The Key Drivers for an Effective Security and Risk Leader

Sam Olyaei

Gartner®

Why are we here?

Disengaged

Benchmarking = Decisions

Too Technical

Compliance Driven

Protector / Cost Center

Gartner

Feedback — The Business View

“As much as they talk to us, I don’t feel like they really understand **MY** business.”	**Insurance BU Head**
“All my CISO does is come to us once a quarter and tell us she needs more money, more people, more tools. Why?”	**Healthcare CEO**
“We know we should care about cybersecurity. But when the CISO leaves the board meeting, I don’t feel like I know anything new. I don’t feel it.”	**Multifirm Board Member**

Feedback — the SRM view

“I do not trust my business leaders with any security decisions...”	**CISO – EU**
“My board of directors just want to sign off on a piece of paper that says they talked to me.”	**CISO – Finance**
“My effectiveness is measured based on compliance with NIST CSF”	**CISO – Govt.**

Gartner

Status Quo is Fraught With Difficulty

"Always On" Mindset	"I'm constantly checking what's going on, even when I'm not at work. Maybe it's an occupational hazard." CISO, Insurance
Poor Time Allocation	"I need to be spending time with non-IT stakeholders. Right now 95% of my time is spent in IT." CISO, Government
Misaligned Expectations	"If something goes wrong, I'm on the line." CISO, Healthcare
Struggle to Pace Business Speed	"No matter how fast you run, it won't be fast enough [to keep up with the business]." CISO, Insurance

We will cover three key issues

What makes an Effective CISO?

What opportunities and obstacles will you face on your “effectiveness” journey?

What does the future of the role look like?

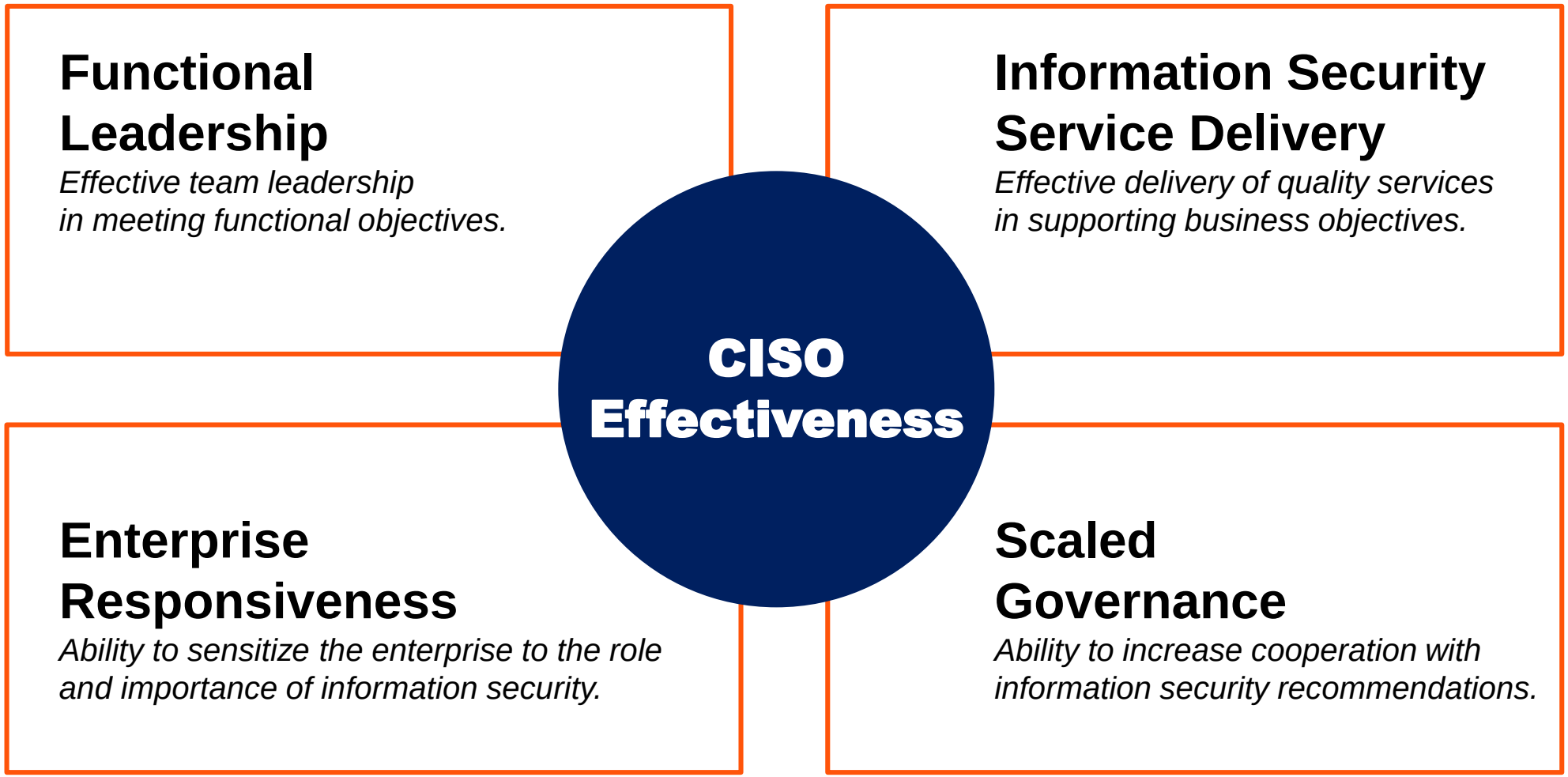
Gartner

Introducing Gartner's CISO Effectiveness Index

We analyzed data from 129 CISOs to understand what distinguishes the most effective CISOs from their peers.

Gartner

CISO Effectiveness, Defined



Source: Gartner 2020 CISO Effectiveness Survey

Result : Only a Few CISOs excel in every category

Prevalence of CISOs Exceeding Expectations of Peers in Effectiveness Category

Percentage of Respondents

Only 12% of CISOs are able to exceed expectations of peers in all four areas.

N=129 CISOs

Source: Gartner 2020 CISO Effectiveness Survey

The Costs of Ineffectiveness

Experience increase in security incidents that cause business disruption

Experience project delays that impact business goals

Feel overloaded with security alerts

Poor Work-life Balance

Selected negative organizational and personal outcomes, comparison of top 3rd and bottom 3rd CISOs in the Gartner CISO Effectiveness Index

N=129 CISOs

Source: Gartner 2020 CISO Effectiveness Survey

Gartner

Defining your Personal Effectiveness

Gartner

Four Facets of Effective CISOs

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

Executive Influencer — Top Differentiators

1 Executive Influencer

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

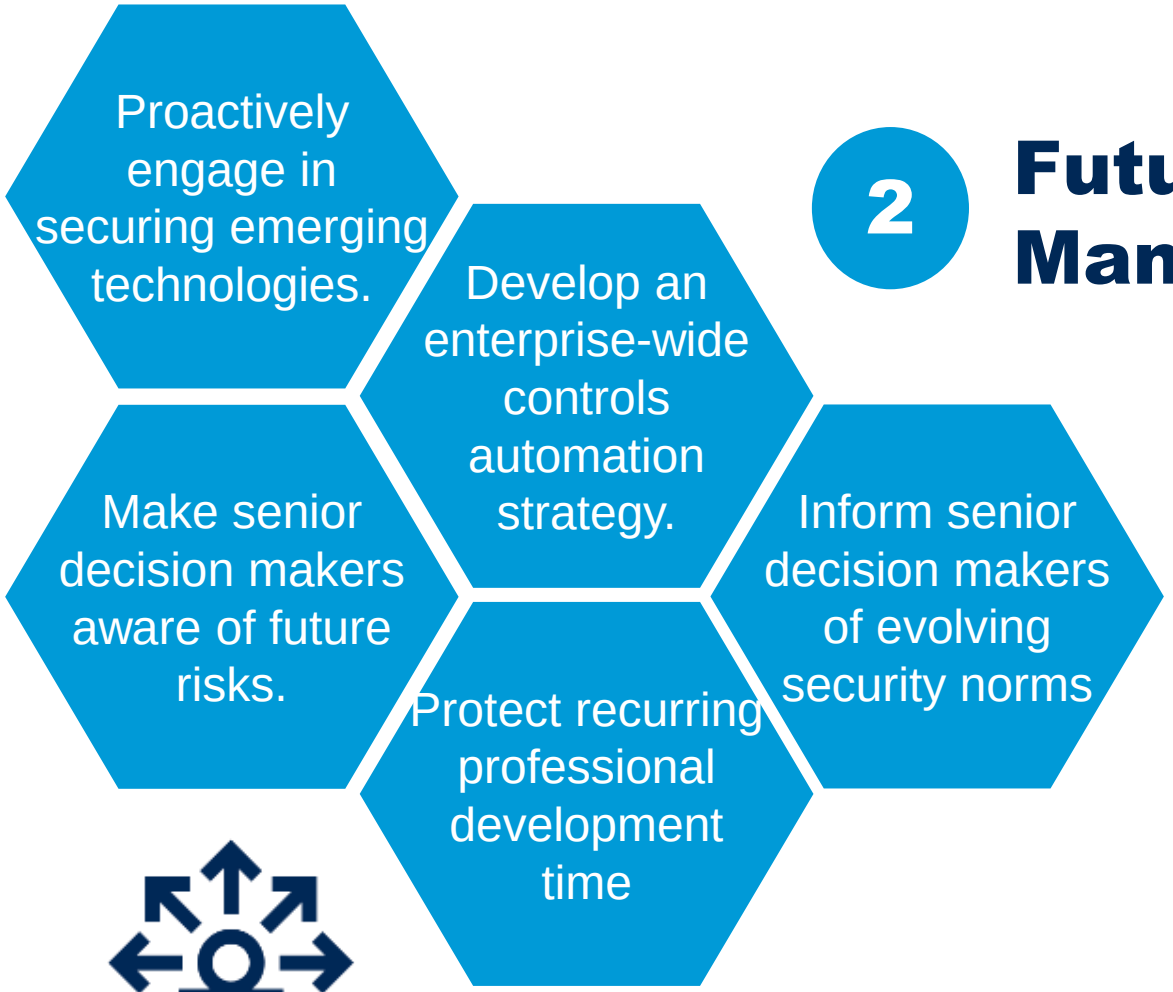
“Relentless incrementalism is the antidote to complacency.”

“Someone in [a leadership role] is that they’re self-actuated, constantly working on how to become more effective individually and, more importantly, how they’re leading their part of the organization.”

Executive Influencer – Omar Khawaja

Gartner

Future-Risk Manager — Top Differentiators



2 Future-Risk Manager

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

“It’s okay if they [the business] want to accept a risk, but do they know what that means?”

“It’s not about me, it’s about what the business wants me to do.”

“When I started here, I thought my biggest job was to secure the details of our products, our IP. But the main thing for us is continuity and limiting down time at the factories.”

Trusted Partner on Information Risk – Todd Bearman

Gartner

Workforce Architect — Top Differentiators

Effective CISO

Develop a formal and actionable succession plan.

Focus talent strategy on future security skills needs of the enterprise.

3 Workforce Architect

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

“A CISO is only as good as the team they surround themselves with”

“Ask yourself: How many potential CISOs have you helped create in your organization?”

“At every organization I’ve left, I’ve trained my successor”

Workforce Architect – Christopher Blake

Gartner

Stress Navigator — Top Differentiators

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

“Mindful Leadership: How important mindfulness and taking care of yourself is to how you show up at work. Its how I got through the breach. I showed up to my yoga classes, I ate right, the whole thing.”

Stress and Fatigue Manager – Sarah Engstrom

Gartner

You cannot achieve all of this overnight — focus on one facet at a time

1 **Executive Influencer**

2 **Future-Risk Manager**

3 **Workforce Architect**

4 **Stress Navigator**

N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Gartner

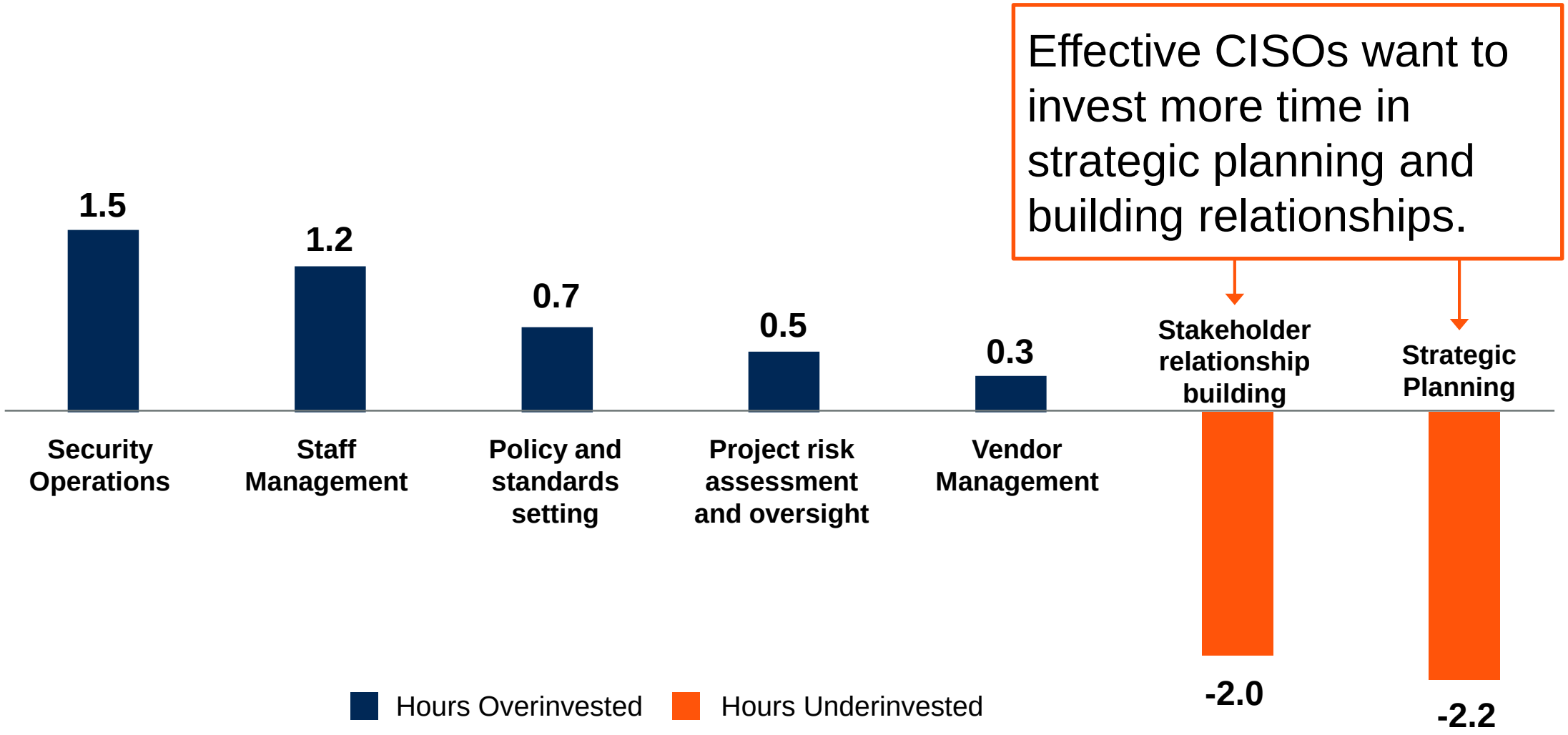
Common Obstacles That Prevent CISOs from Being "Effective"

Gartner

How many of you spend most of your time on day-day operational activities and staff management?

Gartner

Balancing your time is key to Effectiveness

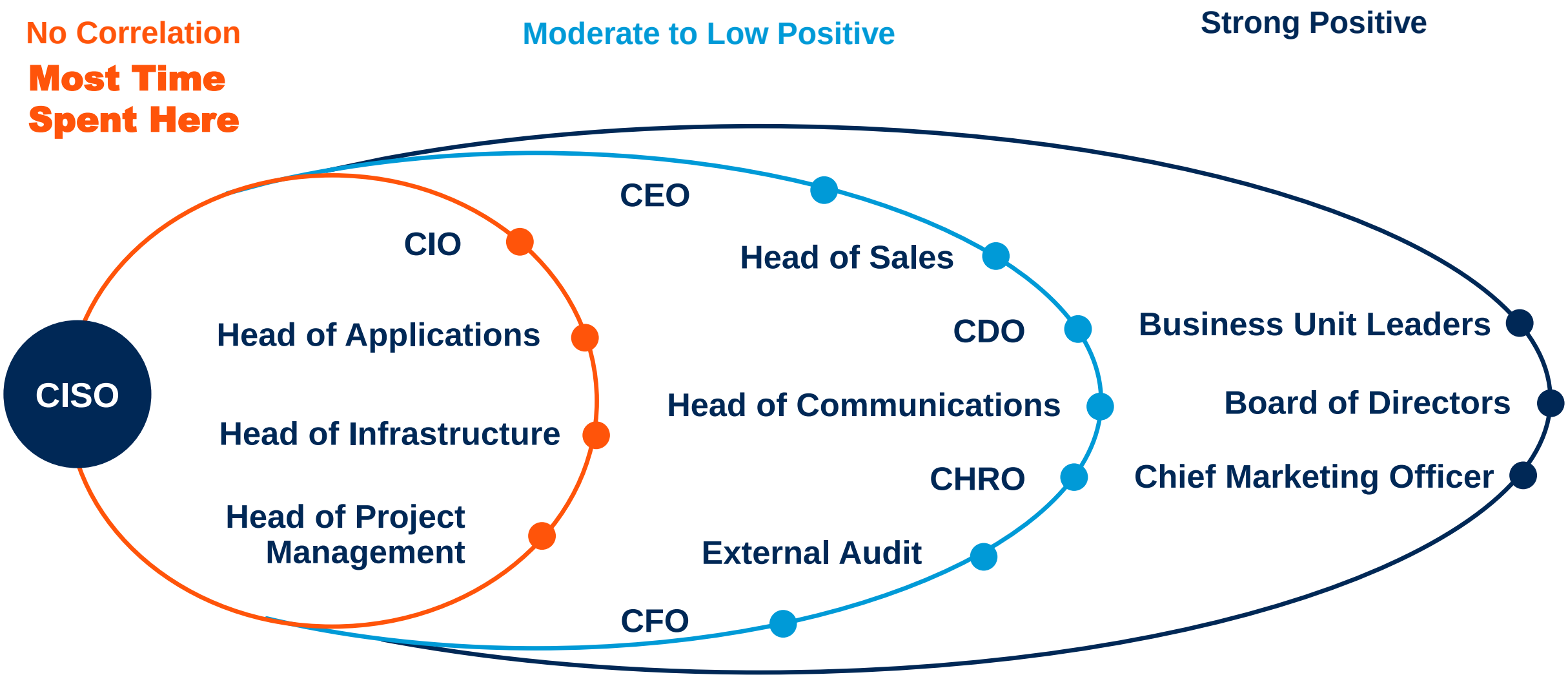


N=129 CISOs
Source: Gartner 2020 CISO Effectiveness Survey

Which stakeholder is most critical to your effectiveness?

Gartner

Which Relationships Matter Most?



Gartner

How many of you work 50+ hours a week?

Gartner

Many of the Usual Suspects Debunked

- ⊗ Work greater number of hours
- ⊗ Have more years of IT experience
- ⊗ Have more certifications
- ⊗ Work in a larger organization
- ⊗ Have an optimal reporting structure

Most characteristics associated with effectiveness are **myths.**

- ✓ Have more years of experience in current role
- ✓ Have more years of experience in current industry
- ✓ Work in an industry with high regulatory/risk burden

Top 3 characteristics are associated with effectiveness.

Gartner

Future of the CISO Role?

Gartner

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 (ex.M&A)
Secure the Perimeter	Assess “Information” Risk	Facilitate Risk Decisions w/ Business Owners	Manage Value Generation Activities
Manage Firewalls	Presumed Owner of Risk	Manage Business Stakeholder Relationships	Executive Leader

In 2016, we said:

By 2020, 30% of large enterprises will have a digital risk officer (DRO) or equivalent role that addresses IT, operational technology (OT), Internet of Things (IoT) and technology-related safety risks.

Gartner

We are getting there….

50%	of CISOs expect to have a greater set of responsibilities
54%	of CISOs expect their roles to move away from oversight over tactical processes such as SecOps to business-oriented processes that involve enterprise-risk stakeholders.
40%	of CISOs expect their span of control to expand beyond “information security”

But… One Role (CISO) Cannot Do It All

By 2021, **30% of security programs** will incorporate at least two new roles due to new risks in digital ecosystems.

Not all may be in the security team.

New Roles for Cybersecurity?

Chief of Staff for Security

Cloud Security Architect

Business Liaison

Security Ombudsman

Data Security Scientist

Digital Ecosystem Manager

And More …

Gartner

Stay ahead of the curve:

- ✓ Identify gaps in behavior 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 against proactive risk decisions
- ✓ Establish more regular relationships with stakeholders that will influence your ability to become a trusted partner
- ✓ Balance and reallocate your time towards activities that encourage business participation and decision making
- ✓ Benchmarks are useful data points – but your risk appetite, value management and cost optimization initiatives are what drive your decision making process.

Recommended Gartner Research

- **CISO Effectiveness: A Report on the Behaviors and Mindsets That Impact CISO Effectiveness**
  Information Risk Research Team (G00728433)
- **Optimize Risk, Value and Cost in Cybersecurity and Technology Risk**
  Paul Proctor (G00466056)
- **The Urgency to Treat Cybersecurity as a Business Decision**
  Paul Proctor (G00466055)
- **New Security Roles Emerge as Digital Ecosystems Take Over**
  Sam Olyaei (G00347561)
- **Cyber Judgment: Navigating the Era of Distributed Risk Decision Making**
  Information Risk Research Team (G00711001)

For information, please contact your Gartner representative.

Gartner

Appendix

Respondent Profile

Percentage of Respondents by Revenue (USD)

Less than $1 Billion	5%
$1 billion - $2.9 billion	22%
$3 billion - $4.9 billion	19%
$5 billion - $9.9 billion	14%
$10 billion - $20 billion	19%
More than $20 billion	18%
Private enterprise, gov. /not-for profit	2%

Percentage of Respondents by Security Employees

1 to 19 employees	32%
20 to 49 employees	28%
50 to 99 employees	15%
100 to 249 employees	14%
250 or more employees	12%

Percentage of Respondents by Enterprise Employees

500 to 999 employees	2%
1,000 to 2,499 employees	11%
2,500 to 4,999 employees	16%
5,000 to 9,999 employees	20%
10,000 or more employees	51%

N=129 CISOs
Note: Totals may not sum to 100% due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Respondent Profile

Percentage of Respondents by Region

North America	82%
EMEA	11%
APAC	7%

Percentage of Respondents by Risk Environment

Operational Focus	5%
Process Focus	12%
IP Protection Focus	40%
High Security and Regulatory Burden	43%

Percentage of Respondents by Industry

Financial Services	17%
Healthcare Providers	9%
Insurance	9%
Energy	6%
Manufacturing	6%
Pharmaceuticals, Biotechnology & Life Sciences	6%
Retail	6%
Education	5%
Information Technology	5%
Services (Business & Consumer)	5%
Construction	4%
Transportation	4%
Government	2%
Utilities	2%
Media	2%
Wholesale	2%
Agriculture	1%
Natural Resources	1%
Nonprofit/Charity and NGO	1%
Real Estate	1%
Telecommunications	1%
Other	7%

N=129 CISOs
Note: Totals may not sum to 100% due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Respondent Profile

Percentage of Respondents by CISO Direct Manager

CIO	64%
Head of Operations	7%
Head of Risk	7%
Board of Directors & CEO	6%
Head of Legal/General Counsel	3%
Chief Financial Officer	2%
Chief Privacy Officer	2%
Other	8%

Percentage of Respondents by Reporting Function

Corporate or Business Unit IT	56%
Security	12%
Corporate Strategy	9%
Data Privacy	9%
Enterprise Risk Management	5%
Legal	3%
Operations	2%
Finance/Accounting	1%
Other	3%

Percentage of Respondents by Span of Ownership

Enterprise-wide Security Ownership	88%
Regional-level Security Ownership	12%

N=129 CISOs
Note: Totals may not sum to 100% due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Respondent Profile

Percentage of Respondents by Experience within IT

Up to 5 years	2%
6-10 years	8%
11-15 years	5%
16-20 years	33%
21-25 years	26%
Greater than 25 years	26%

Percentage of Respondents by Experience in Enterprise's Industry

Up to 5 years	20%
6-10 years	23%
11-15 years	17%
16-20 years	14%
21-25 years	14%
Greater than 25 years	12%

Percentage of Respondents by Tenure in Current Role and Enterprise

Up to 2 years	34%
3-5 years	38%
6-10 years	20%
Greater than 10 years	8%

N=129 CISOs
Note: Totals may not sum to 100% due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Respondent Profile

Percentage of Respondents by Age

Up to 40	14%
41 to 55	66%
56 or more	20%

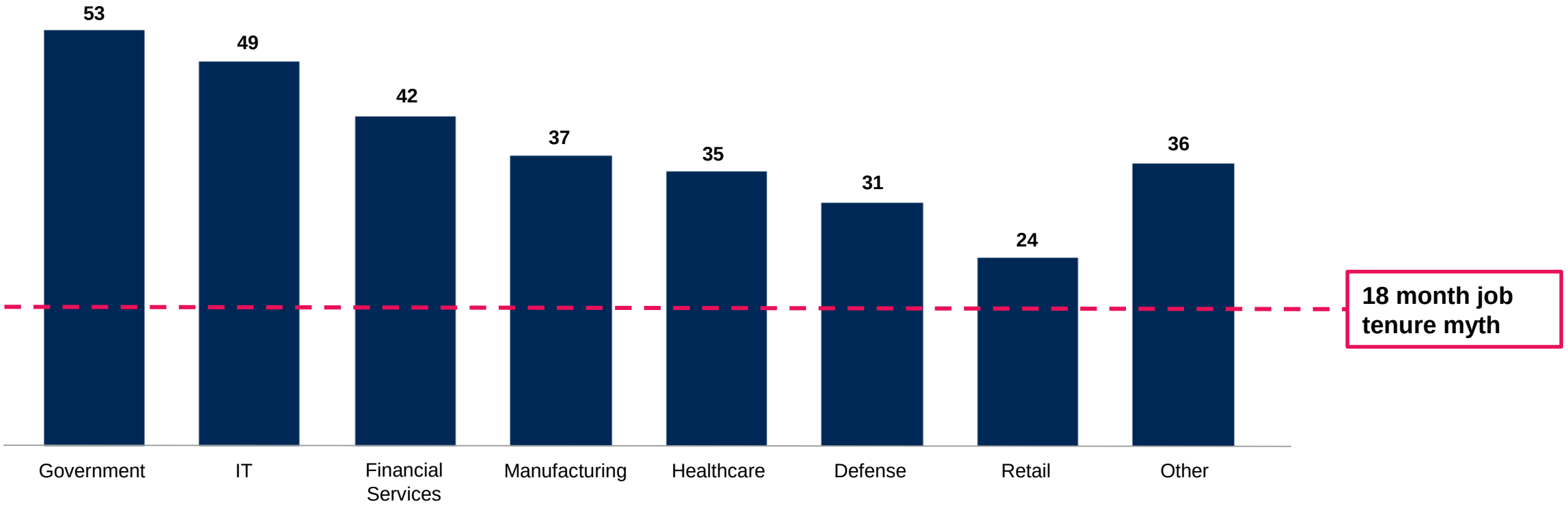
Percentage of Respondents by Gender

Male	81%
Female	17%
Non-binary	1%
Prefer not to answer	1%

N=129 CISOs
Note: Totals may not sum to 100% due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Job Tenure Not Affected by Breaches

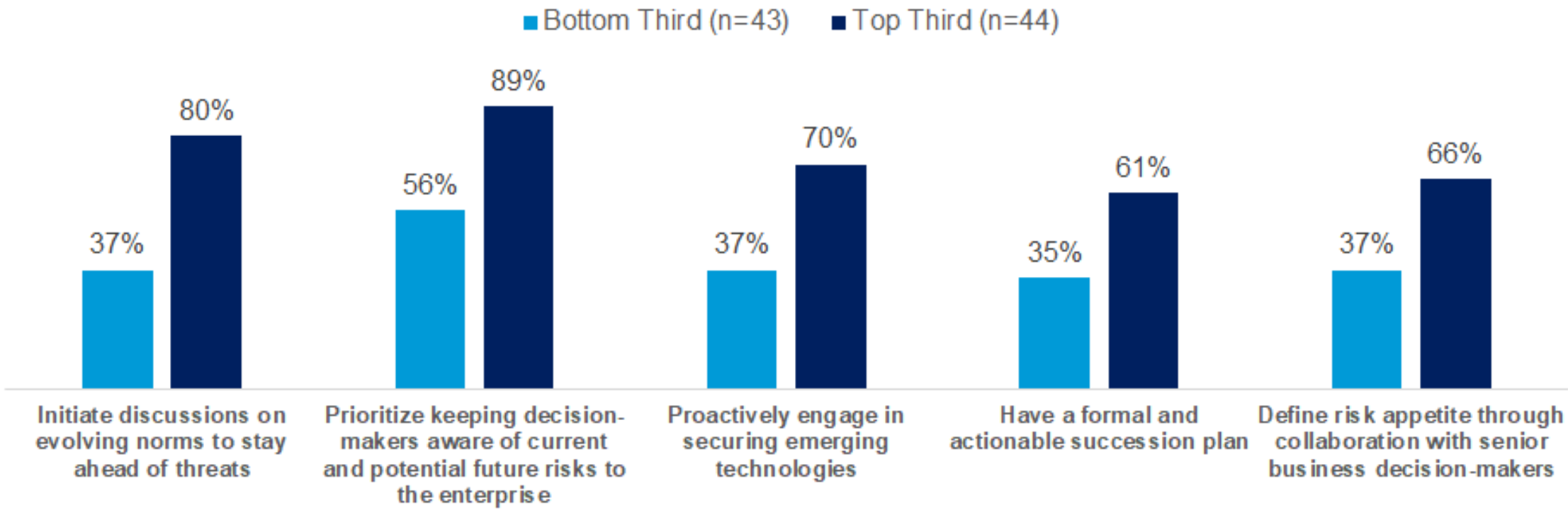
Length of CISO Job Tenure by Industry
Analysis of LinkedIn CISO Profiles



N=150 LinkedIn CISO Profiles
Source: Gartner Research Note, *Do Breaches Really Shorten a CISOs Tenure?*

Top Five Game-Changing Characteristics

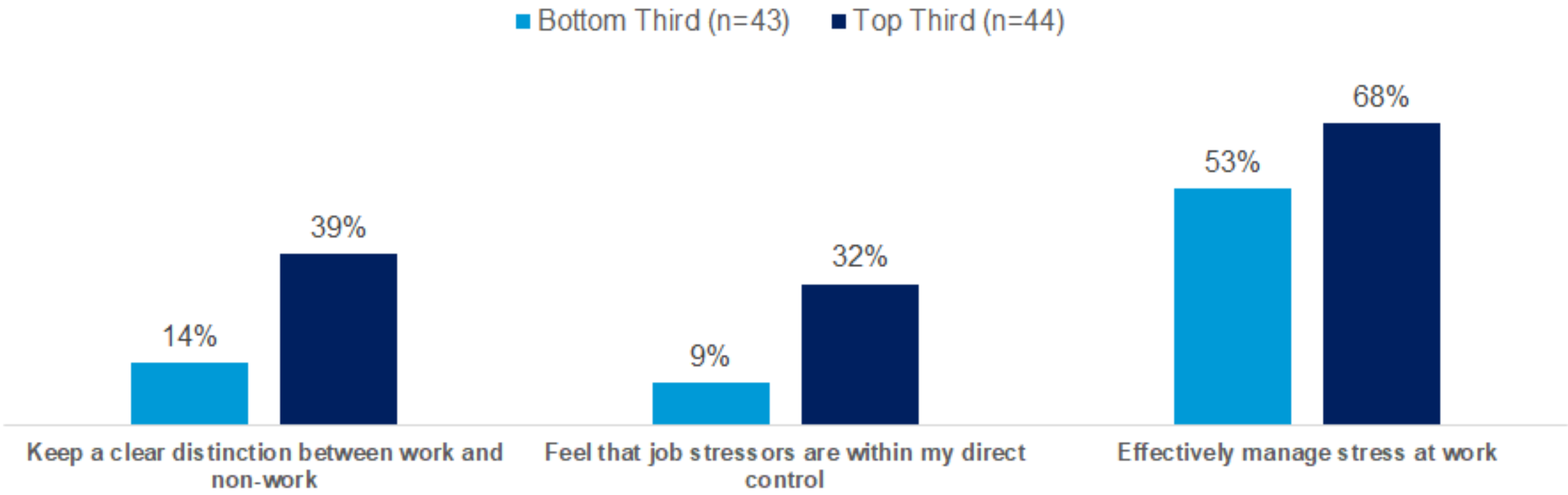
Prevalence of Behaviors Among CISOs by Performance
Percentage of Top & Bottom Third Performers Exhibiting Each Behavior



N=129 CISOs
Note: Percentage point difference may be slightly different from the gap between the top and bottom third due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Effective CISOs Better Manage Stress

Prevalence of Behaviors Among CISOs by Performance
Percentage of Bottom Third & Top Third Performers Exhibiting Each Behavior



N=129 CISOs
Note: Percentage point difference may be slightly different from the gap between the top and bottom third due to rounding.
Source: Gartner 2020 CISO Effectiveness Survey

Other interesting findings

>50	More than half of the top performers have greater than fifty employees in their security function.
>2/3	More than two thirds of top performers have somewhere between 16-45 security “tools” in their portfolio.
62%	of CISOs reported business disruptions due to security incidents at either the same or higher proportion than 2018
1/3	of CISOs do not trust their staff to engage “independently” with the business
250K	Almost half of the CISOs report an annual compensation package of over $250K!

None Of These Have Any Correlation To Effectiveness!

Gartner