IANS

IANS Executive Competencies:

Research Report

Table of Contents

Executive Summary

As the importance of infosec grows, so, too, do expectations for infosec leaders. Increasingly, organizations want them to work closely with business functions. On their end, infosec leaders want to be more plugged into the business and be influential when doing so.

This trend raises a new set of questions with infosec leaders:

- **What skills do they need to be more aligned with the business?**
- **What type of leadership roles can they grow into?**
- **What are their individual areas of development?**

To find answers to these questions, IANS launched a research project. We interviewed influential CISOs and executive search professionals who specialize in CISO placement. The findings allowed us to build an infosec-specific competencies framework that lays out the most important existing and upcoming competencies for infosec leaders.

In addition, the research distinguished five infosec leader types. Lastly, the research findings allowed us to develop an assessment tool that evaluates the skill set of individual leaders. We fielded this tool with CISOs and analyzed the results. This report presents findings in each of these areas.

The Infosec Executive Competencies Framework

Three types of competencies matter most for infosec leaders, covering 10 competencies in total.

1. **Functional Competencies:** Technical Expertise; Operations Management; and Governance, Risk and Compliance (GRC).
2. **Business Competencies:** Business Acumen, Business Risk Management and Talent Management.
3. **Leadership Competencies:** Communication, Culture and Collaboration, Executive Presence, and Leadership Agility.

Each of these 10 competencies is defined by a set of skills, for a total of 45 skills that leaders can assess, develop and strengthen.

5 infosec leader personas emerge

Infosec leaders develop and apply competencies at their own pace, based on the needs of the company they work at and personal career objectives. The research distinguished five infosec leader personas, each with a separate set of dominant competencies and leadership behaviors.

These personas are Technical-Focused, Compliance-Driven, Business-Aligned, Business-First and Agile leaders. The first two personas are mostly tactical, while the latter two are strategic in nature.

The Executive Competencies Assessment Tool

From the research we created an Executive Competencies Assessment Tool that lets leaders evaluate their skill level for the infosec competencies, understand their leadership behavior and identify their infosec persona.

A group of CISOs took the self-assessment and shared their results. Most had strong Business and Leadership Competencies ratings. Their scores matched the Business-Aligned and Business-First personas. These CISOs indicated they had undergone extensive leadership training, including one-on-one executive coaching. Their skill set allows them to be solidly plugged into the business.

A few excelled in Functional Competencies and fell in the Technical-Focused and Compliance-Driven leader types. These CISOs indicated they have more operational involvement in the day-to-day decision-making and execution.

The Executive Competencies for Infosec Leaders

Business expectations for infosec leaders are rapidly changing

One by one, organizations—entire industries even—are transforming into digital businesses. That shift has elevated the importance of infosec and the professionals in this domain. The result: rapidly changing expectations for infosec leaders. Business leaders increasingly expect to partner with security leadership and need them to "speak their language." The C-suite needs CISOs to take on an organizational leadership role that drives cultural change.

These changes require infosec leaders to adopt a broader set of skills—in particular, nontechnical skills. The following story illustrates that.

A midsize financial services company was looking for a new CISO to be comped at $500,000 a year. The hiring team, consisting of the CEO, CIO and chief human resources officer, turned to an executive placement firm to help them with the search. Shortly thereafter, the recruiter had lined up a half dozen accomplished candidates. They were experienced infosec executives with the deep domain expertise and infosec credentials the hiring team was looking for.

"We could make do with most of these candidates," the hiring team responded. But it was clear to the recruiter that none of the applicants particularly excited his client. Nobody separated from the pack and differentiated themselves. Given the lukewarm reaction, he presented them with an out-of-the-box alternative. Abigail was in her 30s. She had a technical degree from an Ivy League school and national security experience. Though she never held a CISO role and didn't have an industry fit, she wowed the hiring team. Confident that Abigail would learn easily and grow into the position within six months, they hired her.

What did the last candidate bring to the table that the initial lineup of solid, highly qualified infosec executives didn't? As the recruiter put it, "Like the other candidates, she ticked all the boxes for technical expertise. The real difference was that her pedigreed education trained her on being business-savvy, polished and articulate. She showed up with what the hiring team described as executive presence. That was what this company needed."

The importance of nontechnical skills for infosec leaders

The story represents what is happening throughout the infosec domain. In varying degrees, organizations expect their infosec leaders aligned with the business, especially at large firms, where executives need their infosec leaders to spend most of their time engaging across nontech disciplines with the C-suite and board of directors.

Some organizations require their infosec leaders to spend more of their time addressing everyday technical issues and managing the security technology stack—in the weeds. In these cases, we often hear that infosec leaders themselves want a tighter relationship with business stakeholders. They often strive for a proverbial seat at the table—to help make business decisions with the infosec perspective baked in, instead of as an afterthought.

To evolve and to meet the new expectations, infosec leaders need to understand what additional skills such a transition calls for. Then, they need to know their own proficiency in these skills to assess which ones they should develop or strengthen.

In short, infosec leaders want and need to know where they currently stand. Only then can they decide where they want to go as leaders and plan their path to get there.

> "What type of CISO do you want to be? Do you want to have to deal with the organizational dynamics of a large multinational bank? Or do you enjoy hands-on innovative protecting at smaller firms?"
>
> **— CISO at a Fortune 500 financial services firm**

Introducing an Executive Competencies Framework for infosec leaders

In response to these questions, we started a research project to find out what skills—technical and nontechnical—infosec leaders should be developing and to what end. We interviewed CISOs, we spoke with recruiters who specialize in the placement of infosec leaders and we studied other leadership competencies models. We spent months putting the pieces together and testing them with infosec leaders.

"If there's one thing that made me more successful than anything else, it was emotional intelligence; it was the ability to read a room, the ability to figure out the pain points of various people and quickly find common goals."

— Former CISO at a global media firm

Our work produced a leadership competencies framework specifically for infosec professionals. The model uncovers 10 dominant competencies, grouped in three categories (see FIGURE 1).

Firstly, Functional Competencies. These are foundational to the infosec role and include Technical Expertise; Operations Management; and Governance, Risk and Compliance. They are critical competencies and unique to the infosec leader.

Next, a set of Business Competencies. Engaging with the business requires building relationships with business leaders. In turn, this calls for an understanding of the business, its customers and its financials. Competencies in this category are Business Acumen, Business Risk Management and Talent Management.

Lastly, there are Leadership Competencies. They center on the infosec leader as a business executive, effective at engaging with the upper echelons of the organization. This calls for skills like reading the room, understanding power dynamics and assessing what motivates stakeholders. The competencies in this category are Communication, Culture and Collaboration, Executive Presence, and Leadership Agility.

"When I am in the executive team meeting, I look at it as a potluck: The CFO brings his checkbook, the CMO [chief marketing officer] brings the trimmings and, as the CISO, I bring all things security. Everybody brings something to the table. We all show up with Executive Presence."

— CISO at an F500 consumer electronics company

FIGURE 1

The Infosec Executive Competencies Framework

Infosec leaders' competencies and their underlying skills

Each of the 10 competencies is made up of a set of underlying skills that leaders can acquire, refine and put to practice. In the table, we describe the 10 competencies and list the skills that define them (see FIGURE 2).

FIGURE 2

Competencies and Their Underlying Skills

Foundational Competencies

1 Technical Expertise | 2 Operations Management | 3 GRC

Technical Expertise	Operations Management	GRC
The skills and knowledge of IT, security technology, infosec concepts, security operations and controls.	The ability to plan, run and report on the day-to-day operations of the security organization and manage the security roadmap.	The ability to manage the organization's governance, technical risk management and compliance with regulations.
Underlying skills - Tech expertise application - Technical domain expertise - New technologies influential to security	Underlying skills - People management - Security operations - IT operations - Security strategy and roadmap development - Metrics and oversight	Underlying skills - Security regulations - Privacy regulations - Compliance audits - Business data protections

Business Competencies

4 Business Acumen | 5 Business Risk Management | 6 Talent Management

Business Acumen	Business Risk Management	Talent Management
The understanding of the business, its concepts and how it makes money, as well as the ability to understand and speak in business terms.	Knowledge of the organization's risk tolerance and the ability to take a holistic approach to risk management.	The ability to acquire, build and retain talent and diversity within the security organization, as well as in the wider company.
Underlying skills - Corporate strategy and go-to-market - Product and services portfolio - Customers and experiences - Company revenue and financials - Market landscape and differentiation - Security market landscape	Underlying skills - Risk quantification - Risk-based decision-making - Business impact assessment - Risk tolerance framework	Underlying skills - Diversity - Career development - Skills development - Personnel advocate - Coaching skills

Leadership Competencies

7 Communication | 8 Culture and Collaboration | 9 Executive Presence | 10 Leadership Agility

Communication	Culture and Collaboration	Executive Presence	Leadership Agility
The ability to listen and communicate effectively and to know your audiences and tune your messaging accordingly.	The ability to build trusting relationships with leaders across functions and to be able to influence them to make favorable decisions from a security perspective.	The ability to be persuasive, direct and decisive in interactions with the C-level and board.	The ability to keep on top of and in control of rapidly changing technology, market dynamics and business models.
Underlying skills - Communication skills - Crisis communication - Translating tech to business	Underlying skills - Collaboration skills - Trust building - Culture understanding - Culture change - Security evangelist	Underlying skills - Executive engagement - Storytelling - Situational awareness - Style shifting	Underlying skills - Personal agility - Organizational agility - Personal resilience - Team growth mindset - Strategic thought leadership

The Executive Competencies Framework: A Closer Look

Not all infosec leaders apply the 10 competencies equally. As we saw earlier, more hands-on, technical problem-solvers rely heavily on their Functional Competencies—in particular, their Technical Expertise. Other infosec leaders spend more time engaging with executives and actively help drive business growth and business transformation. For these leaders, Business Competencies dominate and Functional Competencies play a supportive role.

5 infosec leader personas emerge

We identify five distinct infosec leader personas. They are the result of the varying needs and expectations across different organizations and job roles. For each, a distinct set of competencies are:

Dominant: They are differentiators for a leader's success in the role.

Supportive: A leader is proficient in this competency, but the skills are neither highly nuanced nor specialized.

Nascent: It is in the early stages of development for the leader but is rarely, if ever, used at an executive level of sophistication.

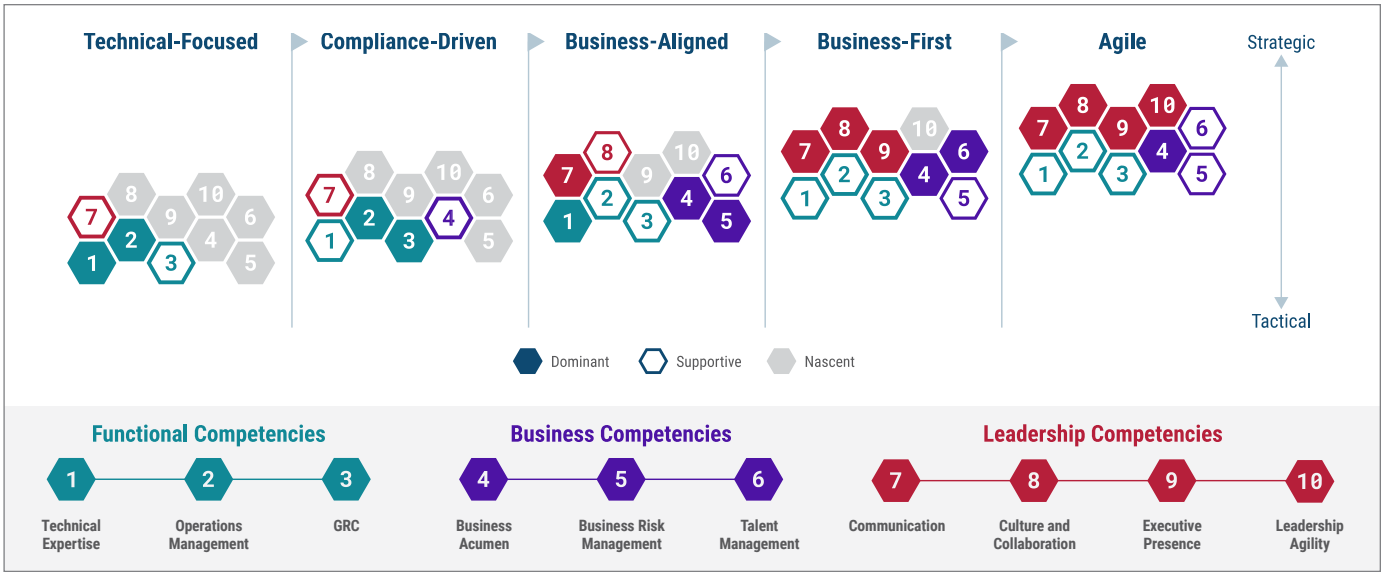
Most infosec leaders will identify strongly with one of the five personas. Others will find they veer between two or more personas throughout their daily routine. The five personas are (see FIGURE 3):

Technical-Focused: In every organization, regardless of sector and size, we find Technical-Focused leaders. They bring deep technical know-how and operational prowess. The value to their organizations is clear: These are the people who solve security problems. They focus on keeping systems, information, networks and products safe from threats.

> "I am very technical. The main part of my job is the 911–the emergency response, making sure everything's good. I really don't have a lot of expertise and understanding of the business landscape and how different stakeholders across the organization relate, how to work with suppliers and things like that."
>
> **— CISO at a tech startup**

FIGURE 3

The Infosec Leadership Journey



Compliance-Driven: Organizations in sectors with stringent and rapidly evolving regulations, including financial services, utilities, healthcare and retail, find value in a Compliance-Driven infosec leader. For this leader type, GRC skills dominate. Further, they typically invest in building connections with business stakeholders to explain and ensure compliance. You'll often find them working closely with the legal or risk team to coordinate operations. This type of leader helps build business confidence by reducing the risk of regulatory exposure and sanctions.

"I don't have a strong IT background, but I am strong as a liaison to the business and can talk to the business, as well as run technical projects. I got into identity and access management and SAP security. And then I took over the policy and procedures and the governance component, which remains my core focus."

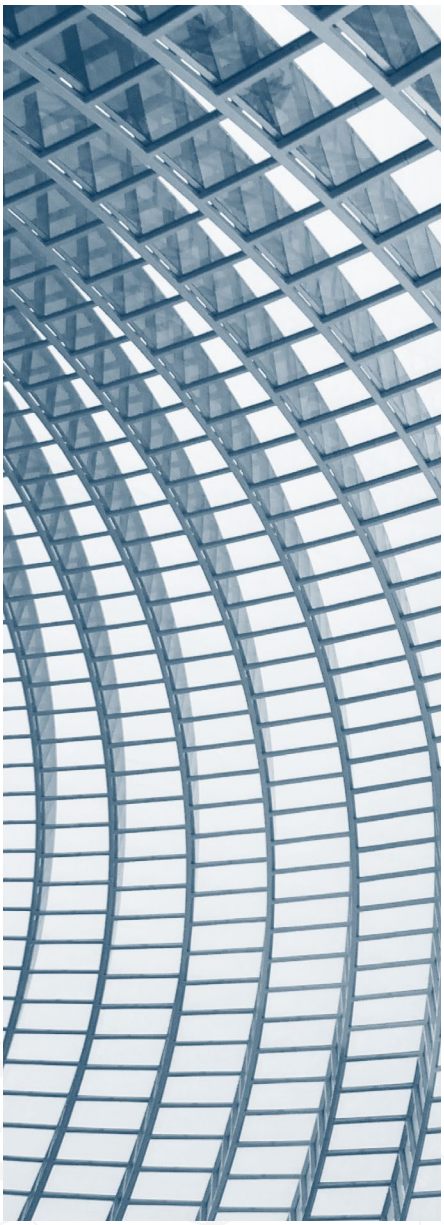
— CISO at a nonprofit organization

Business-Aligned: Mid- and large-size organizations increasingly need their infosec leaders to connect more closely with business operations. They need someone who ensures the infosec agenda isn't carried out in isolation from business needs, digital initiatives or innovation. They benefit from a Business-Aligned infosec leader. This leader type takes a business approach to risk management and can articulate security requirements in business terms and vice versa. They build relationships with business leaders and help find and solve security problems—for instance, in product development or customer outreach programs. They execute on the infosec agenda in response to the shifting needs of business stakeholders.

"I understand how to translate the technical into the business speak. So, being able to align, being able to explain and being able to quantify and qualify the impact that security has to the business and business operations."

— CISO at a health tech company

Business-First: Multinational and global firms invest in Business-First infosec leaders who know how infosec fits in the bigger picture and can help drive, and even define, business priorities. These companies further benefit from this persona's strong leadership skills, allowing them to take on an organizational leadership role. Individuals who fit this profile are skilled communicators and can help change the organizational culture. The Business-First leader moves in lockstep with the organization, incorporating security and risk conversations into business decision-making.



"When I started at my current company, my first order priority was to understand the business strategy, revenue mix, business line structure, go-to-market strategies, what affected their stock prices and those types of things. Only after I understood that well, I looked into the data centers, the platforms, the systems, the infosec team and things like that."

— CISO at a Global 500 financial services company

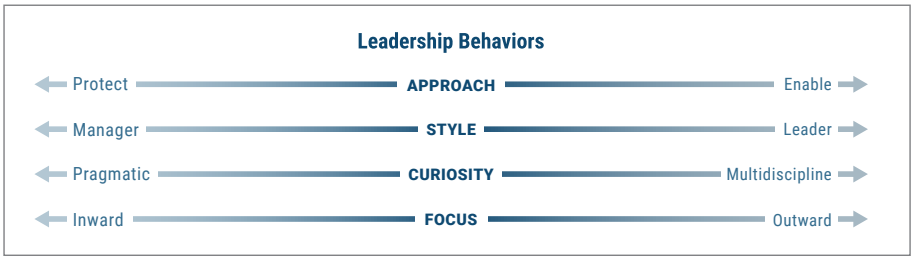
Agile: A select few firms, mostly global that are at the spearpoint of digital transformation and strive to continually disrupt their business models, require an Agile infosec leader. These organizations innovate at speed and need infosec leaders who can stay on top of emerging trends and develop new skills quickly. These leaders are exceptionally skilled at Business and Leadership Competencies, in particular Leadership Agility. They act as partners and trusted advisors to the CEO and the board of directors. They have stepped out of the weeds. Why can they afford to do so? They have a battery of infosec leaders from the other personas reporting into them.

"For me, it is no longer about business acumen or having the infosec skills and capabilities. It is all about agility: How fast can I learn and take in new information; how fast can I understand a new business strategy; how fast can I go to market with a new product? It is about personal agility, process agility, organizational agility. The switch for me was agility for everything."

— CISO at a Global 500 financial services company

FIGURE 4

4 Behaviors of Infosec Leaders



Leadership Behaviors Matter as Much as Competencies

Skill and experience clearly matter a great deal, but they are not the sole influencers of an infosec leader's effectiveness. Behaviors also play a key role. Behaviors impact decision-making, shape the perceptions of others and, ultimately, affect career advancement. It is important for infosec leaders to understand their go-to behaviors and consider where they help or hinder them in meeting their career objectives.

For infosec leaders, our research surfaced four key behaviors. They typically evolve with maturity. We describe the four behaviors most relevant to infosec leaders (see FIGURE 4):

Approach—how leaders approach their overall remit: We distinguish leaders for whom the primary goal of the security agenda is to protect their organization. For them, risk management starts with understanding tech vulnerabilities, rather than with understanding the business tolerance for risk. To them, some business objectives get in the way of security objectives. At the other end, we see leaders who have an overarching goal to enable the business. They seek to accelerate the business with the infosec agenda and security objectives set in support of business objectives.

"Someone who is business-first pushes forward a vision of how infosec actually enables and improves the business. For me, that meant figuring out how we sell security as a product feature and differentiate ourselves from competitors."

— CISO at a healthcare company

Style—the way in which leaders engage with their teams: In many settings, a practical, hands-on managerial approach is the right style. For the top infosec leaders, especially at larger organizations, businesses will often need their infosec head to take on an organizational leadership role and steer the culture toward one of caution and security. They typically consider the big picture and proactively set goals and agendas. These leaders exert influence to drive organizational change and delegate day-to-day management to their direct reports.

Curiosity—leaders' natural tendency to stray from their comfort zone: In our interviews, CISOs often talked about curiosity as a hallmark trait of the infosec professional in general. They distinguished two types of curiosity. At one end are leaders who are curious within their current domain. They would seek to deepen their knowledge in one or more tech or infosec specializations. We call that pragmatic curiosity. At the other end are leaders who have expanded their curiosity beyond the infosec realm. They will naturally ask about the business and want to learn about customers and the competitive playing field. We call that multidiscipline curiosity.

Focus—where leaders mostly direct their attention: The research identified an inward versus outward focus. An outward-focused leader has greater attention to outer forces like the economic influences, customer trends and competitive dynamics. And they are often involved in community programs. For example, one CISO told us they lead a cyberbullying awareness campaign for children and volunteer for a human trafficking prevention program using their infosec talents. For organizations, this type of community involvement by an executive contributes to positive brand awareness.

"I see people getting stuck on looking inward versus looking outward. They're always looking at the infrastructure of the plumbing. You'd be amazed at how many of them never look at any of this through the lens of a customer."

— CISO, retired from a global telecommunications firm

"If you don't care about the business, you're probably going to just stick in the [security operations center] or somewhere in the technical world. The employees and the managers who start asking questions like, 'How does this impact the customer?' or, 'How are we making money?' Those are ones who I tag as high-potential."

— CISO at a financial services firm

How CISOs Assess Themselves on Competencies and Behaviors

Based on our research, IANS developed a comprehensive assessment tool to help infosec leaders evaluate their individual performance along the 10 competencies. Infosec leaders take it to find out where they stand, which persona they align with and which competencies are areas of development for them. They can complement their results with a 360-assessment from within their organization.

Armed with the results of the assessment, leaders can engage with a personalized development plan to build the skills needed for the next leg of their career journey.

Our sample contains mostly CISOs with vast experience and in high-level positions

An initial sample of infosec leaders—most of them CISOs—took the survey between June and August of 2021. Given the seniority of the people in the sample and the mostly large size of the companies they work at, this sample skews toward Business-Aligned and Business-First personas. The sample includes less than a handful Compliance-Driven and Technical-Focused leaders. Unsurprisingly, Agile leaders are absent from the sample. We believe the Agile persona is currently a niche role that will become more prominent in the next two to three years, as organizations demand more agility from all leaders, including those in infosec (see FIGURES 5.1 and 5.2).

FIGURE 5.1

Most CISOs Who Took the Assessment Are Business-Aligned

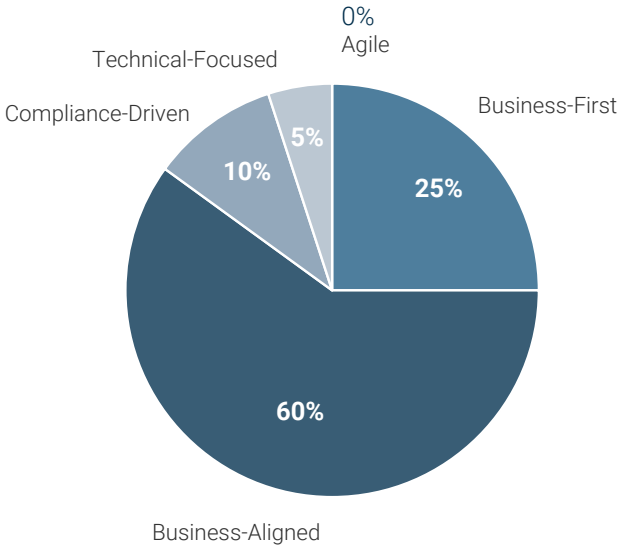
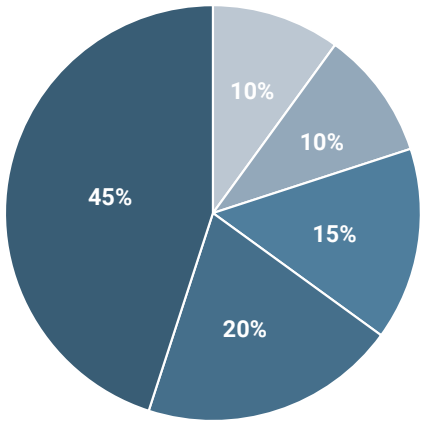


FIGURE 5.2

Most CISOs Who Took the Assessment Had Formal Leadership Training



- No formal leadership training
- Up to five days of formal leadership training
- Up to four weeks of formal leadership training
- Several months of formal leadership training
- Several months of formal training with one-on-one executive coaching

Also noteworthy of this sample of seasoned infosec leaders is that the vast majority has undergone leadership training and one-on-one executive coaching. Their investment in developing Business and Leadership Competencies helped them achieve their career objectives.

Senior infosec leaders have moved past Functional Competencies

Zooming into just the Business-First and Business-Aligned personas, our sample scores strongest in the Business and Leadership Competency categories and lower on the group of Functional Competencies. This makes sense. These CISOs tell us their technical knowledge runs more broadly than deep, so they can ask the pointed questions with infosec leaders one or two layers down from them on the org chart (see FIGURE 6).

Our sample scores highest on Communication, lowest on Executive Presence

Across the entire sample of CISOs who took the assessment, the two competencies they rate themselves strongest on are Communication and Talent Management. They tell us that communication skills, crisis communication and the ability to translate technology to business speak are critical throughout their careers and refined over time.

For Talent Management—a necessary competency to retain key staff in the tight infosec talent pool—these leaders rate themselves strongest on their ability to coach and help their staff with career development. They see room for improvement in team diversity and helping their staff develop key skills (see FIGURE 7).

Our sample rates themselves strongly on leadership skills. Within the technical trenches, elevated leadership skills will more easily stand out. That picture changes when technical leaders must hold their ground next to business executives in functions that revolve around soft skills like influence, persuasion, empathy, relationship management, active listening and clarity of messaging. The CMO, head of sales or chief product officer got their positions by being strong communicators.

Thorough understanding of the customer, the market, the business and its financials are not added skills. They are what define these leaders.

To gain and keep a seat at the table alongside such business executives, infosec leaders should assess their leadership skills from a bar that is higher than in the technical domain.

FIGURE 6

Business-First and Business-Aligned Leaders Score Lower in Functional Competencies

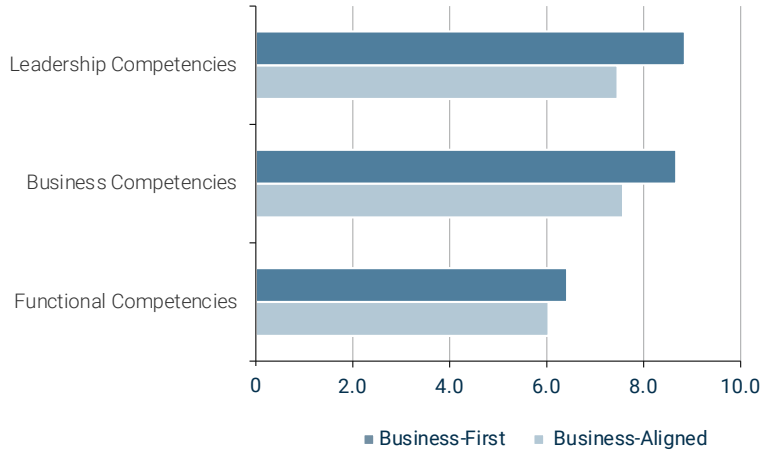
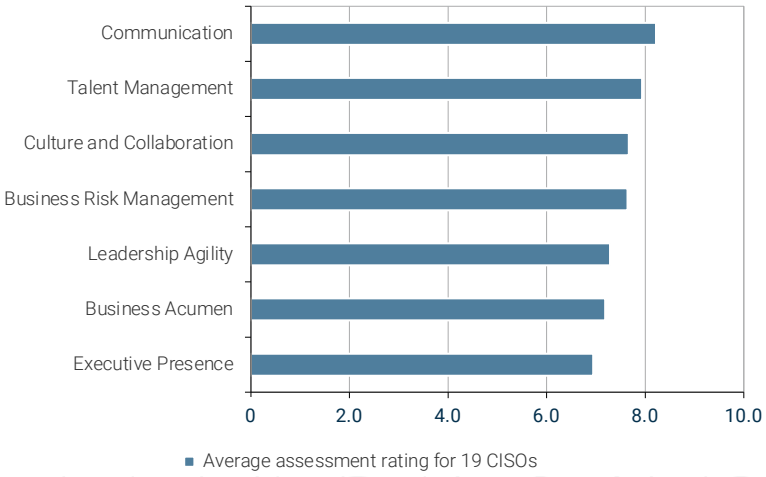


FIGURE 7

CISOs in Our Sample Rate Themselves Strongest on Communication and Talent Management



The same graphic shows that our sample of CISOs can further strengthen their Executive Presence and Business Acumen. Looking at the scores for the underlying skills within these two competencies, we see that executive engagement is lagging. That may come with strengthening other Executive Presence skills including situational awareness and the corresponding style shifting (see FIGURE 8).

Upon a closer look at the Business Acumen, we see from our sample of CISOs that their knowledge of the go-to-market, customer segments and customer experiences still has room for further strengthening. Why should they care? These are areas of strategic importance that every business leader including the C-suite and board of directors care deeply about. What's more, different customer segments have different attitudes toward the information security offered. And the infosec agenda affects customers and their experiences (see FIGURE 9).

Looking across both Executive Presence and Business Acumen competencies, our sample's lower scores for both indicate the interconnectedness between these two skill sets. For example, in the C-suite, it is difficult to portray Executive Presence when much of today's C-level discussions revolve around go-to-market strategy and differentiation on customer experiences. CISOs who lack a complete understanding of these and other business subjects will not be able to easily relate to the conversations happening in the C-suite and exhibit appropriate situational awareness.

FIGURE 8

CISO Assessment Ratings for Executive Presence Skills

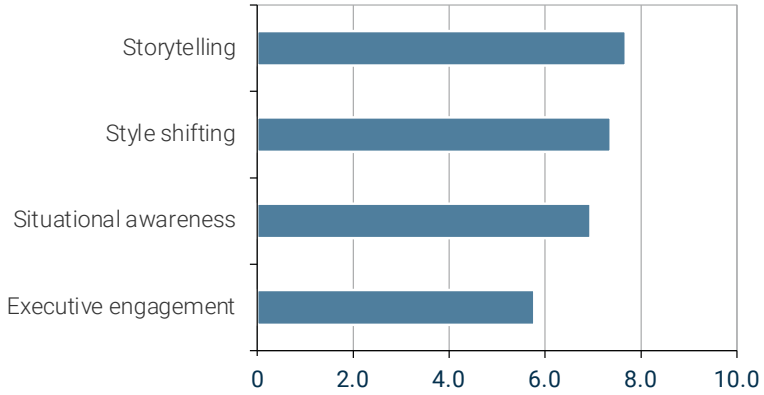
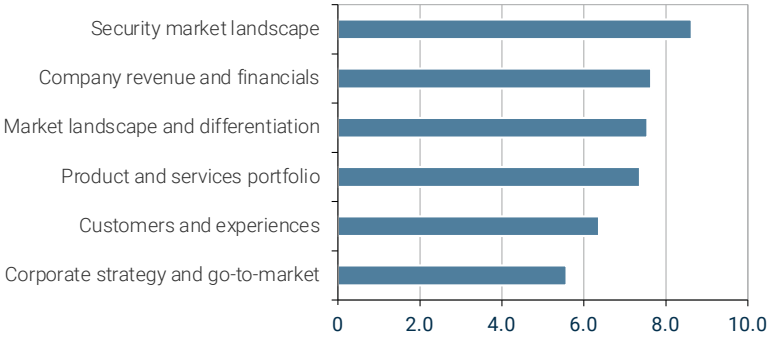


FIGURE 9

CISO Assessment Ratings for Business Acumen Skills



Our sample leans toward an enabling approach and a leader style

For all four behaviors, our sample tends to lean more to the right hand of the spectrum. For example: The average score for the Approach behavior of this group is a 7.1, on a scale of 1 to 10. That rating puts them in the "Enable" column.

For Style, the average rating is 6.8, also more to the right, which means the CISOs in this group are more Leaders than Managers. The scores for other two behaviors, Curiosity and Focus, also lean more to the right-hand side (see FIGURE 10.1).

The tool assesses the behavioral style using five statements for each behavior. This section provides insight into how the sample scored on the statements in each case.

They take a mostly Enabler Approach. They think of themselves more as business leaders than technology leaders and find Business Acumen a must-have competency. Their main goal of the security agenda is to accelerate the business, while at the same time, keeping the business safe from threats (see FIGURE 10.2).

The organization recognizes them as Leaders. Nontechnical colleagues come to them for advice on a regular basis. Rather than using their control and power to get things done, they use softer approaches like influence and inspiration of others. They see themselves more as generalists than specialists (see FIGURE 10.3).

FIGURE 10.1

CISO Leadership Behaviors Lean to the Right End of the Spectrum

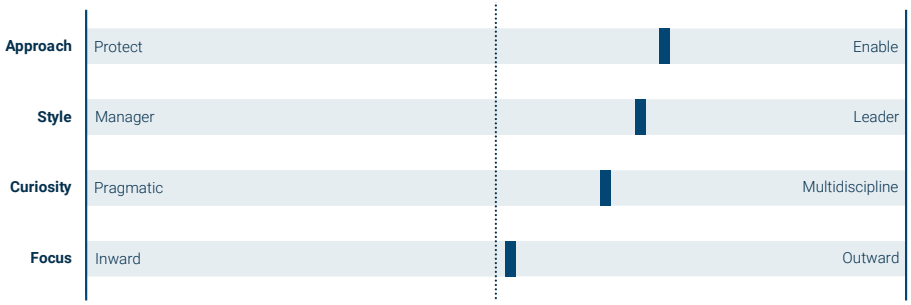


FIGURE 10.2

CISOs' Approach Is Mostly to Enable the Business

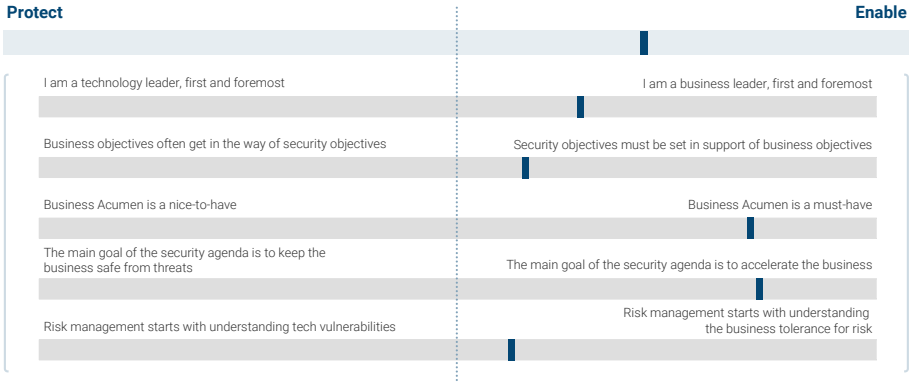


FIGURE 10.3

The Dominant Style Is That of a Leader

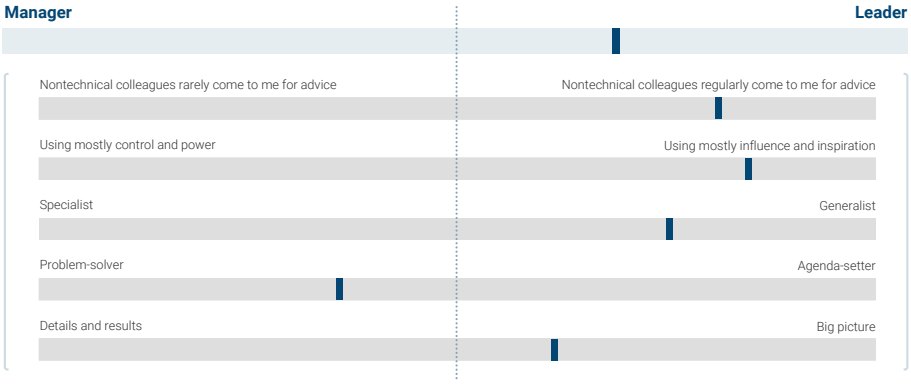


FIGURE 10.4

CISOs Express a Multidiscipline Curiosity

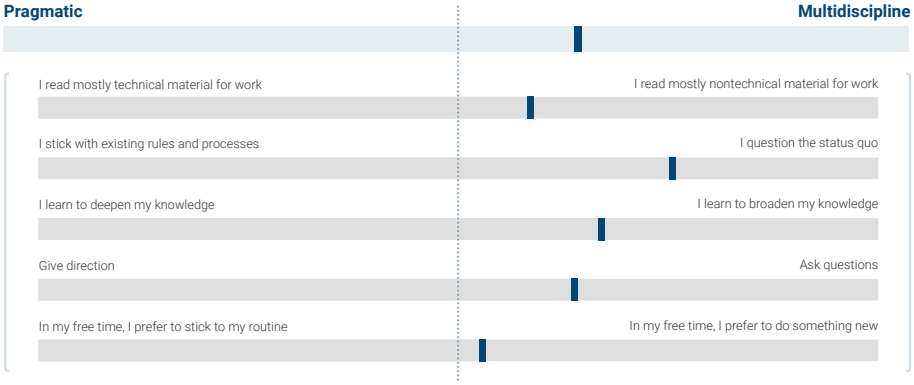
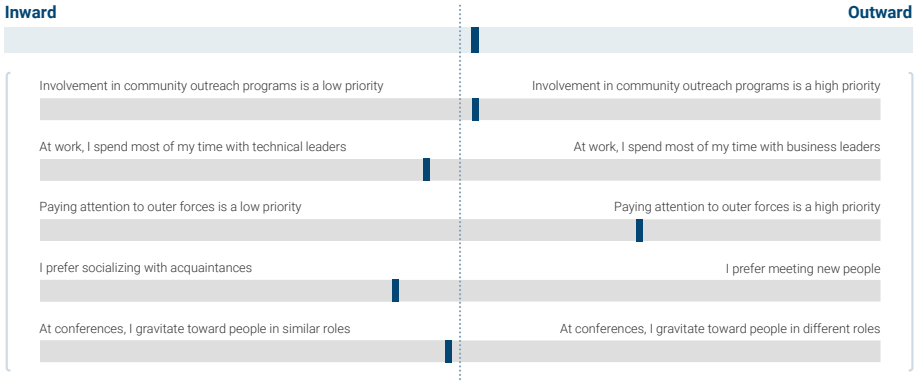


FIGURE 10.5

On Focus, CISOs Lean Slightly More Outward than Inward



Their curiosity extends across multiple disciplines. They read more nontechnical material for work and consciously seek to broaden their knowledge, rather than deepen it. This behavior shows up outside work settings as well, indicating they prefer to do something new over sticking to the routine (see FIGURE 10.4).

Their focus is slightly more outward. Like Curiosity, leaders' natural Focus tends to shift as they get more plugged into the business. In our sample, we see this strongly with paying attention to outer forces like economic factors, customers or competitors. These Leaders also tend to give back to the community (see FIGURE 10.5).

In Closing: Expert Recommendations for Your Journey

This Executive Competencies Model represents an opportunity to jumpstart your career journey. It is a great moment for self-reflection, deciding on your next career objectives and planning your development required to meet these goals.

What more can you do? The top-grade CISOs and executive search experts we interviewed for this project offered up additional recommendations, taken from their own careers:

Don't wait to be invited. A CISO at a global tech firm recommended infosec leaders go where they are not invited. Once there, participate and bring value so you cannot be ignored. Don't wait for an invitation to explain your infosec strategy to the business. Take the first step in reaching out. In the same vein, another interviewee experienced great value from working on internal branding and messaging. Doing this successfully positioned their infosec organization as a business enabler and a problem-solver. With that, they no longer needed an invitation.

Find your training ground. A CISO in the global finance sector took on a position as the regional head of security at a satellite office abroad. It simulated being at a small company that gave direct exposure to business departments. It was a great training ground to improve business and leadership skills. Other interviewees had similar experiences. One took on a business CISO—a BISO—position and learned to seamlessly translate cybersecurity and technical risk into business speak. Others went from the No. 1 infosec leader at a small firm to a lower-ranked position at a much larger firm and learned to cope with the complexities that come with size.

Write your story. One of the executive search experts we spoke with said too many candidates cannot articulate their personal narrative. What should it say? It should convey your philosophy on security and on leadership; the vendors you like to work with and why; the inner circle you lean on in the face of adversity; your relationship with the business; and what you think success looks like. Have your story ready for the next time you are interviewing, whether to profile yourself for an internal promotion or with prospective future employers. Your story will help you stand out from other candidates.

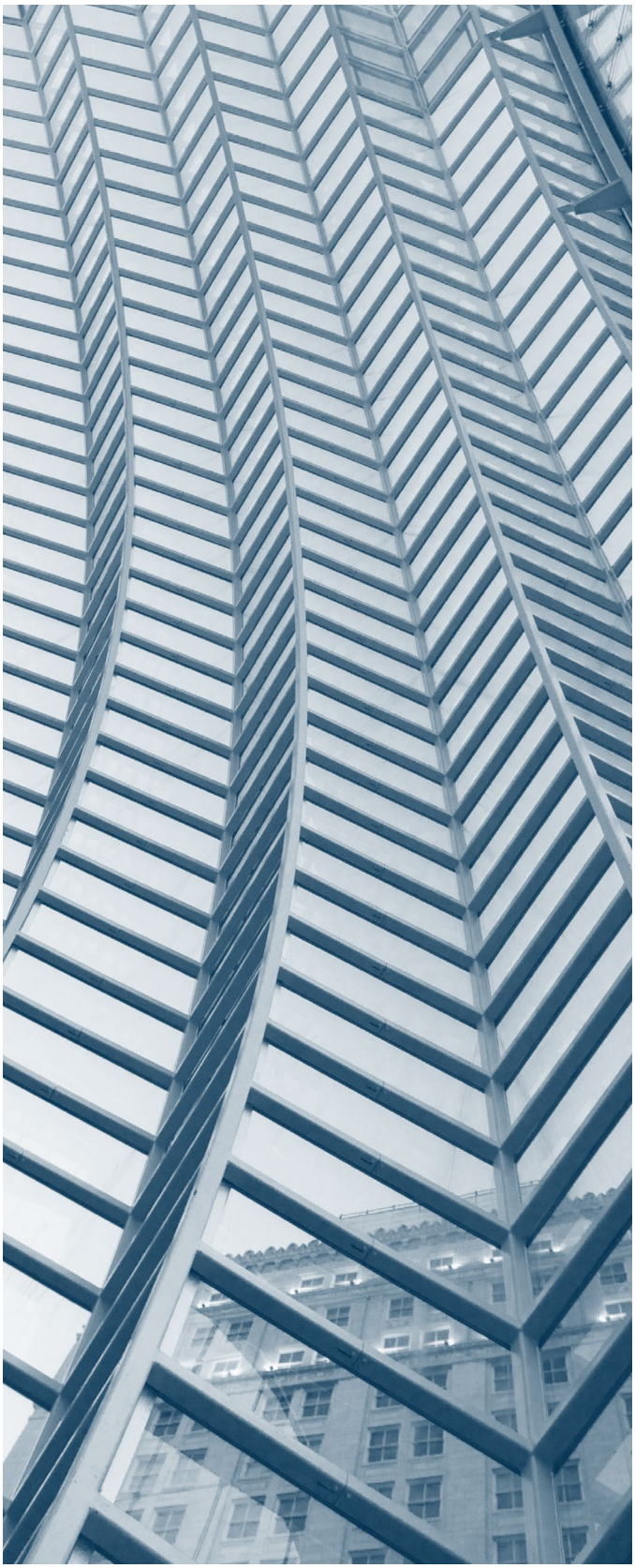
Don't go it alone. Without exception, our interviewees pointed out the benefits of formal leadership training to jumpstart their personal growth and soft skill development. Nobody expects you to figure this out on your own. Chances are your manager will promote leadership training like the CISO at a Global 500 insurance firm we interviewed. They talked about their ongoing efforts to have their team formally trained in communication and leadership skills. These efforts tied directly to the organization's performance review and promotions cycle.

How IANS Executive Development can help

IANS offers an Executive Competencies program that is rooted in the research laid out in this report and is created for and offered exclusively to infosec leaders. The program helps participants develop and strengthen their Business and Leadership Competencies. The CISOs and executive recruiters we interviewed expressed a strong preference for an infosec-specific program because of its benefits compared with generic leadership development programs.

Key pillars of the IANS Executive Development program are the self-assessment and 360-assessment; the personal development plan; the online personal development portal; its broad set of learning pathways that are customizable to the needs of the individual and their organization; and one-on-one executive coaching with top-tier current and former CISOs.

To learn more about IANS Executive Development options for you or for members of your team, find details online or contact us via info@IANSresearch.com.



Methodology

IANS fielded a 10-month long research project in the fall of 2020. Our fieldwork started with interviews with 22 CISOs from sectors including financial services, healthcare, tech, U.S. government, professional services, retail, insurance, telecommunications, manufacturing, utilities and media. Seven of the interviewees are from Global 500 firms and 12 work at Fortune 500 firms. In addition, we interviewed executive search experts who specialize in the placement of infosec leaders. The interviews formed the basis of the Executive Competencies Framework and the Competencies Assessment Tool.

Next, we rigorously tested and refined these outputs with help from our 70-plus client panel consisting of CISOs and infosec leaders throughout North America. The group includes leaders from public organizations and private companies ranging from midsize to global and from all major industries. Twenty members of the IANS client panel took the self-assessment to help us vet the questions and the results.

The entire IANS team is grateful to the interviewees and members of the IANS client panel whose time and insights have been invaluable to this work.