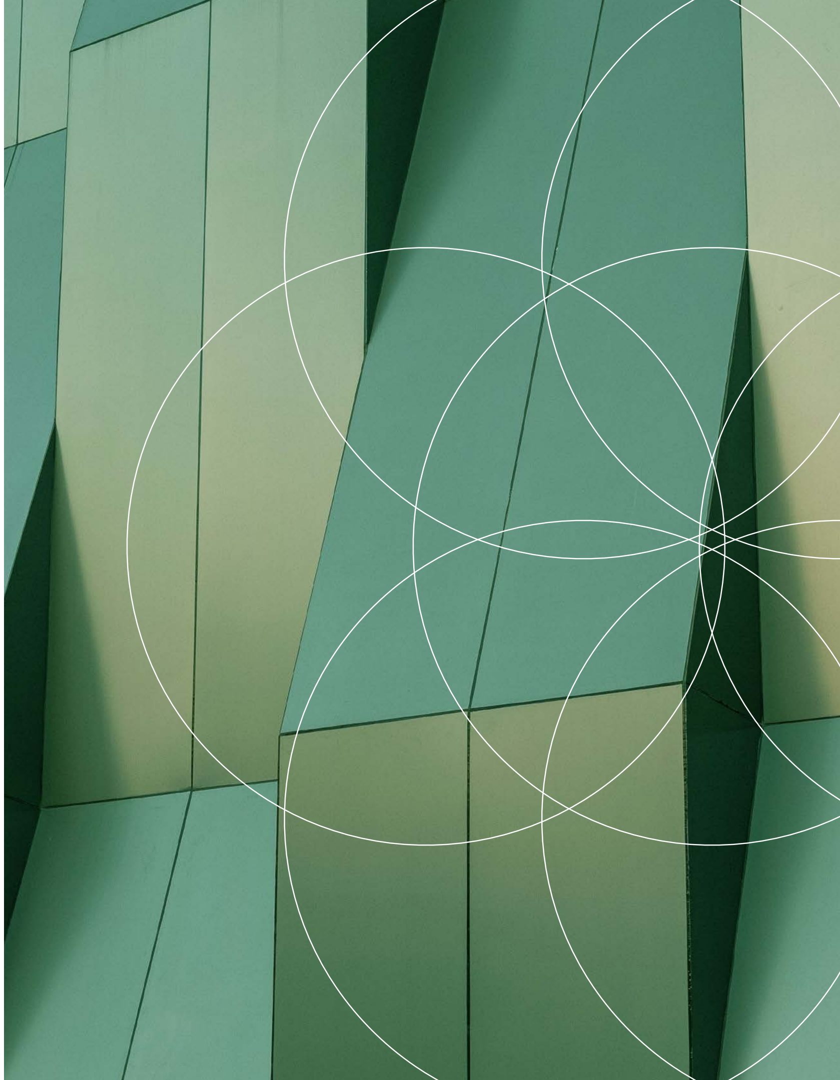
Protect Your Organization’s Future With A Proactive Cyber Risk Management Strategy

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CRITICAL START | JANUARY 2024



Overview
Situation
Approach
Opportunity
Conclusion

Overview

In today's world, it's increasingly challenging for security and risk teams to know if their current cyber risk management efforts are adequate. Knowing where to invest and what to prioritize regarding risk reduction requires a substantial effort that many security teams are unequipped to manage. Limited organizational visibility and lack of training also prevent many organizations from being more proactive with cyber risk management. This hampers teams' ability to reduce the number of security incidents and puts pressure on staffing that is already limited in terms of capacity and expertise. Security and risk teams struggling to keep up need to consider ways to make their cyber risk management approach more holistic, or better identifying risk and vulnerabilities while also improving the ability to detect and mitigate attacks. This will ease the pressure on teams and make them feel more confident in their cyber risk management posture.

Key Findings

Eighty-one percent of respondents believe that their current cyber risk management approach is inadequate at addressing the full scope of threats facing their organization.

Ninety-seven percent of security and risk leaders surveyed agree their organizations need to be more proactive in the way they manage cyber risk.

Third-party service providers can offer valuable technology, expertise, and staffing resources to help organizations better execute holistic risk reduction strategies.

Overview
Situation
Approach
Opportunity
Conclusion

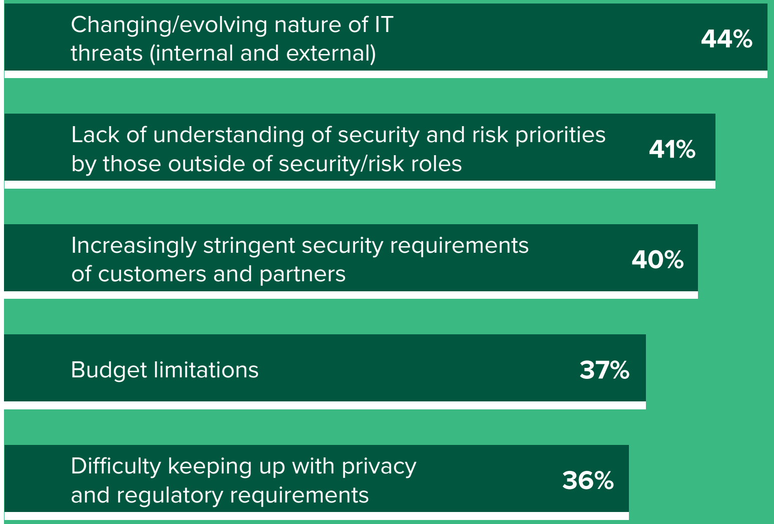
Current Cyber Risk Management Approaches Are Falling Short

One of the top challenges that security and risk leaders face today is the evolving nature of cyber risks and threats. As organizations grow and change, security and risk teams must be vigilant to ensure they have insight into all potential risks and vulnerabilities within their environments. When combined with pressure from customers and partners to tighten security requirements and budget challenges, executing an effective cyber risk management strategy can be extremely difficult. Surveyed security and risk leaders agree this is a challenge, as 81% believe that their current cyber risk management approach is inadequate at addressing the full scope of risks facing their organization. Not to mention the 41% who reported a lack of understanding of security and risk priorities by those outside the security organization, which makes it harder to establish and execute key cyber risk reduction priorities.

81%

of respondents agree their organization's cyber risk management approach is inadequate at addressing the full scope of risks.

Top Cyber Risk Management Challenges



Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Top five responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Overview
Situation
Approach
Opportunity
Conclusion

Effective Cyber Risk Management And Reduction Requires Holistic Vision And Strategy

Over 90% of security and risk leaders from our survey agree their organization needs a more comprehensive cyber risk management approach that spans multiple cybersecurity domains. This requires two fundamental pieces that more than one-third of risk and security leaders struggle with: not having a full view of potential risk vectors across the business and limited access to siloed enterprise and application data. Both hinder teams from quickly uncovering actionable insights in cyber risk management.

Security and risk team teams need better visibility of their organizational risk. Areas that especially need this include asset inventory, security controls and safeguards, controls gaps, and incident response plans. Without a clear view of risks, 39% of leaders surveyed reported being unable to connect risk reduction metrics to key business strategies and investments. These challenges, coupled with the ongoing need to address active security threats, hinder proactive risk and security improvements, leading to a reactive approach in cyber risk management.

92%
of respondents agree their organization needs a more comprehensive cyber risk approach that spans multiple cybersecurity solutions (e.g., IAM, vulnerability, patch, cloud, etc.).

Technical Capability Gaps In Cyber Risk Reduction Support

40% Overly manual and cumbersome risk reduction-related tasks

39% Limited view of all potential risk vectors across the business

38% Inability to connect risk reduction metrics with budgets and investments

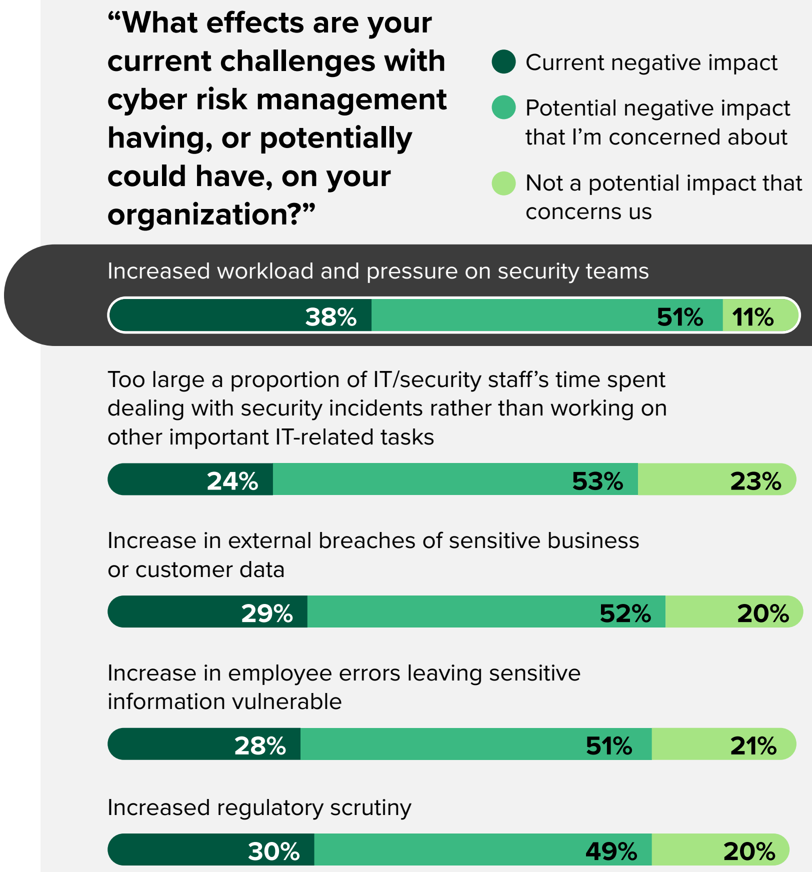
37% Difficulty accessing the right enterprise and application data to properly assess cyber risk

37% Inability to act quickly on risk-related issues

Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Top five responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Reactive Cyber Risk Approaches Are Overburdening Security Teams

Security and risk leaders are worried that continuing with their current reactive approaches to cyber risk management will increase the workload and pressure on security teams. This could lead to errors and allow future attacks to be more successful, resulting in potential losses or regulatory actions. Responding to the steady assault of cyberattacks will continue to dominate much of the time and energy of security teams without a clear strategy to preempt attacks, and they will eventually be overburdened if changes are not made. Furthermore, 77% of security and risk leaders are concerned about overspending their staff's time on responding to security incidents versus working on other essential tasks. A more proactive cyber risk reduction approach could help address risks sooner and faster and allow more time for staff to work on other important IT-related tasks.



"What effects are your current challenges with cyber risk management having, or potentially could have, on your organization?"

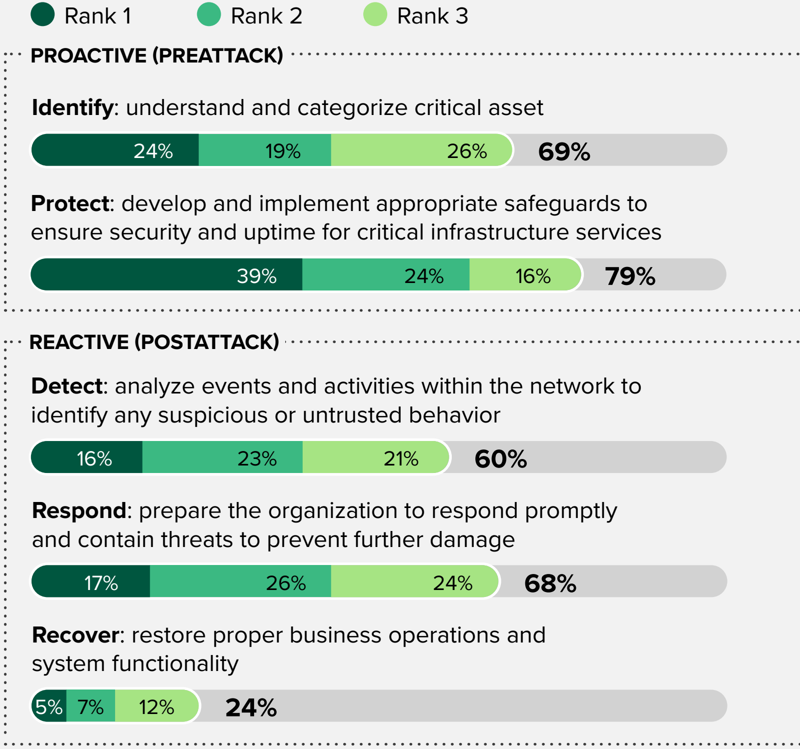
Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Top five responses shown; Percentages may not total 100 due to rounding
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Overview
Situation
Approach
Opportunity
Conclusion

Proactive Cyber Risk Management Practices Are Essential For Risk Reduction

Knowing the steady workload of security incident responses that security teams face, 97% of surveyed security and risk leaders agree that their organizations need to be more proactive in managing cyber risk. A more proactive cyber risk management approach should focus on improving visibility of risks across the organization so that proper precautions can be taken before security incidents occur. Investment in better proactive security — such as risk assessment tools, security control monitoring, and risk mitigations — ideally results in fewer security incidents to deal with, thereby alleviating some of the existing capacity constraints on security teams. With these outcomes in mind, leaders plan to focus more on proactively identifying risks and protecting critical business functions.

"Please rank the importance of these categories as it relates to where your organization wants to focus its cyber risk strategy and investments."



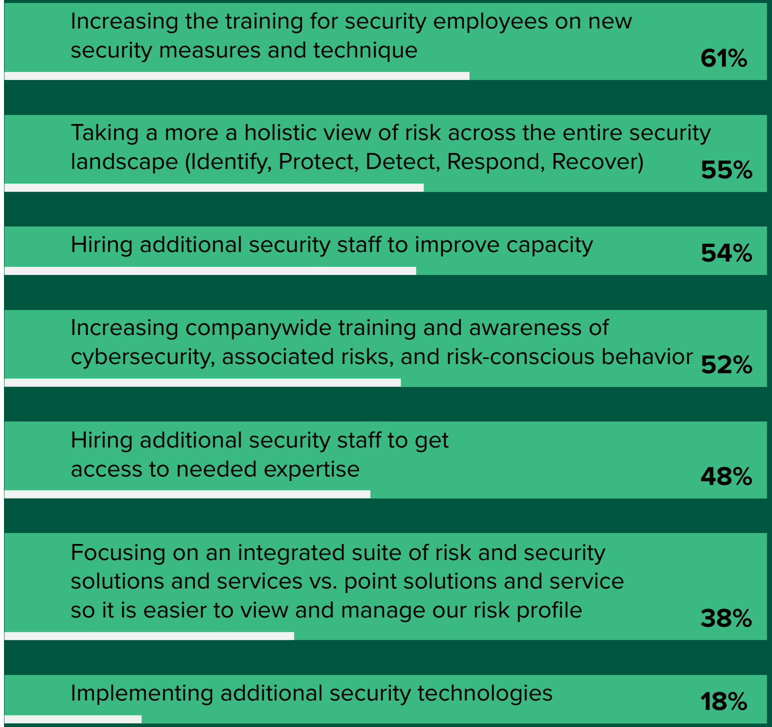
Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Total percentages may not equal separate values due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Risk Reduction Investments Focus On Expertise, Staffing, And Holistic Cyber Risk Management

Our study revealed that the most common investments risk leaders are making to be more proactive with cyber risk management are:

- Increasing training for security staff to ensure they have the right skillsets to manage current and new cyber risk management approaches.
- Increasing training for nonsecurity employees to help encourage more risk-conscious behavior and help reduce risk related to internal factors.
- Increasing security capacity through new technology and third-party services to help alleviate resource constraints on current teams and allow more time for proactive risk reduction initiatives.
- Focusing on holistic risk insights centered in a risk management framework — like the NIST Cyber Security Framework (CSF) — that emphasizes the importance of proactive and reactive risk management priorities.

"What security areas is your organization making investments in, or planning to invest in, to be more proactive with cyber risk management?"



Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Top responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Third-Party Providers Are Crucial For Risk Reduction

As security and risk leaders start to invest more in cyber risk management, they are looking to partners to bring valuable technology, expertise, and staffing resources to help them better execute their holistic risk reduction strategies.

Managing cyber risk with third-party support allows leaders to enable and accelerate both proactive and reactive approaches. Experienced third parties can bring the right skills and technology to holistically assess risk and help prioritize actions with the greatest reduction per dollar invested. Nearly 40% of surveyed leaders also value partners for helping them stay aware of emerging threats and risks. Additionally, 51% of leaders intend to use third parties to support security training for their teams, and 45% will use third parties to increase security staffing and bring needed expertise into the organization.

"What advantages do you anticipate by working with a third-party to manage your cyber risk?"

39%	Better ability to stay current with new threats and risks
37%	Better scalability
36%	Taking a more proactive approach to security
35%	Access to the most up-to-date security tools
35%	Faster breach response and mitigation
34%	Cost efficiency over building or hiring internally
33%	Faster recovery of compromised data and/or systems
32%	Faster time to value with implementation

Base: 231 security and risk leaders responsible for cyber risk strategy at North American enterprises
Note: Top eight responses shown
Source: A commissioned study conducted by Forrester Consulting on behalf of Critical Start, December 2023

Conclusion

Today's security and risk leaders can no longer afford to be solely reactive with their cyber risk management strategy. The constant pressure of new and emerging threats will push security teams to their breaking point unless a change is made. More holistic strategies that blend proactive (i.e., identify, protect) and reactive components (i.e., detect, respond, recover) will have the greatest overall business impact. For organizations looking to make this change, a new, proactive cyber-risk management approach, enabled by third-party support, is key for improving overall security and risk readiness.

With the help of partners to access the right tools and skillsets, security leaders can gain more accurate visibility and insight into their organizations' risk and use that to guide cyber risk reduction investments as part of a more comprehensive and proactive cyber risk management strategy.

Project Team:

Chris Taylor,
Principal Consultant

Contributing Research:

Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Critical Start, Inc. To create this snapshot, Forrester Consulting supplemented this research with custom survey questions asked of 231 security and risk leaders responsible for cyber risk strategy at North American enterprises. The custom survey was completed in December 2023.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Demographics

COUNTRY	
United States	**52%**
Canada	**48%**

INDUSTRY	
Financial services	**18%**
CPG/manufacturing	**17%**
Healthcare	**17%**
Government	**17%**
Technology	**16%**
Business or professional services	**15%**

COMPANY SIZE	
1,000 to 4,999 employees	**55%**
5,000 to 19,999 employees	**36%**
20,000 to 24,999 employees	**10%**

TITLE	
C-level	**16%**
Vice president	**37%**
Director	**47%**

Note: Percentages may not total 100 due to rounding.

FORRESTER®