Gartner®

Four Facets of Effective CISO Leadership

How best-in-class cybersecurity leaders tackle their expanding remit

Effective CISOs play a multifaceted role

The role of the chief information security officer (CISO) is growing in size and scope as business demands intensify.

Digitalization continues apace. Among board directors, 64% say their organization is trying to significantly alter its economic architecture to put more emphasis on digital (revenues, margins, productivity, etc.). At the same time, 88% say they recognize cybersecurity is a risk to the business.

Best-in-class cybersecurity leaders focus squarely on protecting and enabling enterprise priorities. But to do that, they need a range of capabilities and competencies to be effective in their increasingly multifaceted role.

Compared to less effective CISOs, top performers prioritize conversations with different stakeholders, flag future risks more aggressively, pursue more future-forward talent strategies and maintain stricter boundaries between work and personal time.

This quick guide to effective CISO behaviors and mindsets helps security leaders understand the need for certain competencies and stay alert to what they may lack — a critical first step in formally evaluating their skills and capabilities and plotting a path to even greater effectiveness.

CISO effectiveness means delivering on four critical outcomes

Functional Leadership

Effective team leadership in meeting functional objectives, such as:

- Functional performance outpaces peers
- Staff adapts to enterprise change
- Functional performance satisfies the C-suite

Information Security Service Delivery

Effective delivery of quality services in supporting business objectives, such as the function meets:

- Service delivery timelines
- Project timelines
- Service quality standards

Leadership Habits of Effective CISOs

Enterprise Responsiveness

Ability to sensitize the enterprise to the role and importance of information security — for example, employees:

- Meet the information security baseline
- Limit policy deviations
- Make informed, independent risk decisions

Scaled Governance

Ability to increase cooperation with information security recommendations, such as:

- Information risk influences enterprise-level decisions
- Decision makers involve information security in enterprise-level decisions
- Information security advice balances security and business objectives

The research included a quantitative survey (2020 Gartner CISO Effectiveness Survey [n = 129 CISOs]) and dozens of CISO interviews. It deployed an Effectiveness Index developed from 60 behaviors, mindsets, traits and organizational factors and gap analysis between top and bottom thirds of the sample. The research is continually reviewed for updates and is the basis for all quantitative data in this guide.

The cost of CISO ineffectiveness is steep

Only 12% of CISOs execute against all four key outcomes, but the Gartner CISO Effectiveness Index reveals a range of negative organizational and personal outcomes among poorer-performing CISOs.

Critical Costs of CISO Ineffectiveness: Examples

Negative impacts felt by the organization	• Increased number of security incidents that cause business disruption • Project delays that impact business goals
Negative impacts felt by the CISO as an executive	• Overloaded with security alerts • Poor work-life balance

Effective CISOs require multiple capabilities

Gartner research found 14 controllable variables positively correlated with CISO effectiveness. These variables fall into four categories of behaviors and mindsets that differentiate effective CISOs from their lower-performing peers.

We refer to these categories as "facets" of effective CISOs.

Security leaders must understand what it means to excel in each of these role dimensions (see pages 6 – 9) to plot a path to greater effectiveness.

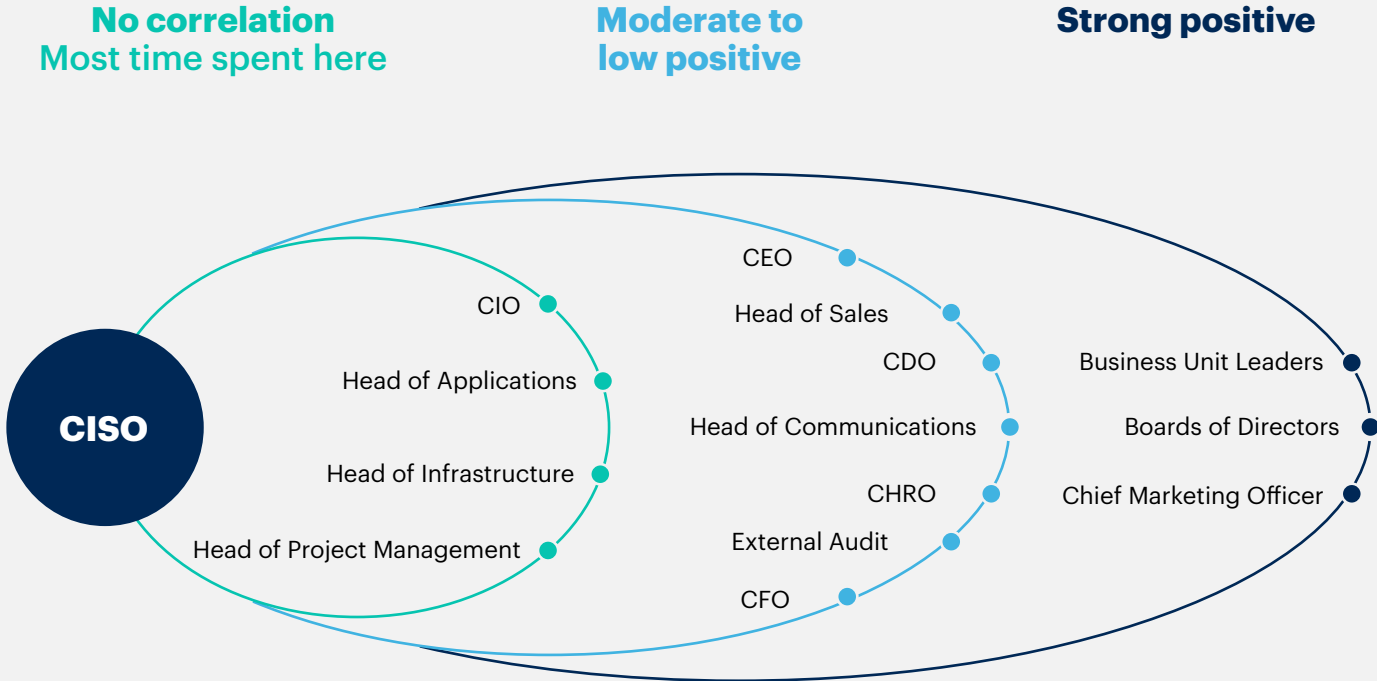You cannot achieve success on all facets at once. Focus on one at a time.

Four Facets of the Effective CISO

Executive Influencer

Future-Risk Manager

Effective CISO

Stress Navigator

Workforce Architect

How to be an executive influencer

Effective CISOs:

- Make it a point to regularly interact with executives outside of corporate IT

- Recognize the influence of non-IT executives on the effectiveness of the security function

- Seek to nurture meaningful relationships with these executives outside of individual projects

- Align with non-IT executives on risk appetites, and influence enterprise-level decisions by clarifying information risk trade-offs

Spend more time in the sphere that drives the most influence

No correlation
Most time spent here

Moderate to low positive

Strong positive

CISO

CIO

Head of Applications

Head of Infrastructure

Head of Project Management

CEO

Head of Sales

CDO

Head of Communications

CHRO

External Audit

CFO

Business Unit Leaders

Boards of Directors

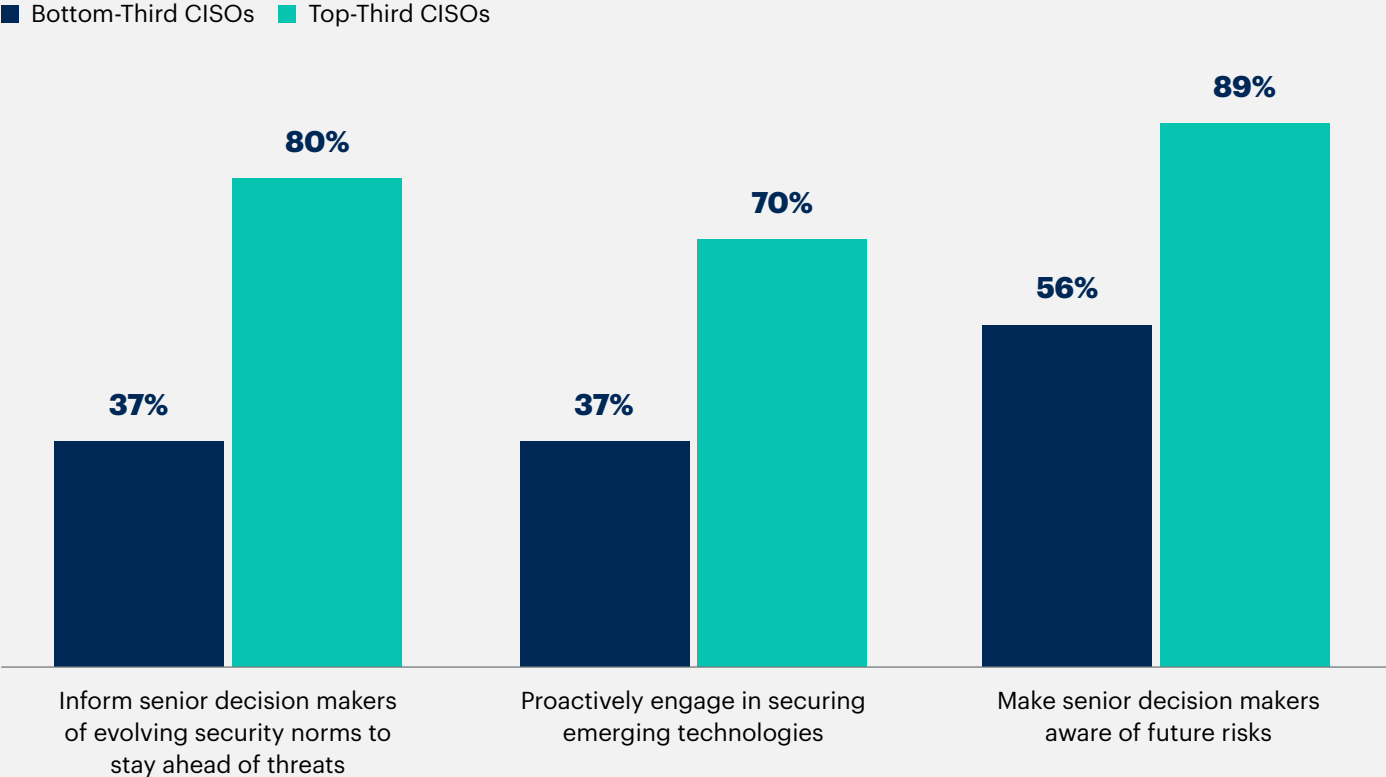Chief Marketing Officer

Source: Gartner

How to be a future-risk manager

Effective CISOs:

- Position information risk management as an accelerator of emerging technology adoption in the organization

- Inform senior decision makers of new security norms and technologies

- Make senior decision makers aware of future risks

- Develop automation strategies to prepare the organization

Future-risk focus of top-third vs. bottom-third CISOs

■ Bottom-Third CISOs　■ Top-Third CISOs

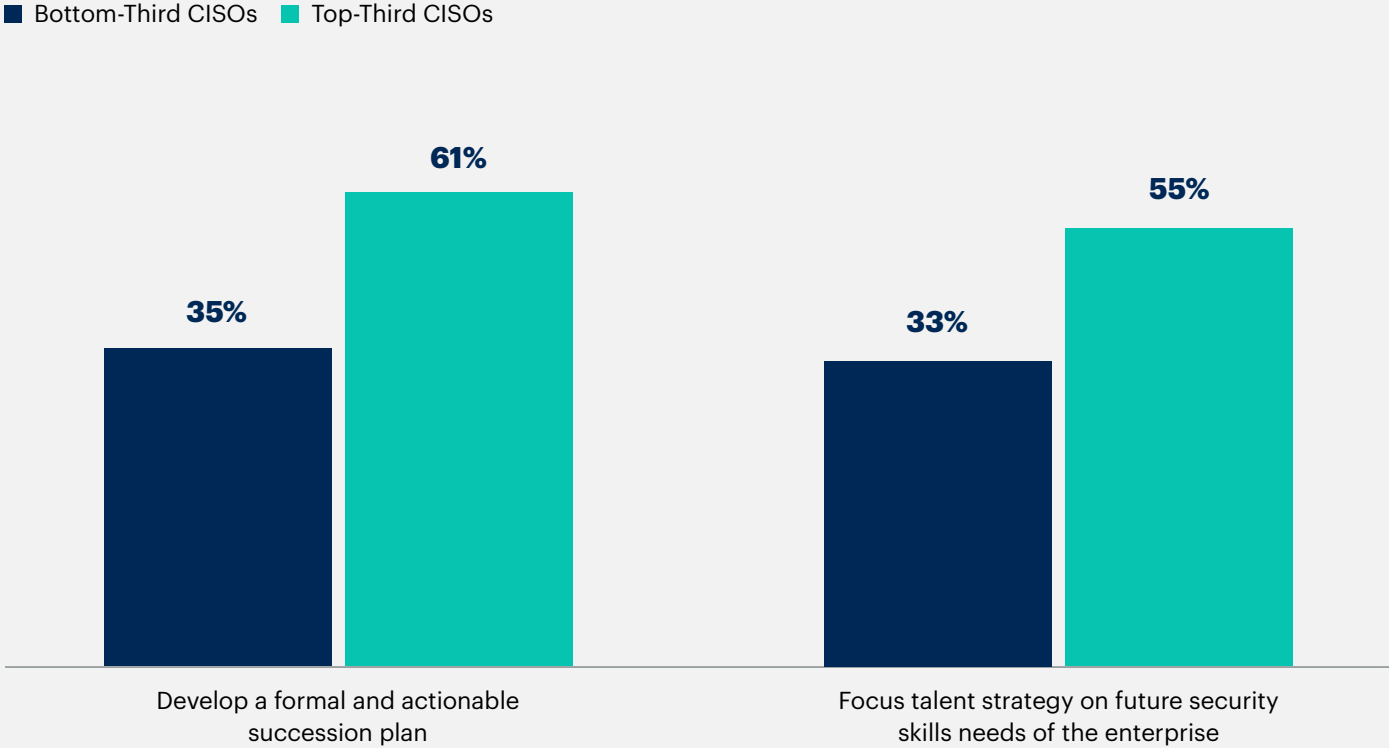|	Inform senior decision makers of evolving security norms to stay ahead of threats	Proactively engage in securing emerging technologies	Make senior decision makers aware of future risks
Bottom-Third CISOs	37%	37%	56%
Top-Third CISOs	80%	70%	89%

n = 129 CISOs
Source: Gartner

How to be a workforce architect

Effective CISOs:

- Have a future-focused talent strategy to meet the rising skills needs of the enterprise

- Increase the output and effectiveness of their existing staff by:

  – Upskilling cybersecurity staff on business competencies

  – Leveraging noncybersecurity staff creatively

  – Developing a formal, actionable CISO succession plan

Workforce architect approach by top-third vs. bottom-third CISOs

■ Bottom-Third CISOs ■ Top-Third CISOs

Develop a formal and actionable succession plan: Bottom-Third 35%, Top-Third 61%

Focus talent strategy on future security skills needs of the enterprise: Bottom-Third 33%, Top-Third 55%

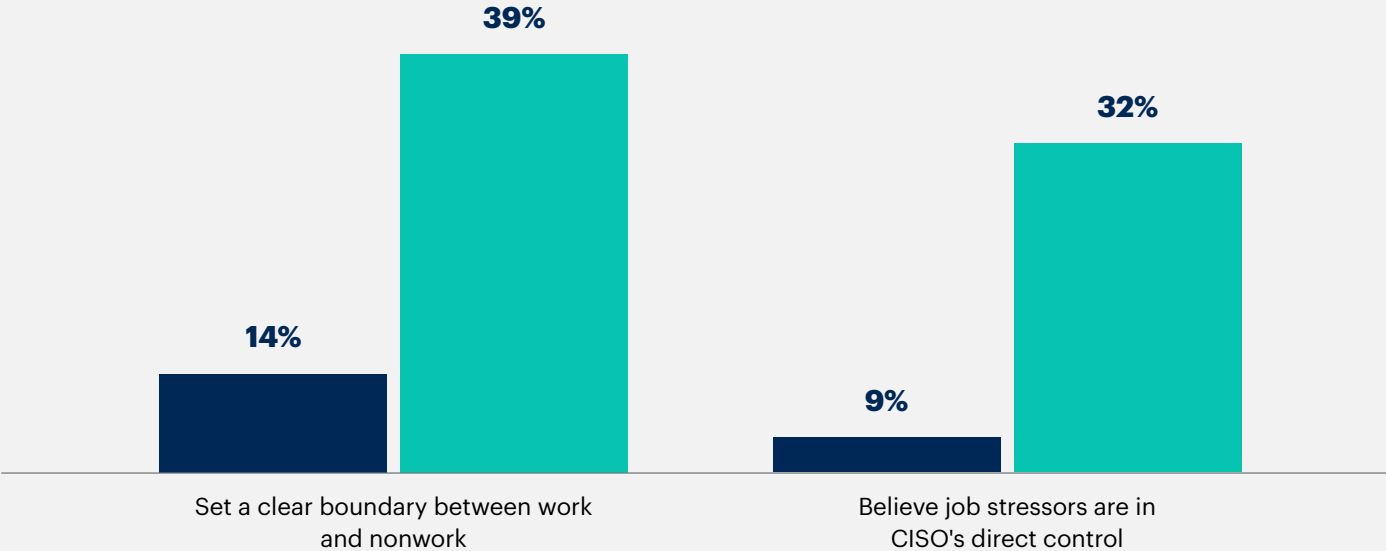n = 129 CISOs
Source: Gartner

How to be a stress navigator

Effective CISOs:

- View their well-being as a critical performance driver

- Maintain rigid boundaries between their working hours and their personal time

- Proactively manage their calendars

- Define their responsibilities from the onset of their work

- Routinely evaluate whether the projects they are involving themselves in are within scope

Stress navigator approach by top-third vs. bottom-third CISOs

■ Bottom-Third CISOs ■ Top-Third CISOs
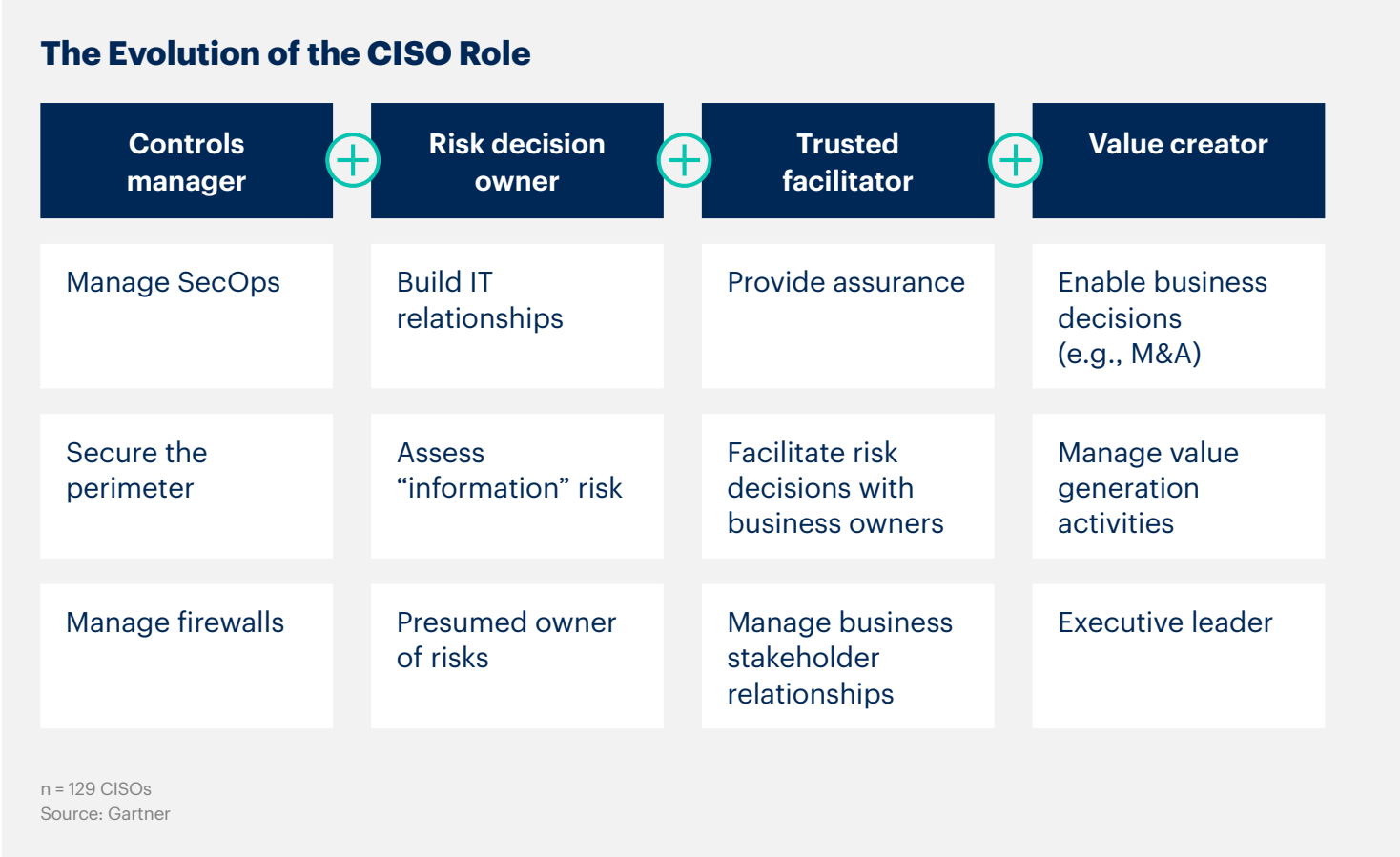
Working more hours per week negatively correlates with effectiveness.

39%

32%

14%

9%

Set a clear boundary between work and nonwork

Believe job stressors are in CISO's direct control

n = 129 CISOs
Source: Gartner

What's next for CISOs? Staying ahead of the curve.

✓ Identify gaps in traits, behaviors and soft skills that will enable you to be more effective in your role.

✓ Focus on the future of your role by balancing your need to fight immediate fires vs. proactive risk decisions.

✓ Establish more-regular relationships with stakeholders that will influence your ability to become a trusted partner.

✓ Balance and reallocate your time toward activities that encourage business participation and decision making.

✓ Keep benchmarks as useful data points, but make sure your risk appetite, value management and cost optimization initiatives are what drive your decision-making process.

The Evolution of the CISO Role

Controls manager		Risk decision owner		Trusted facilitator		Value creator
Manage SecOps	+	Build IT relationships	+	Provide assurance	+	Enable business decisions (e.g., M&A)
Secure the perimeter		Assess "information" risk		Facilitate risk decisions with business owners		Manage value generation activities
Manage firewalls		Presumed owner of risks		Manage business stakeholder relationships		Executive leader

n = 129 CISOs
Source: Gartner

Actionable, objective insight

Explore these additional complimentary resources and tools
for security and risk leaders:

Research

Drive Urgency to Treat
Cybersecurity as a Business
Decision

Consider the risks, priorities and investments
that impact business outcomes.

Download Now

Research

How to Prepare for
Ransomware Attacks

Prepare for the security challenges
organizations are facing today.

Download Research

Webinar

Identify and Embrace New Collar
Workers to Boost Cybersecurity

Explore nontraditional education
forums that provide training.

Watch Now

Roadmap

Protect Your Business Assets
With a Roadmap for Maturing
Information Security

Adapt your security program to meet
new landscape threats.

Download Roadmap

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 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

Gartner