FORRESTER®

Amplify Resilience, Productivity, And Competitiveness With Cybersecurity: A Spotlight On Industry

Industry Results From The March 2023 Thought Leadership Paper, “The Value Of Putting Security Outcomes First”

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER SPOTLIGHT COMMISSIONED BY WITHSECURE, JULY 2023

Executive Summary

Shifts in the business landscape and rapidly changing digital transformation efforts means that cybersecurity needs to evolve from an obligation to a proactive contributor to business outcomes.[1] Increased resilience, productivity, and competitiveness are imperative security outcomes. However, without an effective approach, cybersecurity and IT leaders risk continually increasing their cybersecurity spends without materially improving. Organizations must move beyond reactively responding to cybersecurity incidents towards taking a proactive and then progressive strategic, outcome-based approach 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, 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. Regardless of industry, decision-makers cited reducing risk, increasing revenue, and increasing resilience among the top business outcomes their organizations want to achieve with cybersecurity. However, more than half said their organization deploys a reactive/ad hoc approach to cybersecurity incidents that leaves it struggling to meet these outcomes.

All industries are challenged by aligning cybersecurity priorities to business outcomes. Ninety-seven percent of respondents' organizations experience challenges with aligning cybersecurity priorities to business outcomes, and those in the retail and wholesale industry find it the most difficult to do so. Contributing to this are the struggles organizations experience with capturing meaningful data to identify their cybersecurity maturity levels and being able to effectively use them to measure business outcomes.

Future-fit organizations are adopting outcome-based security. Eighty-three percent of decision-makers said their organization is interested in, planning to adopt, or expanding its adoption of outcome-based cybersecurity solutions to achieve its business outcomes, and an additional 16% said their company has already adopted this approach. Furthermore, 72% of respondents want their organization to switch to a vendor that delivers security outcomes, and those from manufacturing (76%) and utilities and communications (73%) were the most likely to say their firm will switch.

Imperative Cybersecurity Outcomes: Resilience, Competitiveness And Productivity

Geopolitical upheaval, accelerating digital transformation, and a flood of regulatory requirements have amplified the need for organizations to continuously improve their resilience, competitiveness, and productivity. Business and technology leaders across all industries are acutely aware of the importance of cybersecurity in reducing risk while not stifling business continuity and market competitiveness. Hence, it is no surprise that three out of four surveyed global cybersecurity and IT decision-makers identified cyber risk as a paramount concern for their organization. This sentiment is particularly prevalent in the financial services and utilities and communications industries: 87% and 78% of respondents from those respective industries underlined cybersecurity as a key business priority (see Figure 1).

71% of respondents from manufacturing firms said their company uses a reactive approach to cybersecurity as compared to 53% from those in the financial services and insurance industry.

Figure 1

Level Of Agreement

(Showing "Strongly agree" and "Agree")

● ≥5% increase compared to total ● ≥ 5% decrease compared to total

STATEMENT	TOTAL	FINANCIAL SERVICES AND INSURANCE	MANUFACTURING	RETAIL AND WHOLESALE	BUSINESS SERVICES AND CONSTRUCTION	MEDIA, ENTERTAINMENT, AND LEISURE	UTILITIES AND TELE-COMMUNICATIONS	PUBLIC SECTOR AND HEALTHCARE
The overall cybersecurity threat we face each year is increasing.	80%	91%	79%	73%	80%	76%	85%	68%
Cyber risk is a top priority for my organization, and directors want it managed as such.	75%	87%	73%	76%	76%	53%	78%	73%
Cyber risk management is receiving increased attention from the board.	74%	72%	77%	78%	74%	56%	77%	73%
We are spending more on cybersecurity each year.	71%	84%	77%	73%	65%	61%	65%	76%

Base: 409 cybersecurity and IT decision-makers at global organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

Although resilience, competitiveness, and productivity are vital to the success of all organizations, the reactive approach to cybersecurity adopted by most respondents' firms (60%) has left them struggling to keep up. The manufacturing industry is especially stuck in a rut of responding to issues as they arise: 71% of decision-makers from manufacturing firms said their firm uses this approach compared to 53% from the highly regulated financial services and insurance sector. Most notably, however, is the fact that across every industry, more than half of all respondents said their organization deploys a reactive/ad hoc approach to cybersecurity.

This reactive stance toward cybersecurity is not merely a tactical misstep. It significantly undermines the potential success of security leaders and, by extension, the overall ability of their organizations to boost resilience, competitiveness, and productivity. Part of a senior security professional's role is to articulate the value of cybersecurity, incite behavioral change, and offer insights into the potential risks that could compromise the organization's cybersecurity posture and broader business health.[2] By merely reacting to security issues as they arise, security teams may find themselves mired in tactical activity, thereby undermining their capacity to strategically execute cybersecurity plans that align with business goals and desired outcomes. As such, this necessitates a shift in approach from reactive to progressive, allowing businesses to actively safeguard their interests while also supporting their growth objectives.

OUTCOME-BASED SECURITY: ELEVATE FROM REACTIVE TO PROACTIVE TO PROGRESSIVE

For cybersecurity to become a strategic and proactive driver of business outcomes, security leaders must demonstrate the value of their organizations' investments and how they can help achieve business goals. Respondents from all industries cited risk reduction, revenue growth, and increased resilience among the top five business outcomes their firms want to achieve with their cybersecurity goals, so there is an opportunity for security investments to strategically facilitate achieving these outcomes through 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-based, activity-based, or ROI-based methods. Consequently, organizations seek an outcome-based approach to cybersecurity to not only tackle risk, but also to proactively support business goals.

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

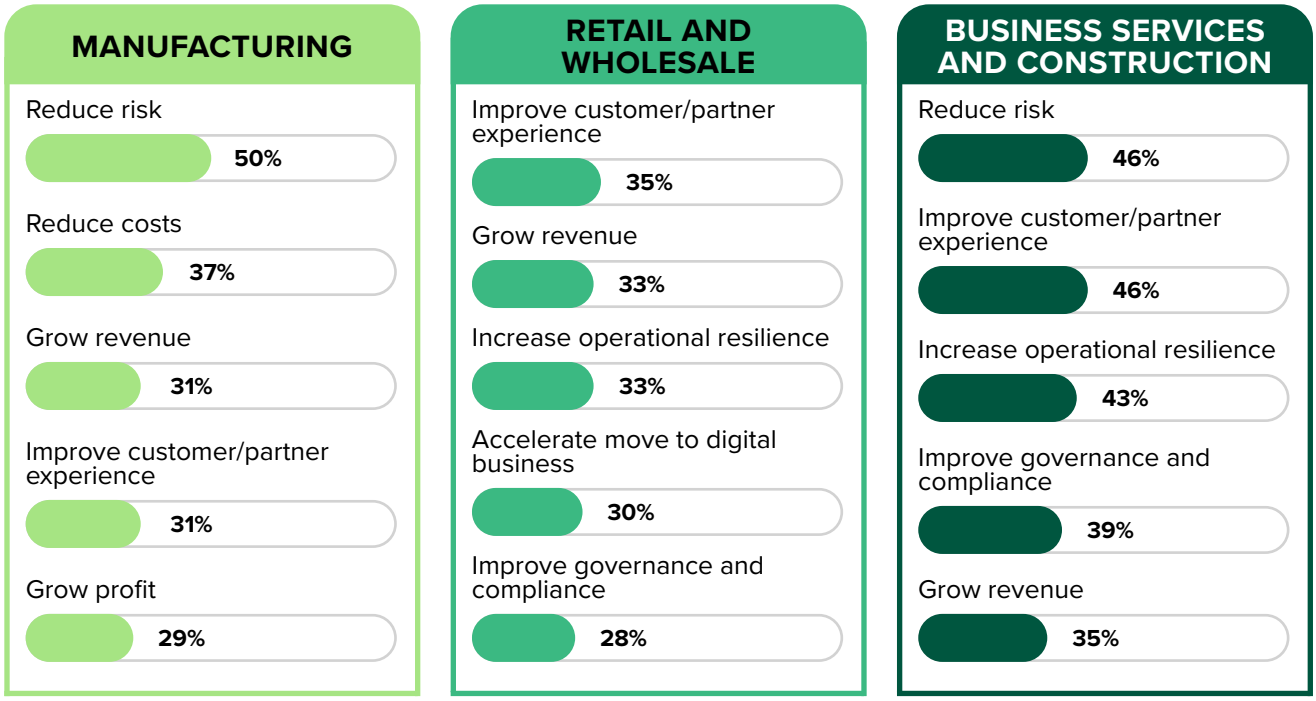
- **Reduce risk effectively.** In the dynamic landscape of today's digital world marked by a dramatic rise in complexity, an unprecedented level of connectivity, and a rapid escalation of both traditional and novel threats, the importance of effective risk reduction becomes abundantly clear. Survey respondents underscored this reality, with risk reduction prominently featured as the primary business outcome they seek from cybersecurity. A substantial 55% of decision-makers from public sector and healthcare firms identified this as their organization's top objective, closely followed by 50% from manufacturing firms. The pressing necessity of risk reduction as a strategic lever against the evolving tapestry of cyberthreats offers a compelling argument for an outcome-driven cybersecurity approach.
- **Elevate competitiveness.** While product offerings are core to an organization's business success, its customers are crucial. Cybersecurity is central to helping organizations safeguard their data and manage reputational risk. It does more than merely fulfill regulatory requirements. Cybersecurity strategically assures customers about the secure stewardship of their data and the company's readiness to resolve any privacy issues swiftly. Validating this perspective, half of the respondents in the media, entertainment, and leisure industries, 45% in utilities and telecommunications, and more than a third in retail and wholesale said customer experience (CX) enhancement is their firm's top cybersecurity-led business outcome. Likewise, a significant 46% of those in business

services and construction and more than a third in financial services and insurance ranked improved CX among their firm's top five cybersecurity goals.

- **Optimize productivity.** Effective cybersecurity boosts organizational productivity. Security professionals play a key role in ensuring cybersecurity practices enable their organization's employees to get their work done efficiently, hence elevating time to results while still ensuring that the security is robust enough to assure operational resilience. Therefore, a top business outcome for cybersecurity goals is to improve operational resilience, as nearly half of respondents from financial services and insurance (44%) and business services and construction (43%) chose this as their second highest desired outcome of cybersecurity.

Figure 2

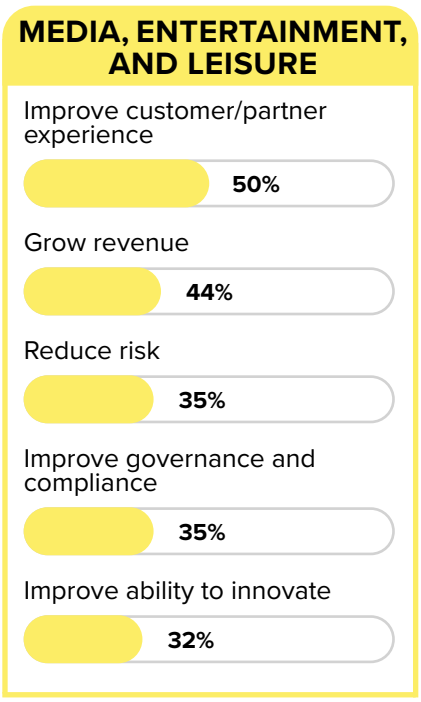
"What business outcomes does your organization hope to achieve with your top cybersecurity goals?"



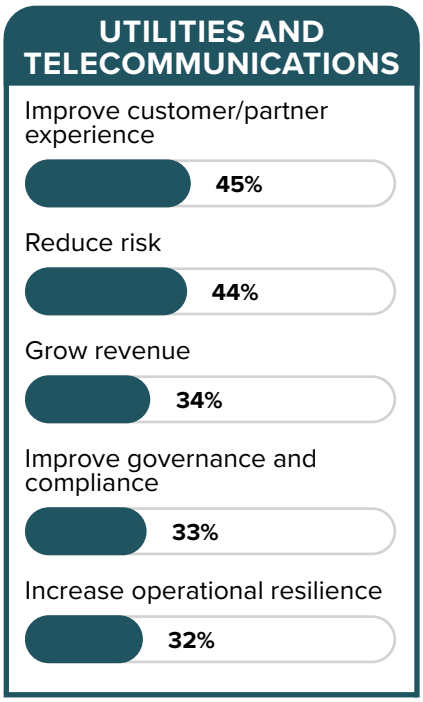
Base: 62 decision-makers from manufacturing organizations

Base: 40 decision-makers from retail and wholesale organizations

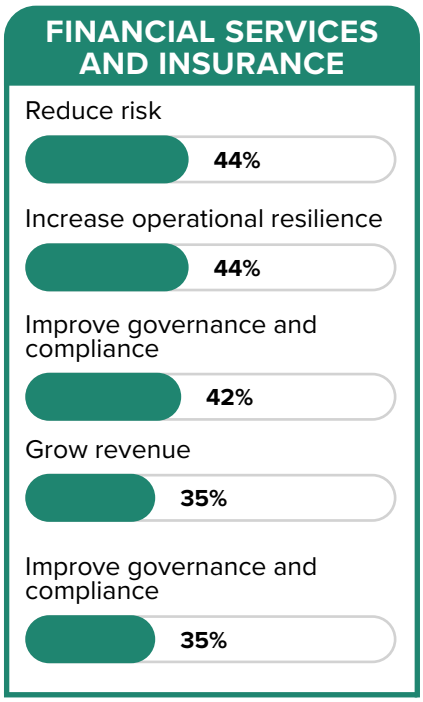
Base: 46 decision-makers from business services and construction organizations



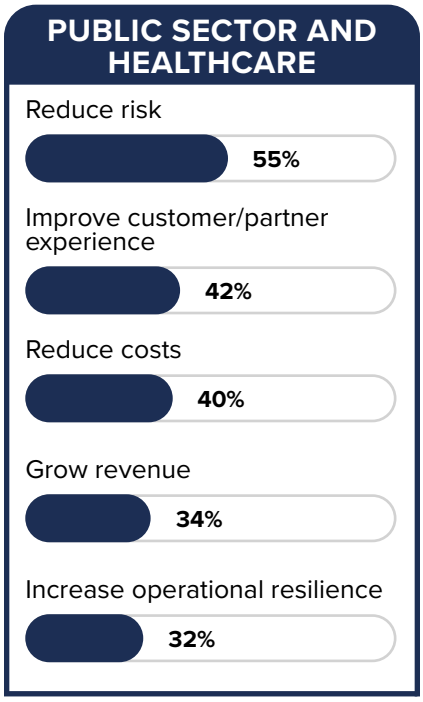
Base: 34 decision-makers at media, entertainment, and leisure organizations



Base: 128 decision-makers at utilities and telecommunications organizations



Base: 43 decision-makers at financial services and insurance organizations



Base: 53 decision-makers at public sector and healthcare organizations

Note: Showing top 5.
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

How Is Your Industry Challenged By Aligning Cybersecurity Priorities To Business Outcomes?

Few firms can report complete alignment between their cybersecurity priorities and business outcomes, as 97% of cybersecurity and IT decision-makers cited a cross-section of challenges their organizations experience. These challenges fall broadly into three categories: conflicting goals, complexity of environment, and privacy requirements. Our survey revealed which industries face the following top challenges when aligning cybersecurity priorities to business outcomes:

- **Handling conflicting cybersecurity and business goals.** Almost half of the respondents from public sector and healthcare firms (49%) and 43% from retail and wholesale firms pointed to the challenge of harmonizing cybersecurity and business goals as a primary hurdle when trying to align cybersecurity priorities with business outcomes. For public sector and healthcare firms, it's about aligning objectives that reflect a commitment to societal well-being with robust cybersecurity measures for incident readiness, response, and recovery. Meanwhile, organizations in the retail and wholesale sector are tasked with balancing the need for quick, user-friendly web and mobile experiences for their customers with the necessity for stringent data protection. These two objectives can sometimes seem to be at odds.

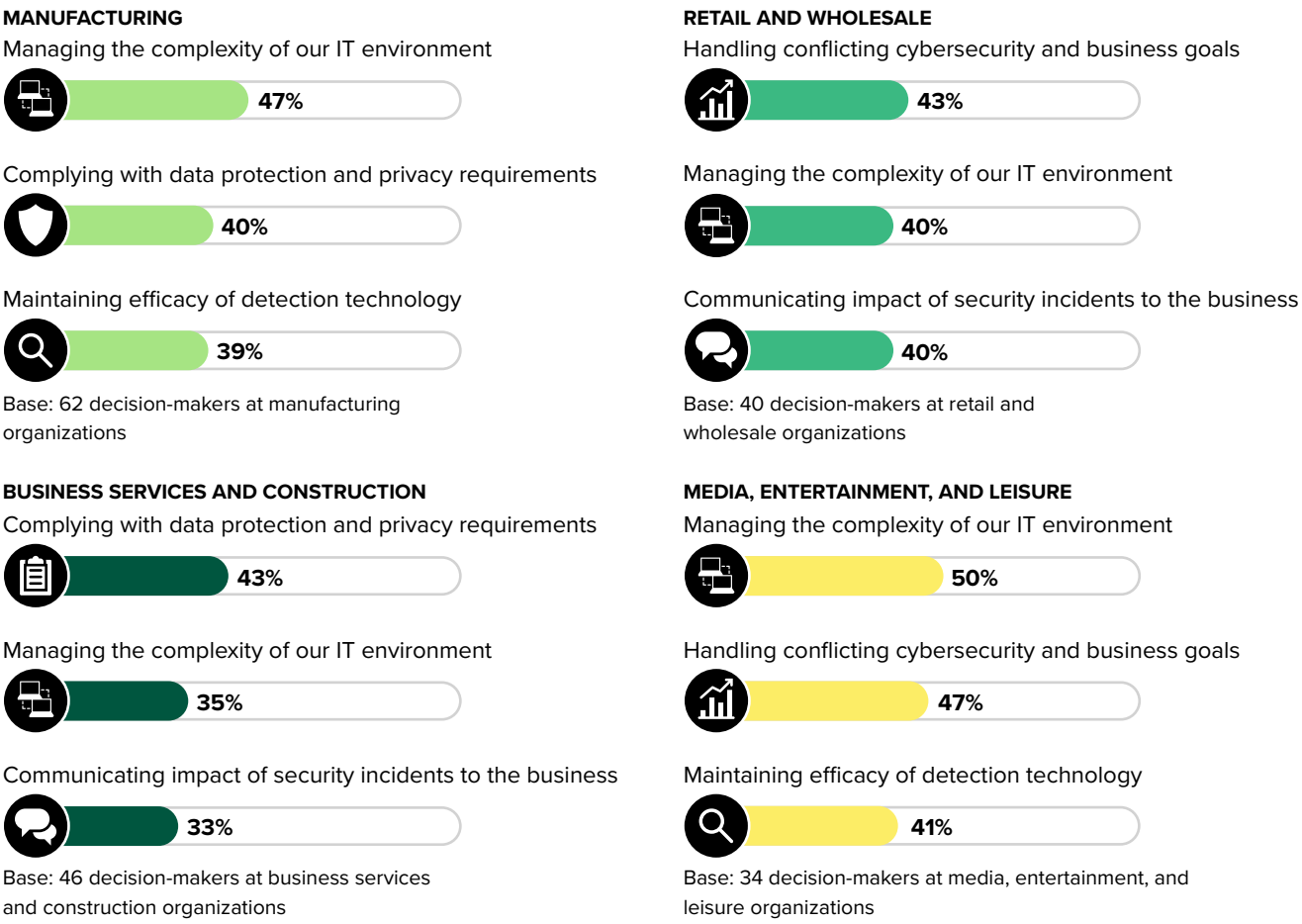
Respondents from five of the seven industries included in the survey cited that their firm having insufficient understanding of its current and desired target state for cybersecurity maturity is its top challenge.

- **Managing a complex IT environment.** Nearly half of the respondents from the media, entertainment, and leisure industry and 47% from manufacturing firms cited managing a complex IT environment as their organization's top challenge. Deploying resources to navigate this complicated domain and execute tactical security activity is often time-consuming and can be a strain on productivity. This can ultimately impact an organization's time to result and resolution.

- **Complying with data protection and privacy requirements.** Remaining compliant and mitigating risk is of the utmost importance for organizations in highly regulated industries, so it is therefore unsurprising that nearly half of respondents from the financial services and insurance industry (47%) as well as the business services sector (43%) cited complying with data protection and privacy requirements as their most common challenge. However, competing in an environment that is strictly regulated heightens the need for improved productivity and resilience beyond that of competitors. Cybersecurity must tackle the tricky challenge of helping in the pursuit of growth and digital innovation while handling the increased exposure to vulnerabilities that threat actors willingly exploit.

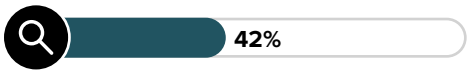
Figure 3

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

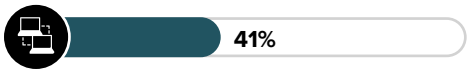


UTILITIES AND TELECOMMUNICATIONS

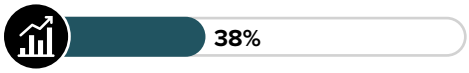
Maintaining efficacy of detection technology



Managing the complexity of our IT environment



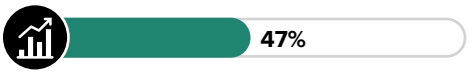
Handling conflicting cybersecurity and business goals



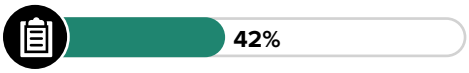
Base: 128 decision-makers at utilities and telecommunications organizations

FINANCIAL SERVICES AND INSURANCE

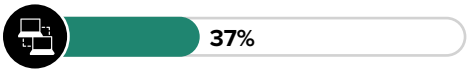
Handling conflicting cybersecurity and business goals



Complying with data protection and privacy requirements



Managing the complexity of our IT environment

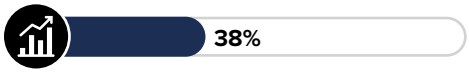


Base: 43 decision-makers at financial services and insurance organizations

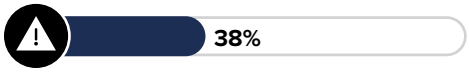
PUBLIC SECTOR AND HEALTHCARE

Complying with data protection and privacy requirements

Handling conflicting cybersecurity and business goals



Managing time demands of day-to-day tactical activities



Base: 53 decision-makers at utilities and telecommunications organizations

Base: 406 global cybersecurity and IT decision-makers who are either the final decision-maker, part of team that makes 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 YOUR CYBERSECURITY MATURITY MATTERS

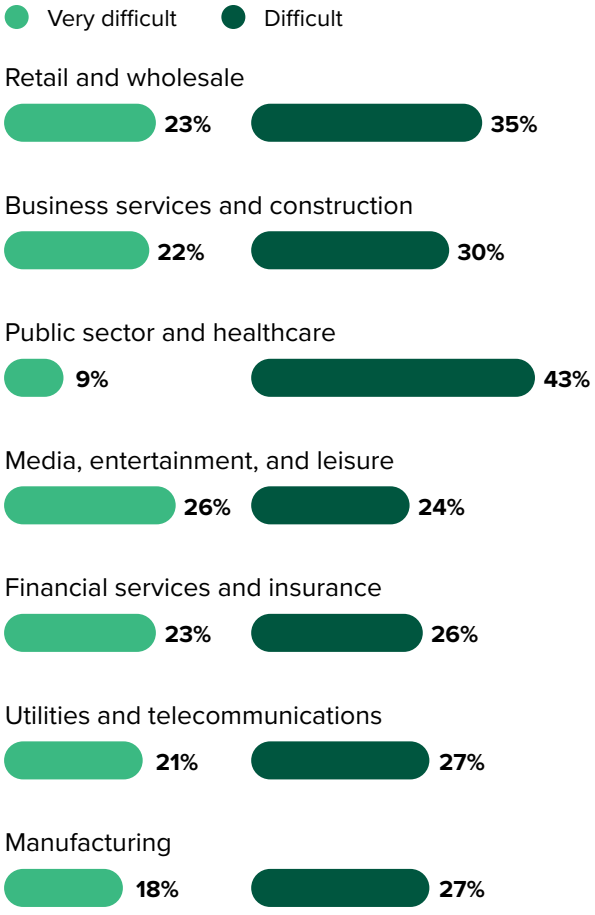
Many IT and cybersecurity leaders grapple with articulating the value of their firm's security programs and constructing a strategic roadmap to enhance its maturity level. Lacking the performance metrics necessary to demonstrate value undermines the position of cybersecurity as a driver of business outcomes, and it keeps security professionals trapped with the burden of proving the value of nothing happening.[3] For cybersecurity executives to become change agents who contribute to the success of their company's performance, security programs must be able to demonstrate how cybersecurity strategy and investments have actively assisted in achieving business outcomes. Our survey revealed which industries encounter the following obstacles on their cybersecurity maturity journeys:

- **Aligning cybersecurity priorities with business outcomes.** Growing consumer expectations about online shopping have put pressure on retailers and wholesalers to balance security with meeting customer demands for speed, ease, and efficiency. Hence, 58% of respondents from these kinds of organizations find it difficult to align cybersecurity priorities with business outcomes. For example, retailers need to walk a fine line between effective identity and access management to maintain customer confidentiality and providing a smooth checkout experience. Creating a good customer experience and maintaining a strong security posture can be challenging to put it mildly.
- **Measuring whether cybersecurity priorities are delivering the outcomes that the business seeks.** Ninety-three percent of all respondents said their organization has challenges in measuring its cybersecurity performance in relation to delivering business outcomes. More than half of respondents from the business services and construction industry (54%) said measuring whether cybersecurity priorities deliver the outcomes their firm seeks is the most difficult challenge. So did 53% from the utilities and telecommunications industry and 52% from the manufacturing industry.
- **Having insufficient understanding of current and desired target states for cybersecurity maturity.** Measuring cybersecurity performance is crucial to illustrating performance and progressing organizations' cybersecurity maturity journeys. However, gathering meaningful data

needs to be underpinned by an understanding of the current state and desired future state against which security value should be assessed. Otherwise, measuring frameworks and practices becomes redundant. This is an issue for respondents from five of the seven industries included in the survey, especially for those from the retail and wholesale industry (50%) and the financial services and insurance industry (40%).

Figure 4

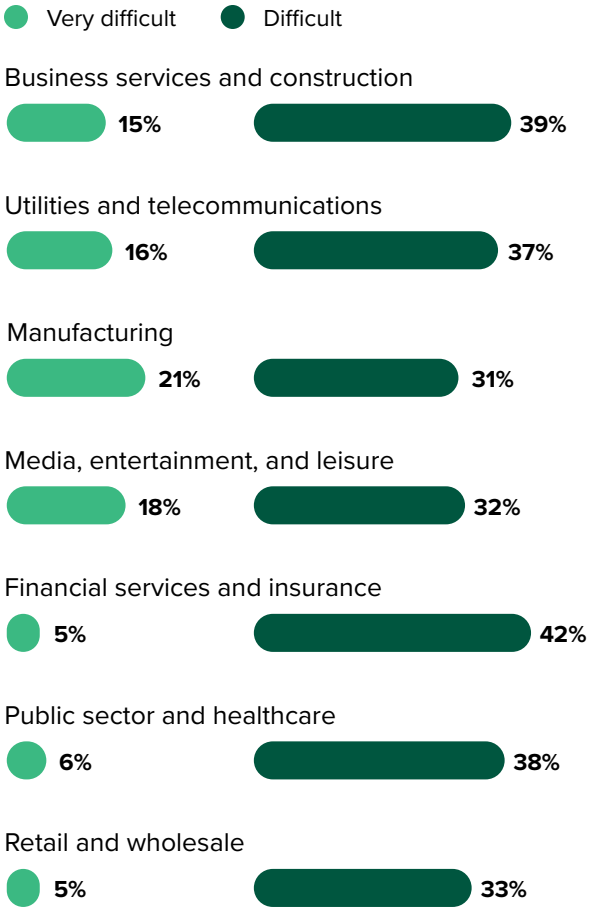
"How difficult is it for your organization to align cybersecurity priorities to business outcomes?"



Base: 202 global cybersecurity and IT decision-makers who are either the final decision-makers, part of team that makes decisions, or influences decisions when their organization purchases cybersecurity solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

Figure 5

"How difficult is it for your organization to measure whether cybersecurity priorities are delivering the outcomes that your business seeks?"



Base: 199 global cybersecurity and IT decision-makers who are either the final decision-makers, part of a team that makes decisions, or influences decisions when their organization purchases cybersecurity solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of WithSecure, December 2022

An Outcome-Based Approach Is The Future Of Cybersecurity

Future-fit organizations are exploring and embracing a new approach to cybersecurity in order to give security decision-makers a seat at the table in actively contributing to business outcomes. Leaders are aware of the key role cybersecurity can play beyond reducing risk to aid their organizations' market competitiveness and productivity.

Virtually all respondents (99%) said their organization is looking at outcome-based security, with 83% interested in, planning to adopt, or expanding adoption of outcome-based cybersecurity solutions and services to achieve business outcomes. The remaining respondents said their organization has already adopted the approach. The financial services and insurance sector leads the charge as 77% of respondents in the industry said their firm plans to adopt outcome-based cybersecurity in the next 12 months or that it plans to expand or upgrade its adoption. Interestingly, 100% of the respondents from the manufacturing, financial services and insurance, and retail and wholesale industries are interested in outcome-based cybersecurity, and their organizations fall into different levels of maturity when it comes to implementing the approach.

To not approach cybersecurity with a strategic lens is to fall behind. And firms can't do it alone. Seventy-two percent of respondents revealed their company wants to switch to a vendor that delivers security outcomes, and those in manufacturing (76%) and utilities and telecommunications (73%) are the most likely to switch. They recognize that orienting contracts with cybersecurity vendors around outcomes is a progressive approach that will help their firms 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 buyers want), organizations will look elsewhere. This shifts the relationship with security vendors to be a truly a strategic partnership. Decision-makers said they expect a range of benefits in risks, costs, and operations from outcome-based cybersecurity (see Figure 6).

Figure 6

Benefits Of Reducing Risk With Outcome-Based Cybersecurity

Increased resilience. Security threats rarely work in a silo, and organizations have become more interested in solutions that are able to bring a holistic view to cyber risk management. Organizations that expedite detection, response, and recovery from attacks will be better able to protect their business continuity and brand reputations.

Improved productivity. Outcome-based security enables flexibility. Solutions tied to outcomes as opposed to rigid frameworks are less challenging to swap for alternative solutions. If a security product or service doesn't contribute to your desired outcome, then get rid of it; you can invest the time, money, and effort that you save into something that does. This results in less wastage of money, time, effort, and resources, which amplifies productivity.

Enhanced competitiveness. Outcome-based cybersecurity aligns the incentives of security vendors and their buyers. This allows organizations to grow revenue and improve their long-term profitability.

MAKE PROGRESS ON YOUR OUTCOME-BASED CYBERSECURITY JOURNEY

Where are you on your outcome-based cybersecurity journey? Most respondents' organizations have begun their outcome-based cybersecurity journeys; however, some industries are further along than others. A comparative analysis across industries indicates that the three sectors furthest ahead are: financial services and insurance (86%), retail and wholesale (85%), and public sector and healthcare (84%) in so far as organizations in these industries either plan to adopt the approach in the next 12 months, have adopted outcome-based security already, or are planning to expand/upgrade their products/services.

The expected benefits from adopting outcome-based cybersecurity differ depending on the firm's maturity level. The survey revealed the following:

- **Journey starters expect outcome-based security to excel their efforts of proactively supporting business outcomes.** For respondents from organizations that are planning to adopt outcome-based security in the next 12 months, the top expected benefits closely align to the business outcomes they want to achieve. For 46% of respondents from utilities and telecommunications as well as media, entertainment, and leisure, one of the top expectations of cybersecurity is to provide competitive advantage through increased agility. The increased flexibility cybersecurity offers through this approach pivots it from sometimes being an obstacle within competitive markets to becoming a flexible aid when organizations need to meet growing consumer expectations or quickly adapt to market changes.

- **Advance adopters expect outcome-based security to improve long-term profitability and assure regulators of cybersecurity quality.** Respondents whose organization is expanding or upgrading its adoption of outcome-based security said their firm has shifted its focus toward the long-term view. Having boosted their resilience, productivity, and assurance that cybersecurity can aid their competitiveness, advanced adopters look to the approach as a source of profitability. Fifty percent of respondents from retail and wholesale, as well as more than a third from business services and construction and media, entertainment, and leisure have this expectation. Those in highly regulated sectors such as financial services and insurance (56%) and utilities and telecommunications (39%) said that as their firm's maturity in outcome-based security grows, they expect it will assure regulators about the quality of the cybersecurity.

The three sectors furthest ahead on the outcome-based cybersecurity journey are:

1) Financial services and insurance

2) Retail and wholesale

3) Public sector and healthcare

Figure 7

"What benefits do you expect as a result of adopting an outcome-based approach for cybersecurity?"

MANUFACTURING

Planning to adopt in the next 12 months

Reduced business risk — **50%**

Greater cybersecurity cost control — **46%**

Effective response to cyberthreats — **42%**

Base: 24 decision-makers from manufacturing organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption

Base: 20 decision-makers from manufacturing organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

RETAIL AND WHOLESALE

Planning to adopt in the next 12 months

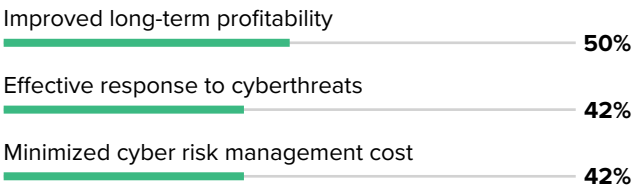
Reduced business risk — **57%**

Greater cybersecurity cost control — **43%**

Effective response to cyberthreats — **36%**

Base: 14 decision-makers from retail and wholesale organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

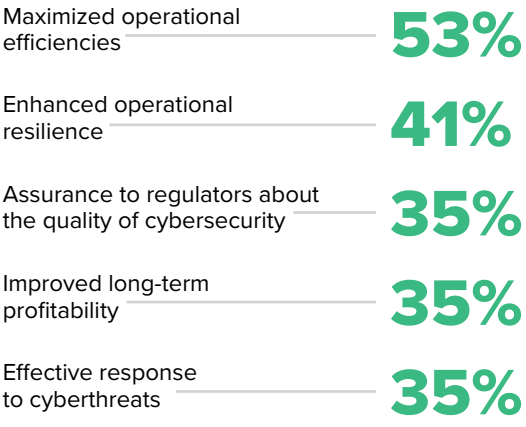
Expanding or upgrading adoption



Base: 12 decision-makers from retail and wholesale organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

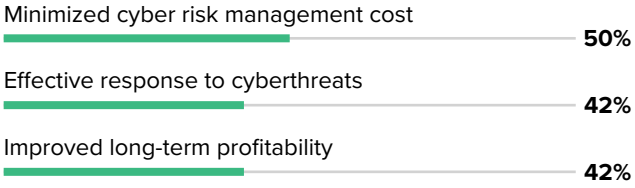
BUSINESS SERVICES AND CONSTRUCTION

Planning to adopt in the next 12 months



Base: 17 decision-makers at business services and construction organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption



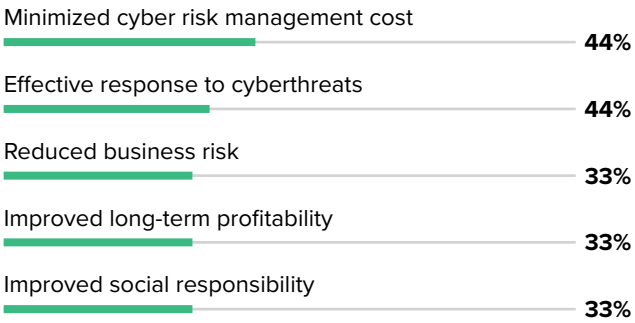
Base: 12 decision-makers from business services and construction organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

MEDIA, ENTERTAINMENT, AND LEISURE

Planning to adopt in the next 12 months

Base: 13 decision-makers at media, entertainment, and leisure organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption



Base: 9 decision-makers at media, entertainment, and leisure organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

UTILITIES AND TELECOMMUNICATIONS

Planning to adopt in the next 12 months

Greater cybersecurity cost control — **46%**

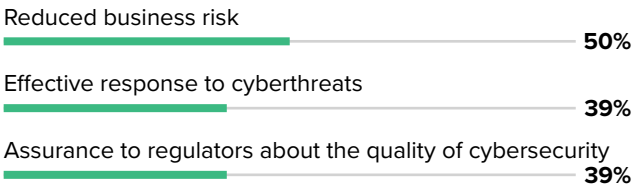
Competitive advantage through increased agility — **46%**

Cybersecurity that proactively supports business goals — **43%**

Improved long-term profitability — **43%**

Base: 35 decision-makers at utilities and telecommunications organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption



Base: 36 decision-makers at utilities and telecommunications organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

FINANCIAL SERVICES AND INSURANCE

Planning to adopt in the next 12 months

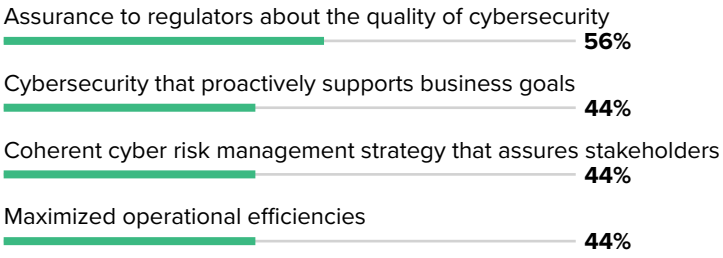
Cybersecurity that proactively supports business goals — **65%**

Reduced business risk — **53%**

Coherent cyber risk management strategy that assures stakeholders — **35%**

Base: 17 decision-makers at financial services and insurance organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption



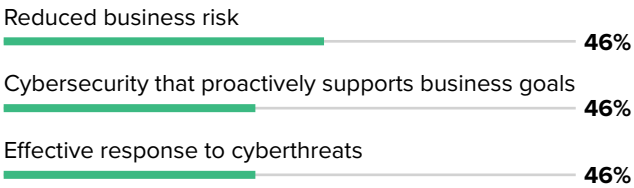
Base: 16 decision-makers at financial services and insurance organizations that are expanding or upgrading adoption of an outcome-based approach for cybersecurity

PUBLIC SECTOR AND HEALTHCARE

Planning to adopt in the next 12 months

Base: 21 decision-makers at public sector and healthcare organizations that are planning to adopt an outcome-based approach for cybersecurity in the next 12 months

Expanding or upgrading adoption



Base: 13 decision-makers at public sector and healthcare organizations that are upgrading adoption of an outcome-based approach for cybersecurity

Base: 326 global cybersecurity and IT decision-makers who are either the final decision-makers, part of a team that makes decisions, or influences decisions when their organization purchases cybersecurity solutions
Note: Showing top 3.
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.) on the outcomes that the company is pursuing and explain how the proposed security investments will contribute.

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

Shift your stakeholder communications from "We're adding X security measure because it's better" to "Here are the specific benefits we receive from this specific security measure." For example: An organization may use risk-based authentication in e-commerce to improve its customer experience by eliminating extra steps or friction from low-risk transactions and improve monitoring by reducing false positives and enabling anomaly detection.

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 just 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 pursue it. This will also help you stay relevant in light of emerging technology risks.

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

Analyzing and phasing out security technology that doesn't help you achieve your desired outcomes allows you to redirect that spending toward desired ones. In addition, IT asset complexity remains a top challenge, and it is a common root cause of security incidents. Trimming your portfolio also improves your visibility and helps you spot blind spots more quickly.

Encourage collaboration.

Security does not exist in a silo, and it is a means to an end: staying in business. Interfacing frequently with stakeholders beyond security and IT will provide invaluable input when aligning your outcomes with the business. The outcomes defined will be essential in determining crown jewels, influencing target maturity definition, and revealing how to recover from existential threats.

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. This means these contracts will look different than traditional agreements. To avoid such agreements hitting 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.

Implement monitoring to ensure that your efforts are achieving 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. 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 global organizations to evaluate their firms' approaches to cybersecurity and their 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.

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by WithSecure titled, "The Value Of Putting Security Outcomes First."

Project Team:
Ashleigh Cohen,
Market Impact Consultant

Tanvi Dahiya,
Associate Market Impact Consultant

Contributing Research:
Forrester's European Technology Architecture & Security research group

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 to 499	**5%**
500 to 999	**45%**
1,000 to 4,999	**37%**
5,000 to 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%

INDUSTRY (CONTINUED)	
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 because of rounding.

Appendix C: Endnotes

[1] Source: "Build The Business Case For Cybersecurity And Privacy," Forrester Research, Inc., January 12, 2022.
[2] Source: "Role Profile: Director Of Cybersecurity Influence And Engagement," Forrester Research, Inc., March 10, 2023.
[3] Source: "Assess Your Security Program With Forrester's Information Security Maturity Model (FISMM)," Forrester Research, Inc., July 3, 2023.