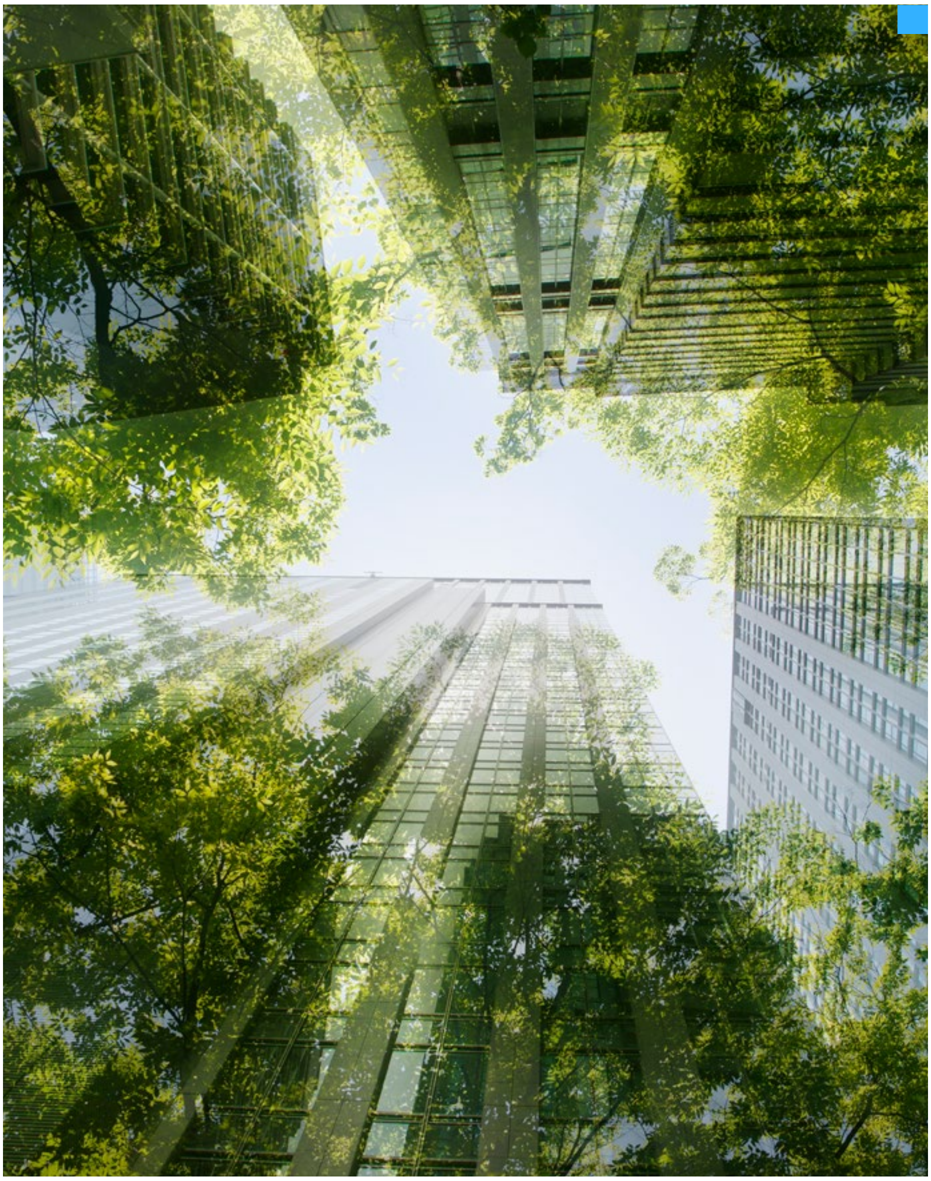
IBM Institute for Business Value | Research Insights



Prosper in the cyber economy

Rethinking cyber risk for business transformation

How IBM can help

IBM Security® works with you to manage cyber risk and accelerate business transformation. By aligning your security strategy to your business, we can help you make security a revenue enabler. For more information, please visit: https://ibm.com/security

Key takeaways

"Today, the cyber economy is the economy. Corrupt those networks and you disrupt this nation."[1]

Condoleezza Rice, former
US National Security Advisor

66% of respondents view cybersecurity primarily as a revenue enabler.

Rethinking security through a lens of value instead of as a budget line item can lead to transformative growth.

Mature security organizations see a 43% higher revenue growth rate over five years than the least mature organizations.

Those with advanced security capabilities are converting them into significantly better business outcomes.

43% of organizations report outsourcing their security program governance and operations to partners.

Shared responsibility is becoming essential to security operations, with 57% of respondents standardizing their security architecture in coordination with security partners.

Operations leaders need to flip the cybercrime equation—not by matching dollars lost with increased spending, but by changing how they think about cybersecurity.

10 trillion reasons to act

The disparity is striking. Over the next four years, the costs associated with cybercrime—$10.5 trillion annually by 2025—are estimated to exceed worldwide cybersecurity spending—$267.3 billion annually by 2026—by *40 times.*[2]

Threat actors are winning in the cyber economy, seizing on the expansion of organizations' overall attack surfaces and increased vulnerabilities introduced by society's reliance on connected services. It's time for operations leaders to flip the equation—not by matching dollars lost with increased spending, but by changing how they think about cybersecurity.

Rather than living in a state of perennial defense, where attention is focused on mitigating threats and surviving to fight another day, leaders need to recognize security as an essential common thread that ties together the organization's business and technology strategies. Technology-enabled business transformation is no longer about investing in individual areas simply to achieve functional maturity. Instead, it must be about combining technologies and capabilities to unlock larger pools of value, aligning operations to achieve greater efficiencies, and collaborating more effectively to deliver better business outcomes.[3]

To make security a critical enabler of successful transformation and growth, organizations are shifting their focus from risk exposure to cyber resilience (see Figure 1). The result is an organization less reliant on fixed boundaries, more integrated with partners, and more resilient to the unknowns characterizing today's operating environment. This newfound and more mature security posture will manifest itself differently within specific industries as well as within each organization's transformation journey.

Effective cybersecurity is less about responding to adverse events and more about preventing, mitigating, and avoiding them.

To better understand enterprise perceptions of cyber risk and cybersecurity, the IBM Institute for Business Value (IBV) partnered with Oxford Economics to interview more than 2,300 business, operations, technology, cyber risk, and cybersecurity executives across 18 industries and 25 countries (see Study approach and methodology on page 28).

This research presents one of the most comprehensive analyses to date of insights from leaders responsible for driving their organizations' IT and information security (IS) transformation agendas. The findings paint a compelling picture of cybersecurity evolving into a core strategic capability that can reduce financial risk exposure, enable greater operational efficiencies, and unlock new sources of value.

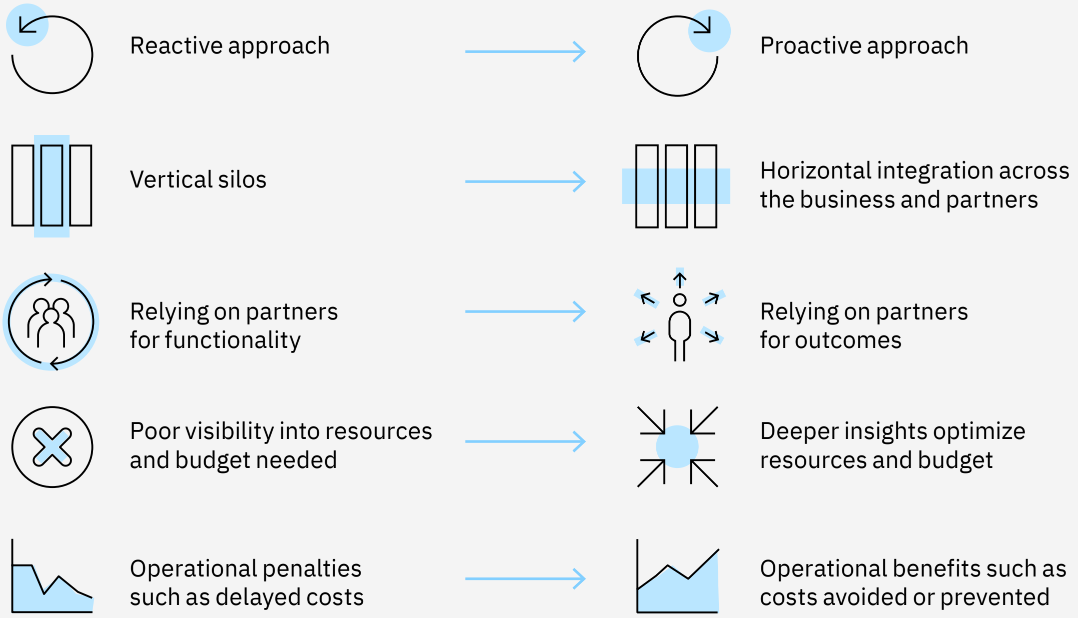
FIGURE 1

Cybersecurity strategy evolution

Refocusing from risk exposure to resilience results in a more mature security posture that can fuel business transformation and enable greater value.

From ad hoc risk remediation and threat management

To a focus on risk and resilience across the security lifecycle



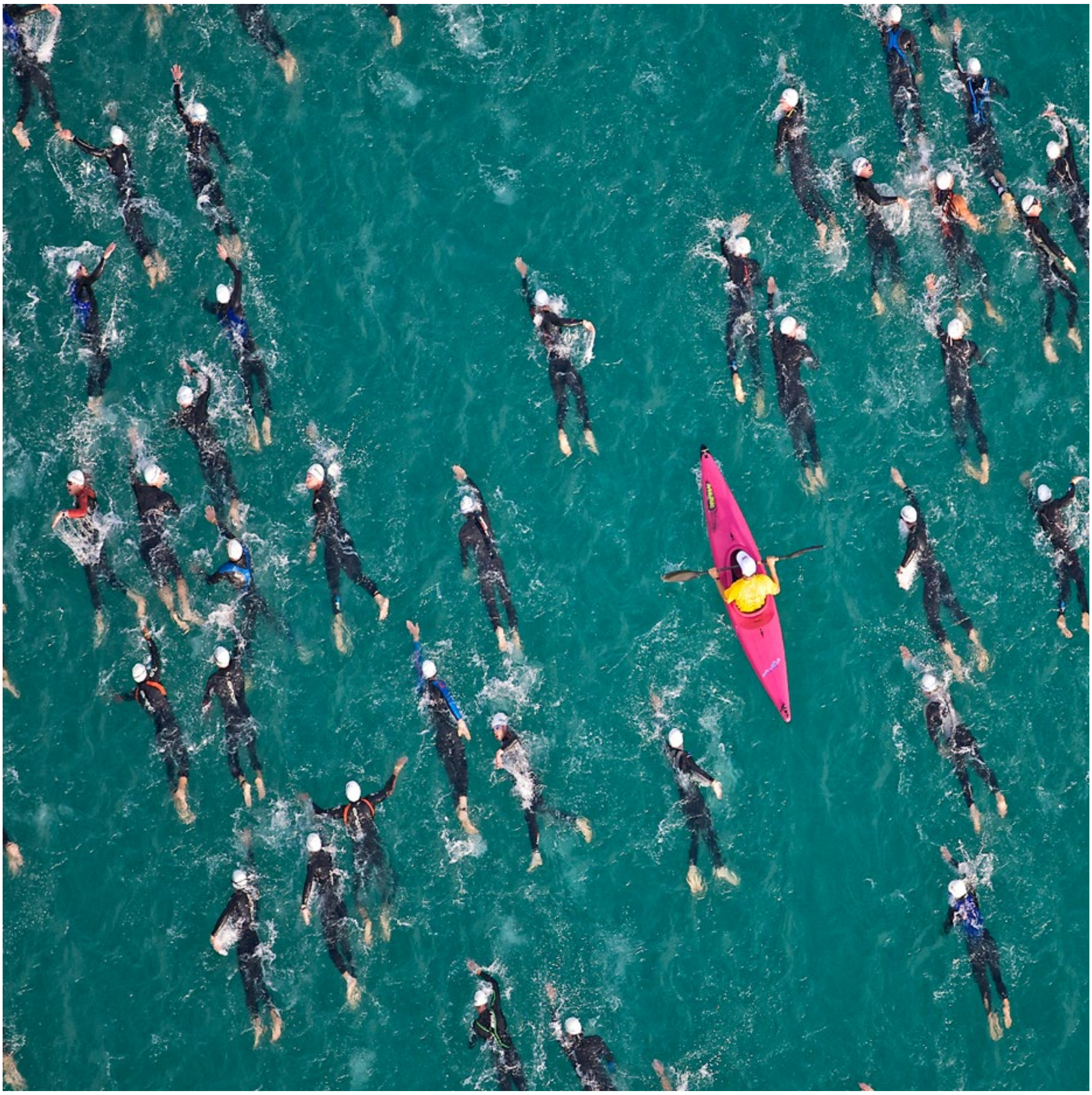
Reactive approach → Proactive approach

Vertical silos → Horizontal integration across the business and partners

Relying on partners for functionality → Relying on partners for outcomes

Poor visibility into resources and budget needed → Deeper insights optimize resources and budget

Operational penalties such as delayed costs → Operational benefits such as costs avoided or prevented



"Cybersecurity is the issue of the decade."[4]

Arvind Krishna, CEO, IBM

The new economics of cybersecurity

While cybersecurity has climbed the list of C-suite priorities, operational maturity—and the value of investments—is still developing. For example, in the 2022 IBV CEO study, cybersecurity ranked as the third most important business challenge over the next two to three years, with 45% of CEOs viewing cyber risk as one of their major business challenges in 2022, up 15% from 2021.[5]

Concurrently, our research indicates security spending is becoming a more significant portion of IT spending, increasing from an estimated 9% today to more than 10% in 2024.

But moving from aspiration to action is a challenge. While 86% of respondents report they've adopted a security strategy, only 35% of organizations have started executing that strategy. And only about 50% align their security and business strategies.

Meanwhile, survey respondents indicate, on average, their organizations have faced 349 cybersecurity incidents and 9 data breaches in the past year alone. And as reported in the 2022 IBM and Ponemon Institute Cost of a Data Breach study, the average cost of a data breach was $4.35 million.[6] Why is stemming the tide of cyber threats so difficult?

One reason: it's simply not a fair fight, economically speaking. Cybercriminals typically take a patient, opportunistic, methodical approach, operating under an economic model that has historically been based on extremely low-cost, low-risk yet high-reward opportunities. They routinely face little or no consequences for their actions. And they only need to get it right once to reap substantial rewards.

For cyber defenders, the economics are noticeably more complex. Organizations bear the brunt of costs. This includes direct costs associated with threat mitigation and recovery—and even more significantly—indirect costs associated with losses of reputation, intellectual property, brand prestige, customers, and competitive advantage, as well as disruption of operations, increases in insurance rates, and regulatory fines—all of which can accrue for years after the incident.[7]

Add to the equation the talent differential. Unlike threat actors, who may employ relatively low-skill, low-wage contractors and automated bots to probe for vulnerabilities, cyber defenders are paying a premium for high-skill, hard-to-find talent. In fact, the need for both skill capacity and high-skill specialization is driving change in the cyber talent market: respondents report that 58% of their security workforce is now outsourced.

It's not just the economics working against cyber defenders. Operational complexity also presents barriers.

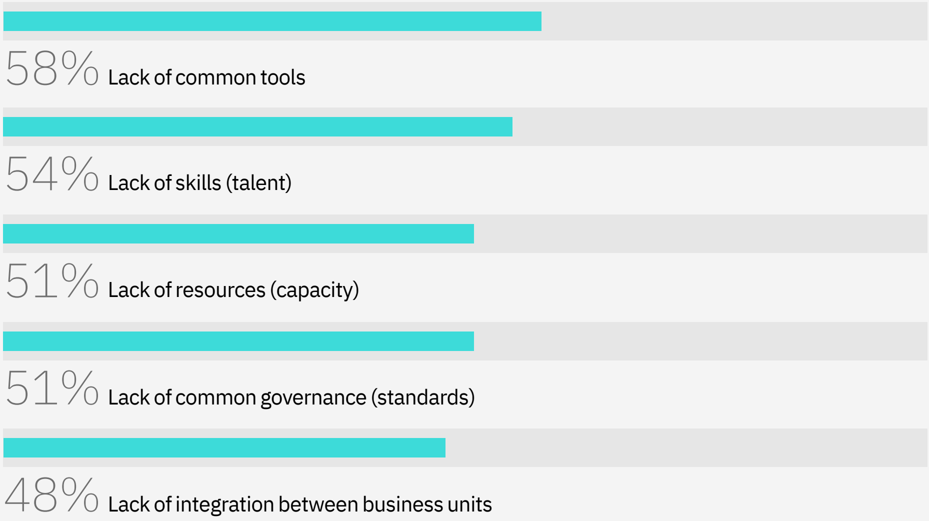
Organizations must maintain vigilance across a broad, expanding attack surface, contending with both internal and external threats, while managing relationships with stakeholders, customers, employees, partners, competitors, policymakers, and regulators. If they slip up just once, they expose themselves to significant potential liability, especially if risks compound each other in unpredictable ways or arise from hard-to-notice systemic vulnerabilities. Cyber defenders must get it right all the time. Yet, even the most capable teams are subject to the limits of time, attention, skills, capacity, and tools. Inevitably, mistakes are made.

Our research revealed that the greatest obstacles to the organization's overall cyber resilience center on coordination issues as well as capacity and skills (see Figure 2).

FIGURE 2

Operational obstacles

Integrating the necessary tools and talent across the business is critical to cyber resilience but difficult to achieve.



Q: What are the greatest obstacles to your organization's cyber resilience?

A lack of strategic alignment on security within the C-suite poses yet another challenge. Cyber strategy development appears split among CIOs (36%), CTOs (35%), and CEOs (35%). And if CIOs focus on operational goals, CTOs target technical goals, and CEOs emphasize strategic visibility, the organization may not benefit from higher value opportunities requiring coordination across business, IT, and IS teams.

The evolution of the security portfolio means IT and IS concerns are increasingly interdependent. 74% of respondents report their cybersecurity budget is part of the larger IT budget and its approval process, with only 26% indicating they maintain a standalone IS budget. Today's security operating model involves critical collaboration across functional areas—with either CIOs, CISOs, or CTOs (in that order) responsible for leading most areas of the security portfolio.

And finally, factor in the many unknowns in today's uncertain business environment. For instance, increasing support from third-party services is compounding the complexity of security operations—especially if not approached strategically. This can accentuate both systemic and transitive risks—relationship-driven risks generated by interconnections with third parties—both of which are difficult to understand, predict, or model.

Today's security operating model involves critical collaboration across functional areas—with either CIOs, CISOs, or CTOs (in that order) responsible for most areas of the security portfolio.

The complexity of administering a multidisciplinary cybersecurity program is prompting 43% of respondents to outsource full security program governance and operations to partners.

Reliance on shared infrastructure, connected services, and the proliferation of devices and machine identities means many organizations are at greater risk than they realize. Yet, we found respondents estimate the business impact to be about the same for different types of risks, indicating leaders may not have insights about the magnitude and financial consequences associated with different risk vectors. These operational blind spots are a major risk in themselves.

As a result, business leaders are often left with poor visibility into the cyber risks they do face, particularly the downstream operational and financial impacts. For many cybersecurity leaders, the critical challenge is one of capacity, both in terms of resources and decision-making. Executives are scrambling to reconcile operational and resource constraints, competing priorities, and a lack of understanding about which IS investments contribute most to business outcomes.

These uncertainties contribute to operational complexity, often resulting in the inefficient allocation of cybersecurity spend and an operations environment that is more difficult to support. Indeed, the potential complications of administering a multidisciplinary cybersecurity program are prompting 43% of respondents to outsource full security program governance and operations to suppliers.

Cyber risk management shifts security from budget line item to value enabler

Organizations are looking for ways to help them understand where and how to prioritize their security investments. One of the best options is risk quantification and related measures such as Return on Security Investment (ROSI), which supplements traditional ROI calculations with the financial benefits gained from risks avoided or mitigated. Understanding the value-at-risk measure is critical to supporting decisions across the cyber risk and cybersecurity lifecycles.

That's because the value basis for security is changing. While cybersecurity has historically been regarded as a necessary expense, it can now play a key role in spearheading strategic transformation programs—as we've seen of late with investments in cloud security and zero trust capabilities.[8] (See case study "US airline accelerates transformation by reducing cyber risks.")

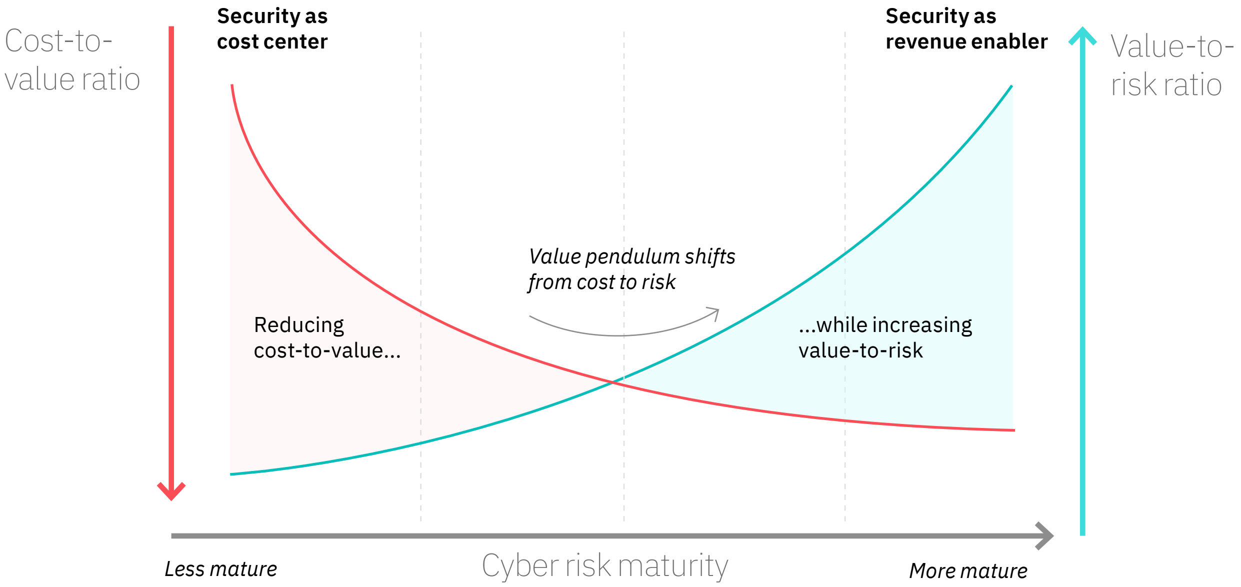
Across the C-suite, this perspective is evident. 66% of respondents view cybersecurity primarily as a revenue enabler, while 34% see it as a cost center. When adjusted for sentiment, 4 in 5 respondents indicate they perceive security as a value enabler, highlighting security's role in business and IT/IS transformation programs.

Adept leaders sense opportunity: cyber risk is often overlooked for improving operations and financial performance. If an organization can gain efficiencies, mitigate financial impacts, and avoid the loss of revenue, it has significantly improved its bottom line. In addition, an organization less susceptible to risks is more resilient and less vulnerable to disruptions that impede the execution of its long-term strategy. This enables growth and top-line improvement (see Figure 3).

FIGURE 3

Risk awareness pays off

A better understanding and avoidance of security risks power performance.


Cost-to-value ratio
Security as cost center
Security as revenue enabler
Value-to-risk ratio
Value pendulum shifts from cost to risk
Reducing cost-to-value...
...while increasing value-to-risk
Less mature
Cyber risk maturity
More mature

Case study

US airline accelerates transformation by reducing cyber risks[9]

With a broad digital transformation initiative that included migration of applications to the cloud, a US airline recognized it was facing a fundamentally different threat landscape. It needed to move aggressively to improve its cyber resilience posture, setting a goal to reduce cyber risk and develop a zero trust strategy aligned with its transformation journey.

The airline's cloud and security leadership team chose a cloud security architecture designed to deliver agility as well as a significantly more mature security posture. Initially, the team focused on micro-segmentation and a zero trust approach applied across the airline's IT environment. This was intended to prevent intruders from accessing sensitive data or posing a ransomware risk. With this enterprise-wide solution in place, the airline gained greater visibility into cyber risks and the ability to quickly isolate threats and quarantine high-risk systems in real time.

The team then turned their attention to developing a DevSecOps model to transform their application development processes. This helped increase developer awareness and enabled a more proactive approach to security.

After more than a year in production, the enterprise-wide security solution has accelerated the airline's digital transformation journey by reducing residual risks across new applications and new cloud environments. With security at the core of its transformation, the airline can move operations to cloud confidently and surpass competitors by enabling more tailored customer experiences and more efficient, cost-effective operations.

The emergence of Governance, Risk, and Compliance (GRC) programs spanning IT and IS functions is compelling evidence for the strategic benefits of cyber risk management.[10] As a complement to traditional security operations, this approach emphasizes protection and prevention activities, moving from reactive threat management to proactive risk mitigation and risk avoidance.

Many organizations seem to be heading in this direction. Respondents say cyber risk and cybersecurity responsibilities are shared across the executive ranks, mostly among CIOs, CISOs, and CTOs. Because cyber risk practices are inherently multidisciplinary, they are one of the most straightforward means of breaking down operational silos. (See case study "Insurance company aligns security and business strategies to support transformation.")

Because cyber risk practices are inherently multidisciplinary, they are one of the most straightforward means of breaking down operational silos.

61% of respondents say improving cyber resilience is an important business driver for cybersecurity investments, yet only 25% have implemented cyber risk quantification capabilities.

Yet, the desire to develop more mature cyber risk capabilities has not been matched by implementation. For example, while 61% of respondents say improving cyber resilience is one of the most important business drivers for their cybersecurity investments, 54% indicate their security controls are either not aligned or only partially aligned with their organization's risk posture. Perhaps most revealing: only 25% of respondents are implementing, operating, or optimizing cyber risk quantification capabilities.

Developing advanced cyber risk capabilities is one of the most promising areas for rapidly improving the organization's overall security posture. As we'll explore in the next section, organizations proficient in cyber risk management—along with the more forward-looking ecosystem attunement—are realizing higher levels of financial and operational efficiency, performance, and resilience.

Case study

Insurance company aligns security and business strategies to support transformation[11]

In pursuit of a long-term growth agenda, a property and casualty insurance company needed to refine its cybersecurity strategy by incorporating forward-looking cyber resilience capabilities. This required a holistic assessment of how industry trends and emerging technologies were impacting its business, technology, and security capabilities. The outcomes enabled the insurer to define a new path forward, anchored on cyber resilience, innovation, people, and customers.

Following a series of capability-focused workshops to define the “art of the possible” with cross-functional teams at all levels, the company developed a zero trust reference architecture to guide the design and deployment of least-privilege access policies. This had the operational benefit of informing technology decisions for establishing restricted, segmented access across the network environment.

After several months, leaders concluded the solution had delivered the necessary strategic business alignment across both security and technology portfolios. They can be more confident that the company’s security strategy will continue to support its digital transformation journey for the foreseeable future. The company also boosted its overall cyber resiliency by improving its ability to respond to emergent threats. Additionally, it could use insights from the transformation effort to build stronger business cases for future cybersecurity investments.

> *"Security spending is tied into our customers' desires to move to the cloud, drive more direct relationship with their customers, and modernize their IT infrastructure, as well as drive efficiencies while adapting to a new way of working."*[12]

Nikesh Arora, CEO, Palo Alto Networks

Attuning security capabilities for value realization

Our findings suggest there is no single way to go about security transformation. To better understand how different organizations approach their security evolution, we looked at how security capabilities are impacting business outcomes.

First, we assessed respondent organizations' security maturity in five areas. To attain maturity in an area requires specific actions and capabilities, which build on each other to yield more value (see Figure 4).

FIGURE 4

Rethinking security through a value lens

Modern security capabilities build upon each other to enable broader enterprise and ecosystem-level value propositions.

1

Strategy and cyber risk

Execute on security strategy and ensure controls are aligned with risk posture

2

Functional maturity

Modernize and coordinate delivery of core security capabilities in areas such as cloud security, DevSecOps, and security architecture

3

Security operating model

Design, build, and orchestrate technology, processes, skills, and governance across the security function

4

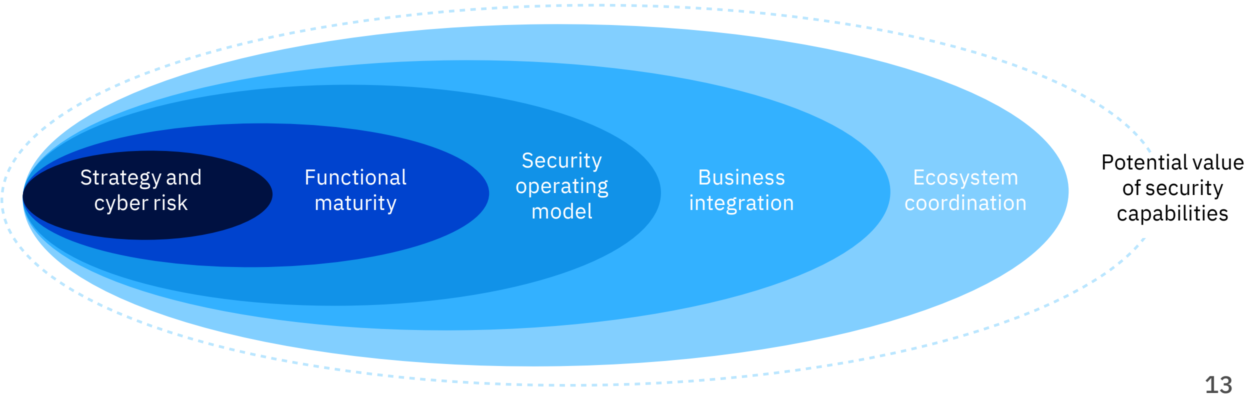
Business integration

Strategically extend security capabilities across core business functions

5

Ecosystem coordination

Engage ecosystem partners in design and delivery of security capabilities and new value propositions



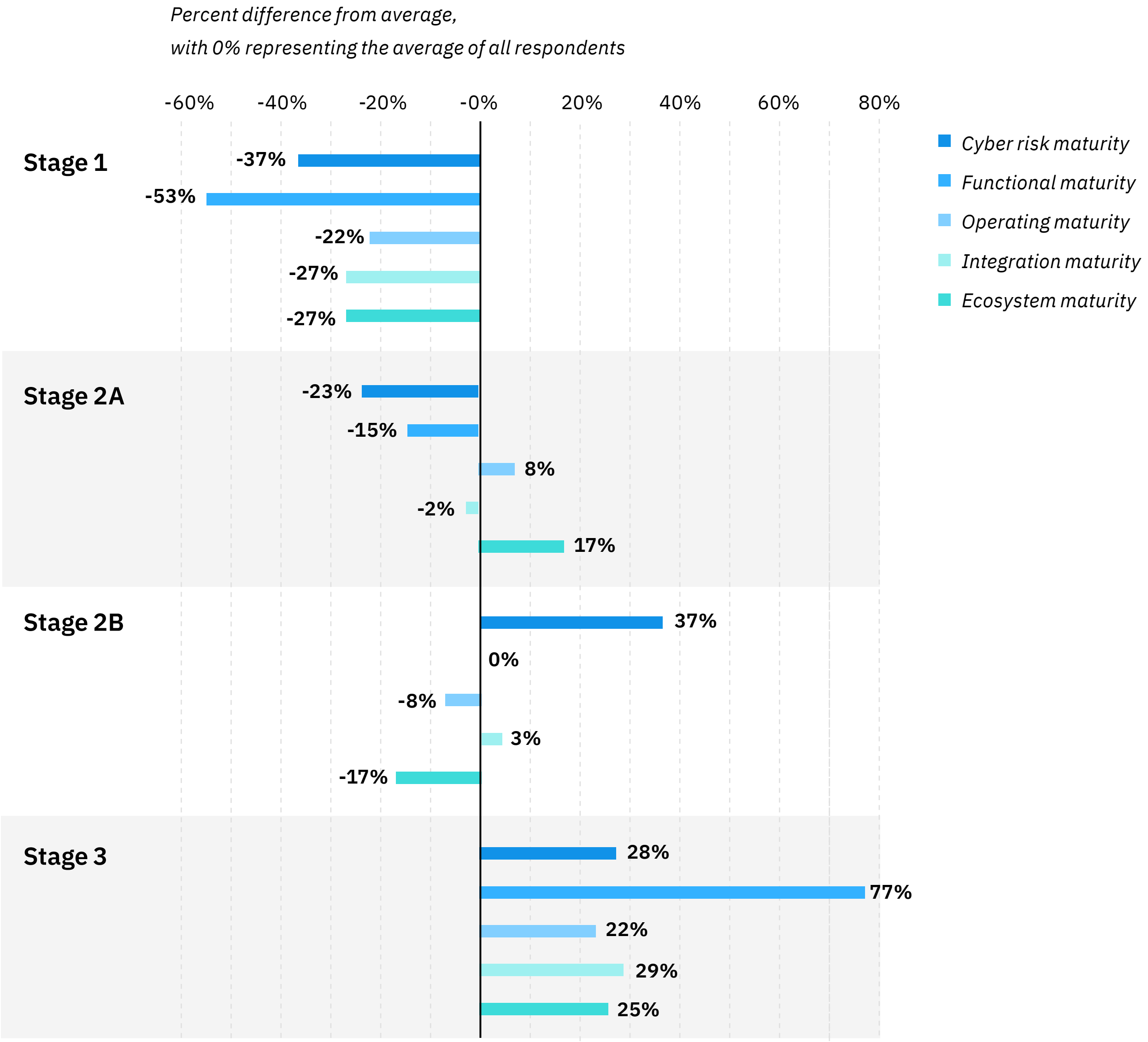
Our analysis revealed that organizations fall into different stages of security maturity, from least mature (Stage 1) to moderately mature (Stages 2A and 2B) to more mature (Stage 3; see Figure 5). When comparing the Stage 1 and Stage 3 organizations, the differences are stark:

– Stage 1 organizations are typically smaller (based on revenue) with less complex environments, are less mature in terms of technology and operations, and have made the least progress on implementing new security capabilities.

FIGURE 5

Stages of security maturity

Respondents are at different points based on their advancements in these areas.



Based on IBV analysis.

- Stage 3 organizations are larger, have adopted emerging technologies such as cloud and AI, and embed security across the enterprise and out into their ecosystems.
- Only 1 in 3 of the lower maturity organizations view their security function as a revenue enabler compared to 9 in 10 among executives in the higher maturity organizations.
- Only 22% of executives in Stage 1 organizations indicate that cybersecurity is contributing positively to ecosystem integration compared to 52% among Stage 3.

We also found the journey from lower to higher security maturity is not the same for all organizations. As shown by the Stage 2A and 2B groups, the path to maturity depends on how they prioritize capabilities in certain areas (see Figure 6).

Stage 2A organizations are transitioning from strategy to capabilities by focusing on both the security operating model and ecosystem coordination areas. As they develop a more sophisticated security operating model, they are relying on partners for specialized skills and capabilities.

When enabled as part of a modern security strategy, extending security capabilities into the ecosystem can be an equalizer in the battle against cybercrime, rather than only a source of greater vulnerability and risk. By allowing partners to share risks and responsibilities, these organizations are developing a more sophisticated security posture through practices such as information sharing, collective defense, and defense-in-depth.[13]

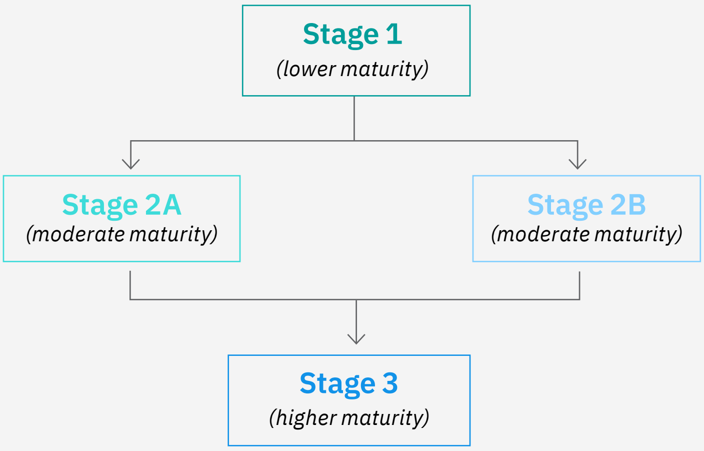
In contrast, Stage 2B organizations are concentrating on understanding their cyber risk and aligning that to their cyber strategy. This is paying off in terms of a lower ratio of security breaches to security incidents, suggesting greater efficiency in their security operations. Stage 2B organizations are also making strides toward integrating security into the wider enterprise.

To progress to the higher security capabilities of Stage 3, Stage 2A and 2B organizations need to broaden their focus and extend their capabilities in other maturity areas. Both groups indicate they see the potential of security to generate opportunities—with 59% of Stage 2A and 83% of Stage 2B executives viewing security as a revenue enabler.

FIGURE 6

Security transformation paths

The fork in the road is defined by how an organization's business and security strategies influence operational priorities.



Stage 1
- Limited use of major new security capabilities
- Limited technological maturity
- Significant blind spots for risk
- 33% see security as a revenue enabler

Stage2A
- Prioritizes security coordination with partners
- Advanced security operating model
- Limited alignment of security posture with cyber risk
- 59% see security as a revenue enabler

Stage 2B
- Prioritizes alignment of security posture with cyber risk
- Limited security coordination with partners
- Immature security operating model
- 83% see security as a revenue enabler

Stage 3
- Security embedded across the enterprise
- Security strategy aligned with business strategy
- Strong security governance processes
- 90% see security as a revenue enabler

The reward: Security boosts business performance and transformation

The cumulative effects of security transformation are evident in the Stage 3 group. They—more than any other group—are converting their advanced security capabilities into significantly better business performance, as measured by financial factors such as growth and profitability.

Over a five-year period, organizations in Stage 3 report a 43% higher average revenue growth rate compared to those in Stage 1. They also experience higher profitability, measured by operating margins (see Figure 7).

While organizations in Stages 2A and 2B have focused on different areas in building their security capabilities, they are seeing comparable business performance. This reinforces that the most appropriate steps taken toward Stage 3 depend on the circumstances of the organization, namely how business and security strategies influence operational priorities.

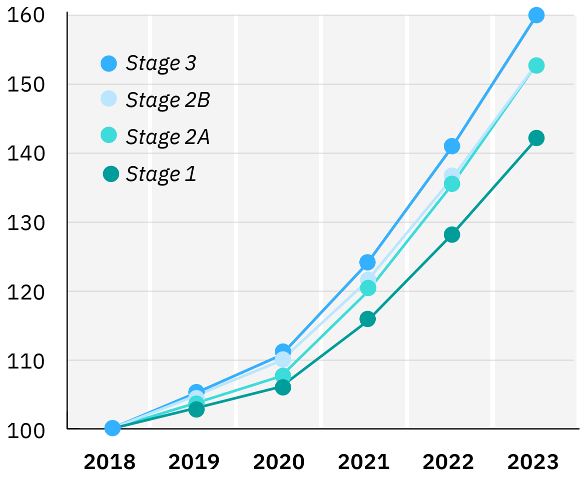
Figure 7

Security maturity fuels growth

Stage 3 organizations have experienced a higher revenue growth rate (43% over 5 years) and higher profitability (41% higher in 2021) than those in Stage 1.

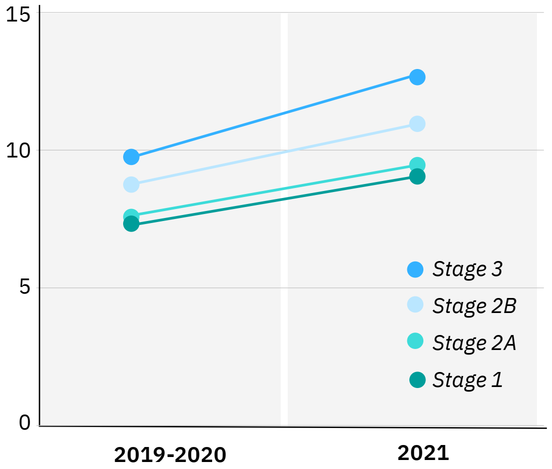
Cumulative revenue by stage

Percentage revenue growth (Index 2018 = 100)



Annual average operating margin by stage

Operating margin as a percent of revenue



Based on IBV analysis.

When looking at other performance factors, organizations in Stage 3 are far more likely to outperform their peers in key areas such as agility, innovation, data management, and talent development—all areas of critical importance for transformation. These organizations are converting their security capabilities into tangible benefits that range from greater IT resilience inside the organization to far-reaching impacts such as ecosystem engagement and open innovation with partners outside the organization (see Figure 8).

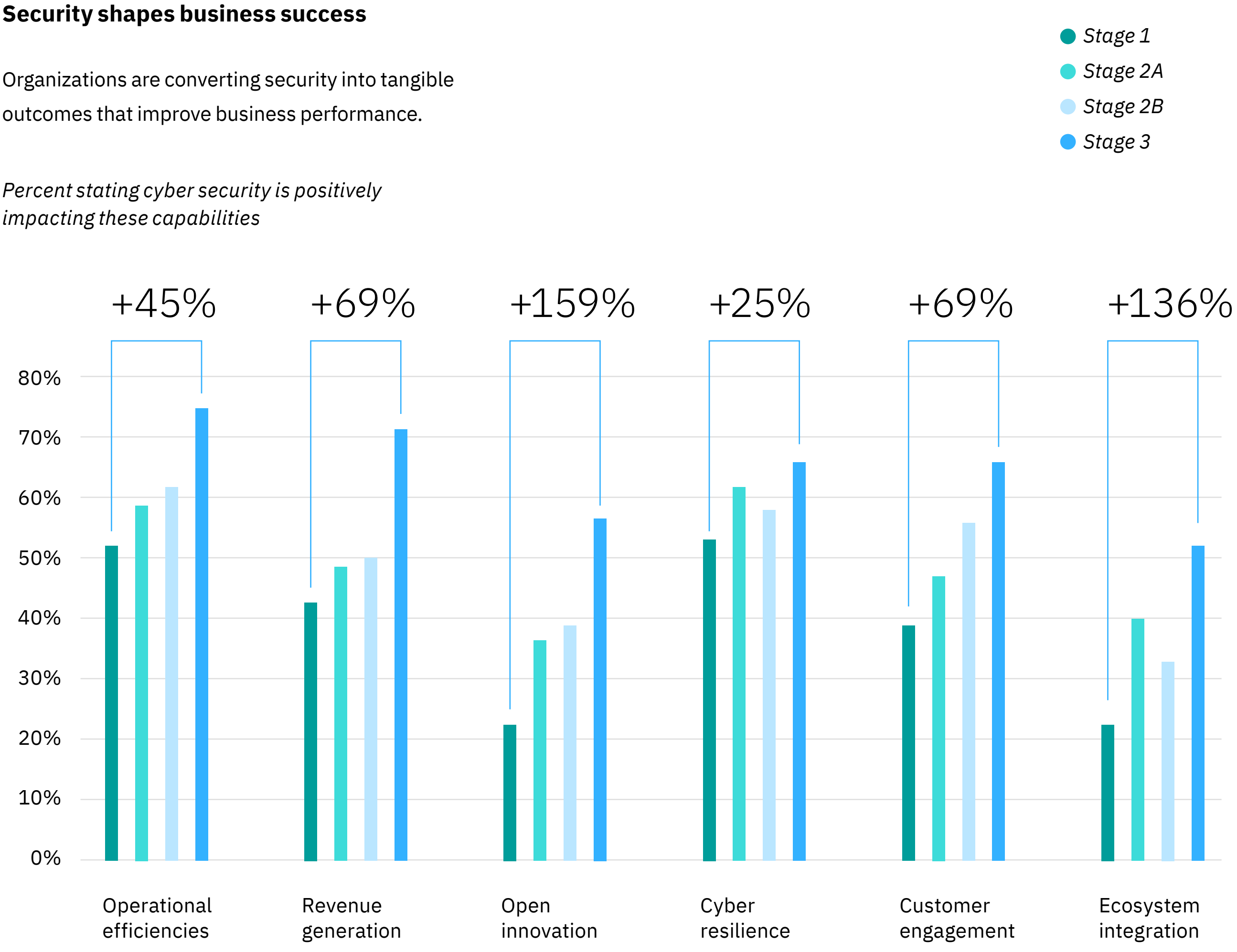
Stage 3 organizations are more likely to outperform peers in key transformation areas, such as agility, innovation, data management, and talent development.

Figure 8

Security shapes business success

Organizations are converting security into tangible outcomes that improve business performance.

Percent stating cyber security is positively impacting these capabilities



For ROSI—the financial measure identified by respondents as most important when evaluating potential security investments—organizations report a healthy return. Across all respondents, the average ROI reported is 184% while the average ROSI is 292%. Perhaps unexpectedly, organizations in Stage 1 report a higher ROSI than those in Stage 3. This is likely a case of diminishing marginal returns. In other words, the higher the investments required to cover larger, more complex operations, the lower the overall ROSI. In comparison, smaller organizations that have not yet made significant security investments often benefit from higher ROSI given the relative abundance of investment opportunities in the form of "low-hanging fruit."

While the most mature organizations are demonstrating how security investments become revenue enablers, Stage 3 should not be considered the end of the journey. To continue adapting to dynamic security demands, leaders must look inside and across their organization for new ways to extend the value of security services, as well as to external partners and suppliers in the extended ecosystem. This is where they can find opportunities to address new risk vectors, develop a more comprehensive shared responsibility model, and use open innovation to enable emergent value propositions.

"Adding security should be a business enabler. It should be something that adds to your business resiliency, and it should be something that helps protect the productivity gains of digital transformation."[14]

George Kurtz, CrowdStrike, CEO

Unlocking greater value by sharing risk, responsibility, and resilience

In the parlance of economics, shared resilience has the characteristics of a public good—a common resource that promotes the general welfare of all participants in the cyber economy.

The shift toward shared responsibility signifies a remarkable evolution in security strategy, one that is increasingly evident as organizations move from perceiving security as a cost center to security as a value enabler. The question is: how do you convert shared responsibility into business outcomes?

This evolution begins internally as more effective working partnerships are developed across the C-suite and with line-of-business leaders. Breaking down functional silos is essential to understanding cyber risks and articulating a consolidated business, IT, and IS strategy. Doing so empowers these executives to elevate security operations to the next level.

Taking shared responsibility even further involves engaging multilaterally with ecosystem partners whose strategy, approach to risk, and ability to execute are complementary. This facilitates both specialization and the ability to capitalize on shared investments (for example, hyperscale infrastructure and services). This, in turn, allows organizations to realize a combined value more significant than what they can achieve on their own. (See case study "Life sciences manufacturer positions security as a business enabler" on page 21.)

Stage 3 respondents demonstrate how the most mature organizations are extending capabilities beyond the shared responsibility model, evolving toward a security framework that combines the benefits of shared value and shared resilience (see Figure 9). For these organizations, partners are using standardization and common governance to advance their mutual interests. This includes supporting mutual communities of interest, knowledge, or practice as well as standardizing incident response procedures and security policies across partner operations.

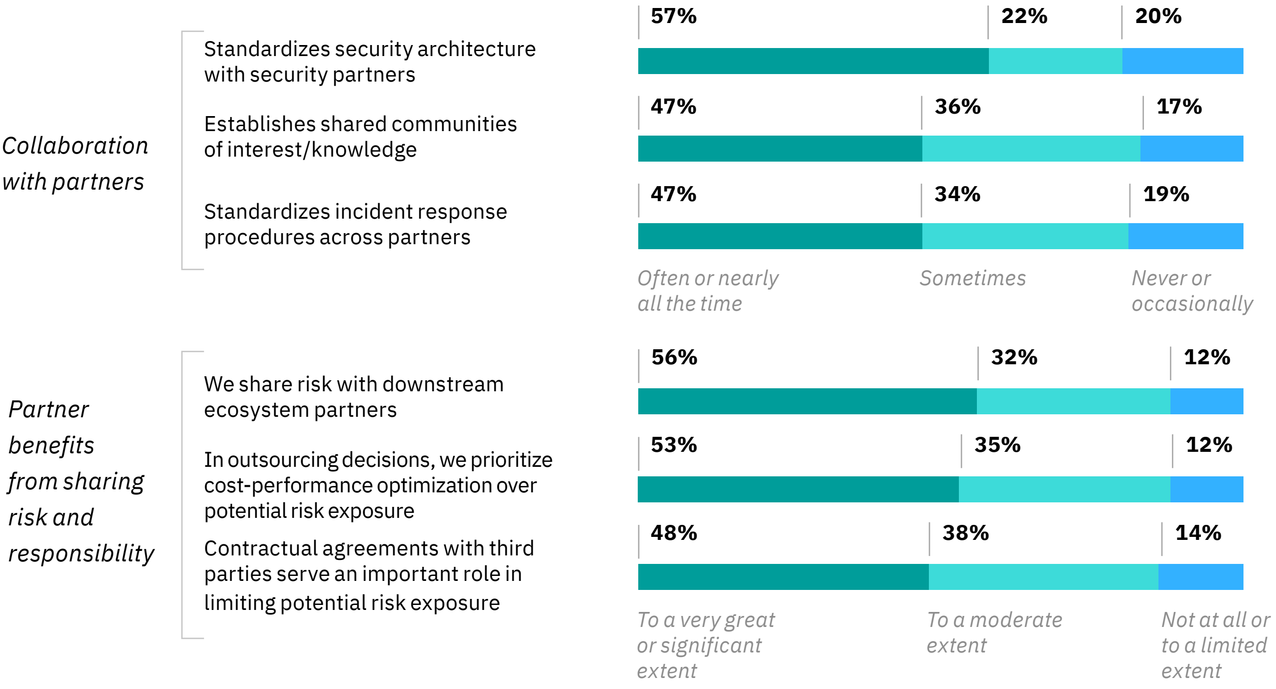
For many organizations, shared value is generated through greater collaboration and greater operational integration. 56% of respondents cite sharing risks with their downstream business partners as the most common benefit. Other gains involve limiting risk exposure through methods such as contractual agreements. But respondents are also prioritizing cost-performance considerations over potential risk exposure when choosing their ecosystem partners. This suggests that transitive risk may become more of an issue as ecosystem relationships grow more complex.

> *Many organizations are generating shared value through greater collaboration and operational integration with partners.*

Figure 9

Extending security into the ecosystem

Organizations are collaborating more often with partners, sharing risk and responsibility and ultimately value.



Q: How does your organization work with partners to implement a shared responsibility/shared accountability cybersecurity model?
Q: To what degree are your ecosystem partners benefiting from your cybersecurity investments and capabilities?

Case study

Life sciences manufacturer positions security as a business enabler[15]

Faced with cost pressures across non-core functions and skill shortages across its IT and IS portfolio, a life sciences manufacturing company decided to outsource IT operations. To help ensure separation of duties between the client's IT provider and IT security functions, the company chose to supplement IT services with a managed security services provider (MSSP) that could successfully integrate with other partners across the organization's ecosystem. Through integrated operations and shared governance, multiple parties across the ecosystem could realize operational benefits.

The solution began with an aggressive transition plan and associated transformation roadmap designed to steadily mature the company's security capabilities. It included an open platform that provides 24x7 threat management capabilities, enabled by an accelerated transition to new IT and IS service providers. The company established a common governance model to provide continuous alignment across multiple strategic partners.

Now with consolidated security operations and increased security maturity, the company has gained improved management of cyber risk as well as more efficient threat management. Application of a streamlined transition methodology enabled the company to accelerate cost savings and time to value. Through this transformation, the life sciences company has repositioned security as a business enabler.

Most notably, Stage 3 organizations are succeeding in shifting their security approach from value-at-risk to value-to-risk by working horizontally within their organization and collaborating with partners to share risk, enable new value propositions, and coordinate operations. As measured by factors such as the ratio of breaches to incidents, these organizations are working with partners to enhance their collective cyber resilience (see Figure 10). When compared to their peers, these organizations stand out in one crucial way: they position security as a critical component of their overall transformation programs.

What makes these organizations better at security is what makes them better at converting opportunities to growth. They possess more mature capabilities in cyber risk and ecosystem partner coordination as well as greater efficiency, speed, specialization, and scale—all the attributes of a more open—and more resilient—organization.

Stage 3 organizations are prospering because they position security as a critical component of their overall transformation program.

For the more mature organizations, security outcomes are viewed as business outcomes.

This change in strategy depends on how an organization approaches its cloud transformation. The key difference is that security outcomes are viewed as business outcomes.[16] The organization moves from an initial focus on connected services and shared operations to a "deep cloud" approach, which concentrates on driving greater business performance by prioritizing business-critical value streams. By changing their perspective to risk, value, and resilience, leaders can better address the myriad challenges and uncertainties that complicate the security operations environment. This enables them to prioritize investments that generate the greatest operational and financial benefits.

Given an increasingly unpredictable business environment, the emergence of the cyber economy as the *de facto* economy represents a watershed moment with longstanding repercussions over the decade to come. Those that embrace this new paradigm are better positioned to capitalize on these opportunities. The accompanying action guide provides additional guidance for how to get started.

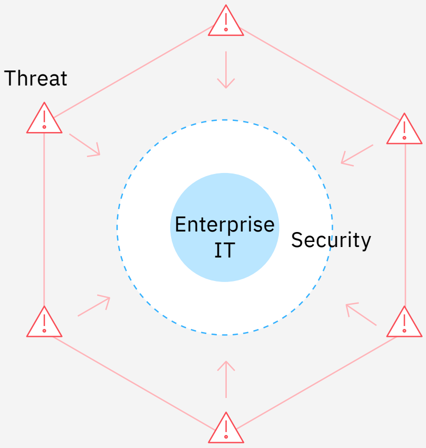
Figure 10

Security for the public good

Ecosystem partnerships based on shared responsibility, shared resilience, and shared value are transforming security operations.

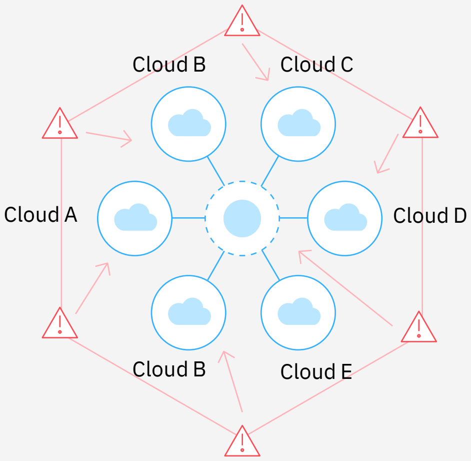
Traditional security (pre-cloud era)

- Enterprise builds own defense against cyber attackers
- Emphasis on security perimeter
- High cost, low effectiveness
- Limits collaboration



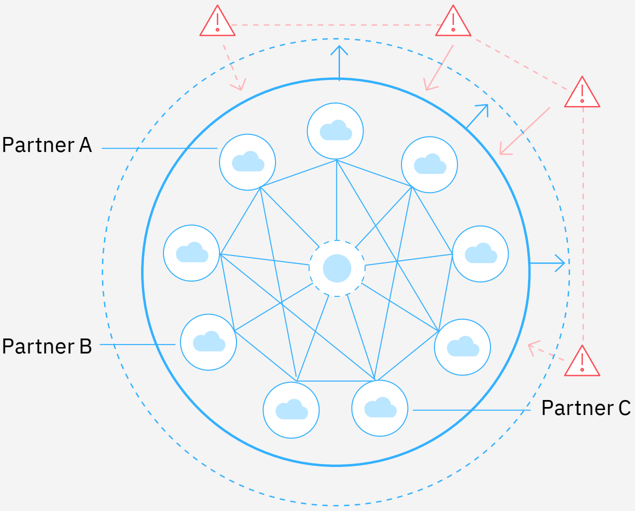
Shared responsibility (shallow cloud era)

- Some IT moves to different clouds, each with own security posture (stronger than enterprise IT)
- Bilateral security coordination
- Higher efficiency, improved security posture
- Bilateral approach and “lock-in” impede transformational value



Shared resilience (deep cloud era)

- Multilateral coordination among ecosystem partners
- Strong collective security posture proactively reduces attackers’ capabilities
- Security as shared public good
- Reduces risk; enables openness, value creation, and transformation



Action guide

General recommendations for all stages

1\.

Build consensus around strategies

- Make a holistic assessment of your current security transformation roadmap in relation to your organization's business, IT, risk appetite, and security strategies.
- Work with peers to better understand your organization's approach to cyber risk management.
- Focusing on shared responsibility and shared accountability, work with peers to understand where to rely on partners to share or transfer risk.
- With an emphasis on shared value, consider where your organization should work with partners to achieve greater economies of scale, or where you can prioritize investments to achieve greater specialization and differentiation.

2\.

Break down silos

- Think horizontally to enhance decision flow across your organization by emphasizing security maturity along the five capability dimensions: strategy and cyber risk, functional capabilities, security operating model, business integration, and ecosystem coordination.
- Use value stream assessments to determine which parts of the IT and IS portfolio contribute the most value to your broader transformation efforts.
- Working with peers across the IT/IS portfolio, estimate the common value pool from aligning business, IT, and IS investments.
- Qualify and quantify the investments required to achieve desired business outcomes based on your business strategy, IT/IS strategy, and risk posture.

3\.

Share governance—and value—with ecosystem partners

- Engage internal partners to remove functional silos, improve efficiency, and refine the strategy to achieve common objectives. Look at security as a horizontal capability across the enterprise rather than a business vertical.
- Engage external ecosystem partners in open innovation, align your approach to cyber risk management, and foster opportunities to work together to achieve strategic objectives. Focus on the principles of collective defense, cyber resilience, and defense-in-depth.

Action guide

Stage-specific recommendations

Stage 1

Refine your strategy

- Work across your organization to develop a transformation roadmap based on shifting security operations from a cost center to a revenue enabler.
- Capitalize on abundant opportunities for high ROI and high ROSI investments to enhance cyber risk and cybersecurity capabilities, and broader IT/IS transformation.

Stage 2A

Understand risks and rewards

- Prioritize improvements to your cyber risk management maturity.
- Continue enhancements to the operating model and ecosystem partner maturity while deepening business integration and functional maturity.

Stage 2B

Extend efforts into your ecosystem

- Take advantage of the improvements in business outcomes from cyber risk management (for example, reduction in financial risk exposure and decreased likelihood of adverse events).
- Focus on enhancing your business integration and ecosystem partner efforts to achieve better efficiency and economies of scale.

Stage 3

Develop capabilities to capitalize on new opportunities

- Re-assess your security strategy based on internal versus external factors, the organization's changing risk profile, and how business and IT/IS factors create new challenges and opportunities.
- Recognize that your organization can still benefit from improvements in capability maturity and identify which capabilities can generate the greatest impact.

About
the authors

Chris McCurdy

Worldwide Vice President
and General Manager,
IBM Security Services
linkedin.com/in/chrismmccurdy/
cmccurdy@us.ibm.com

For more than 15 years, Chris has held multiple leadership positions directing sales and strategy for IBM Security Services, consistently driving rapid growth of the security business. Before joining the company, he was a managing consultant at several consulting firms including Andersen, International Network Services, and Lucent Technologies. He was also CIO at a large US retail automotive group. Chris holds a BBA in Information Systems from Baylor University and is a Certified Information Systems Auditor.

Shlomi Kramer

Global Partner, IBM Security Services
linkedin.com/in/shlomi-k/
SHLOMIK@il.ibm.com

Shlomi has more than 20 years of professional experience in infrastructure and security service. He has worked internationally across various industries, collaborating with clients to simplify complex business and technology issues linked to secure digital transformation. Over the years, he has served in business leadership roles working with clients and an international network of business executives to develop and execute sales transformation programs that helped address their digital transformation agendas.

Gerald Parham

Global Research Leader,
Security and CIO
IBM Institute for Business Value
linkedin.com/in/gerryparham/
gparham@us.ibm.com

Gerald leads the security and CIO research areas within the IBM Institute for Business Value. He advises senior executives and board members on technology and security strategy, cyber risk, and cyber value chains. Gerald has more than 20 years of experience in executive leadership, innovation, and intellectual property development. He holds advanced degrees in science and fine arts from the California State University and the University of Southern California, as well as a BA in writing from Johns Hopkins University.

Jacob Dencik, PhD

Global Economic Research Leader
IBM Institute for Business Value
linkedin.com/in/jacob-dencik-126861
jacob.dencik@be.ibm.com

Jacob is responsible for leading IBV's research on topics related to technology and implications for the global economy. He has extensive experience advising companies around the world on their global operations and location strategies. He also has advised governments globally as an expert and economist on competitiveness, foreign direct investment (FDI), sector/cluster analysis, and innovation. Jacob holds a PhD in public policy and economics from Bath University in the United Kingdom.

Acknowledgments

We would like to thank many colleagues for their efforts, guidance, and support of this research. From the IBV, we would like to single out Joanna Wilkins, Lily Patel, and Kristin Biron. We would also like to express our gratitude to Dave Zaharchuk, Haynes Cooney, Kathleen Martin, Steve Ballou, Jana Chan, and many other folks who helped with editorial reviews, study deployment, and activation. From IBM Security, we would like to extend our thanks to Tanner Sandoval and Danielle Ivannikova. In addition, stakeholders across the IBM Security community have contributed their guidance and expertise at many stages long the way. We deeply value our partnership with you.

About Research Insights

Research Insights are fact-based strategic insights for business executives on critical public- and private-sector issues. They are based on findings from analysis of our own primary research studies. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Related reports

AI and automation for cybersecurity

Muppidi, Sridhar, Lisa Fisher, and Gerald Parham. "AI and automation for cybersecurity: How leaders succeed by uniting technology and talent." IBM Institute for Business Value. June 2022. https://ibm.co/ai-cybersecurity

The new era of cloud security

Thompson, Shue-Jane, Shamla Naidoo, Shawn Dsouza, and Gerald Parham. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. April 2021. https://ibm.co/cloud-security-cyber-resilience

Unlock the business value of hybrid cloud

Payraudeau, Jean-Stéphane, Anthony Marshall, and Jacob Dencik. "Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation." IBM Institute for Business Value. July 2021. https://ibm.co/hybrid-cloud-business-value

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at https://ibm.co/ibv-linkedin.

Study approach and methodology

To better understand enterprise perceptions of cyber risk and cybersecurity, the IBM Institute for Business Value partnered with Oxford Economics to interview more than 2,300 business, operations, technology, cyber risk, and cybersecurity executives across 18 industries and 25 countries.

This research presents a comprehensive analysis of insights from leaders responsible for driving their organization's IT and information security (IS) transformation agenda, including CEOs, COOs, CIOs, CTOs, CISOs, Chief Risk Officers (CROs), Chief Supply Chain Officers, Chief Procurement Officers, Chief Privacy Officers (CPO) or Data Protection Officers (DPO), as well as senior executives (VP or above) within the information security (IS) function, cyber risk management function, and information technology (IT) function.

Our analysis focused on how security capabilities are impacting security operations and business outcomes. This included descriptive analysis of the data as well as a more detailed analysis assessing organizations' security maturity in five areas:

- Strategy and cyber risk. How they execute on security strategy and ensure controls are aligned with risk posture
- Functional maturity. How they modernize and coordinate delivery of core security capabilities in areas such as cloud security and security architecture principles
- Security operating model. How they design, build, and orchestrate technology, processes, skills, and governance across the security function rating model maturity
- Business integration. How they strategically extend security capabilities across core business functions
- Ecosystem coordination. How they engage ecosystem partners in design and delivery of security capabilities and new value propositions.

We then performed a cluster analysis that grouped organizations into four distinct clusters based on their capabilities in each of the five areas. A comparative analysis of the different clusters on their approach to security, the impact of security on business performance, as well as their overall financial performance allowed us to ascertain the role of security maturity in delivering business value.

Notes and sources

1 "Cyber Operations and Cyber Terrorism." US Army Training and Doctrine Command. DCSINT Handbook No 1.02. August 2005. https://nsarchive.gwu.edu/document/15676-us-army-training-and-doctrine-command-dcsint

2 Morgan, Steve. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Cybercrime Magazine. November 2020. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; Upadhyay, Shailendra, Rahul Yadav, et al. "Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 2Q2022 Update. https://www.gartner.com/document/4016190?ref=algobottom-rec&refval=4004647 (Access required.)

3 Payraudeau, Jean-Stéphane, Anthony Marshall, and Jacob Dencik. "Unlock the business value of hybrid cloud: How the Virtual Enterprise drives revenue growth and innovation." IBM Institute for Business Value. July 2021. https://ibm.co/hybrid-cloud-business-value

4 "Cybersecurity is the issue of the decade: IBM chair & CEO Arvind Krishna." CNBC. August 25, 2021. https://www.cnbc.com/video/2021/08/25/cybersecurity-is-the-issue-of-the-decade-ibm-chair-ceo-arvind-krishna.html

5 "2022 IBM CEO Study. Own your impact: Practical pathways to transformational sustainability." IBM Institute for Business Value. May 2022. https://ibm.co/c-suite-study-ceo

6 "Cost of a Data Breach Report 2022." IBM Security and the Ponemon Institute. July 2022. https://ibm.com/security/data-breach

7 Ibid.

8 McCurdy, Chris, Shue-Jane Thompson, Lisa Fisher, and Gerald Parham. "Getting started with zero trust security: A guide for building cyber resilience." IBM Institute for Business Value. July 2021. https://ibm.co/zero-trust-security; Thompson, Dr. Shue-Jane, Shamla Naidoo, Shawn Dsouza, and Gerald Parham. "The new era of cloud security: Use trust networks to strengthen cyber resilience." IBM Institute for Business Value. April 2021. https://ibm.co/cloud-security-cyber-resilience

[9] Based on internal IBM client information.

[10] IBM Cloud Education. “GRC.” Accessed September 27, 2022. https://www.ibm.com/cloud/learn/grc

[11] Based on internal IBM client information.

[12] Novet, Jordon. “Why cybersecurity stocks are beating the market.” CNBC. September 1, 2022. https://www.cnbc.com/2022/09/01/cybersecurity-stocks-are-beating-the-market-in-a-volatile-economy.html

[13] Definition “defense-in-depth.” National Institute for Standards and Technology Computer Security Resource Center. Accessed September 23, 2022. https://csrc.nist.gov/glossary/term/defense_in_depth

[14] Columbus, Louis. “CrowdStrike’s platform plan at Fal.Con melds security and observability.” VentureBeat. September 26, 2022. https://venturebeat.com/security/crowdstrikes-platform-plan-at-fal-con-melds-security-and-observability/

[15] Based on internal IBM client information.

[16] “The deep cloud alternative: Getting to the heart of business performance.” IBM Institute for Business Value. August 2022. https://ibm.co/deep-cloud

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | November 2022

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.