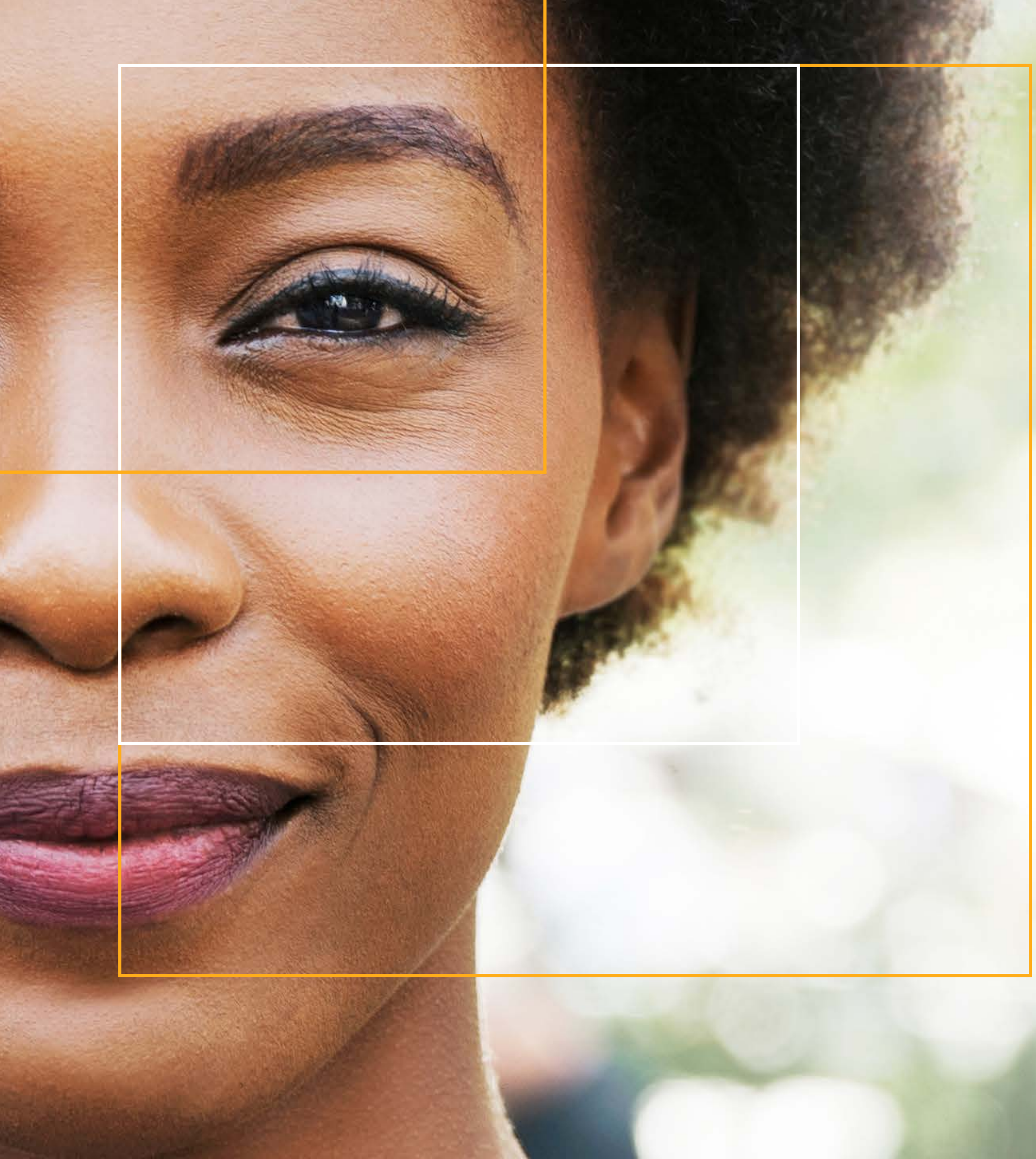


Gartner

Leadership Vision for 2022

Top 3 Strategic Priorities for Security and Risk Management Leaders

From Chris Howard, Chief of Research, Gartner

As we head into 2022, we continue to feel the human toll of the global pandemic, but we already know it has been a watershed period in which attitudes and norms have permanently shifted — in our everyday lives and at work.

Living through COVID-19 has increased social awareness — as have growing demands for equity for those who are underrepresented.

Businesses have also changed. For many organizations, the pandemic has catalyzed digital business initiatives as we adapt to the demands of employees, customers and other stakeholders, who were forced into new digital options that they have now come to favor.

B2B purchasers are happy to buy digitally, without a sales representative; B2C consumers are buying off social media platforms; employees are physically distributed and communicating asynchronously — and IT infrastructures must secure the organization despite this “anytime, anyway, anywhere” way in which we’re operating.

> You and your team may be burning out, and it’s never been more important to prioritize your time and energy.

In your role as a leader, you’ve now spent months adapting to change and delivering new solutions at speed. You and your team may be burning out, and it’s never been more important to prioritize your time and energy. To help with that, Gartner Leadership Vision provides top-level guidance to leaders and their teams on where to focus — based on our data-driven research.

We’re providing detailed insights to our clients across dozens of roles, and we’re now excited to share excerpts with the business community beyond our clients. We hope this will help you to focus discussions with your teams, peers and other leaders, so you can more quickly and effectively diagnose priorities and actions, especially as you solidify your strategic plans for 2022.

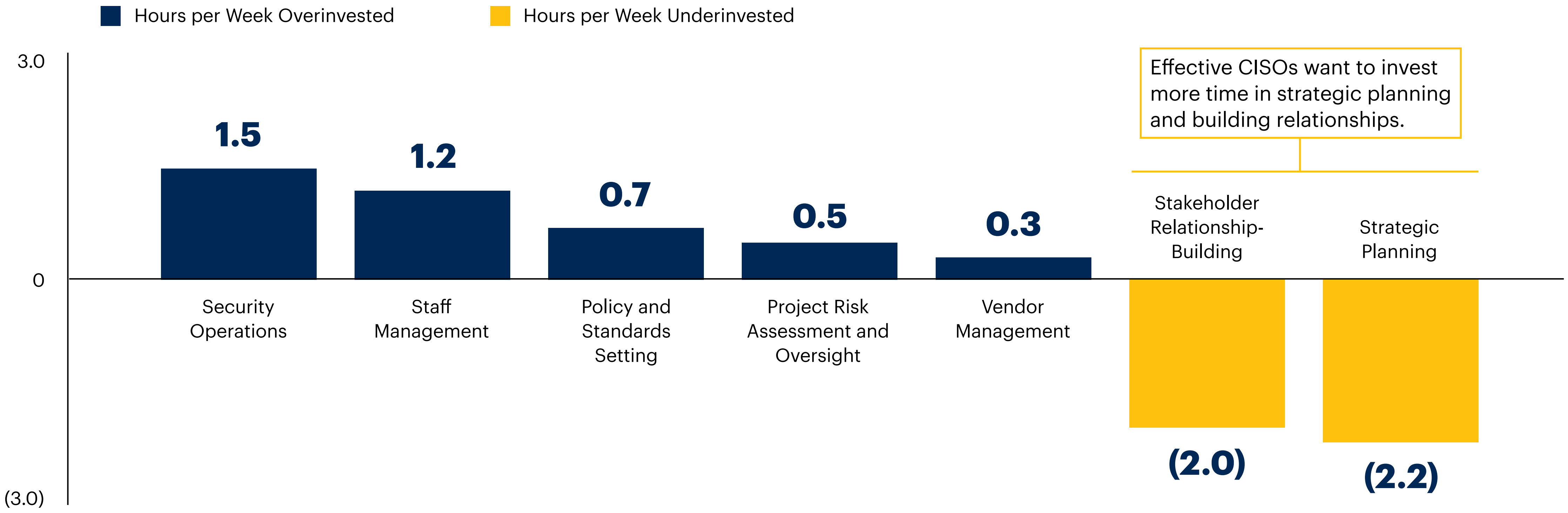
Chris Howard
Chief of Research, Gartner

Job 1: Reframe the Role of the Cybersecurity Leader …

Today, business units and individuals have the ability to make substantial decisions about their digital destiny — which sometimes lead to bad security outcomes. Security and risk management (SRM) leaders are being squeezed between an increasingly aggressive threat environment and the unrealistic expectation that the chief information security officer (CISO) won't ever interfere with business unit computing. Successful CISOs recognize these misconceptions and actively work to change them in 2022 and beyond.

Leadership Misconception	Reframe
"The CISO prevents breaches."	"A leader facilitates risk management."
"Cyber risk is security's problem."	"Cyber risk is a business/ organizational risk."
"Security is a roadblock to speed."	"Security enables agile and secure products."

… And Focus on Adding Value



Effective CISOs want to invest more time in strategic planning and building relationships.

n = 129 CISOs

Source: 2020 Gartner CISO Effectiveness Survey

Three Challenges and Actions for the Security and Risk Management Leader

The loss of control

One in five workers consider themselves digital technology experts since COVID-19. **49%** of “ineffective” CISOs incur unrealistic expectations from stakeholders.

Boards demand value

One in 10 organizations are now creating cybersecurity-specific committees at the board level. Boards identify cybersecurity risk as the second highest source of risk for the enterprise.

A cybersecurity mesh architecture has evolved

If endpoints, digital citizens and IT assets will be located anywhere, then cybersecurity controls need to be able to follow suit.

Actions for the SRM leader

Develop a culture of cyber judgment and align this culture with evolving talent needs.

Prioritize customers and market-facing business relationships and focus on value-generating activities.

Choose cybersecurity technologies that offer high levels of integration, automation and orchestration capabilities.

Source: Gartner

Create Competent Decision Makers Across the Organization

All employees are now citizens in a digital democracy. The security and risk team must equip them with processes and guiderails that encourage them to follow safe paths. Building cyber judgment in this way is a practical risk response to the phenomenon of citizen computing.

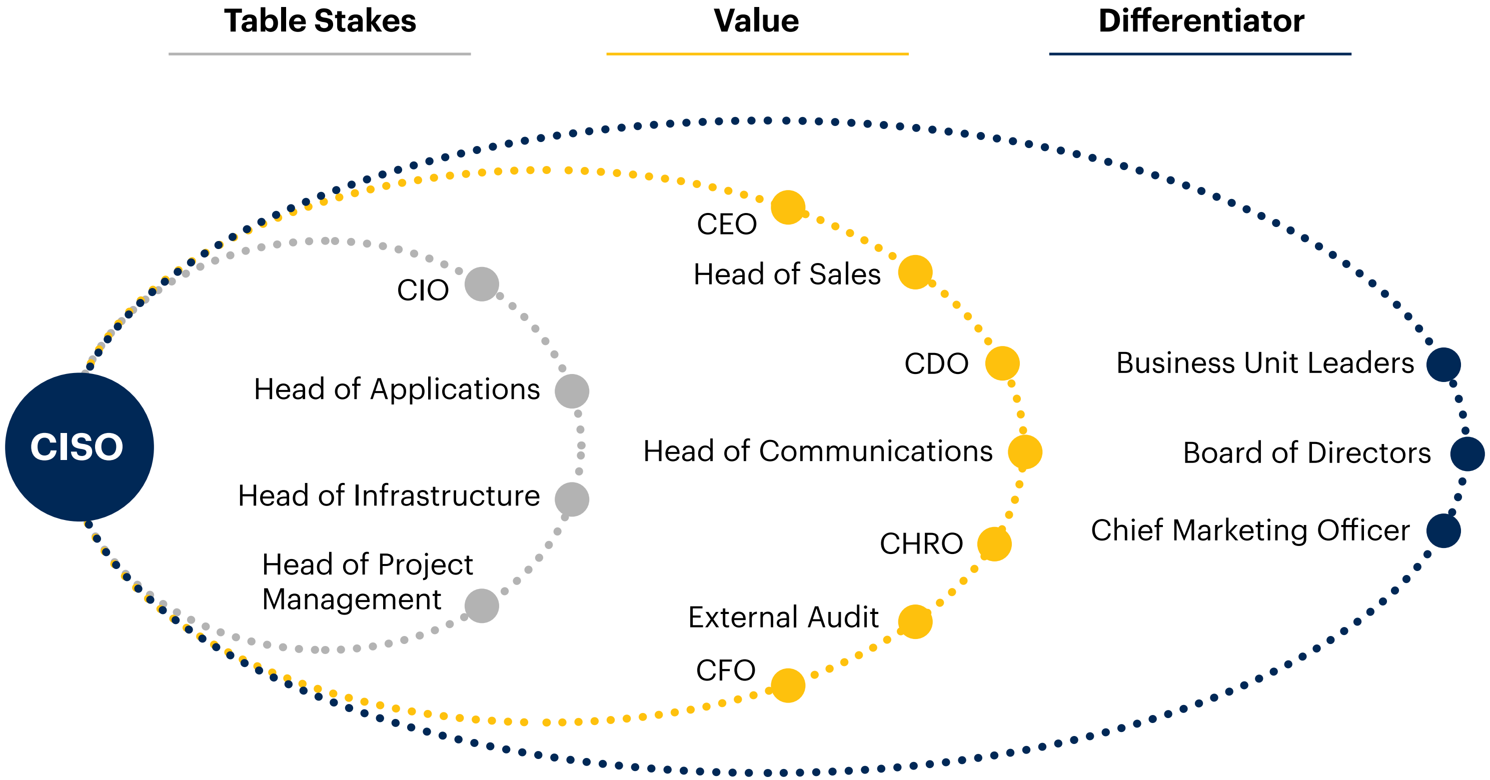
Security Activities	Low Trust	Medium Trust	High Trust
Risk Assessment	Security-led	Self-administered, security reviewed	Self-administered
Control Implementation	Done by security	Controls for high risks are implemented by security	Done by groups
Exception Request	Issued by security	Made independently within a predefined risk range; peer reviewed	Made autonomously within a predefined risk range
Verification	Frequent security reviews	Reviews only in cases of major revision	Self-verification

As digital citizens increasingly demonstrate higher levels of trustability, the need for centralized governance activities decreases.

The ultimate goal of cyber judgment is self-service.

Source: Adapted from client case study

Build Game-Changing Relationships Outside IT



Building relationships with business unit leaders, heads of sales and heads of marketing is key as these are the exact areas where increased technology use is leading to a higher volume and variety of information risk decisions. There is an order of magnitude difference between the number of top- and bottom-performing CISOs who meet with these higher-impact stakeholders on a frequent basis.

Source: Gartner

Prioritize Three to Five Areas With High Business Value

Concentrate on the relatively small number of activities that provide the greatest marginal return on time and resource investment — and make these choices consistent with the reframing of your mission.

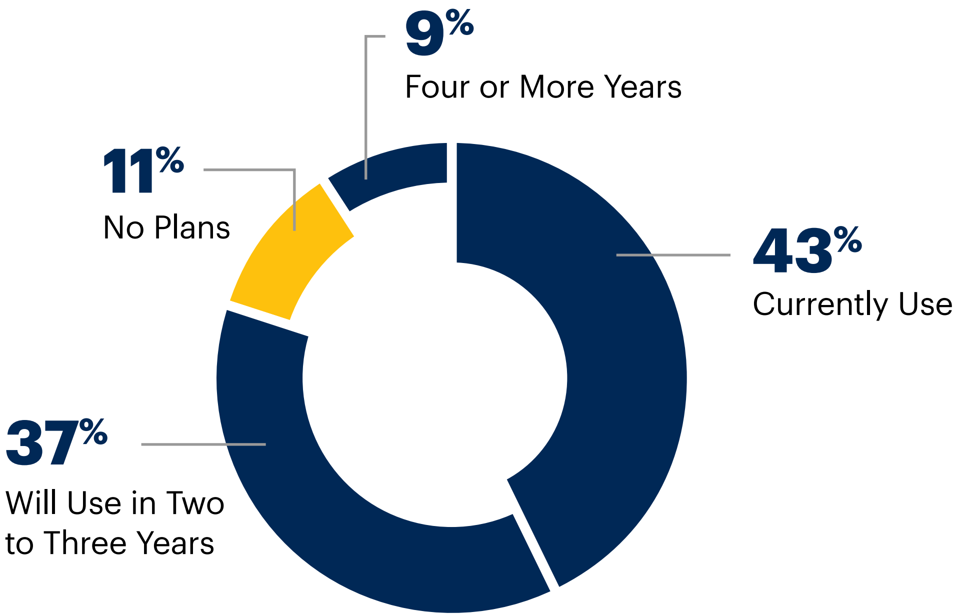
Make it clear to internal customers that you are not there to solve all their problems, but that you will identify and address the significant ones.

Business Value	**Revenue Impact**	**Cost-Efficiency**	**Risk Mitigation**
Top 3 to 5 Value-Impacting IT Services, Applications or Initiatives	Transaction Systems	Productivity	Operational Downtime
	Customer Support	Efficiency	Reputation Loss
	Shopping Cart	Staffing Optimization	Compliance and Audit
	CRM Systems	Asset Optimization	Data and Operational Security
	Order Entry	Service-Level Alignment	Vulnerability Remediation
	Client Support		

Prioritize three to five things you own and control that have the greatest impact on business value priorities.

Source: Gartner

Use Cloud-Delivered Solutions for Scalability, Integration and Automation



80% of organizations surveyed already have or plan to have a cybersecurity product as a service in the next two to three years.

n = 396, all respondents; excluding "don't know"
Q. Are any of your organization's information security products delivered "as a service"?
Source: Gartner 2020 Security & IAM Solution Adoption Trends Survey

Actionable, objective insight

Explore these additional complimentary resources and tools for security leaders:

Tool

Gartner IT Score

Benchmark key processes and activities to advance your function.

Learn More

Tool

Gartner BuySmart™

Reduce costs, avoid pitfalls and buy technology with confidence.

Learn More

Roadmap

The Roadmap for Maturing Information Security

Build a mature program to mitigate cybersecurity risk effectively.

Download Now

eBook

3 Steps to Stop Employees From Taking Cyber Bait

Bring cyber awareness to your employees to manage risks.

Download Now

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

Get More.

Get actionable, objective insight to deliver on your most 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 in 🐦 ▶

Gartner®