Failing To Plan Is Planning To Fail

Take A Proactive Approach To Critical Event Management To Improve Risk Preparedness

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY ONSOLVE, OCTOBER 2021

Table of Contents

Executive Summary 3

Key Findings 4

Overconfidence Is A Threat To Preparedness 5

How A Lack Of Proactive Planning Inhibits Effective Incident Response 9

Drive Effective CEM Response By Mastering The Four Core Competencies 13

Key Recommendations 17

Appendix 18

Project Director:
Nicholas Phelps,
Principal Market Impact Consultant

Contributing Research:
Forrester's Security and Risk research group

ABOUT FORRESTER CONSULTING

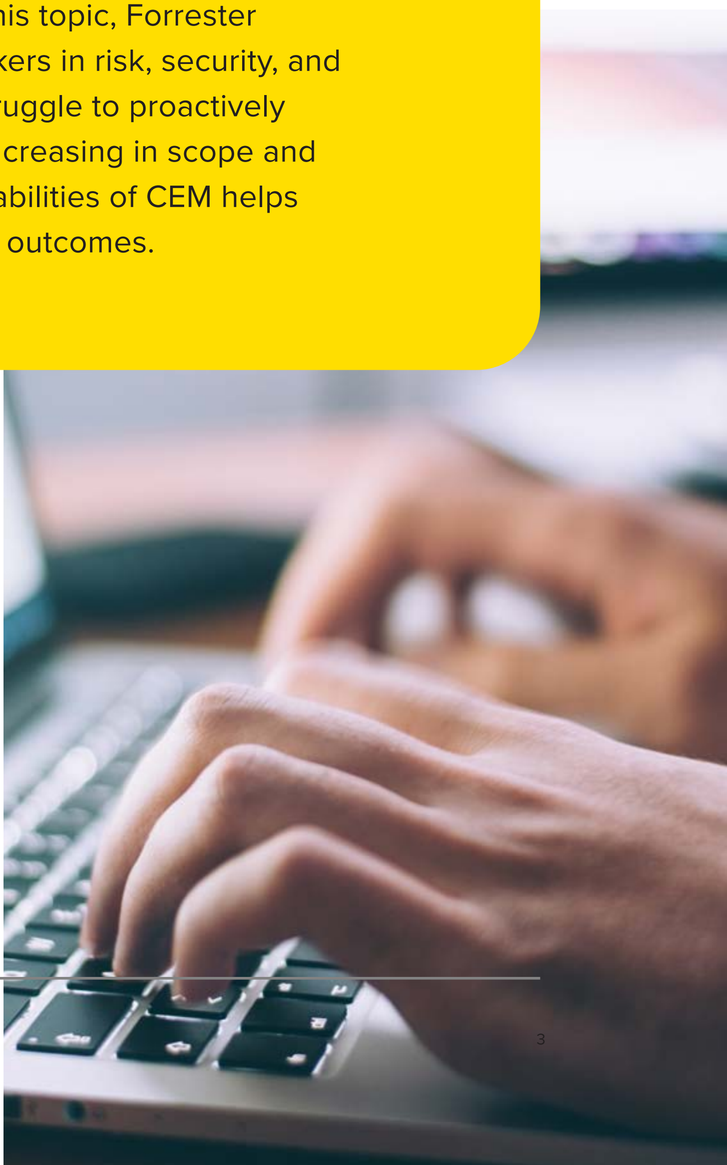
Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

Managing risk is an essential part of any business's success. It's a fallacy to believe that the goal of risk management is to stamp out risk entirely. Instead, risk management is about understanding what risks are necessary to grow, innovate, and compete while creating formal processes to proactively detect and decide which risks are worth taking in pursuit of strategic goals and objectives, and which ones to avoid and mitigate.

Within this structure, effectively managing critical events that disrupt business processes and put workers and even customers in danger has never been more essential, nor more complicated. Organizations of all kinds therefore must ensure they are positioned to identify and respond to business disruption as quickly, accurately, and effectively as possible.

In April 2021, OnSolve commissioned Forrester Consulting to evaluate the state of risk management and critical event management (CEM) at midsize to large enterprises in North America and the UK across many industries including education and government. To explore this topic, Forrester conducted an online survey with 469 decision-makers in risk, security, and business continuity. We found that respondents struggle to proactively manage risks to their organizations that are only increasing in scope and intensity, and that focusing on mastering core capabilities of CEM helps lead to better proactive awareness, response, and outcomes.



Key Findings

Risk management strategies fail to keep pace with existing and emerging risks. Risk factors are inevitable for a business, but undesirable risks are emerging more frequently and from more sources every day. As organizations rely more on cloud architectures, workers are more distributed than ever before, and an unsettled climate, political, and health landscape affects organizations of all shapes and sizes. Unfortunately, too many organizations are unaware of the new face of risk today — much less prepared to tackle it. Effective preparation requires proactive risk management strategies and highly effective, efficient CEM capabilities that let firms quickly identify and respond to incidents. But, these steps manifest more as differentiators than as table stakes among firms today.

Misaligned priorities and technology missteps make proactive, holistic event management harder. Most organizations anoint information security (infosec) or business continuity roles to drive their critical event management programs, and the majority struggle with CEM technologies that fail to interoperate across key functionalities and are cobbled together across built and bought solutions. This situation results in organizational and technological silos that inhibit fast, clear, actionable intelligence and response, and therefore extends the damage an incident can level against a firm’s reputation, revenue, and customer relationships.

By evaluating their core CEM capabilities, organizations can plot a rational course to improvement. To excel at identifying and responding to incidents as quickly and effectively as possible, organizations need to develop strong practices across four key CEM capabilities: risk intelligence, critical communications, incident management, and control-center-level visibility. Today, firms are most likely to struggle in risk intelligence and control-center-level visibility areas that are critical to providing early detection and a holistic understanding of a problem’s scope and impact. Furthermore, organizations that excel across all the dimensions of CEM are shown to have better situational awareness, more effective response to incidents, better alignment of technologies, and ultimately better business and customer outcomes and incident mitigation.

Overconfidence Is A Threat To Preparedness

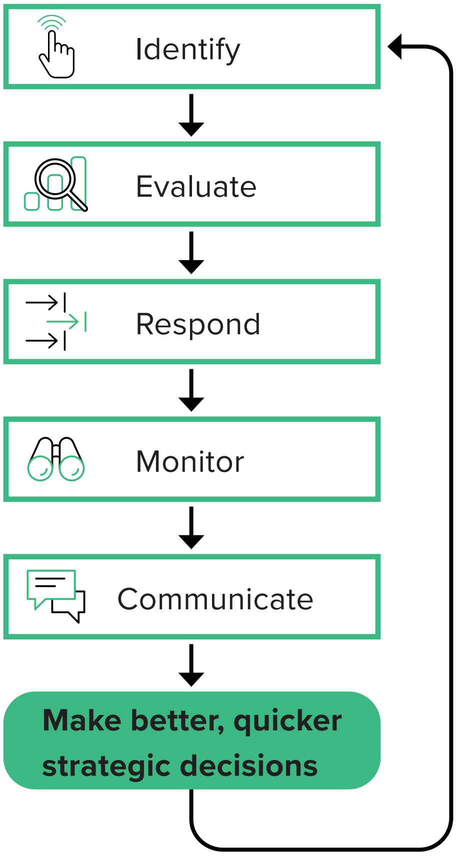
To grow and thrive, entities of all sizes and sectors must have a robust risk management process, access to timely information and analysis, and support from the right technologies to help them make better, quicker strategic decisions. Five competencies drive success in this space: the ability to identify, evaluate, respond, monitor, and communicate.[1] These enable firms to keep pace with the proliferation of business, ecosystem, and systemic risks they face (see Figure 1).

OVERCONFIDENT AND UNDERPREPARED: A RECIPE FOR DISRUPTION

Despite the make-or-break role in driving or undermining resilience, too many firms are stuck underestimating the breadth and depth of risks their organizations face. They are therefore left unprepared to respond to today's risks in a sufficiently proactive and targeted manner — much less to respond to those that will come in the future. Let's start with overconfidence. You can't manage what you can't see, and around half of the respondents' firms fail to appreciate the true nature of risk by:

- **Overlooking the myriad ways risk manifests for organizations.** Just 46% of respondents agreed that risks and business disruption can come from anywhere, including cyberattacks, natural disasters, political or individual violence, or even combinations of the above. However, firms face more risks from more sources than ever before as IT architectures expand into the cloud, as workers become more likely to log in from remote global locations, and as natural disasters pick up in intensity and frequency.

Figure 1



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distributions prohibited

- **Underestimating the rising stakes of risk management.** Fewer than half of respondents said they agree that risk management is likely to be more complex two years from now than it is today. This is despite the ever-increasing complexity of business, which intrinsically brings rising frequency and intensity of business interruptions along with it.
- **Discounting the value of proactive risk mitigation.** Despite the established value of proactively planning for and managing risk, just more than half of respondents (52%) agreed that proactive risk mitigation is as important as effective risk responses, if not more so.
- **Overestimating their own preparedness.** Despite about half of respondents indicating their firm doesn't proactively mitigate risk, 38% said their firm's current risk management strategies are effectively measured or optimized today. That alone doesn't add up, but the equation becomes even more strained when factoring in that respondents said they expect to see a 122% increase in optimized risk management strategies in the next 18 months.

The state of self-awareness described above indicates that organizations aren't in a good position to mitigate risk. Indeed, survey responses illustrate firms' gaps in preparedness:

- **Most organizations have risk response that is suboptimal at best and disastrous at worst.** Across risk categories including information security, company travel, data privacy, and even risks that impact customer experience (CX), more than half of respondents indicated their organization's risk response is less than effective today.
- **This blinds them to the inevitability of disruptive incidents.** Almost all survey respondents (99%) said their organization experienced at least one incident during the past 18 months. Importantly, this was not a pick-one exercise, either. Nearly three-quarters of respondents said their firm experienced at least two types of incidents, more than one-third said their firm had at least three, and 12% said their firm suffered at least four distinct types of incidents during that timeframe.
- **Consequences impact reputation, resilience, safety, and employee morale.** Respondents said the most common impact of incidents on their firms is damage to the company's reputation, followed by

operational disruption and impact to employee safety and morale. Other than the fundamental duty of care protecting employees, impacts to employee experience (EX) have wide-ranging implications for a firm's success. For example, firms with highly mature EX practices are 28% more likely to have higher employee accountability, more innovation, lower attrition, and better customer outcomes.[2]

The vast majority of respondents' organizations experienced multiple critical incidents during the past 18 months.

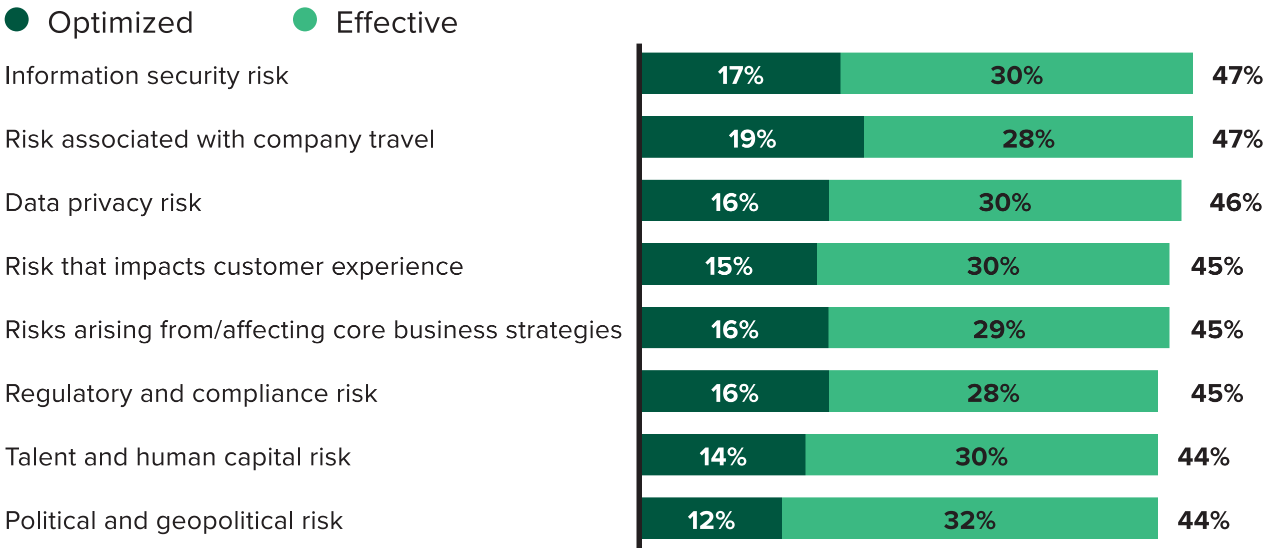
RESPONSE EFFECTIVENESS VARIES BY INDUSTRY

While all respondents showed their risk response has room for improvement (see Figure 2), this study showed that effectiveness varies depending by industry (see Figure 2a). Respondents in this study indicated that response effectiveness varies depending on industry. Averaging the number of respondents within each vertical who described their firm's ability to respond across all the risk incidents indicated that those within the financial services and insurance industries are most confident in their firm's risk response, followed by those in retail and government. On the other hand, respondents representing healthcare and education were less likely to rate their firm's response as highly.

Figure 2

Across Risk Categories, Most Organizations Show Room To Improve

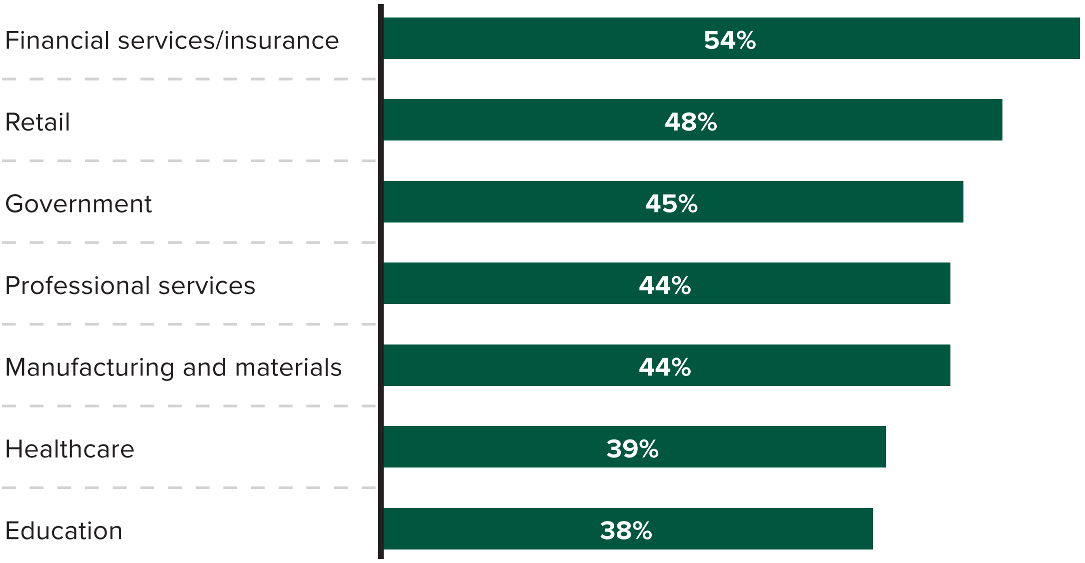
"Which term best reflects how effectively your organization can respond to each of the following business risk categories?"



Base: 469 risk, security, and CEM decision-makers at organizations in North America and the UK
Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

Figure 2a

Respondents Within Each Industry Who Rate Their Incident Response As Effective Or Optimized Across All Risk Vectors



Base: 469 risk, security, and CEM decision-makers at organizations in North America and the UK
Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

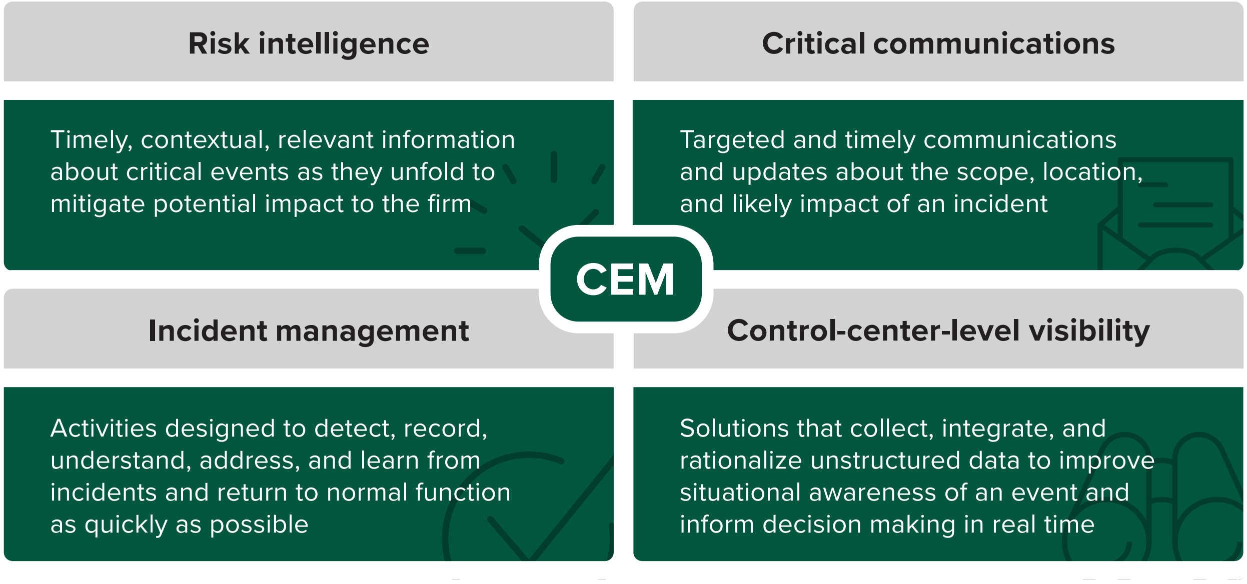
How A Lack Of Proactive Planning Inhibits Effective Incident Response

Effective risk management strategies require that firms respond to events by proactively mitigating, triaging, and remediating risks across the organization. Deciding which risks to respond to first and in what manner requires context and prioritization; however, only 38% of respondents said becoming more proactive is a key goal of critical event management today.[3]

Proactive risk mitigation requires firms to balance the impact of the risks with the cost of investment in technology and resources. An organization's ability to manage critical events as they occur is a key dimension of resiliency. Sometimes referred to as critical event management, effective incident response is made up of four core competencies: risk intelligence, critical communications, incident management, and control-center-level visibility (see Figure 3).

Figure 3

The Core Competencies Of Critical Event Management



Risk intelligence

Timely, contextual, relevant information about critical events as they unfold to mitigate potential impact to the firm

Critical communications

Targeted and timely communications and updates about the scope, location, and likely impact of an incident

Incident management

Activities designed to detect, record, understand, address, and learn from incidents and return to normal function as quickly as possible

Control-center-level visibility

Solutions that collect, integrate, and rationalize unstructured data to improve situational awareness of an event and inform decision making in real time

Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

ORGANIZATIONAL CHOICES MAKE PROACTIVE, HOLISTIC EVENT MANAGEMENT HARDER

In their daily activities, most organizations face an interconnected network of global systems, economies, and networks, and each brings its own risk to a firm's operations. The impact of unplanned events can often cascade horizontally (i.e., across multiple areas of an organization). In this new reality, the traditional siloed approach in which business areas only considered the risk impacts of their own domains simply won't cut it.[4]

With that said, organizations are still very likely to silo CEM today. Only 17% of respondents' firms have tapped an enterprise risk management (ERM) team to lead CEM, and just 1% distribute responsibility across the organization. Respondents' organizations most commonly tapped infosec or business continuity roles to drive CEM. While their respective remits make it clear they play important roles in the resiliency of their organizations, both groups present limitations when pursuing a holistic organizational response. Infosec's focus on information security breaches captures just a part of an organization's overall risk portfolio, albeit a significant part. Meanwhile, business continuity's primary remit within disaster recovery is reactive (rather than proactive) in nature.

Only 17% of respondents have tapped their ERM teams to manage CEM, and just 1% split responsibility for event management across multiple disciplines.

MOST ORGANIZATIONS FAIL TO REALIZE THE FULL VALUE OF CEM INVESTMENTS

Just a quarter of respondents believe the solutions their firms leverage for CEM deliver full value to their organizations. This study suggests two primary factors for why that may be:

- **Many CEM stacks lack key capabilities.** Current security stacks make it harder to monitor and effectively respond to incidents. Forty-four percent of respondents said their firm lacks risk intelligence solutions, more than half said their firm lacks security analytics, and 63% said their firm doesn't have governance, risk management, and compliance (GRC) management technologies in place. This means that even if firms aim to be more proactive, they lack the ability to quickly identify and plan for incidents.

- **Lack of integration hurts effectiveness.** While three-fourths of respondents agreed that integration is important to effective response, only about one-third said their firm's technologies are well-integrated today. Contributing to this challenge, respondents reported a roughly even distribution of homegrown and commercial CEM solutions. These challenges contribute to reactive strategies, because aligning systems of insight and response across a patchwork of commercial systems and unique homegrown solutions makes using a holistic approach all the more difficult. Finally, just 37% of respondents ranked improving integration among their firm's top three CEM objectives for this year, indicating this challenge is likely to persist.

FAILING TO PLAN IS PLANNING TO FAIL

These challenges impede proactive planning and response, and they make it difficult for firms to quickly identify and respond to events. The respondents in our study ranked having the ability to quickly identify critical events and getting employees to respond quickly and consistently as their firms' top two challenges (see Figure 4).

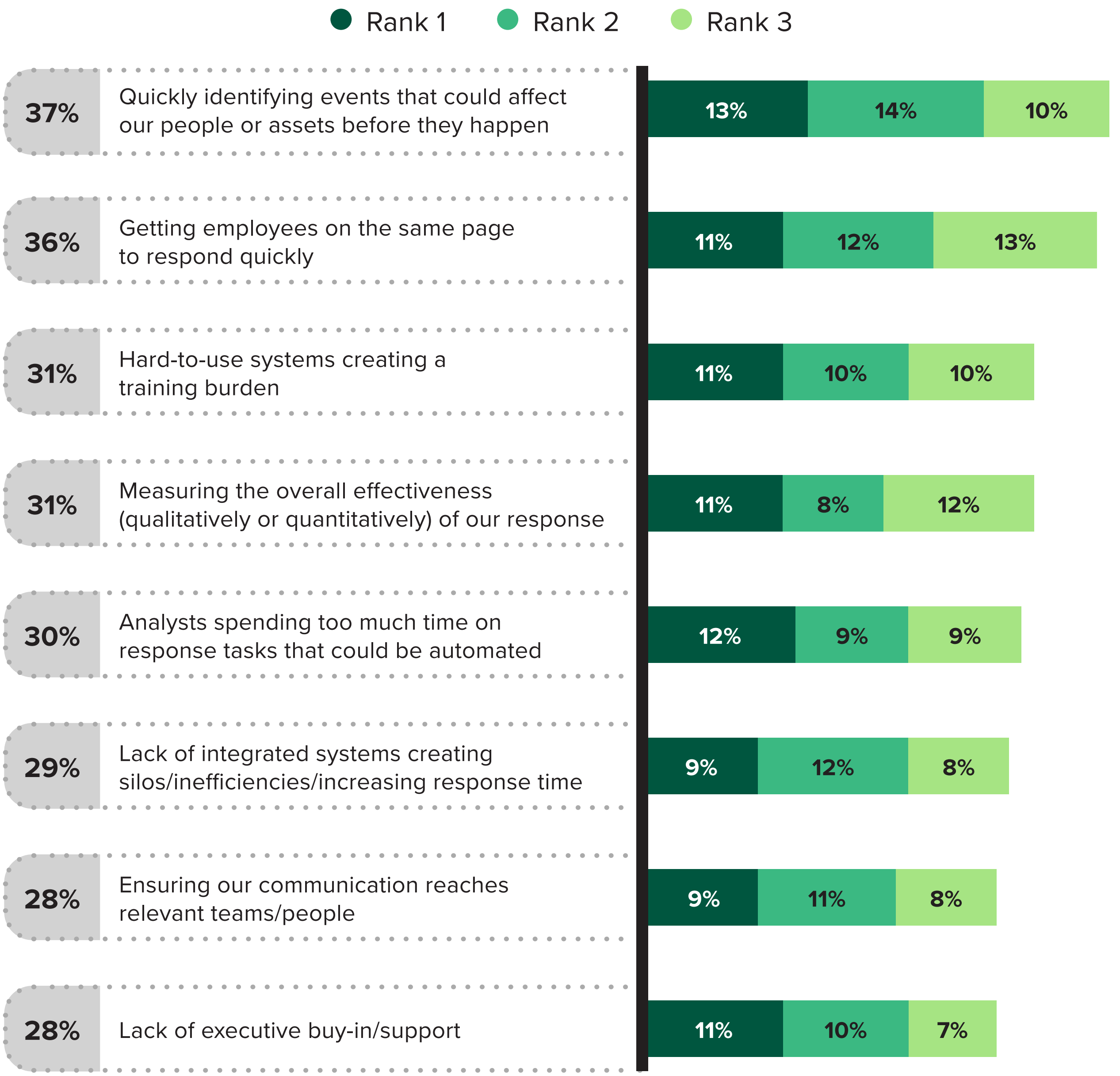
The result of a slow, ineffective response can be severely damaging for an organization. Respondents said that suboptimal CEM leads to poor revenue performance, disrupted operations, regulatory penalties or fines, and damage to employee confidence and morale. All of these repercussions hit an organization's bottom line either directly (in the case of revenue performance and regulatory penalties) or indirectly (in the case of disrupted operations and employee morale). Especially because the great resignation made the already hyper-competitive talent market even tighter, organizations find themselves paying between 150% and 200% of a departing employee's salary to replace them.[5]

Figure 4

Organizations Struggle To Quickly Identify Issues And Mobilize Consistent Responses

“What are the major challenges your organization faces with critical event management today?”

Each respondent’s organization has experienced at least one challenge.



Base: 469 risk, security, and CEM decision-makers at organizations in North America and the UK
Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

Drive Effective CEM Response By Mastering The Four Core Competencies

This study asked respondents to evaluate their firms' current programs across each of the four competencies of CEM in order to understand their areas of strength and focus areas for improvement. Ultimately, the results indicate that firms fare the best with incident management capabilities that focus on delivering a response that lets them return to normal function as quickly as possible and in critical communications capabilities that provide targeted and timely communications and updates about the scope, location, and the likely impact of an incident (see Figure 5).

Figure 5

Most Organizations Show Room To Improve Across Risk Categories

CRITICAL COMMUNICATIONS (SHOWING AVERAGE SCORE FROM 1 TO 5)		
Targeting: Ability to reach the right teams with the critical information they need to respond to an event in near real time	**3.26**	**3.18**
Automation/configuration: Easily configuring and automating alert delivery across channels and devices to the right teams	**3.20**	
Integration: Communications/mass notification solutions that are fully integrated with other relevant business systems and databases to ensure consistency, accuracy, and speed	**3.08**	

INCIDENT MANAGEMENT (SHOWING AVERAGE SCORE FROM 1 TO 5)		
Scope: Quickly determining the scope of an event and its potential impact to initiate rapid recovery and improve resilience	**3.17**	**3.18**
Outreach: A formal, well documented risk response plan and communication strategy that is quickly and seamlessly delivered to relevant teams and across devices	**3.20**	
Optimization: Quickly updating workflows and response plans to account for changes to event conditions and deliver updates to relevant teams in near real time	**3.17**	

Base: 469 risk, security, and CEM decision-makers at organizations in North America and the UK
Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

Respondents said their firms struggle more deeply with control-center-level visibility capabilities that deliver situational awareness and most deeply in risk intelligence that enables them to quickly identify and understand the scope of an event as it occurs. In other words, organizations' response capabilities are stronger than their awareness capabilities, and this is a situation that can only aggravate challenges with proactive response that requires insight and awareness to be effective (see Figure 6).

Figure 6

Most Organizations Show Room To Improve Across Risk Categories

CONTROL-CENTER-LEVEL-VISIBILITY (SHOWING AVERAGE SCORE FROM 1 TO 5)		
Automation: Automating essential workflows that collect, interpret, and prevent incidents before they occur and responding/communicating to events as quickly as possible	**3.18**	**3.12**
Unified visibility: Collecting, integrating, and making sense of unstructured data to provide a single source of truth for risks, impacts, and recommended actions across the organization in near real time	**3.03**	
Orchestration: Responding to critical events through automated and targeted resources and protocol orchestration to mitigate the impact of critical events as effectively as possible	**3.14**	

RISK INTELLIGENCE (SHOWING AVERAGE SCORE FROM 1 TO 5)		
Foresight: Proactively monitoring risk across multiple categories with consistent and documented processes in place to identify, isolate, mitigate, and report on critical risks to our business	**3.09**	**3.10**
Technology: Leveraging technology to identify relevant risks in real time, filter relevant data, and monitor events as they unfold and trigger the steps needed to address them efficiently and effectively	**3.12**	
Situational awareness: Aggregating, correlating, and assessing risk events quickly and contextually based on potential impact to operations, revenue, and brand reputation	**3.08**	

Base: 469 risk, security, and CEM decision-makers at organizations in North America and the UK
Source: A commissioned study conducted by Forrester Consulting on behalf of OnSolve, October 2021

DONE RIGHT, CEM DELIVERS BETTER OUTCOMES FOR ALL STAKEHOLDERS

We analyzed response grades across these core CEM capabilities, and we identified respondents' firms with the strongest overall grades. To be classified as having a strong CEM response, the organization would need a score of at least 48 out of a possible 60 points across all the capabilities, which is about 20% of the total study population. When we isolated this group, we found their strategies and programs reflect a more consistent and proactive approach while delivering better outcomes.

Organizations with highly effective CEM capabilities:

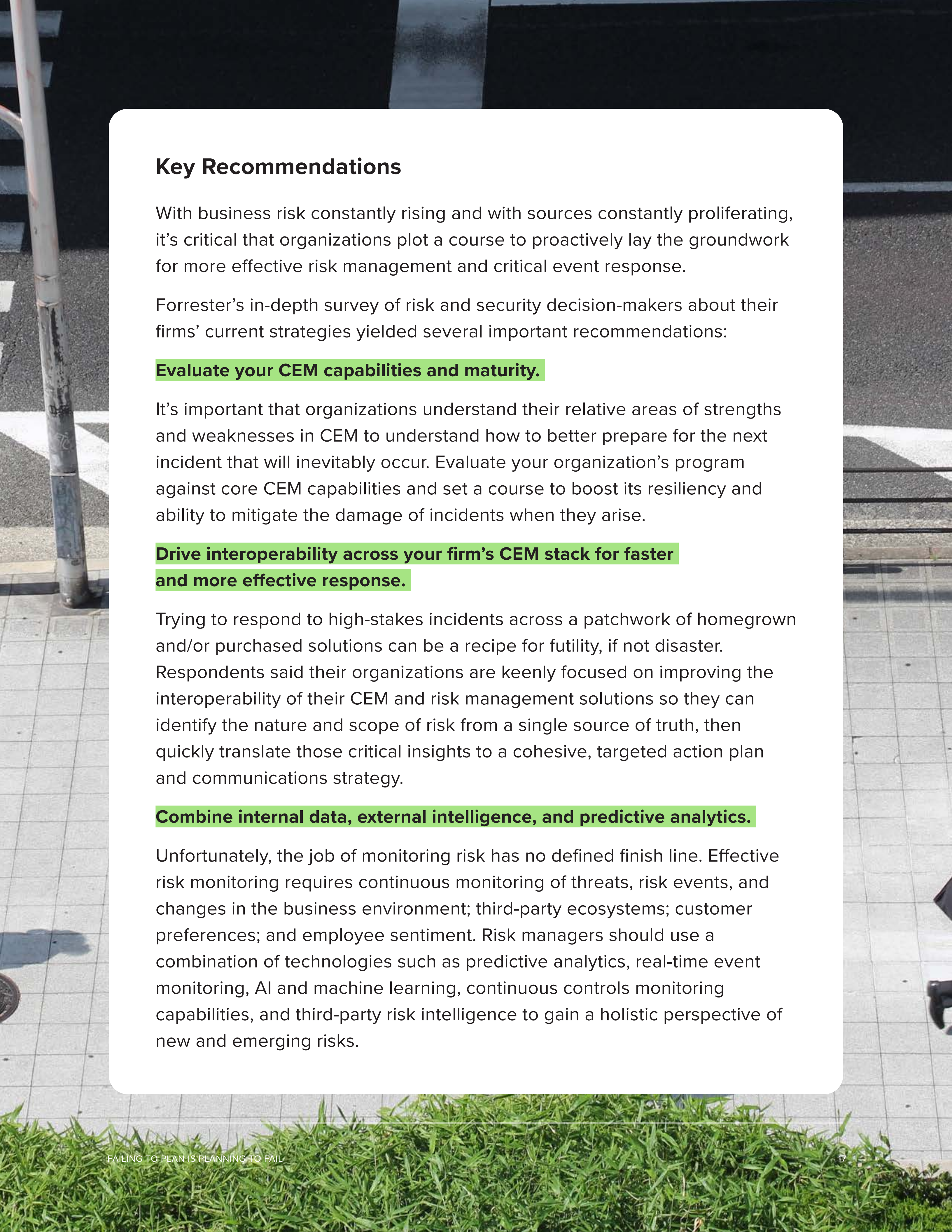
- **Are aware of the true scope of risk.** Respondents from adept firms were 152% more likely to agree that proactive risk mitigation is important than respondents from less capable organizations. They were also 320% more likely to agree that risks come from anywhere, and 180% more likely to agree that risk management is getting progressively more complex. They said their organizations are 1.6 times more likely to monitor information security risk and that they are more likely to monitor all manner of business risk.
- **Are more effective at incident response.** Respondents from highly capable firms said their organization is as much as five times more likely to have an effective or optimized response to all manner of business risk, including information security, travel, employee risk, data privacy, and risk that impacts customer experiences.
- **Leverage effective technology solutions.** Respondents from capable firms were 6.5 times more likely to say their firm's risk management solutions deliver value to the organization, and they were five times more likely to say their firm has thoroughly integrated risk management solutions in place. They said they place greater emphasis on CEM technologies that deliver risk intelligence, critical communications, and incident management capabilities that power fast and effective incident response.
- **Are more confident in their results.** Respondents from highly capable firms were twice as likely to be confident that their firm can keep up with increasingly complicated risk management in the future, and they were three times more likely to say their firm meets its CEM objectives.

They were also 112% more likely to credit CEM with improving employee confidence and morale, 108% more likely to say their firm's programs deliver better customer reputation for their organizations, and 72% more likely to say their firm's CEM program reduces the impact of a critical event to business operations.

ALL ORGANIZATIONS MUST PRIORITIZE THEIR CEM PROGRAMS

It's essential that organizations focus on improving their ability to understand and respond to events as quickly and effectively as possible. However, if their responses are reactive and unplanned, they risk wasting opportunities to mitigate events as thoroughly as possible. Furthermore, the problem will only intensify in the future as events occur more frequently and from more sources than ever before.

All the respondents in the study agreed that improving CEM would deliver better business and customer outcomes for their firm, and they were most likely to say that improving risk intelligence and critical communications are the two CEM capabilities that would most improve their firm's response to recent incidents they experienced. As we've seen, CEM is an important enabler for an organization's overall risk management strategy, and firms have a clear opportunity and requirement to shore up their capabilities to prepare to respond to today's events and tomorrow's threats.



Key Recommendations

With business risk constantly rising and with sources constantly proliferating, it's critical that organizations plot a course to proactively lay the groundwork for more effective risk management and critical event response.

Forrester's in-depth survey of risk and security decision-makers about their firms' current strategies yielded several important recommendations:

Evaluate your CEM capabilities and maturity.

It's important that organizations understand their relative areas of strengths and weaknesses in CEM to understand how to better prepare for the next incident that will inevitably occur. Evaluate your organization's program against core CEM capabilities and set a course to boost its resiliency and ability to mitigate the damage of incidents when they arise.

Drive interoperability across your firm's CEM stack for faster and more effective response.

Trying to respond to high-stakes incidents across a patchwork of homegrown and/or purchased solutions can be a recipe for futility, if not disaster. Respondents said their organizations are keenly focused on improving the interoperability of their CEM and risk management solutions so they can identify the nature and scope of risk from a single source of truth, then quickly translate those critical insights to a cohesive, targeted action plan and communications strategy.

Combine internal data, external intelligence, and predictive analytics.

Unfortunately, the job of monitoring risk has no defined finish line. Effective risk monitoring requires continuous monitoring of threats, risk events, and changes in the business environment; third-party ecosystems; customer preferences; and employee sentiment. Risk managers should use a combination of technologies such as predictive analytics, real-time event monitoring, AI and machine learning, continuous controls monitoring capabilities, and third-party risk intelligence to gain a holistic perspective of new and emerging risks.

Appendix A: Methodology

In April 2021, OnSolve commissioned Forrester Consulting to evaluate the state of risk management and CEM at midsize to large enterprises in North America and the UK. To explore this topic, Forrester conducted an online survey with 469 decision-makers in risk, security, and business continuity. Questions provided to the participants asked about their firm's current risk management strategies and CEM capabilities. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in April 2021 and was completed in October 2021.

Appendix B: Demographics/Data

GEOGRAPHY	
US	**54%**
UK	**30%**
Canada	**16%**

RESPONDENT LEVEL	
C-level executive	**25%**
EVP/SVP/VP	**25%**
Director	**30%**
Manager	**16%**

INDUSTRY	
Education	**22%**
Government	**21%**
Financial services/insurance	**12%**
Healthcare	**12%**
Professional services	**11%**
Manufacturing	**11%**
Retail	**11%**

ROLE	
Business continuity	**40%**
Critical communications	**32%**
Risk management	**32%**
Operational resilience	**29%**
Other risk/security role	**16%**

NUMBER OF EMPLOYEES	
500 to 999	**14%**
1,000 to 1,999	**14%**
2,000 to 4,999	**23%**
5,000 to 9,999	**28%**
10,000 or more	**22%**

RESPONSIBILITY FOR SECURITY INVESTMENTS	
Final decision-maker	**25%**
Part of a team	**25%**
Influences decisions	**30%**

Note: Percentages may not total 100 because of rounding.

Appendix C: Supplemental Material

[1] Source: "Proactively Manage Risk With The Forrester ERM Success Cycle," Forrester Research, Inc., October 2, 2021.
[2] Source: "The ROI Of EX," Forrester Research, Inc., September 3, 2019.
[3] Source: "Drive Faster, Better Strategic Decisions With Enterprise Risk Management," Forrester Research, Inc., August 2, 2021.
[4] Source: "Proactively Manage Risk With The Forrester ERM Success Cycle," Forrester Research, Inc., August 2, 2021.
[5] Source: "Understand Employees' Experiences," Forrester Research, Inc., December 8, 2020.

FORRESTER®