Gartner

Rethink the Security & Risk Strategy

Embrace modern cybersecurity practices while enabling digital business.

EDITED BY
Tom Scholtz
Distinguished VP Analyst, Gartner

Introduction

It goes without saying that 2020 was a highly disruptive year, and prioritizing the health and safety of employees was the main focus of organizations navigating COVID-19.

For many organizations, this meant accelerating their adoption of digitalization. This included shifting as much of the workforce to work from home as possible, as quickly as possible. Some were better prepared for this than others.

COVID-19 refocused security teams on the value of cloud-delivered security, reviewing remote access policies and tools, migration to cloud data centers and SaaS applications, and securing new digitalization efforts to minimize person-to-person interactions.

Tom Scholtz
Distinguished VP Analyst, Gartner

In many ways, the pandemic forced teams to revisit much of the fundamentals of securing the business while enabling business to continue to evolve and grow.

In this e-book, security and risk leaders will learn how to think about strategy, how to communicate security and risk messaging to the board, and how to better staff your team.

Upgrade Your Security and Risk Perspective

Security professionals often focus on the threats and breaches that dominate the headlines — Equifax, SolarWinds, Marriott International, Aadhaar — and not necessarily on those most critical to the organization.

A perfect example is when security teams hold back on cloud initiatives because of unsubstantiated cloud security worries. This exaggerated fear can result in lost opportunity and inappropriate spending.

These high-profile stories are full of doom-and-gloom scenarios. Yet, zero-day vulnerabilities accounted for approximately 0.4% of incidents in the past decade. The amount spent on trying to detect them is out of balance with the actual risks they pose.

Chief information security officers (CISOs) must strike a balance between what is needed in a security program and the risks to undertake for the business to move forward. Without this balance, organizations miss opportunities and the CISO becomes an expensive distraction in the minds of enterprise leaders.

That may be easier said than done. Digital adoption might be moving forward at increasing speed, but the core beliefs wired into our minds often don't help. It's time to reframe your mindset to success in the midst of disruption. Change the conceptual and/or emotional viewpoint with which you view a situation to a new frame of reference that fits the "facts" of your future digital reality. Then you can create the new context for change.

Zero-day vulnerabilities accounted for approximately 0.4% of incidents in the past decade.

Source: Gartner

Build trust and resilience

Digital business has created a new ecosystem, one in which partners add new business capabilities and security complexities. The CISO's vision for risk and security must be based on an ecosystem that enables trust and resilience.

"The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive," says Tom Scholtz, Distinguished VP Analyst, Gartner.

The majority of vulnerabilities exploited will continue to be ones known by security and IT professionals at the time of the incident.

Success, Scholtz adds, is dependent upon CISOs' willingness to adopt a new set of trust and resilience principles:

6 trust and resilience principles

- Shift to risk-based decision making and away from checkbox compliance
- Begin supporting business outcomes rather than solely protecting infrastructure
- Become a facilitator, not a defender
- Determine how information flows; don't try to control it
- Become people-centric and accept the limits of technology
- Invest in detection and response, and stop trying to perfectly protect the organization

Move with the speed of digital business

Embracing these six principles calls for CISOs to deviate from perceived security conventions and best practices.

“We need security that is adaptive everywhere to embrace opportunities that were considered too risky in the past,” says Scholtz.

Equally important, CISOs need to be able to protect their organizations at the speed of digital business. Enter the cybersecurity mesh: a distributed architectural approach to scalable, flexible and reliable cybersecurity control.

Technologies manifesting the cybersecurity mesh

- Cloud access security brokers (CASBs)
- Zero trust network access (ZTNA)
- Secure access service edge (SASE)

Detect, Respond and Report

Although the likelihood of CISOs experiencing a major cyber- or ransomware attack is unlikely, all CISOs can learn from their less-fortunate peers.

For example, hospitals are a highly regulated industry. Each one is responsible for managing and protecting the data of potentially hundreds of thousands of patients, and complying with industry regulations.

However, if a hospital is the victim of a targeted phishing attack, it can be extremely dangerous for staff and patients — especially if it affects the hospital's ability to provide patient care.

A hospital CISO would need to answer a lot of questions about how the attack happened and how it was able to paralyze a healthcare facility.

Dictionary

phish•ing
/'fiSHiNG/

noun

Widespread, high-impact threat that relies on social engineering to enable illicit access to personal and corporate assets

smish•ing
/'smiSHiNG/

noun

Targeted attack through SMS

vish•ing
/'viSHiNG/

noun

Targeted attack through voice communication

For our unfortunate CISO, the answer might be that the information security team is chronically understaffed and under pressure to introduce new technologies with compressed deadlines.

Despite having senior leads, the team might not have the time or resources to keep pace with ever-shifting threats and trends, which left them unable to identify and protect against known vulnerabilities — which are the threats most likely to put an organization at risk.

Organizations are struggling to keep up with the current threat landscape. Too many manual processes are in place, and security and risk managers must wrestle with a lack of resources, skills and budgets.

But what can CISOs do in the face of increasing attacks and lack of resources?

Apply lessons learned

- Address and patch known vulnerabilities. Assess existing resources and ensure investment in an equal mix of detection and prevention solutions.
- Stay abreast of trends and understand their impact. Grant and his team were unable to do so, leaving their hospital vulnerable.
- If attacked, don't blame. One of the most important stages of incident response is to focus on root causes. Pointing fingers at others solves nothing.
- Use anti-phishing behavior management (APBM). This is a critical element of a people-centric security strategy.
- Protect the email gateway. Secure email gateway (SEG) vendors are increasingly incorporating targeted phishing methods. The most effective are proxy and time-of-click analysis-filtering techniques.
- Isolate vulnerable systems. Systems not yet affected by malware may still be vulnerable, and are often the ones relied on most. A useful temporary fix: Limit network connectivity when a breach or attack occurs.
- Reduce reliance on static personal data. Instead, increase reliance on dynamic identity data when engaging in identity verification to limit exposure to Equifax-like data breaches.

Polish, Practice and Present

CISOs of large enterprises are increasingly asked to report to their board of directors on cybersecurity and technology risk at least annually.

Presenting to the board offers new opportunities, but can be a challenging — and intimidating — task. These presentations don't have to be a deep dive into the minutiae of each technology. The key is tying everything to the business. Consider this 15-minute, 7-slide presentation.

Get started

This is your high-level, "call to attention" slide. It sets the scene for the board, and should simply identify the topics you'll cover in the following slides. No details are necessary, but it should signal that the presentation will include information about business execution, strategy, external developments and risk position.

Slide 1: Key Points

Business Execution	Material Risks	External Environment	Security Strategy	Recommendation
We have some bright spots, but continued remedial work in several areas will enhance business performance.	Our recent acquisition has a minor change on our risk position. All other material risks are stable.	External events require only minor tactical responses.	Execution of current security strategy is largely on target. Our process maturity continues to improve, and it exceeds peer benchmarks and approaching target.	Note current state and endorse action plan.

Performance and contribution to business execution

These follow-up slides should link security and risk, implicitly or explicitly, to business elements that board members value. Use them to highlight metrics and how the security team contributes to positive outcomes. Be prepared to explain potential problem areas and implications. Supply detailed documentation on how each metric was produced for board members who ask.

By 2023, 30% of chief information security officers' effectiveness will be directly measured on the role's ability to create value for the business.

Source: Gartner

Slides 2–6: We Have Some Bright Spots, but Continued Remedial Work in Several Areas Will Enhance Business Performance

Financial	Customer	Operational	Learning and Growth
We will use security to help grow the business.	We will provide a high level of service availability and continuity.	Our tools will be fit for purpose.	Our people will be fully engaged.
We will be efficient in our security management.	Customers will have confidence in our services and facilities.	We will execute change efficiently and reliably.	Our people will make the right decisions.
We will execute projects on time and on budget.	We will comply with all applicable regulations.	We will embed continuous improvement in our processes.	We will invest in our people and develop their expertise.
We will manage our suppliers cost-effectively.	The right people will have access to the right information.	We will maintain our operational risk to within a defined risk appetite.	We will protect our know-how as a competitive advantage.

The call to action

Wrap up the presentation with a closing slide to reiterate the main points and any action items. The key is to close strongly, leaving the board confident in your plan and abilities. Summarize the points you've made and be clear about anything you are requesting. Take questions and thank the board for their time.

Slide 7: Action Plan

Board to note current state:

Business-as-usual (BAU) work programs that uplift business performance will continue.	Minor actions in response to external changes will be executed as BAU.	No action is required for minor change in material risk position.	Execution of current security strategy is largely on target. Our process maturity continues to improve, and it exceeds peer benchmarks and approaching target.	Note current state and endorse action plan.

Regular board update to be delivered during the next half year.

Are You Prepared for Your Board's Security Questions?

As board members realize how critical security and risk management is, they are asking leaders more complex and nuanced questions. They are becoming more informed and more prepared to challenge the effectiveness of their companies' programs.

5 security questions your board will inevitably ask

The trade-off question

What it sounds like: Are we 100% secure? Are you sure?

Why it's asked: Questions like this are often asked by board members who don't truly understand security and the impact to the business. It's impossible to be 100% secure or protected. The CISO's role is to identify the highest-risk areas and allocate finite resources toward managing them based on business appetite.

How to respond: Begin with something like: "Considering the ever-evolving nature of the threat landscape, it's impossible to eliminate all sources of information risk. My role is to implement controls to manage the risk. As our business grows, we have to continually reassess how much risk is appropriate. Our goal is to build a sustainable program that balances the need to protect against the need to run our business."

The landscape question

What it sounds like: How bad is it out there? What about what happened at X company? How are we compared to others?

Why it's asked: Board members will come across threat reports, articles, blogs and regulatory pressure to understand risks. They will always ask about what others are doing, especially peer organizations. They want to know what the "weather" looks like and how they compare to others.

How to respond: Avoid guessing at the root cause of a security issue at a different company by saying, "I don't want to speculate on the incident at Company XYZ until more information is available, but I'll be happy to follow up with you when I know more." Consider discussing a series of broader security responses such as identifying a similar weakness and how it's being fixed or updating business continuity plans.

The risk question

What is sounds like: Do we know what our risks are? What keeps you up at night?

Why it's asked: The board knows accepting risk is a choice (if they don't, that's a challenge you need to solve). They want to know that the company's risks are being handled. CISOs should be prepared to explain the organization's risk tolerance to defend risk management decisions.

How to respond: Explain the business impact of risk management decisions and ensure that your positions are supported by evidence. The second part is vital because boards are making decisions based on the risk tolerance. Any risks outside the tolerance level requires a remedy to bring them within tolerance. This doesn't necessarily require dramatic changes in short periods of time; beware of overreacting. The board will be seeking assurances that material risks are being adequately managed, and that subtle, long-term approaches may be appropriate in some instances.

The performance question

What it sounds like: Are we appropriately allocating resources? Are we spending enough? Why are we spending so much?

Why it's asked: The board will want reassurance that security and risk management leaders are not standing still. Board members will want to know about metrics and ROI.

How to respond: Use a balanced scorecard approach in which the top layer expresses business aspirations and the performance of the organization against those aspirations is illustrated using a simple traffic-light mechanism. As much as possible, explain aspirations in terms of business performance, not technology. Performance is underpinned by a series of security measurements that are evaluated using a set of objective criteria.

The incident question

What it sounds like: How did this happen? I thought you had this under control? What went wrong?

Why it's asked: This is asked when an incident or event has occurred and the board either already knows or the CISO is informing them of it.

How to respond: An incident is inevitable, so be factual. Share what you know and what you are doing to find out anything you don't currently know. In short, acknowledge the incident, provide details on business impact, outline weaknesses or gaps that need to be worked out and provide a mitigation plan. Be cautious not to endorse one option as the ultimate choice when in front of the board. The responsibility for oversight of security and risk remains with the security leader, but the accountability has to always be defined at the board/executive level.

Rethink Your Approach to Security Talent

The unemployment rate for IT security professionals is approximately zero.

While the demand for security professionals continues to grow, the number of people with the skills and experience required to fill these positions is not keeping pace. The scarcity of skills is compounded by the fact that IT security teams are expected to play a larger, more strategic role — one that will drive company growth, help organizations take smart risks with new technologies and meet increasing firmwide demands for information security support.

Simply put, it is more difficult to hire security professionals today than it was even three or four years ago.

Key security challenges for CIOs

Today's CISOs are facing new conditions:

1. New security capabilities and roles are required. Digitalization is driving the need for a wider range of roles that entail new skills and knowledge. CISOs are expected to selectively add more than 30 such capabilities to their function over the next 24 months, such as security strategists responsible for setting the security strategy and informing the enterprisewide strategy.
2. It's difficult to hire new security talent. It takes an average of 130 days to fill open IT security positions; openings go unfilled and teams remain understaffed for many months. As a result, CISOs' teams are often pulled into a continuous cycle of high turnover and slow hiring.
3. Demand for security exceeds capacity. The increasing demand for security expertise places significant pressure on CISOs to exponentially scale their teams' work. Demand is driven by massive investments in digital transformation, media reports of data breaches and cyberattacks, and widespread adoption of agile development methodologies — requiring CISOs to do more with existing staff while planning for shifts in future talent needs.

Use data to uncover new sources of talent

Gartner TalentNeuron™ recommends places to find digital talent. CISOs can check with their HR peers on how data can uncover untapped sources of talent.

- **Locations with less of a talent squeeze.** Analyze data for both supply and demand to get a clearer picture of which locations to target.
- **Adjacent companies and industries.** Mine these sources to identify companies actively hiring the talent you want and then add them to your sourcing criteria.
- **Cities with emerging talent pools.** Use data to identify cities with nascent digital talent pools. They enable you to stretch your recruiting resources.

Take the lean team approach

While the solution to data breaches may appear to be a bigger, better IT security team, a lean approach to staffing can alleviate resource challenges without sacrificing reflectiveness. This calls for delegating a portion of security functions to other corporate, business and IT teams.

In interviews with Gartner clients that have, by either design or circumstance, implemented lean security organization strategies, it became clear that such an approach can be used effectively to optimize scarce security resources. The starting point is to move beyond the assumption that an ever-growing security team is the best way to respond to increasing security risk.

“The starting point is to move beyond the assumption that an ever-growing security team is the best way to respond to increasing security risk.”

Tom Scholtz
Distinguished VP Analyst, Gartner

To adopt a lean approach, Gartner recommends these actions:

- **Challenge the status quo of your security organization** by questioning fundamental assumptions about accountability and the role of the information security team, which may have a material effect on the demands on the team and hence, the team's effectiveness.
- **Assess your current security team for effectiveness** to identify functions or capabilities (such as user awareness communication) that can be devolved elsewhere in the business or IT.
- **Identify alternative locations in the business or in IT** for capabilities that are underresourced or performing suboptimally.
- **Identify and communicate** the advantages, disadvantages and prerequisites of adopting a lean approach in your enterprise.

Prerequisites for adopting a lean security organization

Formally adopting a lean security organization strategy is not without risk, and has several key prerequisites:

- **Clear executive support.** This is key. Ensure leadership is fully apprised of the reasons and objectives of the strategy, as well as any associated risks and complications.
- **Security teams experienced in managing distributed teams.** Teams should also be experienced in instituting and managing governance functions such as steering committees, coordination and planning forums.
- **A cultural environment that encourages learning.** It should also encourage personal growth and embracing new responsibilities, as this approach is largely based on the ability, capacity and willingness of nonsecurity employees to embrace new additional responsibilities.
- **Ability and budget to support employee education.** Employees new to their security responsibilities need to be quickly trained. Determine which team will fund the education — the security team or new line management.
- **Higher levels of process maturity.** They are critical. Devolving functions that are not based on process will suffer when shifted to resources that have less risk and security expertise.

Additional Research

Upgrade Your Security and Risk Perspective

Client Research

Clouds Are Secure: Are You Using Them Securely?
Jay Heiser, October 2019

Implement an Agile Cybersecurity Program: Lessons Learned From the Covid-19 Pandemic
(September 2020 — G00727077)

Smarter With Gartner articles

The Gartner IT Security Approach for the Digital Age
Smarter With Gartner, Neil MacDonald, June 2017

Reframe Your Core Mindset Beliefs to Meet Digital-Era Demands
Smarter With Gartner, Graham P. Waller, December 2016

Detect, Respond and Report

Client Research

How to Use Threat Intelligence for Security Monitoring and Incident Response
(September 2020 — ID G00463498)

The Essential Elements of Effective Vulnerability Management
(October 2020 — ID G00734168)

Smarter With Gartner Articles

10 CIO Resolutions for 2019
Mark Raskino, January 2019

Learn From the WannaCry Ransomware Attack
Smarter With Gartner, Jonathan Care, May 2017

Polish, Practice and Present

Smarter With Gartner Articles (continued)

The 15-Minute, 7-Slide Security Presentation for Your Board of Directors
Smarter With Gartner, Rob McMillan, August 2018

5 Security Questions Your Board Will Inevitably Ask
Smarter With Gartner, Sam Olyaei, October 2019

Understand Security and Risk Trends

Client Research

Top Security and Risk Management Trends
(February 2020 — ID G00466211)

Rethink Your Approach to Security Talent

Client Research

IT Quarterly: First Quarter 2018
Gartner, CIO Research Team, February 2018

Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage
Tom Scholtz, April 2019

Smarter With Gartner Articles

5 Places You Didn't Think to Look for Digital Talent
Smarter With Gartner, Dion Love, July 2019

Confront the Cybersecurity Talent Shortage
Smarter With Gartner, Sam Olyaei and Matt Stamper, June 2017

Gartner

Learn more.
Dig deep.
Stay ahead.

Free content

Visit Smarter With Gartner

Stay on top of security and risk trends and insights.

The IT Roadmap for Cybersecurity

Follow these best practices to create a resilient, scalable and agile cybersecurity strategy.

Attend conference

Gartner Security & Risk Management Summit

Learn from Gartner experts how to guide your organization to a secure digital future.

Become a client

1 855 307 8858

gartner.com/en/become-a-client