemed a critical problem. Currently, **44%** of cybersecurity decision-makers say unknown or unmeasurable cyber risks are a challenge. Also, more than two thirds (**69%**) go further, naming unknown cyber risk as a top concern. Notably, these unknowns seem to alarm IT and cybersecurity leaders at the highest-confidence companies according to our Cyber Risk Confidence Index (**79%**).

Automation
to the Rescue?

Automation is seen as the best solution to addressing cybersecurity challenges by almost half (**45%**) of respondents. The biggest organizations are the most eager to automate security: **54%** of those with 20,000 to 25,000 employees. But several other solutions to successfully tackle a cybersecurity headcount shortage are also recognized, ranging from instilling a culture of cyber risk to calling on third-party support.

How can organizations effectively manage their security posture in the face of a headcount shortage in cybersecurity? *(Select all that apply)*



Meanwhile, IT and cybersecurity leaders are split on what must happen next to mitigate cyber risk - and have ranked the measures below by their level of importance.

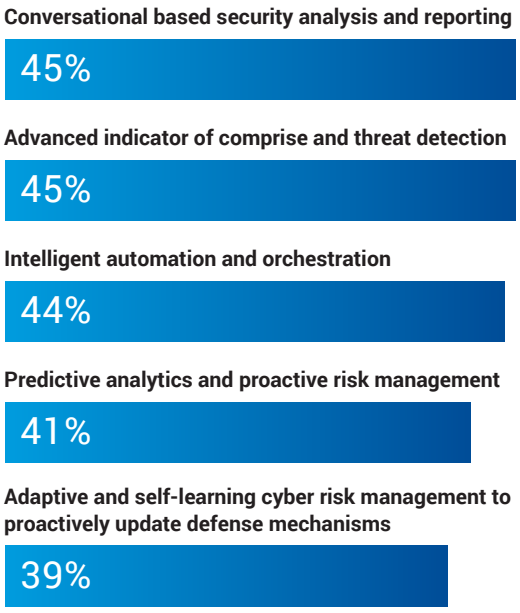
What, if anything, do you need more of to prevent cyber risk? *(Select all that apply)*

To help solve the people problem, **93%** of security leaders plan to offload cyber risk reduction workstreams to external security service providers during the next two years, and more than half (**54%**) will do so for the first time.

The number drops to **86%** at organizations considered to have the lowest confidence according to our Cyber Risk Confidence Index. Companies that are the least confident in their ability to tackle risk are also the most reluctant to outsource security, raising the question of how cyber risk concerns will be alleviated.

With the vast majority of organizations eager to offload more cyber risk tasks to external experts, there is also a groundswell of support for Artificial Intelligence (AI) to enter the fray. **82%** of respondents expect security vendors to leverage AI technology to enhance their cyber risk capabilities in the next 12 months. The companies that have the highest confidence in their current cyber risk reduction tactics are most likely (**55%**) to want AI-based cyber risk services to be provided by vendors within the next year.

What capabilities do you expect AI to provide to enhance your cyber risk management capabilities within the next year, if any? *(Select all that apply)*



Increasing
Cyber Risk Confidence

Security leaders are struggling with balancing the need to mitigate threats against the financial and operational realities of implementing robust cybersecurity measures, while attempting to align their organization's risk appetite and cost constraints. All while looking for comprehensive security protocols that factor in industry benchmarking, best practices, and regulatory requirements.

Cyber leaders have shown there is a need to look at their cybersecurity program and risk profile more holistically and continuously, which can increase stakeholder confidence in reducing their cyber risk aligned to acceptable levels of risk tolerance. To better manage cyber risk and reduce the likelihood of a breach, organizations often turn to frameworks like the National Institute of Technology Cybersecurity Framework (NIST CSF).

The NIST CSF was originally released in 2014, with the latest release in 2018, and has become widely adopted across organizations as a tool for managing cyber risk, and buckets capabilities across five functions: Identify, Protect, Detect, Respond, and Recover.

Managed Detection and Response (MDR) providers add the value of expertise and action to a subset of telemetry and products to reactively contain threats and lower attacker dwell time. As a cornerstone to reducing risk, MDRs are often the quickest time to value for organizations. With security maturity aligned to the "Detection" and "Response" NIST CSF categories, MDR can give organizations the greatest reduction in reactive risk per dollar spent – with the right solution.

Partnering with a trusted third-party security services provider, like Critical Start, can help.

Critical Start is an industry-leading Managed Detection and Response (MDR) provider that offers 24x7x365 monitoring with an expert human-led security operations team that can take actions on your behalf.

Cyber leaders today have shown that there is a need to look at their cybersecurity solutions more holistically, increasing confidence in their cyber risk management. To learn more about taking control of your risk appetite, contact Critical Start to speak with an expert.

[1] Cybersecurity Ventures
[2] (ISC)2
[3] Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, by Deepti Gopal, Leigh McMullen, Andrew Walls, Richard Addiscott, Paul Furtado, Craig Porter, Oscar Isaka, Charlie Winckless, published January 25, 2023
[4] (ISC)2
[5] Panaseer
[6] Gartner Implement a Continuous Threat Exposure Management (CTEM) Program, by Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider, published July 21, 2022
[7] Gartner Emerging Tech: Grow Your Security Service Revenue With Cybersecurity Validations, by Travis Lee, published April 10, 2023


CRITICALSTART®