



THE NEW CYBERSECURITY EQUATION: Risk, Response, and Business Outcomes



Cathy Huang
Research Director,
Security Services Worldwide, IDC



Craig Robinson
Program Director,
Security Services, IDC

Table of Contents



CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

In This InfoBrief	3	No Longer Cost Centers, Cybersecurity Efficacy and Resilience Deliver Business Value	10
The Growing Threat Landscape	4	Key Takeaways	11
The Cost of Cyberattacks Intensifies	5	Recommendations for Security Teams	12
The Real Impact of Cyberattacks: Business Disruption Versus Direct Cyberattack Costs	6	About the IDC Analysts	13
Detection, Talent, and Visibility Are the Top 3 Cybersecurity Gaps	7	Message from the Sponsor	14
Unmanaged Cybersecurity Tools Are Not Helping!	8		
Some Security Outcomes Carry More Weight Than Others	9		

In This InfoBrief

- ▶ In an era where 86% of organizations face increasing cyberattacks, **the cybersecurity landscape is undergoing a fundamental transformation.**
- ▶ In this InfoBrief, we reveal key findings from a survey that we conducted in October 2024 among U.S. cybersecurity decision-makers to understand **the challenges, priorities, and outcomes of their cybersecurity programs.**
- ▶ A total of 260 qualified respondents with the following demographics participated in the survey:



Mid-size companies and large enterprises in the United States with 500+ employees in a cross-section of vertical markets (public sector organizations with 250+ employees qualified)



Companies that use cybersecurity solutions



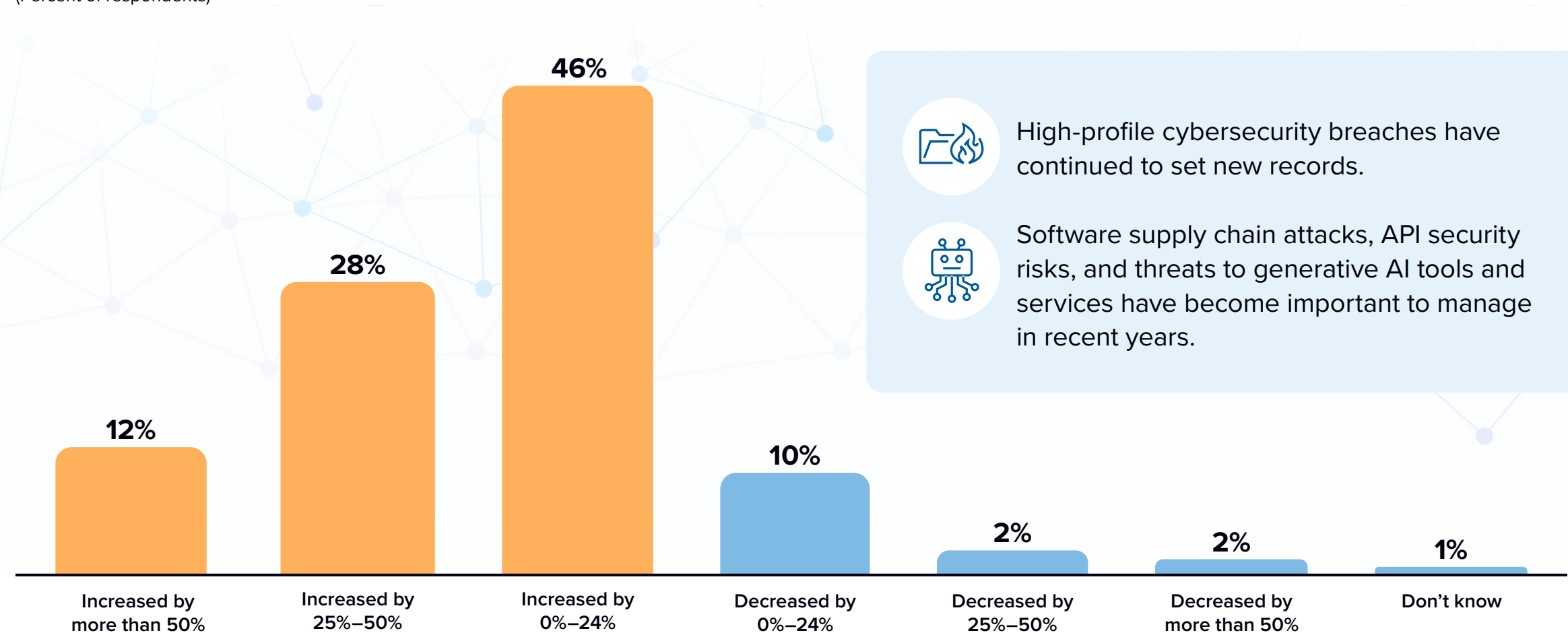
Decision-makers or influencers for cybersecurity tools and solutions, including CIOs, CTOs, and CISOs, as well as IT, security, and LoB directors/managers



The Growing Threat Landscape

86% of surveyed respondents indicated their organizations experienced more cyberattacks compared to the previous year.

(Percent of respondents)

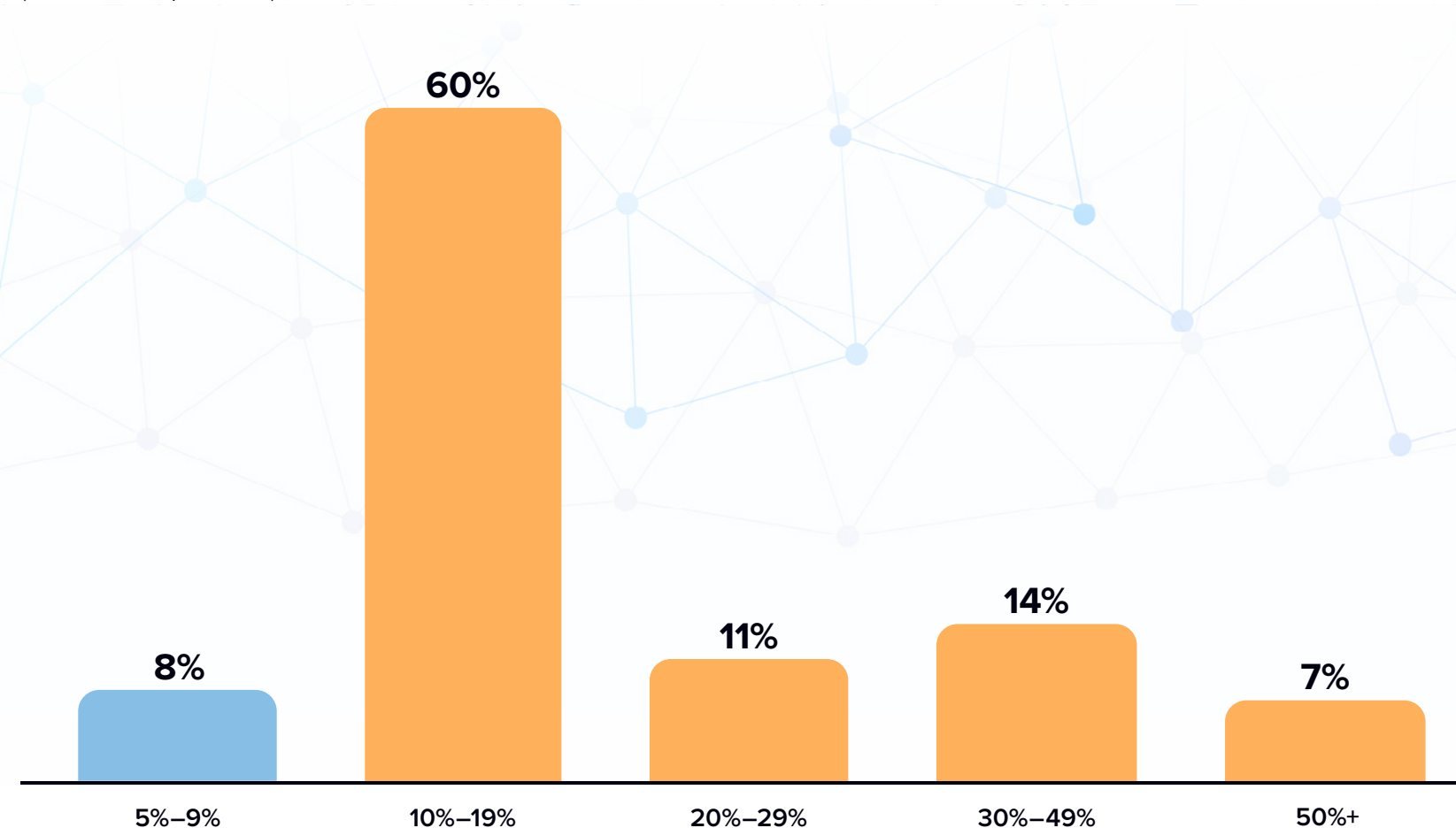


n = 260; Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

The Cost of Cyberattacks Intensifies

Cyberattacks are increasing in frequency, and the resulting financial impact leads to increased awareness and immediate attention in mid- and large-sized businesses.

(Percent of respondents)



n = 223 (respondents that indicated a percentage increase in the number of successful cyberattacks on their organization); Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

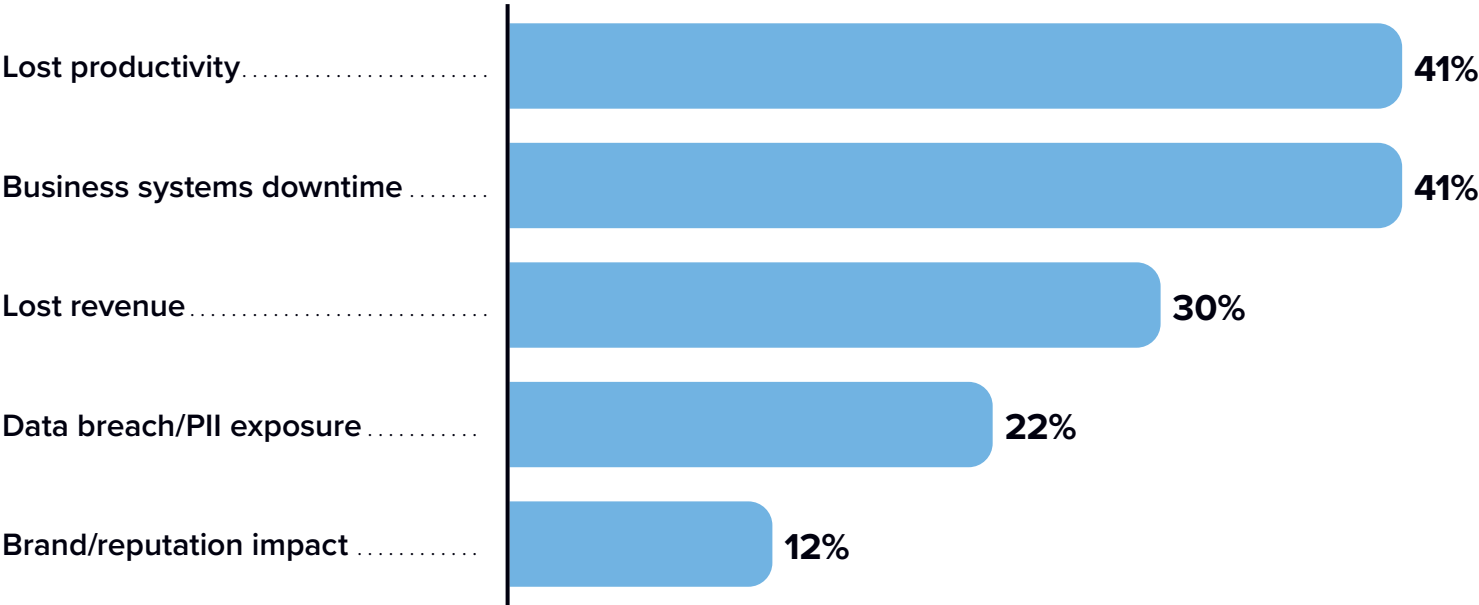


The Real Impact of Cyberattacks: Business Disruption Versus Direct Cyberattack Costs

The impact of cybersecurity attacks can no longer just fall within the traditional technology domains. Digital transformation has intertwined technology with business operations. Cyber-resilience impacts the bottom line, and companies must view it through a holistic lens.

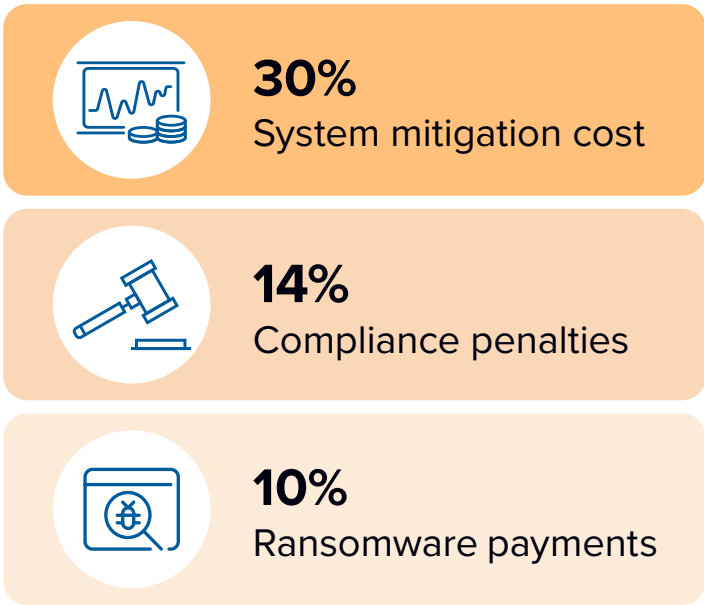
Primary Business Impact

(Percent of respondents)



Direct Cyberattack Costs

(Percent of respondents)



n = 260; Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

Detection, Talent, and Visibility Are the Top 3 Cybersecurity Gaps

Detection dominates the top gaps of an organization's cybersecurity program, especially early threat detection as well as detection of more advanced threats. The next top two gaps include hiring and retaining cybersecurity talent and ensuring visibility across a growing attack surface. Focusing on the top three gaps will improve cybersecurity programs.




**42%
Detection**

Real-time monitoring and threat detection are the primary gaps in cybersecurity programs.



**37%
Talent**

Hiring and retaining skilled cybersecurity professionals remains a critical challenge.



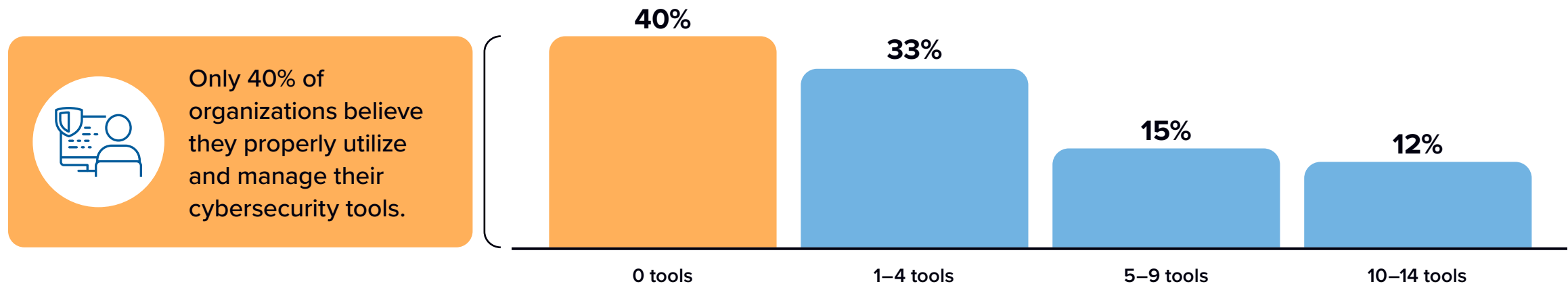
**34%
Visibility**

Maintaining visibility across expanding attack surfaces is crucial for effective security.

Base: all respondents. n = 260; Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

Unmanaged Cybersecurity Tools Are Not Helping!

To the best of your knowledge, how many cybersecurity tools do you have that are not properly monitored and managed?
(Percent of respondents)



Tools need TLC

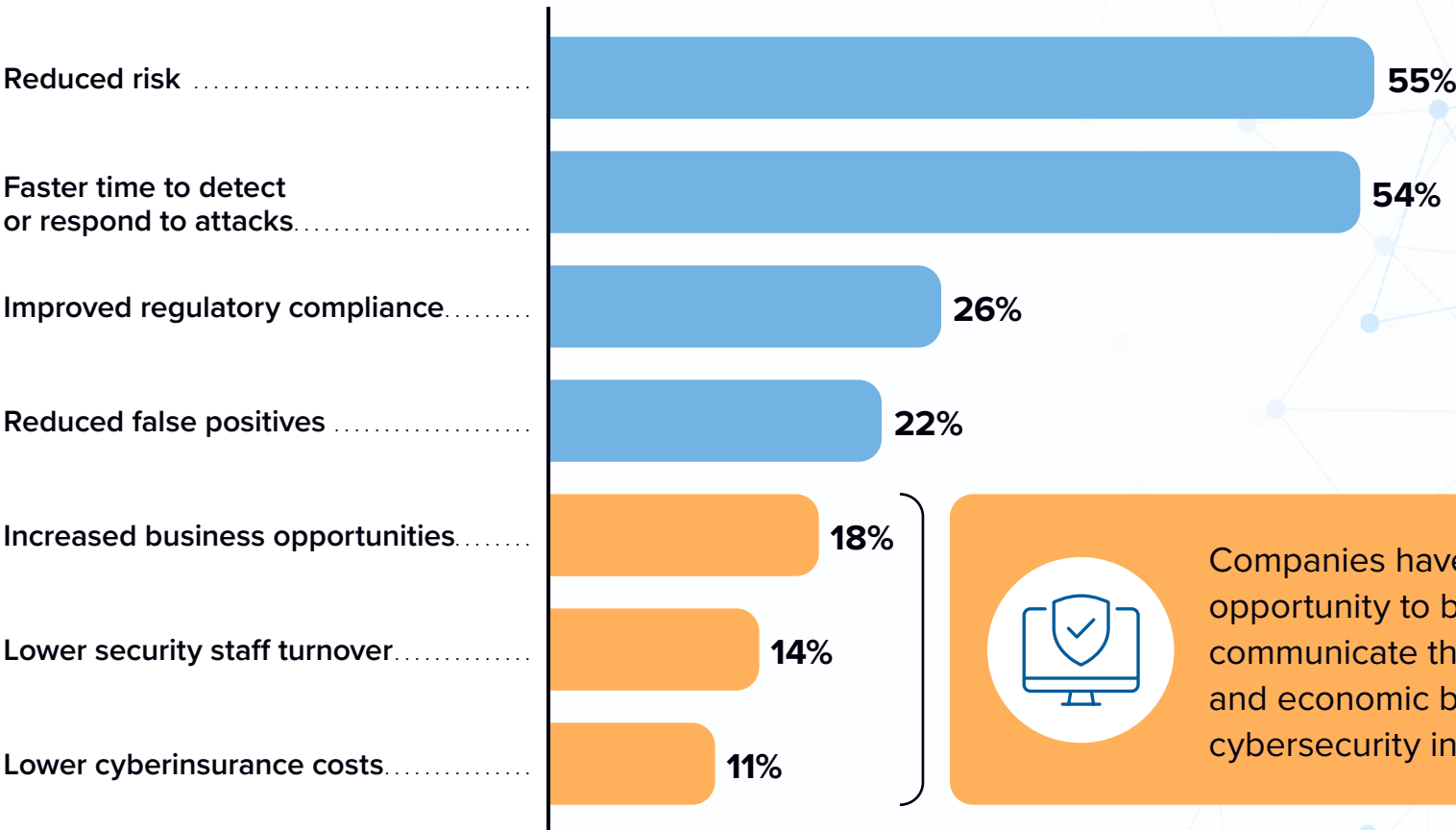
- ✓ **Tie** them together with other tools or platform(s).
- ✓ **Log** relevant data.
- ✓ **Configure** and update them regularly.

Base: all respondents. n = 260; Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

Some Security Outcomes Carry More Weight Than Others

As organizations plan to strengthen their cybersecurity infrastructure, the top security outcomes are risk reduction and faster time to detect/respond to attacks. When communicating cybersecurity investment to stakeholders, use the narrative of primary security outcomes and supporting benefits.

(Percent of respondents)



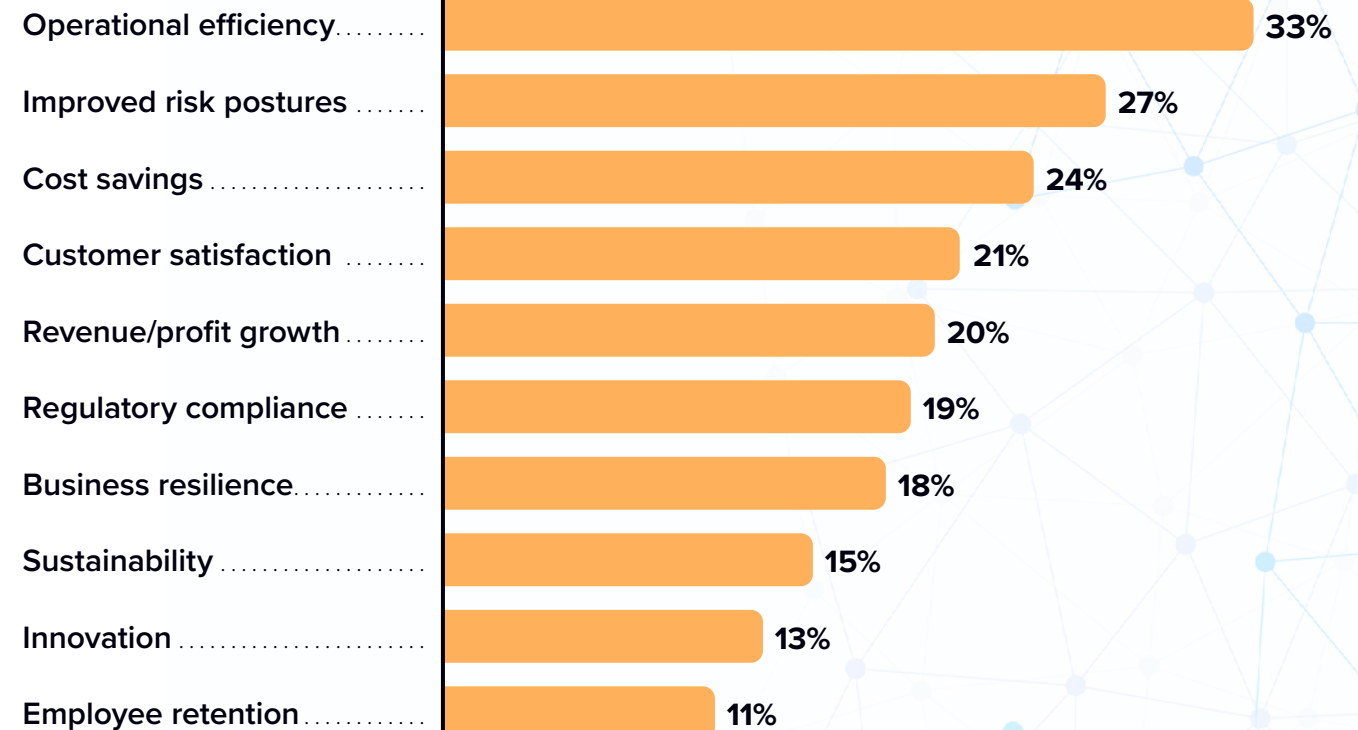
Companies have an opportunity to better communicate the business and economic benefits of cybersecurity investment.

n = 258; Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

No Longer Cost Centers, Cybersecurity Efficacy and Resilience Deliver Business Value

Please select the most important business values to your organization as a result of your cybersecurity efficacy and resilience level.

(Percent of respondents)



n = 260 Source: IDC's *Lumen Cyber Security Services Survey*, October 2024

Key Takeaways



The Business Imperative

- ▶ The increased number of cyberattacks signals that this isn't just a security issue but also a business continuity challenge.
- ▶ The business costs of cyberattacks (productivity, downtime, and revenue) outweigh direct security costs.
- ▶ **92%** of organizations recognize the business impact of cyberattacks, which shows security solutions can be a value creator, not just a cost center.



The Efficiency Mandate

- ▶ **60%** of security programs in mid-sized companies and large-sized enterprises lack efficiency and optimization.
- ▶ Detection capabilities represent the primary gap in security programs.
- ▶ Mid-sized organizations and large enterprises should focus on tool optimization over tool acquisition.
- ▶ Companies should get outside help as needed. Respondents rated “strong in cybersecurity advisory capabilities” (i.e., 21%) as the top reason for selecting their most important cybersecurity services partner, followed by “excellent operational and tactical capabilities” (i.e., 17%).

Recommendations for Security Teams

The Strategic Shift

- ✓ Move from a tools-first to an outcomes-first approach.
- ✓ Focus on early threat detection and advanced threat capabilities.
- ✓ Prioritize visibility and talent retention alongside technical controls.
- ✓ Emphasize demonstrated positive business impacts of implemented cybersecurity programs.
- ✓ Connect security investment to direct benefits in operational efficiency, business resilience, and reduced risk.



About the IDC Analysts

**Cathy Huang**

Research Director,
Security Services Worldwide, IDC

Cathy Huang is the research director for IDC's WW Security Services research practice. In her role, Cathy collaborates with other worldwide and regional analysts to develop a set of thought leadership and actionable research for IT buyers and suppliers. Specifically, she develops core research around managed security services, security consulting, and integration services within the program. She also incorporates IDC's Future of Trust and other FoX agenda to drive new research such as cloud security services and secure edge services for the program. Ms. Huang brings a wealth of security and services expertise and knowledge to the position. She draws on her deep domain expertise across a broad range of ICT segments to support any custom or advisory work with regard to security services.

[More about Cathy Huang](#)**Craig Robinson**

Research Vice President ,
Security Services, IDC

Craig Robinson is a program director within IDC's Security Services research practice, focusing on managed services, consulting, and integration. Coverage areas include IoT security, blockchain services, threat detection, and response services. Craig delivers unparalleled insight and analysis, leveraging his unique experience leading diverse IT teams across several industries. This expertise positions him to provide valuable thought leadership, research, and guidance to vendors, service providers, and clients worldwide.

[More about Craig Robinson](#)

Message from the Sponsor



With a comprehensive portfolio and experienced talent, Lumen is your single provider for enhancing your cybersecurity posture.

Lumen can help safeguard customer experiences, protect your confidential data, and manage potential threats to your business. Backed by the extensive and deeply interconnected Lumen global network, the advanced threat intelligence from Black Lotus Labs, and a team of security experts with the right skills and vast experience, Lumen is a trusted partner dedicated to improving your security posture.

Secure your digital environments and maximize productivity
with our cybersecurity solutions

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

[idc.com](https://www.idc.com)

[in @idc](https://www.linkedin.com/company/idc)

[X @idc](https://twitter.com/idc)

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)