Gartner Research

CISO Edge: 12 Ways to Deliver Cybersecurity Business Value Faster

Richard Addiscott, Tom Scholtz, Christopher Mixter, Tisha Bhambry, Manuel Acosta

15 December 2023

CISO Edge: 12 Ways to Deliver Cybersecurity Business Value Faster

Published 15 December 2023 - ID G00797520 - 18 min read

By Analyst(s): Richard Addiscott, Tom Scholtz, Christopher Mixter, Tisha Bhambry, Manuel Acosta

Initiatives: Cybersecurity Leadership; Build and Optimize Cybersecurity Programs

> Challenging global economic conditions are driving enterprises to accelerate their digital business transformations. Cybersecurity leaders must also accelerate their efforts and demonstrate security's critical role in their organizations' digital ambitions.

Overview

Key Findings

- Boards are responding to ever-greater market uncertainty by raising the pressure on executive teams to accelerate digital business transformation and spur growth. An agile and responsive cybersecurity function enables that growth securely and helps it foster a sustained competitive advantage against those taking more conservative approaches.
- C-level leaders increasingly shift digital budget allocations from central IT functions to business units to accommodate their digital ambitions. This is a move supported by the majority of chief information officers and can increase the number of stakeholders the chief information security officer (CISO) and security team need to work with and satisfy.
- Boards and senior executives need cybersecurity leaders to adapt their security capabilities to support and amplify the business' efforts as their organizations continue to evolve.
- Cybersecurity leaders find it challenging to prioritize and invest in security practices in sustainable ways as business demand increases.

Recommendations

Cybersecurity leaders working to accelerate their security capabilities' ability to adapt to support the organization's increased digital business progress should:

- Shift the team's mindset by asking them to recite the business strategy, showing how their work aligns to it and quoting performance highlights from the annual report.

- Improve stakeholder relationships and amplify security messaging by aligning security initiatives to business priorities and establishing a security champions program.

- Reduce inefficiency and waste by retiring security controls that impact the user experience but have negligible impact on reducing cybersecurity risks.

- Redirect resources and optimize limited security resources by testing robotic process automation and canceling redundant security initiatives.

Introduction

Gartner research shows that 58% of boards of directors expect to increase their risk appetite in between 2024 and 2025, and 58% see digital technology initiatives among their top five business priorities for the next two years. [1] Further, 90% of CIOs say that business area leaders should be responsible for leading digital transformation initiatives. [2]

The shifts in digital decision-making power structures will change the cybersecurity leader's operating context. However, this evolving landscape is further complicated because stakeholder confidence in the cybersecurity leader's ability to support these initiatives as a trusted partner is not assured. Gartner research shows that 47% of CIOs see cybersecurity risk mitigation processes as a hindrance to digital execution. [3]

Beyond the board's increasing risk appetite and wavering confidence levels, other imperatives are driving the need for the cybersecurity leader to accelerate the cybersecurity program:

- **Decentralized digital decision making**, often by people without adequate levels of cybersecurity literacy or risk management experience.

- **Increasing regulatory pressure** on boards of directors to ensure the organization's cybersecurity risk posture is appropriate. This is forcing boards of directors to be increasingly exposed to, and have oversight of, the organization's cybersecurity risk posture and the requirement for them to become more cyber-literate (see Quick Answer: New SEC Cybersecurity Rules — What CISOs Should and Shouldn't Do).

The challenge is that cybersecurity leaders are already struggling to keep up with existing demand. Finding the capacity to deliver more project volume, at a faster pace, with greater flexibility and customization — all without more people or resources — is an impossible endeavor. As a result, cybersecurity leaders often struggle to enable the business and maintain executive confidence.

How do cybersecurity leaders continue to ensure their security capabilities are able to keep pace with the business as digital business leaders continue to accelerate their digital initiatives in pursuit of growth? Further, how do they achieve this when most cybersecurity leaders are already stressed and at increased risk of burnout? [4]

To help deliver business outcomes without burning out, cybersecurity leaders must identify, and then execute, initiatives as appropriate for their organizations. They should help drive security agility and responsiveness as digital business continues to accelerate to help them and their team:

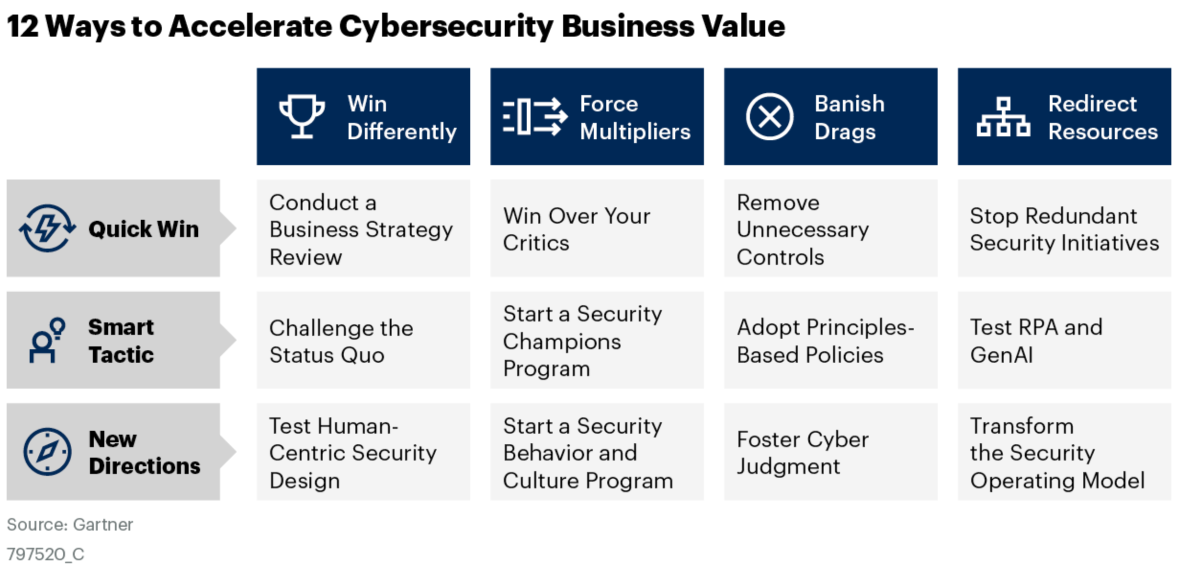
- Win differently
- Unleash force multipliers
- Banish drags
- Redirect resources

Figure 1 shows 12 cybersecurity accelerators that cybersecurity leaders can use to help sustain the pace of their cybersecurity efforts as:

- **A quick win:** Something that can be done in a short space of time with minimal effort to help gain momentum
- **Smart tactics:** Actions cybersecurity leaders can adopt or add to their current approach to gain and sustain momentum
- **New directions:** Potentially new and emerging actions cybersecurity leaders can take that will have a more significant impact over time

Cybersecurity accelerators are leadership tactics to establish and sustain a more agile, responsive and faster cybersecurity capability.

Figure 1: 12 Ways to Accelerate Cybersecurity Business Value



12 Ways to Accelerate Cybersecurity Business Value

	Win Differently	Force Multipliers	Banish Drags	Redirect Resources
Quick Win	Conduct a Business Strategy Review	Win Over Your Critics	Remove Unnecessary Controls	Stop Redundant Security Initiatives
Smart Tactic	Challenge the Status Quo	Start a Security Champions Program	Adopt Principles-Based Policies	Test RPA and GenAI
New Directions	Test Human-Centric Security Design	Start a Security Behavior and Culture Program	Foster Cyber Judgment	Transform the Security Operating Model

Source: Gartner
797520_C

There is no expectation that all the ideas provided in this research are fit for purpose for all organizations. Rather, they are provided for consideration based on each cybersecurity leader's unique operational context. The intent is to provide cybersecurity leaders with a range of actions to ensure the security function supports and enhances the organization's ability to drive its digital agenda at a quicker pace.

> As part of Gartner's CISO Edge series, this research draws on our dealings with a small community of thought leader clients and experts, providing innovative guidance for CISOs driving transformative cybersecurity programs. It offers key suggestions for innovative approaches.

Analysis

Win Differently: Foster Increased Speed and Agility

Sometimes you need to go slowly to go fast. Cybersecurity leaders should pause, take stock of the evolving environment, assess the new risk appetite and engage effectively with business stakeholders to identify where their organization is now and where it plans to go next.

Cybersecurity leaders need to win differently by identifying and capturing the new demand for security capabilities. These have emerged from the economic and digital disruptions over the past 18 months, and the organizational changes triggered in response. Flexibility, autonomy, modularity, discovery and self-service are at the core of digital transformation efforts. This requires creating new or revising existing security strategies, security operating models and ways of working. To win differently, cybersecurity leaders should employ quick wins and smart tactics.

Quick Win: Business Strategy Review

Require the entire security team to read the organization's business strategy or annual report. Have the team develop a short presentation that shows how the security strategy and program support the business's ability to achieve the organization's strategic objectives and expose where alignment challenges may exist. Doing this regularly also helps identify where planned security initiatives are no longer required because of evolving business needs. This helps:

- The security team quickly develop improved familiarity with strategic business direction and priorities
- increase harmonization and alignment between the security team's work practices, security initiatives and business priorities
- Enhance opportunities to improve the reputation and trust in the security function as a strategically aligned, trusted advisor and business-enabling capability

Smart Tactic: Establish "Break the Rules" Meetings

Hold regular "break the rules" meetings where security team members, in a safe and no-consequences space, can challenge the status quo on rules, take existing procedures back to the beginning and start again. This is especially useful to help expose things that the team is working on or the controls being deployed that aren't delivering value. Empowering the security team to do some free thinking that fosters creativity and ideation helps:

1. Deliver new and innovative ideas on how to solve systemic cybersecurity challenges spread across multiple dimensions and scale.

2. Increase opportunities to solve security challenges, delivering real business value that generates positive sentiment with stakeholders.

3. Build a more engaged and motivated security team empowered by being able to showcase their talents — individually or as a group.

New Directions: Test Human-Centric Security Design

2022 Gartner research shows that 69% of employees deliberately bypassed security controls if it meant increased speed and convenience and where the business benefits outweighed the perceived risk to the organization. [5] Human-centric security design (HCSD) puts the employee experience at the center of security control design and implementation to help minimize cybersecurity-induced friction and optimize control adoption. The benefits associated with this approach include:

- Increased control adoption, which makes those controls more effective
- Fewer cybersecurity incidents caused by unsecure employee actions
- Increased value return on security investment.

See Case Study: User-Experience-Focused Cybersecurity Design (Santander) for more information.

Unleash Force Multipliers: Prioritize Changes That Amplify Effort

A force multiplier is an action that serves to create, or amplify, positive momentum toward a desirable outcome. When resources are limited, this should be a core focus for CISOs. Given the force-multiplier effect IT has in delivering scalability, using force multipliers in cybersecurity provides CISOs the opportunity to amplify those effects exponentially. In a cybersecurity context, a force multiplier can be:

- **Internal** — Examples are a security business model creativity workshop or automating incident response efforts where practical to address more incidents faster.
- **External** — One example is introducing new, or revising existing, security regulations for your industry sector. Another example is the merger of two or more solution vendors, so their previously separate security solutions combine to form an exponentially more powerful security control capability.

Force multipliers can be contextual levers that enable changes such as informed security decision making within the current business. They can be strategic levers, like adapting the security operating model so it delivers more value to the organization's internal and, potentially, external customers. A force multiplier can also be an operational lever, like finding ways to improve the communication efficiency and effectiveness between the business and security function. Cybersecurity leaders can unleash force multipliers in the following ways.

Quick Win: Win Over the Critics

Find the security team's biggest critics at the executive level. Address their concerns first by aligning to their goals where practical to help smooth the way for later-stage discussions. This will provide the opportunity to transform critics into key champions for the security program who can help drive increased support from other business areas. By doing this, cybersecurity leaders will:

- Stand a much better chance of securing their critics' support by demonstrating they are mindful of, and are willing to work hard to address, concerns.
- Exploit the 180-degree change in previously critical sentiment to help smooth the path with other stakeholders.
- Help build their and the security team's reputation as a trusted, business-centric partner focused on helping others achieve their goals.

Smart Tactic: Security Champions Program

Establish a security champions program (see Ignition Guide to Designing and Launching a Security Champion Program). This involves identifying and recruiting personnel from across the organization to become communication conduits between the security team and other business units. Key to the success of these programs is selecting security champions from business areas that can demonstrate the requisite aptitude and then investing in them to develop the security knowledge needed to perform their roles effectively. An effective security champions program will help cybersecurity leaders:

- Improve message penetration for security communications into key business areas.
- Raise awareness of security challenges and give rise to improved levels of security consciousness across the organization.

- Identify new internal talent to fill critical vacancies. Security champions who demonstrate a desire and aptitude for security and risk management could become permanent members of the security team as opportunities arise.

See Ignition Guide to Designing and Launching a Security Champion Program for more.

New Directions: Establish a Security Behavior and Culture Program

The vast majority (84%) of cybersecurity leaders have indicated that measurably changing behavior to reduce the risks associated with unsecure employee behaviors is the primary objective of their security awareness programs. [6] Security behavior and culture programs (SBCPs) extend beyond traditional approaches by raising security awareness with a more holistic and integrated program that can help:

- Foster more secure behavior across the organization.
- Cultivate and embed a more security-conscious corporate culture.
- Reduce the number of cybersecurity incidents caused by employee actions.

CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework.

Banish Drags: Reduce Inefficiency and Waste

As power centers in organizations evolve, cybersecurity leaders will face more and more resistance unless they can demonstrate value to business leaders. If cybersecurity leaders wish to advise on security risks and help with trade-off decisions, they need to show they can effectively balance risk management against seamless business enablement. This means that CISOs must be able to influence their peers and senior stakeholders across the business, not just be seen as control managers.

Drags are negative internal or external forces that affect the security team's ability to move faster. External examples include limited access to security talent and pervasive threat-actor activity. Internal examples include legacy security processes that no longer align with how the business wants to operate and security governance frameworks that create unnecessary information risk and decision-making bottlenecks instead of enhancing the security team's visibility.

Quick Win: Remove Unnecessary Controls

As technology and digital business models evolve, existing security controls may cause unnecessary impacts to business unit operations. Where those controls offer little utility in reducing risk, or there are opportunities to use smoother compensatory controls, cybersecurity leaders should consider removing them, as it will help:

- Free up precious security personnel and funding for more important initiatives.
- Improve the security team's operational efficiency.
- Help build positive sentiment with business stakeholders, who will recognize the security function's attention to their needs.

See CISO Foundations: 4 Actions CISOs Must Take to Reduce Cybersecurity-Induced Friction.

Smart Tactic: Adopt a Principles-Based Policy Framework

Overly prescriptive policy settings may be too inflexible for increasingly autonomous business units seeking increased flexibility and agility to explore emerging technologies. Taking a more principles-based approach promotes increased flexibility and enables resource owners to adapt cybersecurity procedures and controls to their specific needs. In turn, this fosters an enhanced sense of ownership and responsibility for risk management, while maintaining policy compliance. Cybersecurity leaders taking a principles-based approach to policymaking will:

- Find policy settings increasingly perceived as business-centric and geared to help the business achieve its strategic objectives.
- Improve the organization's digital dexterity. Resource owners have the latitude to experiment with new digital initiatives within a wider set of guardrails.
- Foster increased trust and more productive relationships. Reduce the number of policy exception requests received.

See CISO Foundations: Making Information Security Policy Accessible (Raytheon).

New Directions: Be Prepared to Let Go!

As digital business decisions move to the edge of the enterprise, so do cyber-risk decisions. As a result, cybersecurity leaders must let go of the notion that their security function will have full visibility of, let alone control over, every cybersecurity risk decision. Fostering cyber judgment helps authorized personnel make decisions that are higher quality and use independent information (see Infographic: Building Cyber Judgment to Improve Risk Decision Making). Cybersecurity leaders who can successfully foster improved cyber-judgment throughout their organization will:

- Contribute to increasing digitization speed and value from decentralized digital initiatives.
- Reduce the likelihood that digital decision makers will introduce unnecessary risk.
- Enhance trust and the security team's reputation across the business.

See Cyber Judgment Presents a New Approach to Informed Risk Decision Making.

Redirect Resources: Adopt an Agile, Responsive and Advisory Approach

The combined impacts of decentralized digital decision making and emerging technology trends present unique challenges for security and risk teams. As digital transformation efforts to experiment with, and operationalize, emerging technologies increasingly move outside traditional enterprise IT, it's very likely that security team skill sets are not keeping pace and upskilling will be needed. This highlights the need to ensure resources are being directed as effectively as possible.

Quick Win: Stop Redundant Security Initiatives

Cybersecurity leaders could miss the opportunity to develop positive sentiment with business decision makers because security program initiatives are no longer aligned to changing business priorities or digital business objectives. Identifying and canceling security initiatives that are no longer required because of shifting business priorities helps the cybersecurity leader:

- Minimize sunk costs and reduce the risk of wasting hard-won security investments on low-value initiatives.
- Free up precious FTE resources, enabling the security team to pivot when needed.
- Foster improved stakeholder perceptions that the security program can keep pace with the business as things change.

See Quick Win: Business Strategy Review and Security Project Prioritization Tool for more.

Smart Tactic: Test Robotic Process Automation and GenAI Where Practical

A key challenge for cybersecurity leaders is being able to do more with the finite FTE resources available to them, especially as the digital ecosystem they must protect continues to evolve and spread. Robotic process automation (RPA) and the emergence of GenAI capabilities provide opportunities for routine, repeatable, procedural tasks to be automated. Candidate security tasks include active threat hunting, low-fidelity security incident remediation, continuous vulnerability assessments, security patch management and security awareness content creation. Cybersecurity leaders who can use RPA and GenAI inside their security programs will:

- Free up precious FTE for more important and interesting initiatives, which also helps retain high-quality security team members.
- Improve standardization and consistency in security processes because they're less prone to human error or an inconsistent adherence to a process.
- Improve overall operational efficiency and productivity, even with the same resourcing levels.

See Magic Quadrant for Robotic Process Automation and 4 Ways Generative AI Will Impact CISOs and Their Teams.

New Directions: Transform the Security Operating Model

Digital decision making rights and accountability for cybersecurity are increasingly decentralizing into lines of business or product teams. They also are increasing the number of stakeholders with demands for the security team's time and efforts. This is altering the playing field for the cybersecurity leader who's used to having minimal channels to monitor to help manage demands on the security team for cyber-risk insight and decision making. As such, the current operating model may no longer be appropriate to adapt to these new ways of working. CISOs should review their current security operating model, and where required, change it to ensure it can meet amplified and evolving business needs without introducing unnecessary risks. While transforming the security operating model is a significant undertaking, cybersecurity leaders who actively seek to adjust how their security team operates and streamline cybersecurity risk governance processes will:

- Align limited FTE and funding to more business-enabling activities.

- Continue to build traction with business stakeholders as they gain autonomy for digital decision making but increase their formal accountability for cybersecurity risks.
- Enable greater levels of consistency in cybersecurity policy settings via a more centralized cybersecurity risk governance framework.
- Build trust in the business by enabling it to become more agile and speed up digitalization initiatives without compromising security.

See CISO Effectiveness: Security Operating Models Are Evolving.

Evidence

[1] **2024 Gartner Board of Directors Survey on Driving Business Success in an Uncertain World:** This survey was conducted to understand the new approaches adopted by nonexecutive boards of directors (BoDs) to drive growth in a rapidly changing business environment. The survey also sought to understand the BoDs' focus on investments in digital acceleration; sustainability; and diversity, equity and inclusion. The survey was conducted online from June through August 2023 among 285 respondents from North America, Latin America, Europe and Asia/Pacific. Respondents came from organizations with $50 million or more in annual revenue in industries except governments, nonprofits, charities and nongovernmental organizations (NGOs). Respondents were required to be nonexecutive members of corporate boards of directors. If respondents served on multiple boards, they answered questions about the largest company, defined by its annual revenue, for which they are a board member. *Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[2] **2024 Gartner CIO and Technology Executive Survey.** This survey was conducted online from 2 May to 27 June 2023 to help CIOs determine how to distribute digital leadership across the enterprise and to identify technology adoption and functional performance trends. Ninety-seven percent of respondents led an information technology function. In total, 2,457 CIOs and technology executives participated, with representation from all geographies, revenue bands and industry sectors (public and private). *Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[3] **2022 Gartner Overcoming the Barriers to Digital Execution Survey.** This survey was conducted online from 1 March through 14 March 2022 to understand how to overcome barriers to digital execution. In total, 96 CIOs and IT and business leaders who were members of Gartner's Research Circle, a Gartner-managed panel, participated. Members from North America (n = 43), EMEA (n = 35), Asia/Pacific (n = 11) and Latin America (n = 7) responded to the survey. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[4] CISO stress and burnout cause high churn rate, TechTarget.

[5] **2022 Gartner Drivers of Secure Behavior Survey.** This survey was conducted via an online platform from May through June 2022 among 1,310 employees across functions, levels, industries and geographies. The survey examined the extent to which employees behave securely in their day-to-day work, root causes of unsecure behavior, and the types of support and training that they received from their organizations to drive desirable secure behaviors. We used descriptive statistics and regression analysis to determine the key factors that drive or impede employees' secure behaviors and develop cyberjudgment.

[6] **2022 Gartner Cybersecurity Awareness Survey.** This study was conducted to get a better understanding of the size, scope and objectives of cybersecurity awareness campaigns in organizations. The online survey was from February through April 2022 and respondents included heads of cybersecurity functions. Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Document Revision History

Cybersecurity Accelerators: Leadership Tactics for Keeping Pace With the Business - 31 March 2022

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Predicts 2023: Cybersecurity Industry Focuses on the Human Deal

Case Study: Framework to Enable Business Ownership of Cybersecurity Activities

CISO Effectiveness: Start Practicing 3 Burnout-Avoiding Behaviors Now

CISO Foundations: Build a Defensible and Agile Security Program

Actionable, objective insight

Position your organization for success. Explore these additional complimentary resources and tools for cybersecurity leaders:

Report

Cybersecurity Trends: Optimize for Resilience and Performance

Equip your cybersecurity function for greater resilience.

Download Now

Roadmap

IT Roadmap for Cybersecurity

Create a resilient, scalable and agile cybersecurity strategy.

Download Now

Tool

Gartner Cybersecurity Business Value Benchmark

Quantify the value of cybersecurity investments.

Learn More

Conference

Gartner Security & Risk Management Summit

Join your peers for the unveiling of the latest insights at Gartner conferences.

Reserve Your Spot

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 866 263 8917

International: +44 (0) 03301 628 476

Become a Client

Learn more about Gartner for Cybersecurity Leaders
gartner.com/en/cybersecurity

Stay connected to the latest insight in 𝕏 ▶

Gartner®