Gartner Research

Cybersecurity Accelerators: Leadership Tactics for Keeping Pace With the Business

By Richard Addiscott, Katell Thielemann

31 March 2022

Gartner®

Cybersecurity Accelerators: Leadership Tactics for Keeping Pace With the Business

Published 31 March 2022 - ID G00744219 - 17 min read

By Analyst(s): Richard Addiscott, Katell Thielemann

Initiatives: Cybersecurity Leadership

Challenging global economic conditions continue to see digital business accelerate. Security and risk management leaders must leverage cybersecurity accelerators to keep pace with the business and demonstrate security's role and criticality as an enabler of the organization's digital ambitions.

Overview

Key Findings

- Boards and CEOs alike are continuing to adapt their organizations to exploit digital business opportunities to enhance customer engagement and accelerate growth.
- Boards are increasingly shifting digital-related budget allocations out of central IT functions to business units to accommodate their digital investments.
- Boards and senior executives need security and risk management (SRM) leaders to ensure their security capabilities support and enable the business as their organizations continue to evolve and digital capabilities transform.
- SRM leaders find it challenging to identify avenues to accelerate security practices and sustain a higher pace of change over time to meet business demand.

Recommendations

SRM leaders that need to adapt and accelerate their security capabilities to support the organization's increased digital business progress should:

- **Win differently:** Assess where you are and where you're going by establishing a cybersecurity strategy think tank or "tiger team" charged with identifying, investigating and reporting on new opportunities to speed up security capabilities without introducing unnecessary risks.

- **Unleash force multipliers:** Take purposeful actions that will create momentum, like implementing a security chatbot to help facilitate faster response times to simple security-related questions from end users.
- **Banish drags:** Get rid of things that limit or restrict the security's function to meet business demand progress, like fostering enhanced cyber-risk decision making by business areas leading the organization's digital agenda.
- **Redirect resources:** Recast existing security roadmaps as necessary, and stop initiatives no longer aligned to the organization's digital trajectory. Transform the security function into a true business-enabling capability by shifting away from risk-averse, control-driven security operating models toward a more agile, advisory-centric way of delivering security services.

Introduction

For some, the last two years have predominantly meant slowdowns or fix-it/exit-related efforts.

SRM leaders in 2022 and beyond face a new reality of rapid business-led technology transformation as new digital commerce, contactless customer interactions, and remote work and learning solutions are deployed within weeks and, often, days. This is highlighted in recent Gartner surveys showing that:

- 83% of CEOs are looking to increase their investment in digital capabilities. [1]
- 76% of CIOs expect to see increased demand for new digital products and services. [2]
- 81% of CIOs expect to see increased use of digital channels to reach customers/citizens. [2]
- 40% of boards have moved digital-business-related budgets to business functions to accommodate digital investments. [3]
- 60% of CISOs are seeing increases in the number of non-IT information-risk decision makers inside their organization. [4]

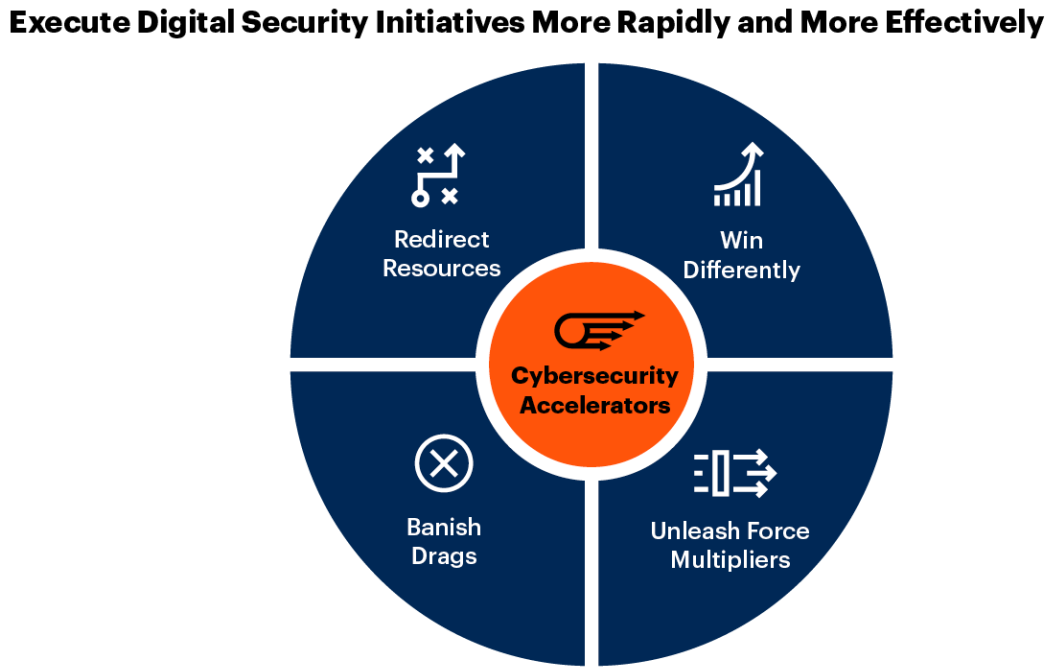
What tactics can SRM leaders use to keep pace with a business that continues to move at an ever-increasing pace? Gartner's Cybersecurity Accelerators present several ways to accomplish this.

Cybersecurity Accelerators — Leadership tactics SRM leaders can apply to establish, and sustain, a more agile, responsive and faster cybersecurity capability.

Gartner's Cybersecurity Accelerators, shown in Figure 1, encapsulate the themes of potential actions SRM leaders can take to help accelerate and sustain the pace of their cybersecurity efforts as either:

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

Figure 1: Execute Digital Security Initiatives More Rapidly and More Effectively



Source: Gartner
744219_C

Gartner

There is no expectation that all of the ideas provided in this research are fit for purpose for all organizations. Rather, they are provided for consideration based on an SRM leader's unique operational context. The key intent is to help SRM leaders ensure the security function not only supports, but also enhances, the organization's ability to drive its digital agenda at a pace needed to achieve its longer-term strategic objectives.

Analysis

Win Differently

The 2022 Gartner View From the Board of Directors Survey shows that 64% of the surveyed boards have made efforts to change their business models, structuring them to a more digital economic architecture. Among respondents, 62% report the primary outcome sought is improving customer engagement and loyalty. [3]

Sometimes you need to go slow to go fast. Security and risk management leaders should pause, step back, 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.

Security and risk management leaders need the ability to win differently by identifying and capturing the new demand for security capabilities emerging from the economic and digital disruptions over the last 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 will require creating new or revising existing security strategies, security operating models and ways of working.

To win differently, SRM leaders should consider the following recommendations.

Quick wins:

- Identify critical business units and their associated security risk appetites, and ensure you've developed an inventory of their highest-value data and information assets.
- Make the entire security team read the organization's business strategy and/or annual report. Have the team develop a short presentation that shows how the security strategy and program support the business' ability to achieve the organization's strategic objectives.

- Interview key business stakeholders to find out what their new priorities are and what they need from the security function in the new normal.
- Review and refresh as necessary your enterprise information security charter to reflect the direction your security program must take to deliver strategic business outcomes (see Tool: Enterprise Information Security Charter Template).

Smart tactics:

- Hold regular “break the rules” meetings where security team members, in a safe/no-consequences space, can challenge the status quo on rules, take existing procedures back to ground zero and start again.
- Work on your business acumen skills. Explaining the minutiae of security controls to senior leaders is not helpful to them. Instead, articulate security in the context of business risks, business value and cost as opposed to “here is our policy.”
- Build an actionable security risk appetite framework that helps guide nonsecurity decision makers to make higher-quality, independent, informed and timely information risk decisions.
- Work with business unit leaders progressing digital initiatives to develop security protection options that balance the value of the asset being protected, the desired residual risk and the cost of achieving that protection (see Optimize Risk, Value and Cost in Cybersecurity and Technology Risk).
- Add a clause to the Enterprise Security Charter stating that the organization’s information risk owners will not make decisions that will see the organization operating outside of agreed risk appetite levels.

New directions:

- Set up a security strategy think tank to investigate and report on emerging security threats and technologies to enhance preparedness and to provide opportunities to stay in touch with, and influence, business digital decision making.

- Allow more flexibility in controls selection by shifting the compliance mindset from mandatory controls (e.g., web applications must use product X for multifactor authentication) to principles and policies (e.g., web applications must have multifactor authentication) supported by security services (e.g., we support product X for multifactor authentication for applications where it is appropriate). For more information, see Implement an Agile Cybersecurity Program: Lessons Learned From the COVID-19 Pandemic.
- Establish a security vision and culture charter designed by the end-user community for the end-user community to improve the adoption of desired security behavior norms in pursuit of reduced human-born cyber risks (see Take 3 Steps to Prove That Your Security Awareness Program Is Actually Working).
- Map the customer and end-user journey beyond security touchpoints to assess the impacts of control implementation and operation on the customer and user experience. Where the impact is material to the user or customer experience, work collaboratively with business stakeholders to ensure key messages on implications and benefits are communicated effectively to minimize disruption to users and optimize the new control's adoption.

Unleash Force Multipliers

A force multiplier is an action that serves to create, or amplify, positive momentum toward a desirable outcome. In a cybersecurity context, a force multiplier can be:

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

Force multipliers can be contextual levers, like enabling changes to where informed security decision making occurs within the current business. They can be strategic levers, like adapting the security operating model so that it delivers more value to the organization's internal and, potentially, external customers to enable the enterprise "to win." And a force multiplier can be operational levers, like finding ways to improve the communication efficiency and effectiveness between the business and security function.

Our 2022 View from the Board of Directors Survey shows that 83% view CIOs as trusted allies (35%) or partners (48%), but 40% have moved digital-business-related budgets to business functions to accommodate digital investments. To assist with ensuring business units can move at the pace they need to without introducing unnecessary risk, here are examples of how security and risk management leaders can unleash force multipliers.

Quick wins:

- Get security team members speaking directly with employees in your service contact center
- Add a prominent "How We Help" section to the Security team's intranet page — teams that position themselves effectively will become more visible to the wider organization.
- Sketch an "antistrategy" — state what the security team won't do and what it won't be.
- Find the security team's biggest "critics" at the executive level. Address their concerns first by aligning to their goals where practicable to help smooth the way for later-stage discussions. This will provide the opportunity to transform them into key champions for the security program to help drive increased support from other business areas.

Smart tactics:

- Establish a work rotation program where security team members are embedded into business units (where practicable) so that they can see and hear firsthand how current cybersecurity controls may be causing issues in business areas.
- Increase the privacy and compliance focus on third-party vendors and other partners. Additionally, conduct risk scoring on vendors to apply the controls in a prioritized way to drive optimal control strength.
- Establish a security champions program (see How to Design a Security Champions Program).
- Execute a security and risk management literacy program to improve cybersecurity wherewithal across the senior executive to help improve the quality of independent information risk decision making.

New directions:

- Baseline security incident data and identify high-volume, low-complexity security incidents where the response could be fully, or at least mostly, automated. Leverage extended detection and response (XDR) and/or security orchestration, automation and response (SOAR) capabilities to help increase visibility over the broader enterprise digital landscape, detect, and then respond faster and at higher volumes to indicators of compromise (see Innovation Insight for Extended Detection and Response).
- Execute a proof of concept for a security chatbot to help facilitate faster response times to simple security-related questions from end users.
- Create a cross-functional team with representation across the business to capture sentiment about the current security awareness campaign. Have this same team leverage design thinking or other human-centric design techniques to design and establish a security behavior and culture program (SBCP) to enhance end-user adoption of the desired security practices.
- Create product security manager or champion roles and start filling them internally.

Banish Drags

As outlined above, Gartner research shows the number of people making information risk decisions has expanded, and CISOs feel that independent decision makers negatively impact the quality of information risk decisions. This is a major disconnect from where the business is headed, which is more decentralization, more self-determination, more self-service, more digitization and more choices.

A changing world needs leaders, not managers. The power centers in organizations are evolving, and, unless you can show business leaders how security can help both value creation and value protection, you will face more and more resistance. If SRM leaders wish to have a place at the table, advising on security risks and helping with trade-off decisions, they will need to develop a trust model for distributed decision making.

Drags are negative internal or external forces that impact the security team's ability to move at a faster pace. External examples include limited access to security talent and pervasive threat actor activity. Internal examples include legacy security processes that no longer align to how the business wants to operate and security governance frameworks intended to enhance the security team's visibility, which are now creating unnecessary information risk decision-making bottlenecks instead.

Here are examples of how security and risk management leaders can defuse drags.

Quick wins:

- Use culture hacks to help the security team identify opportunities for continuous improvement; reduce change fatigue; and instill belonging and pride in the work they do. For example, put up a "state of security" dashboard in common work areas, and run a competition for all employees to encourage and solicit feedback or suggestions on how security can enable the business.
- Accept some degree of sunk cost, and terminate security initiatives that are no longer required as a result of changes to the business' digital trajectory.
- Surface any cybersecurity regulatory changes that constrained digital previously, but have been eased or removed because of lockdown.

Smart tactics:

- Move information risk decisions closer to the business by devolving decision making and unbundling resources (see Expert Insights Video: Cyber Judgment: Navigating the Era of Distributed Decision Making).
- Train security team members in advanced interviewing techniques that help sensitively provoke constructive insight from the business as to where they see security as a drag on progress.
- Define clear guidance for business units and digital decision makers on the minimum security and privacy requirements to be met before establishing commercial arrangements with third-party vendors and other partners. Then, leverage the internal audit program to identify noncompliance.
- Reduce decision scope. Consider how the security and risk management leadership team scopes decisions. Is an unnecessarily large decision scope creating inertia? If so, consider breaking decisions into minimally viable decision increments.

New directions:

- Redesign as needed your security operating model to ensure it is primed for Agile practices, product-based security and increasingly distributed information risk decision making (see Implement an Agile Cybersecurity Program: Lessons Learned From the COVID-19 Pandemic).

- Thaw the frozen middle. Let the progressive security team members who demonstrate aptitude for continuous improvement and innovative thinking lead. Where practicable, reassign or part ways with those in the security team that fail to embrace change or actively block it.
- Formalize how security processes can flex by creating boundaries for business-unit autonomy and proceeding with informed consent rather than waiting for the security team's endorsement.
- Deliver radically transparent security communications. Review and document the most effective communications techniques the enterprise used at the height of the disruption. Institutionalize improved communications going forward by making those techniques best practices, particularly in situations where the enterprise is stressed by further disruption and stakeholder trust is essential.

Redirect Resources

The 2022 Gartner CIO and Technology Executive Survey shows that cloud platforms (41%), analytics platforms (41%) and data platforms (39%) are viewed as the top three technology skills that will be most important to achieving crucial priorities over the next 12 months. These emerging technology trends present unique challenges for security and risk teams. As digital transformation efforts move rapidly outside of traditional enterprise IT, it's very likely that security teams/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.

Here are examples of how SRM leaders can redirect resources.

Quick wins:

- Identify security initiatives that are no longer required due to shifting business priorities and reallocate project resources to other projects to accelerate their delivery or enhance the quality of the outcomes expected (see Recast Your Cybersecurity Roadmap to Aid Organizational Recovery in 4 Steps).
- Create security acceleration goals and KPIs such as reducing the time it takes for digital decision makers to gain the insights needed to make informed and independent information risk decisions.

Smart tactics:

- Use robotic process automation (RPA) to automate mundane security tasks and free up scarce security resources for other security initiatives (see Four Steps to Ensure Robotic Process Automation Security).
- Undertake a forensic review of the current security vendor and tool landscape to identify areas of capability duplication. Where duplication is identified, consolidate to reduce contract management overhead and enhance operational efficiency by reducing the number of systems required to protect the environment.
- Use Gartner's Risk, Value, Cost (RVC) Optimization model to evaluate the balance of controls investments in different business units or application domains (see Optimize Risk, Value and Cost in Cybersecurity and Technology Risk).

New directions:

- Formalize a lean security organization strategy by divesting as many functions as possible from the security team to nonsecurity teams elsewhere in the enterprise (see Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage).
- Review existing security capabilities to map them to the organization's digital transformation agenda. Then reassess the current internal versus outsourced resourcing mix, and migrate commoditized security skills to outsourcing partners to free up internal resources in preparation for the introduction of new digital capabilities.
- Retrain and transfer interested technical security staff who display sound risk acumen and commercial aptitude to become governance risk and compliance specialists or security advisors to core business units.

Evidence

[1] **The 2021 Gartner CEO and Senior Business Executive Survey** was conducted from July 2020 through December 2020, with questions about the period 2020 to 2023. One-quarter of the sample was collected in July and August, and three-quarters from October through December. In total, 465 actively employed CEOs and other senior executive business leaders qualified and participated. The research was collected via 390 online surveys and 75 telephone interviews. The survey was developed collaboratively by a team of Gartner analysts that examines technology-related strategic business change, and was reviewed, tested and administered by Gartner's Research Data, Analytics and Tools team. The results of this study are representative of the respondent base and not necessarily business as a whole.

[2] **The 2022 Gartner CIO and Technology Executive Survey** was conducted online from 3 May 2021 through 19 July 2021 among Gartner Executive Programs members and other technology executives. The total sample is 2,387, with representation from all geographies and industry sectors (public and private). The survey was developed collaboratively by a team of Gartner analysts, and was reviewed, tested and administered by Gartner's Research Data, Analytics and Tools team.

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

[3] **The 2022 Gartner View From the Board of Directors Survey** was conducted to understand how boards of directors (BoDs) will address the risk from economic and political volatility and a multipolar world, and their intent to convert digital acceleration to digital momentum. The survey also helps understand the impact of the key societal issues that took center-stage during the pandemic on BoDs' strategy and investment approaches.

The survey was conducted online from May through June 2021 among 273 respondents from the U.S., Europe and Asia/Pacific. Companies were screened to be midsize, large or global enterprises. Respondents were required to be a board director or a member of a corporate board of directors. If respondents serve on multiple boards, they answered for the largest company, defined by its annual revenue, for which they are a board member. The survey was developed collaboratively by Gartner analysts and the Research Data, Analytics and Tools team.

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiments of the respondents and companies surveyed.

[4] **Gartner's cyber judgment research** was conducted via an online survey from 12 April through 24 April 2019 with 60 Gartner clients with the objective of understanding how CISOs approach information risk decision facilitation throughout the enterprise. Clients from various revenue groups and industries participated in the initiative.

In addition, this research was informed by interviews conducted with over 70 organizations focused on best practices for driving informed risk decisions in the organization.

Recommended by the Authors

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

Digital Business Acceleration: Where to Focus Now?

Expert Insights Video: Cyber Judgment: Navigating the Era of Distributed Decision Making

Designing Work to Unlock a Responsive Culture

Agile Learning Manifesto

Mastering Business Dynamics

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."

Actionable, objective insight

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

eBook

Four Facets of Effective CISO Leadership

Discover how cybersecurity leaders tackle their expanding remit.

Download eBook

Research

Measure the Real Cost of Cybersecurity Protection

Learn how to make informed cyber risk acceptance decisions.

Download Research

Research

Drive Business Action With Cyber Risk Quantification

Identify best practices for driving business action at scale.

Download Research

Tool

Gartner IT Score for Security and Risk Management

Gain perspective on your highest-priority activities.

Download Now

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

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

© 2022 Gartner, Inc. All rights reserved. CM_GTS_1839153

Gartner®