



FORRESTER®

# The Value Of Putting Security Outcomes First

Rethink Cybersecurity To Amplify Resilience,  
Productivity, And Competitiveness

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY WITHSECURE, MARCH 2023

## Table Of Contents

3	<a href="#"><u>Executive Summary</u></a>
4	<a href="#"><u>Key Findings</u></a>
5	<a href="#"><u>Cybersecurity Is Well-Established But Remains Reactive</u></a>
7	<a href="#"><u>An Outcome-Based Approach Connects Cybersecurity To Your Business</u></a>
9	<a href="#"><u>Reactivity Stifles Progress</u></a>
11	<a href="#"><u>Few Firms Achieve Alignment Between Cybersecurity Priorities And Business Outcomes</u></a>
15	<a href="#"><u>Outcome-Based Cybersecurity Supports Achieving Business Goals</u></a>
18	<a href="#"><u>Key Recommendations</u></a>
20	<a href="#"><u>Appendix</u></a>

### **Project Team:**

Ashleigh Cohen,  
Market Impact Consultant

Tanvi Dahiya,  
Associate Market Impact  
Consultant

### **Contributing Research:**

Forrester's European  
Technology Architecture &  
Security research group

#### **ABOUT FORRESTER CONSULTING**

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit [forrester.com/consulting](https://forrester.com/consulting).

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [forrester.com](https://forrester.com). [E-56231]

## Executive Summary

Cybersecurity has long been seen as a compliance and risk-management-driven activity necessary to protect organizations from attacks. Shifts in the business landscape and rapidly changing digital transformation efforts mean that cybersecurity needs to evolve from an obligation to a proactive contributor to business outcomes.<sup>1</sup> Without an effective approach, cybersecurity and IT leaders risk continually increasing their cybersecurity spending without materially improving. Organizations must move beyond reactive and ad hoc responses to cybersecurity incidents and adopt a proactive, strategic, outcome-based approach to cybersecurity that measures and improves cybersecurity based on how well it protects business goals and reduces risk. This enables leaders to create better-informed risk management strategies and focus cybersecurity investments on business objectives.

In October 2022, WithSecure commissioned Forrester Consulting to evaluate current cybersecurity approaches, gaps, and opportunities for improvement. Forrester conducted an online survey with 409 global cybersecurity and IT decision-makers at companies with at least 250 employees to explore their organizations' cybersecurity priorities and business goals, their challenges, and what they hope to achieve with cybersecurity investments. We found that organizations follow a reactive approach to cybersecurity that stifles progress in demonstrating value and aligning with business outcomes. They seek an outcome-based approach to cybersecurity to drive business outcomes and improve resilience, productivity, and competitiveness while keeping the business secure.

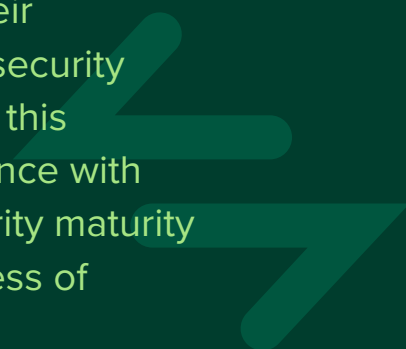


## Key Findings

**Cybersecurity is reactive and stifles progress.** Sixty percent of respondents revealed their organizations react to individual cybersecurity problems as they arise. Constantly operating in firefighting mode creates obstacles in aligning security with business outcomes.



**Organizations' cybersecurity priorities and business outcomes are unaligned.** Only one in five respondents claim their organization has complete alignment between cybersecurity priorities and business outcomes. Key contributors to this misalignment are the struggles organizations experience with capturing meaningful data to identify their cybersecurity maturity and being able to effectively use it to measure progress of business outcomes.



**Organizations are adopting outcome-based cybersecurity to drive their businesses forward.** Eighty-three percent of respondents said their organization is interested in, planning to adopt, or expanding its adoption of outcome-based cybersecurity solutions and services to achieve business outcomes. Firms believe that through adopting an outcome-based approach, they can effectively link security and organizational goals and increase their success in achieving their business outcomes while being more secure in the process.



## Cybersecurity Is Well-Established But Remains Reactive

Geopolitical upheaval, accelerating digital transformation, and a flood of regulatory requirements have put cybersecurity in the forefront of organizations' priorities (see Figure 1).

Threats from bad actors remain unpredictable as they change tactics to avoid detection and maximize success, and organizations are trying to keep up. Surprisingly, most firms today adopt a reactive and/or ad hoc approach to cyber risk management, and this creates misalignments across people, processes, and technology. In surveying more than 400 global cybersecurity and IT decision-makers, 60% of respondents said their organization reacts to individual cybersecurity problems as they arise. These misalignments leave security professionals trapped in tactical activity and responding to incidents as they arise, rather than following courses of action that are reflective of their strategies.

Business decision-makers were more likely to agree that their organization's primary approach to cybersecurity investment is reactive, rather than strategic. Sixty-six percent of business leaders said their organization reacts to cybersecurity problems as they arise as opposed to 54% of IT cybersecurity decision-makers. Similarly, across industries, 71% of respondents from manufacturers highlighted this reactivity compared to just more than half from organizations in the highly regulated financial services sector.

Having clear cybersecurity vision and goals aligned to business outcomes is critical for organizations'

**Figure 1**

### Cybersecurity Remains Top Of Mind For Organizations



**80%**

The overall cybersecurity threat my organization faces each year is increasing.

**75%**

Cyber risk is a top priority for my organization, and directors want it managed as such.



**74%**

Cyber-risk management is receiving increased attention from the board.

**71%**

My organization is spending more on cybersecurity each year.



Base: 409 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influence decisions when their organization purchases cybersecurity solutions

Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

cybersecurity strategies to succeed. However, with goal setting for cybersecurity originating from many different directions, the pressure and difficulty to succeed heightens.

The survey highlighted that the way organizations determine which goals to focus on is inconsistent. Thirty-six percent of respondents said their organization's cybersecurity goals are determined by what is important at the planning stage of the business cycle, 31% said goals are determined by individual business units, and 30% said goals are determined based on compliance needs. Cybersecurity goals are coming from different directions and hindering organizations' abilities to be effective in protecting their business.

**60%**  
of respondents' organizations react to individual cybersecurity problems as they arise.



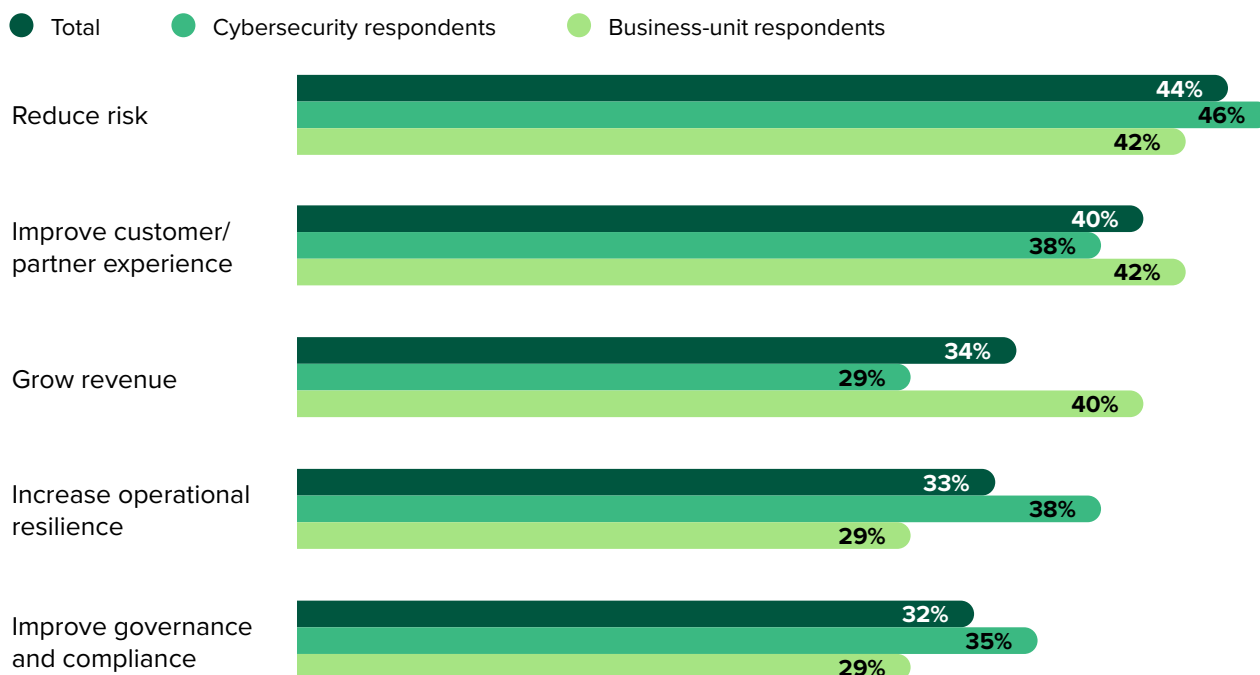
# An Outcome-Based Approach Connects Cybersecurity To Your Business

For cybersecurity to become a trusted partner for the business, security leaders must demonstrate that investment in cybersecurity can help businesses achieve their goals. As organizations globally begin to look beyond tech-centric approaches and threat prevention, they should focus on an outcome-based security approach.

Forrester defines outcome-based cybersecurity as an approach that enables business leaders to simplify cybersecurity by cultivating only those capabilities that measurably deliver their desired outcomes as opposed to traditional threat, activity-based, or ROI-based methods. Consequently, organizations seek an outcome-based approach to cybersecurity not only to tackle risk but also to proactively support business goals.

**Figure 2**

**“What business outcomes does your organization hope to achieve with your top cybersecurity goals?”**



Base: 409 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influence decisions when their organization purchases cybersecurity solutions

Note: Showing top 5.

Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

The following are key business outcomes that organizations must align their cybersecurity strategies to include (see Figure 2):

- **Risk management.** In today's hyperconnected world, using a strategic-risk-based approach is imperative for effective and efficient risk management, and this is critical to an organization's reputation, resilience, and productivity. Forty-four percent of survey respondents said their organization wants to reduce risk to meet its top cybersecurity goals. Security leaders' risk-reduction objectives need to align specifically to the business in a clear, precise, and pragmatic way.
- **Customer experience (CX).** Two of every five respondents said their organization hopes to improve CX with cybersecurity goals. Leaders recognize that cybersecurity can evolve from a compliance and risk-management-driven activity to become a business driver. For instance, if customer or partner data gets compromised, it's detrimental to the company's brand. Companies lose clients and buyers lose trust. Additionally, customers want a flawless experience (e.g., quick authentication, better mobile and web experiences). If they experience that, they're more likely to spend more time engaged, and boosting revenue is the third most important business outcome for 34% of total respondents. Revenue growth is even higher on the agenda for business-unit respondents (40%) versus cybersecurity respondents (29%).
- **Increased operational resilience.** Understanding an organization's current and desired levels of cybersecurity resilience will make a "golden thread" visible from control implementation to businesswide risk reduction, and this can then improve operational efficiency. Thirty-three percent of respondents cited this as a business outcome they hope their organization achieves, and this included 38% of cybersecurity respondents and 29% of business-unit respondents.

Organizations in the manufacturing (50%) and public sector/healthcare (55%) industries are looking to reduce risk the most.



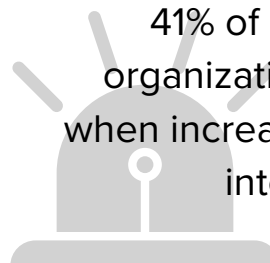


## Reactivity Stifles Progress

Our survey found that more than 90% of organizations incur challenges when they react to cybersecurity incidents as they arise, and that the top challenges include (see Figure 3):

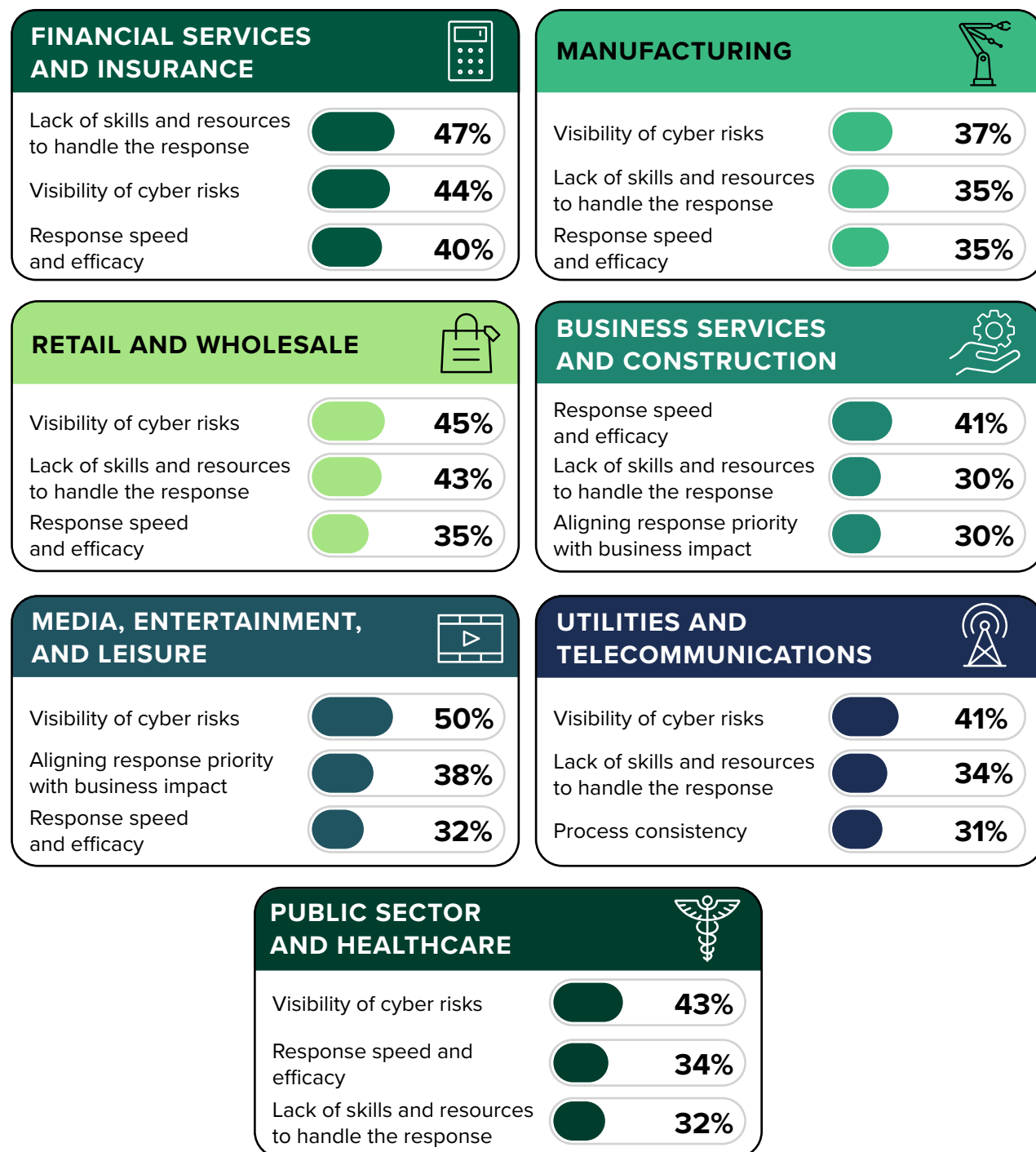
- **Having visibility into cyber risks.** As cyber-crime becomes increasingly intolerable, stakeholders – including boards, regulators, investors, business partners and customers expect greater visibility into an organization’s cybersecurity risk management strategy. Constantly operating in firefighting mode as incidents arise have left 41% in a bind when increasing visibility into cyber risks. Without structure and oversight, cybersecurity strategies will fall short of their potential to deliver the visibility expected, identify risks, create business value, and elevate performance. Fifty percent of respondents from media and entertainment firms said their organization finds it particularly difficult to identify cybersecurity incidents as they arise compared to respondents from other industries.
- **Finding the required skills and resources.** Firms everywhere struggle to find qualified cybersecurity staff at the salaries they can afford. It’s no surprise then that 35% of respondents identified it as one of the top challenges when reacting to cybersecurity incidents. This was the top challenge for respondents within the financial services sector (47%), but respondents from most sectors ranked this challenge in their top three.
- **Responding quickly and effectively.** Security technology is effective for a limited time, but understanding the types of risks and their value to attackers is a key step toward hygiene practices. Yet, 34% of survey respondents cited speed of response coupled with the lack of effectiveness as challenges, which makes it more difficult to react to cybersecurity issues. This was a challenge for respondents from larger organizations with more than 1,000 employees (39%) versus those from organizations with less than 1,000 employees (30%). Similarly, 40% of respondents from financial services organizations stated this is a key challenge.

Constantly operating in firefighting mode as incidents arise leaves 41% of respondents’ organizations in a bind when increasing visibility into cyber risks.



**Figure 3**

**Cybersecurity Challenges By Industry**



Base: 409 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influence decisions when their organization purchases cybersecurity solutions

Note: Showing top 3 responses for each industry.

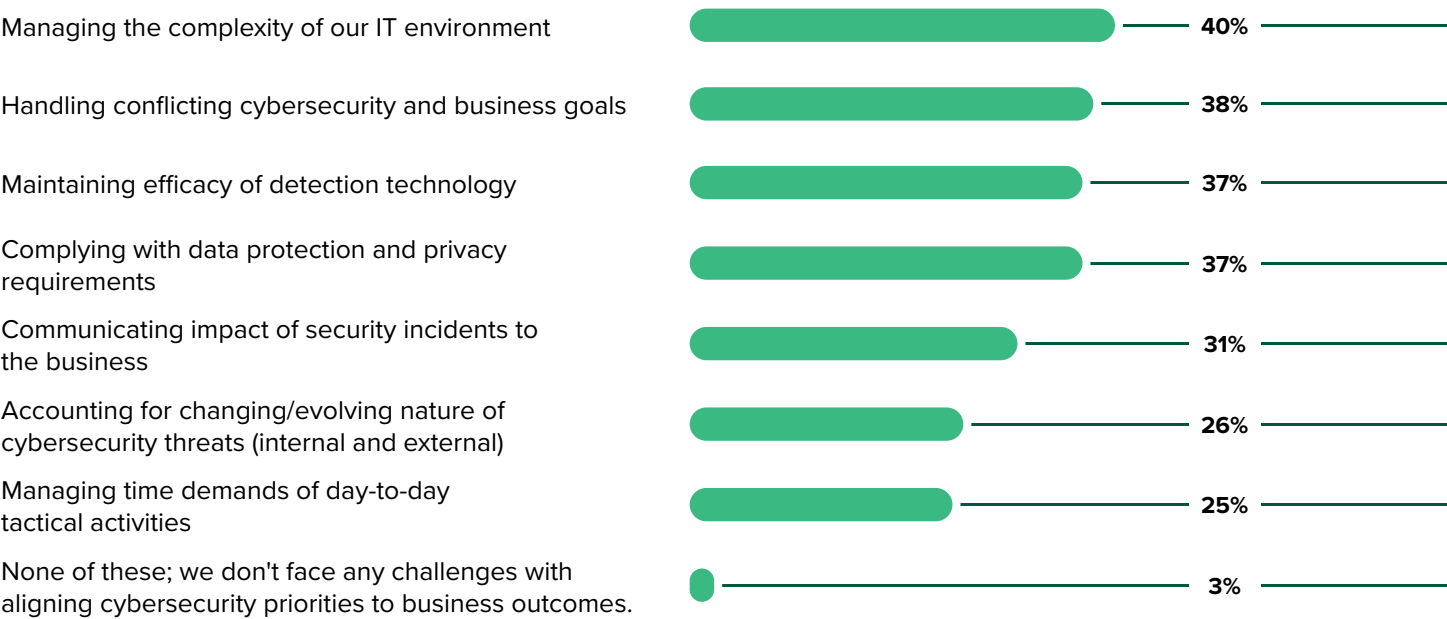
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

# Few Firms Achieve Alignment Between Cybersecurity Priorities And Business Outcomes

While cybersecurity leaders fail to gain a holistic view of their technology landscapes and strategically address how cybersecurity can support business outcomes, it comes as no surprise that only one in five respondents said their organization claims to have complete alignment between cybersecurity priorities and business outcomes. Our survey revealed that the following top challenges are obstacles in aligning cybersecurity priorities to business outcomes (see Figure 4):

Figure 4

“What challenges, if any, does your organization face with aligning cybersecurity priorities to business outcomes?”



Base: 409 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influences decisions when their organization purchases cybersecurity solutions  
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

- **Managing a complex IT environment.** As a result of digital transformation, ever-increasing amounts of data, and the changing and evolving nature of threats, 40% of respondents said their firm currently struggles to manage the complexity of the IT environment hindering its ability to align with business outcomes. This is particularly challenging

for respondents within the media industry (50%) and manufacturing sector (47%). And this challenge will continue to grow as firms continue investing in different solutions as response to individual cyberincidents creates a fragmented technology landscape.

- **Handling conflicting cybersecurity and business goals.** Too often, when firms pursue their business objectives or develop new products and services, cybersecurity is treated as a bolt-on or ineffective afterthought, and this results in conflicting priorities. With competing cybersecurity priorities from different stakeholders, 38% of our survey respondents said their organization faces conflicting cybersecurity and business goals that paralyzes its ability to protect the business efficiently.
- **Maintaining desired results of detection technology.** As attack surfaces broaden and ecosystems become more complex, the likelihood of exposure grows. Thirty-seven percent of respondents said this fragmentation makes even the most basic tactical activities time-consuming and difficult to manage. Weaknesses in armor give rise to more opportunities for the infiltration of weak points, and detection efficacy becomes a concern.

## **FIRMS STRUGGLES TO ASSESS MATURITY, MEASURE VALUE, AND CAPTURE MEANINGFUL DATA**

Cybersecurity maturity and measurement challenges hinder the pursuit of business outcomes, and current efforts leave cybersecurity leaders burdened with having to prove the value of nothing happening. Commonly, tech execs can document the link between security and business outcomes, but they lack the performance metrics required to connect the two.

Our survey revealed that cybersecurity leaders struggle to (see Figure 5):



Half of respondents' companies find it difficult to align cybersecurity with business outcomes.



Nearly half of respondents said their organization finds it difficult to measure whether cybersecurity priorities are delivering required outcomes.

Figure 5

**“What challenges, if any, does your organization face with aligning cybersecurity priorities to business outcomes?”**



Base: 409 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influences decisions when their organization purchases cybersecurity solutions

Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

- **Understand their organization’s cybersecurity maturity.** Security leaders need to understand where they are in order to formulate a roadmap to direct them to their desired end goals. However, nearly two in five respondents (42%) said their organization does not have a clear understanding of its current and desired target-state maturity levels to measure their security postures against. Fifty percent of respondents from retail organizations highlighted this as their top challenge.
- **Measure cybersecurity value.** To secure boardroom attention and elevate the relationship security has with the business, cybersecurity leaders must be able to measure the value their strategies deliver to support business outcomes. Thirty-seven percent of respondents highlighted this as a challenge to measure how effectively their cybersecurity priorities support business goals. Furthermore, nearly 50% of firms struggle to measure cybersecurity value and have trouble articulating the contribution of security to business outcomes.

- **Capture consistent and meaningful data.** More than a third of respondents stated that capturing consistent and meaningful data is a challenge when measuring how well cybersecurity priorities achieve business outcomes. Having the right data and insights underpins making informed decisions about cybersecurity strategies, policies, and approaches. In turn, this will also help organizations better understand key performance metrics necessary for success to showcase achievements in a clear and effective, data-driven manner.

Organizations also face additional complexities. More than a third of respondents stated that their organization has executive leadership or a board that does not understand cybersecurity needs. Without being able to discuss risk in terms of business impact, security professionals will struggle to optimize cybersecurity strategy, build business cases for cybersecurity investments, and achieve budget sign-off. And all of these are key enablers of utilizing cybersecurity to achieve business outcomes.



## Outcome-Based Cybersecurity Supports Achieving Business Goals

To address the challenges posed by the evolving threat landscape and the difficulty of articulating cybersecurity value will require new thinking. Organizations understand the need to approach security with a more strategic lens, and the time to act is now.

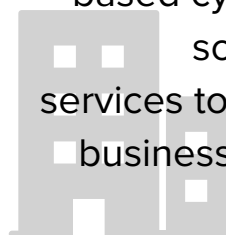
Eighty-three percent of respondents said their organization is interested in, planning to adopt, or expanding its adoption of outcome-based cybersecurity solutions and services to achieve its business outcomes. And more than a third of respondents said their firm is actively progressing towards this goal and planning to pivot to an outcome-based approach in the next 12 months. Of these respondents, half also said their organization finds it difficult to align cybersecurity priorities with business outcomes.

Decision-makers expect a range of benefits in risk, costs, and operations from outcome-based cybersecurity, and their firms can't do it alone. Our survey revealed that most respondents (72%) want their organization to switch to a vendor that delivers security outcomes.

They recognize that orienting contracts with cybersecurity vendors around outcomes is a progressive approach that will help their organizations augment the chance of success. This is because outcome-based cybersecurity aligns the incentives of security vendors and their buyers; if the solutions don't achieve the promised business outcomes (i.e., what the buyers want), organizations will look elsewhere. This shifts the relationship with security vendors to be a truly strategic partnership.

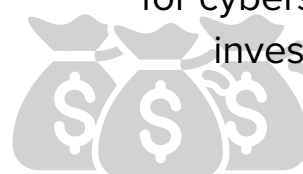
# 83%

of respondents said their organization is interested in, planning to adopt, or expanding its adoption of outcome-based cybersecurity solutions and services to achieve its business outcomes.



# 64%

of firms are willing to spend 6% or more of their operational profit to achieve the benefits they see in adopting an outcome-based approach for cybersecurity investments.



## OUTCOME-BASED SECURITY WILL UNLOCK BENEFITS AS YOUR JOURNEY EVOLVES

The survey data indicates that it is not so much a matter of if firms will pivot toward outcome-based cybersecurity, but rather when they will do so and how far along they are.

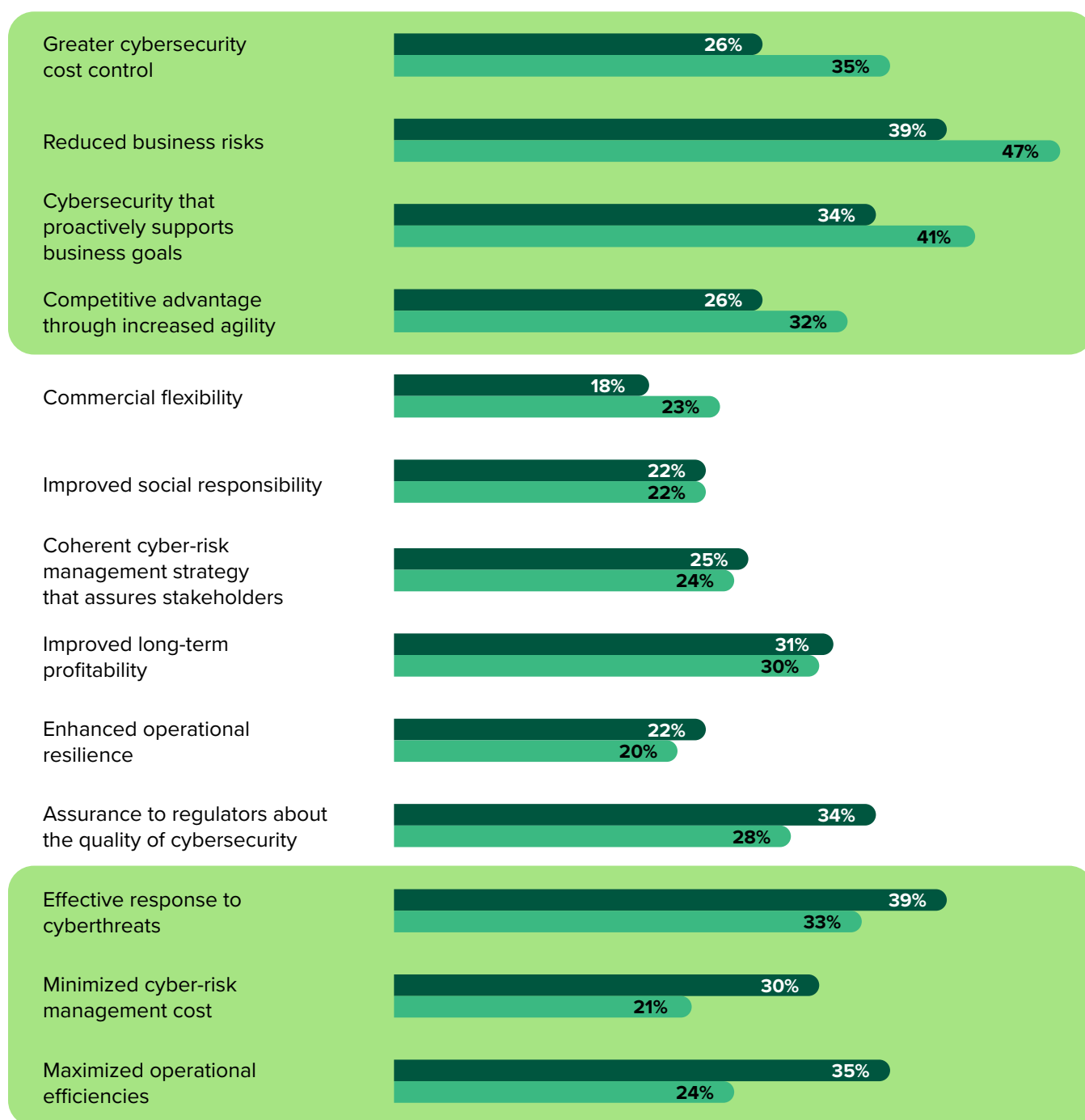
The expected benefits differ depending on where a firm is in its journey of adopting outcome-based cybersecurity (see Figure 6). The survey revealed:

- **Everyone wants to manage costs better.** Cybersecurity professionals who can align security-cost management efforts and business objectives provide invaluable strategic input. More than a third of respondents from organizations at the beginning of their outcome-based journey hope their firm benefits from greater cost control by adopting it in the next year. Thirty percent of those from organizations that are further along on their outcome-based security journey expect to minimize cyber-risk management costs after having gained control. In both cases, cost management is a major anticipated benefit of adoption.
- **Journey starters expect to gain a competitive edge through increased agility.** Understanding and proactively acting on the risk implications of business decisions can help a company better serve its customers, adopt new technologies, or penetrate new markets faster. Nearly a third of respondents from firms planning to adopt outcome-based security in the next 12 months foresee it as an enabler of gaining competitive advantage.
- **More advanced adopters expect to maximize operational efficiencies.** Nearly half of respondents from organizations that are expanding or upgrading their adoption of outcome-based security anticipate that their firm will maximize operational efficiency. Using the approach enables organizations to make faster decisions so they can identify which cybersecurity processes or solutions need streamlining, and this speeds up further investment or divestment.

**Figure 6**

## Benefits Of An Outcome-Based Cybersecurity Approach

- Expanding or upgrading adoption
- Planning to adopt in the next 12 months



Base: 262 global cybersecurity and IT decision-makers who are either the final decision-maker, part of a team making decisions, or influences decisions when their organization purchases cybersecurity solutions and whose organization is expanding or upgrading adoption or planning to adopt a solution in the next 12 months

Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

## Key Recommendations

Positioning cybersecurity as a proactive business driver relies on aligning cybersecurity with wider business objectives. Using an outcome-based approach provides business leaders with an opportunity to simplify cybersecurity by dispensing with traditional threat-based, activity-based, and ROI-based methods to cultivate only those capabilities that measurably deliver desired outcomes.

Forrester's in-depth survey of cybersecurity and IT decision-makers about outcome-based cybersecurity yielded several important recommendations:

**Agree on business outcomes with your stakeholders and map those to your security investments, threat model, and security controls.**

Get explicit agreement from the relevant stakeholders (e.g., board, executive team, etc.) about the outcomes that the company is pursuing and explain how your proposed security investments will contribute.

**Express your desired security outcomes in terms of the business benefits they deliver or enable.**

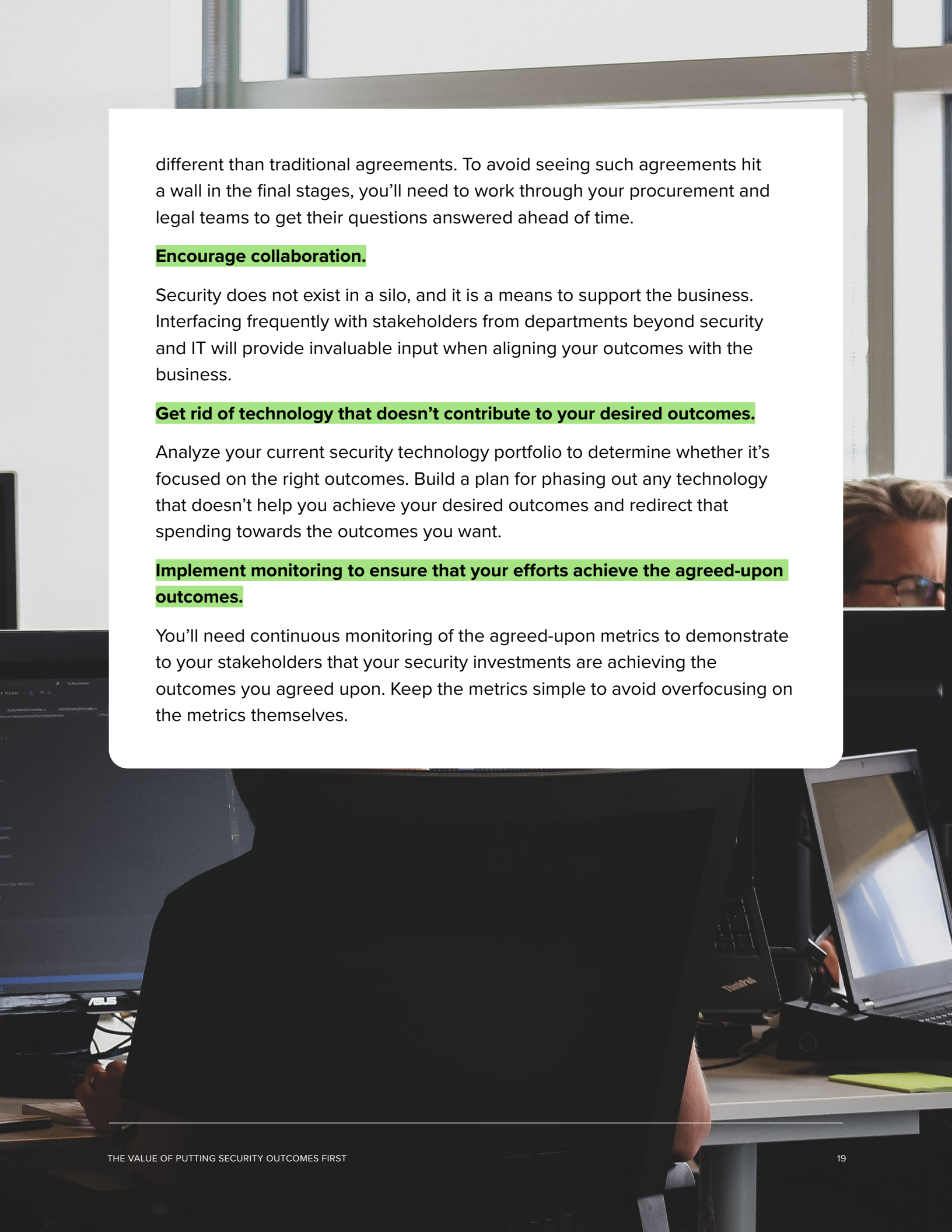
Shift your stakeholder communications from “We’re adding this security measure because it’s better” to “Here are the specific benefits we receive from this specific security measure.” For example, using risk-based authentication in e-commerce improves CX by eliminating extra steps and friction from low-risk transactions.

**Rerun your security maturity assessment to ensure that your priorities correlate with the outcomes you’re trying to achieve.**

You don’t need perfect security. You need sufficient security. If your desired business outcomes don’t require you to achieve the highest level of maturity in a given area of security, then don’t.

**Prepare your procurement and legal teams for outcome-based security purchasing.**

Vendors will only commit to delivering a given security outcome if they can capture the upside if they succeed, and this means the contracts will look

A person is seen from behind, sitting at a desk in a dimly lit office. They are looking at several computer monitors. One monitor on the left shows a dark screen with some text. Another monitor in the center is partially visible. To the right, a laptop is open, displaying a bright screen. The person's hands are resting on the desk. The overall atmosphere is professional and focused.

different than traditional agreements. To avoid seeing such agreements hit a wall in the final stages, you'll need to work through your procurement and legal teams to get their questions answered ahead of time.

**Encourage collaboration.**

Security does not exist in a silo, and it is a means to support the business. Interfacing frequently with stakeholders from departments beyond security and IT will provide invaluable input when aligning your outcomes with the business.

**Get rid of technology that doesn't contribute to your desired outcomes.**

Analyze your current security technology portfolio to determine whether it's focused on the right outcomes. Build a plan for phasing out any technology that doesn't help you achieve your desired outcomes and redirect that spending towards the outcomes you want.

**Implement monitoring to ensure that your efforts achieve the agreed-upon outcomes.**

You'll need continuous monitoring of the agreed-upon metrics to demonstrate to your stakeholders that your security investments are achieving the outcomes you agreed upon. Keep the metrics simple to avoid overfocusing on the metrics themselves.

## Appendix A: Methodology

In this study, Forrester conducted an online survey of 409 cybersecurity and IT decision-makers at organizations globally to evaluate their firms' approaches to cybersecurity and interest in adopting an outcome-based approach. Questions provided to the participants asked about business objectives, cybersecurity goals, challenges, and investment approaches. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in November 2022 and was completed in December 2022.

## Appendix B: Demographics

COUNTRY	
Denmark	12%
Finland	12%
France	12%
Germany	12%
Japan	12%
Sweden	13%
United Kingdom	13%
United States	13%

COMPANY SIZE (EMPLOYEES)	
250–499	5%
500–999	45%
1,000–4,999	37%
5,000–19,999	10%
20,000+	3%

DEPARTMENT	
Cybersecurity	14%
Finance	12%
Human resources/training	3%
IT	26%
IT audit	10%
Marketing/advertising	10%
Operations	13%
Procurement	6%
Sales	5%

INDUSTRY	
Advertising and/or marketing	3%
Agriculture, food and/ or beverage	3%
Business or professional services	7%
Chemicals and/ or metals	2%
Construction	4%
Consumer product goods and/or manufacturing	3%
Consumer services	3%
Education and/or nonprofit	3%
Electronics	3%
Energy, utilities, and/or waste management	5%
Financial services and/or insurance	11%
Government	3%
Healthcare	7%
Technology and/or technology services	12%
Legal services	1%
Manufacturing and materials	7%
Media and/or leisure	2%
Retail	7%
Telecommunications services	8%
Transportation and logistics	4%
Travel and hospitality	2%

Note: Percentages may not total 100 due to rounding.



## Appendix C: Endnotes

<sup>1</sup> Source: “Build The Business Case For Cybersecurity And Privacy,” Forrester Research, Inc., January 12, 2022.





FORRESTER®

(NOTE 12) UNREGULATED