Planning for the Future of Security Leadership: RRA's Cyber Leadership Index

The security landscape is rapidly evolving. Globally, we are seeing more companies investing the right amount of capital and resources to ensure the appropriate security footprint and posture is in place. This has been a consistent positive trend stretching back several years. Security is part of the conversation in the boardroom and key strategy sessions.

While cyber security capabilities are critical, program leadership is equally as important. These leaders must be able to:

1. Partner effectively across the organization (with technology and well beyond into the business).
2. Develop a roadmap and strategy that aligns to the digital, technology, and OT strategy and evolution of the enterprise.
3. Build an effective team, with opportunities for growth and well thought out succession planning across key roles.
4. Work closely with the board and the leadership team to develop a rapport and partnership with open lines of communication and an ability to articulate key risks and security topics in an effective manner to all audiences.

Technological change was considered the

4th largest threat to business health over the next 12 to 18 months

In digital-first companies, **cyber security** specifically was called out as the

6th most major threat affecting the business

Only

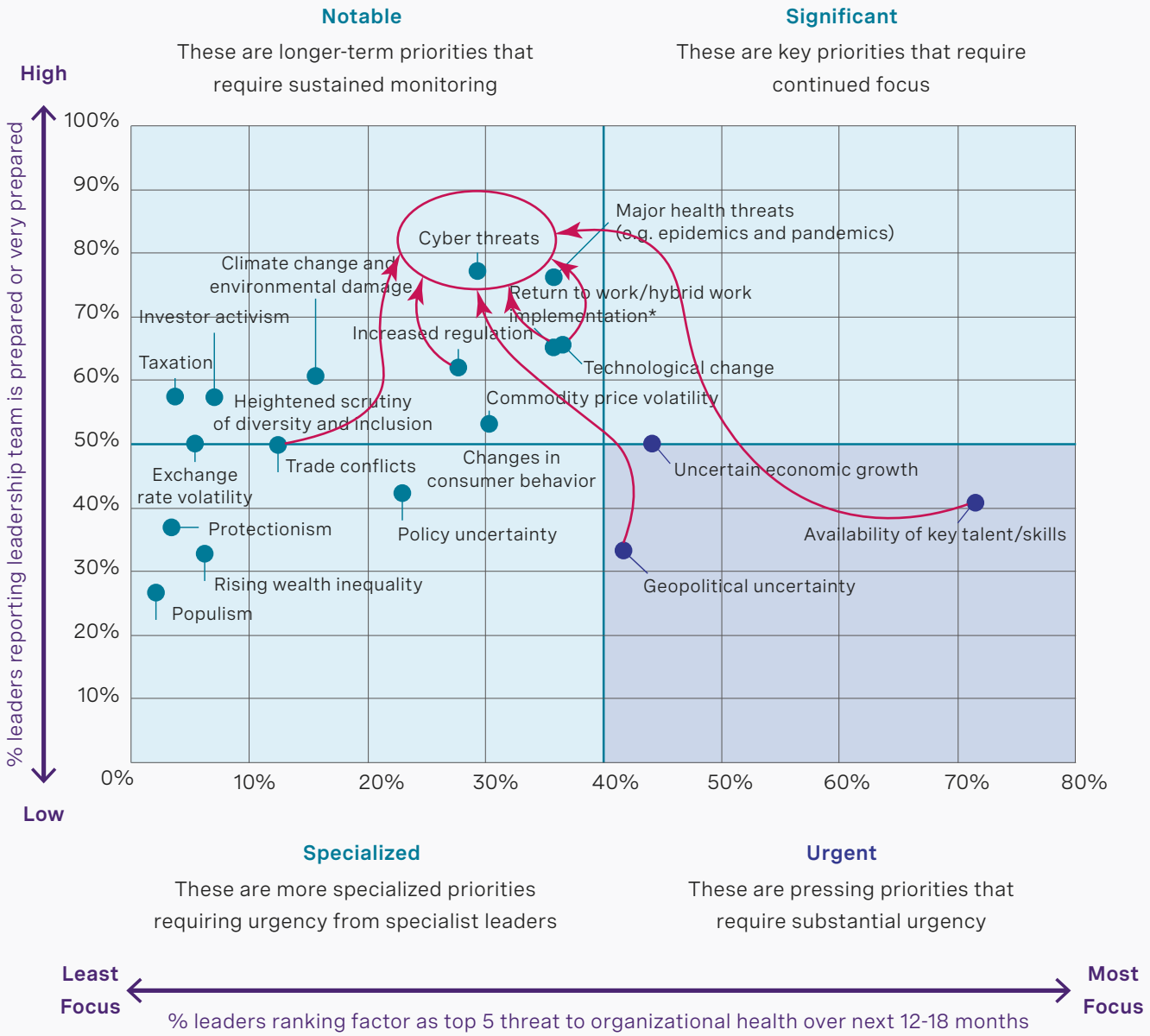
36%

of leaders believe their organization currently has the **right talent** to drive the digital journey

In our annual Global Leadership Monitor survey, we asked leaders globally what would impact their business most in the next 12-18 months, and how prepared they felt to deal with that problem. Respondents ranked cyber security as a definite challenge, but also rated their ability to deal with that challenge highly. But this does not tell the whole story. Many leaders predicted challenges — from key talent shortage to geopolitical uncertainty — that create challenges specific to cyber security leadership. From the security challenges of hybrid working, to consumer behavior change and the associated data protection issues, and the threat of geopolitical conflict, we see that most business challenges will impact the day to day leadership of a cyber security function.

Relative Importance of Factors vs. Leadership Preparedness to Respond

% of leaders



*Respondents were only asked to rate their leadership team prepardness if they selected the factor as a top 5 issue

Source: Russell Reynolds Associates' 2022 Global Leadersehip Monitor Survey, n1,590 CEOs, C-level leaders, next-generation leaders, and non-executive board directors

The Cyber Leadership Index: A tool for assessing your organization's security and the leaders responsible for it

Numerous frameworks exist to benchmark and assess an organization's security program. These provide a point of view on where the program stands relative to best in class, peer group, and baseline organizations and targets. These are tremendously helpful in benchmarking and ensuring a strong posture. Where many of our clients struggle is in evaluating the extensions of the function's capability.

We developed the Cyber Leadership Index with a focus on helping organizations evaluate where they stand, not just across the capabilities of the function, but also, crucially, on the dimensions that signify how the security function fits within the organization, and how its leadership is driving the function forward.

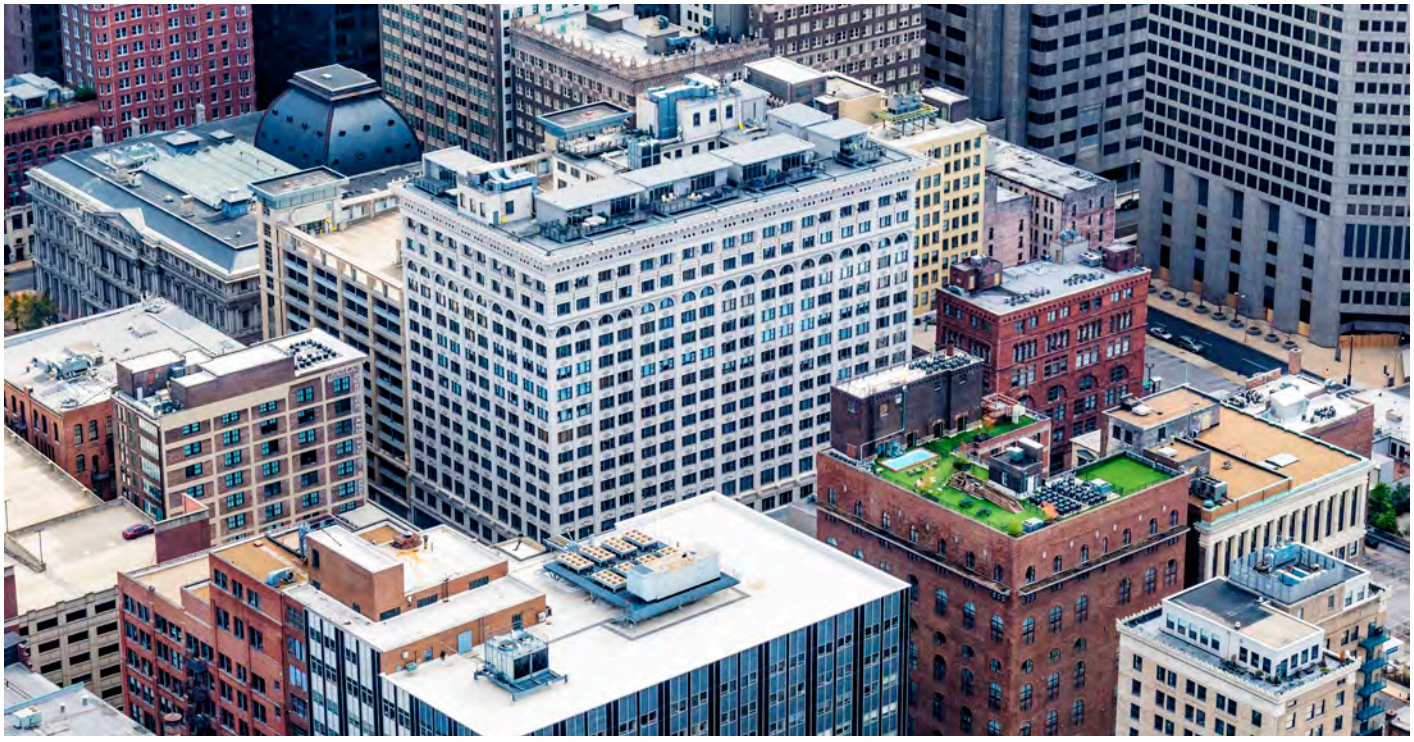
The Cyber Leadership Index can be a tool to evaluate the current state of the program, just as much as it can be a mechanism for organizations to think through where they aspire to be, and how to get there. The framework leverages methodologies used across other security frameworks, to provide a common point of reference in evaluation.

Strategy

Execution

Leadership

Relationships



The framework works by assessing four key dimensions of the cyber security function, each with four sub-dimensions, and acts as a tool both to guide conversation and assess an organization's cyber function, where that function stands and where future opportunities lie.

	LIMITED	AD HOC	PROACTIVE	INTEGRATED
Strategy Alignment of the cyber roadmap to the organization strategy, and evolution of the roadmap in tandem with strategic changes.	Alignment of cyber strategy to the tech/digital roadmap and business	Development of a roadmap and strategy for the cyber function	Degree to which cyber program is 'at the table' as strategy is developed	Ongoing refreshing /evolution of cyber roadmap and strategy
Execution Execution excellence across regulatory compliance, and alignment with the organization's tech ecosystem and risk profile.	Security program matches with the tech ecosystem and risk profile	Coverage of relevant regulatory & compliance frameworks and controls	Core program capabilities: identify, protect, detect, respond, recover	Coverage of customer, 3rd party and vendor risk
Leadership Strength in attracting and retaining a team, ensuring talent gaps are filled, and succession plans exist for critical roles.	Buildout of security team capabilities - full time & 3rd party members	Provides opportunities to help team members grow and evolve	Ability to communicate effectively at all levels	Focus on enhancing bench strength and developing credible successors
Relationships Ability to build relationships and influence across the organization and with regulatory bodies externally.	Reshapes the organization culture to enhance cyber awareness	Develops positive relationships with internal stakeholders	Maintains external relationships e.g. regulatory bodies and agencies	Engages and communicates effectively with non-tech stakeholders

Strategy

The cyber roadmap should be aligned with organizational strategy, and constantly evolving in tandem with technological, strategic, or regulatory changes.

	LIMITED	AD HOC	PROACTIVE	INTEGRATED
Alignment of cyber strategy to the tech/digital roadmap and business	Absent from leadership discussions; not "at the table;" not always informed of key decisions impacting security.	Bolted on at the back end; brought to the table or informed at the end of all conversations.	Cyber is brought to the table on some key decisions, and cyber security advice is sought and leveraged.	Cyber informs decisions on digital and technology and is actively engaged.
Development of a roadmap and strategy for the cyber function	Strategy and roadmap are developed separately with little overlap and little alignment.	Strategy and roadmap are occasionally or loosely aligned	Roadmap and strategy are mainly aligned, though changes in strategy may not always map onto roadmap.	Roadmap and strategy are constantly evolving in tandem, consistently weaving in the business and technology strategy.
Cyber program's level of involvement in strategy development	Not at the table; not always informed of key decisions impacting security. Expected to "figure it out."	Bolted on at the back end; brought to the table or informed at the end of all conversations.	Brought to the table on some key decisions, and cyber security advice is sought on a needs basis.	Informs decisions on organization-wide strategy and is actively engaged.
Ongoing refreshing / evolution of cyber roadmap and strategy	Cyber roadmap is event-driven and reactive	Cyber roadmap is periodically refreshed as needed, or on an annual basis.	Cyber roadmap anticipates and adapts to needs, accounting for new technologies, new strategies, and new regulations.	Cyber roadmap is constantly in flux and evolving.

Execution

Executing a security program encompasses both regulatory compliance and aligning with the organization's technology ecosystem and risk profile.

	LIMITED	AD HOC	PROACTIVE	INTEGRATED
Security program matches with the tech ecosystem and risk profile	Security is siloed in the organization and has little to no connection with other functions or organization strategy.	Security is largely siloed except for pockets where closer interaction with other areas of the business is needed.	Security is embedded with technology and strategy on ongoing basis.	Security is embedded across the business, and proactively informs decisions.
Coverage of relevant regulatory & compliance frameworks and controls	Does enough to be compliant with regulatory mandate, and fixes problems reactively where they arise.	Plans for near term changes to regulations as they arise.	Anticipates emerging regulations, creates a strategy and executes accordingly.	Two-way close relationship and partnership with regulators; may influence regulation.
Core program capabilities: identify, protect, detect, respond, recover	Little or no framework. Security function "runs by feel" and need.	Framework leveraged occasionally to provide structure to the security function.	Full framework adapted ad hoc to external requests and regulatory requirements	Continuous security innovation; e.g., security automation / proactive offensive security
Coverage of customer, 3rd party and vendor risk	Reactive to incoming requests or events.	Seeks to understand how new customer streams and vendors could impact security needs.	Aligned with vendor and partnerships strategy and new customer streams. Embedded as part of the conversation internally.	Security highly engaged with external entities. Security has trust elements with external partners.

Leadership

Cyber security leadership should attract and retain a strong team, ensuring talent gaps are filled and succession plans exist for critical roles.

	LIMITED	AD HOC	PROACTIVE	INTEGRATED
Buildout of security team capabilities - full time & 3rd party members	Some capability. People mismatched to responsibilities. Low alignment of skills / talent and responsibilities.	Pockets of high skill and of low skill, with little people strategy to fill gaps.	Skills are proactively spread with a few gaps	Well-balanced, mature capabilities.
Provides opportunities to help team members grow and evolve	Builds the team to fit reactionary needs of the function. Few opportunities to develop / rotate.	There are occasional and ad hoc opportunities to progress.	Team has opportunities to progress or rotate, with a learning budget and time	Strategy implemented for people development, career pathing, DEI, rotations, step up opportunities and active engagement with junior leadership.
Ability to communicate effectively at all levels	Still communicates in technical jargon. Needs handholding at board level. ExCo Tech officer would present the risk conversation with board.	Ability to present on certain topics at board level. May be assisted by another more senior tech leader.	Strong ability to present at board and ExCo level, translating complex technical needs into business requirements.	Strong relationships with ExCo and board. Can be called on informally. Board directors may call on CISO for advice in their respective companies.
Focus on enhancing bench strength and developing credible successors	No succession or contingency plan. Significant key person risk.	No successor; starts succession planning for the team as needed depending on suspected flight risk.	Has a successor. May have succession plans for some of the broader team.	Having a succession plan throughout the function - factors in other key functions - consistent pipeline.

Relationships

Building relationships and influence across the organization, as well as with external regulatory bodies, is crucial.

	LIMITED	AD HOC	PROACTIVE	INTEGRATED
Reshapes the organization culture to enhance cyber awareness	Limited impact on culture. Security is seen as off to the side or 'shouting from the rooftops	Awareness training, programs and ongoing education of leadership and employees follows breached or risks.	Awareness training, programs and ongoing education of leadership and employees is constant.	Cyber is embedded in the culture of the organization. Leaders are well versed on security risks. Employees inform the cyber function of risks organically.
Develops positive relationships with internal stakeholders	Cyber consistently bolted on the back end. Not well connected with business needs.	Occasionally brought into relevant ExCo meetings. Some proactive relationships built with internal stakeholders.	Consistently brought into meetings on strategy. Proactively builds relationships with all internal stakeholders.	Maintains a continual presence on the ExCo.
Maintains external relationships e.g. regulatory bodies and agencies	Security function is reactive to inbound approaches.	Security function proactively connects with external bodies as needed.	Security function proactively partners with external bodies.	Collaborates with external regulators to build and influence future regulation and policies.
Engages and communicates effectively with non-tech stakeholders	Security function is disconnected from the business with a rudimentary understanding of its needs.	Business leaders connect with security on an ad hoc and need basis. Some but limited proactive connection.	Security function proactively connects and partners with business leaders to assess needs.	Security informs the business. Security is brought in early and often to partner with the stakeholders on their functional needs.

Authors

George Head leads Russell Reynolds Associates' Technology Officers Knowledge Team. He is based in London.

Ahmed Jamil leads Russell Reynolds Associates' Cyber Security Practice. He is based in Chicago.

Angela Jung is a senior member of Russell Reynolds Associates' Cyber Security Practice. She is based in Miami.

Harriet Wood is a senior member of Russell Reynolds Associates' Cyber Security Practice. She is based in London.

References

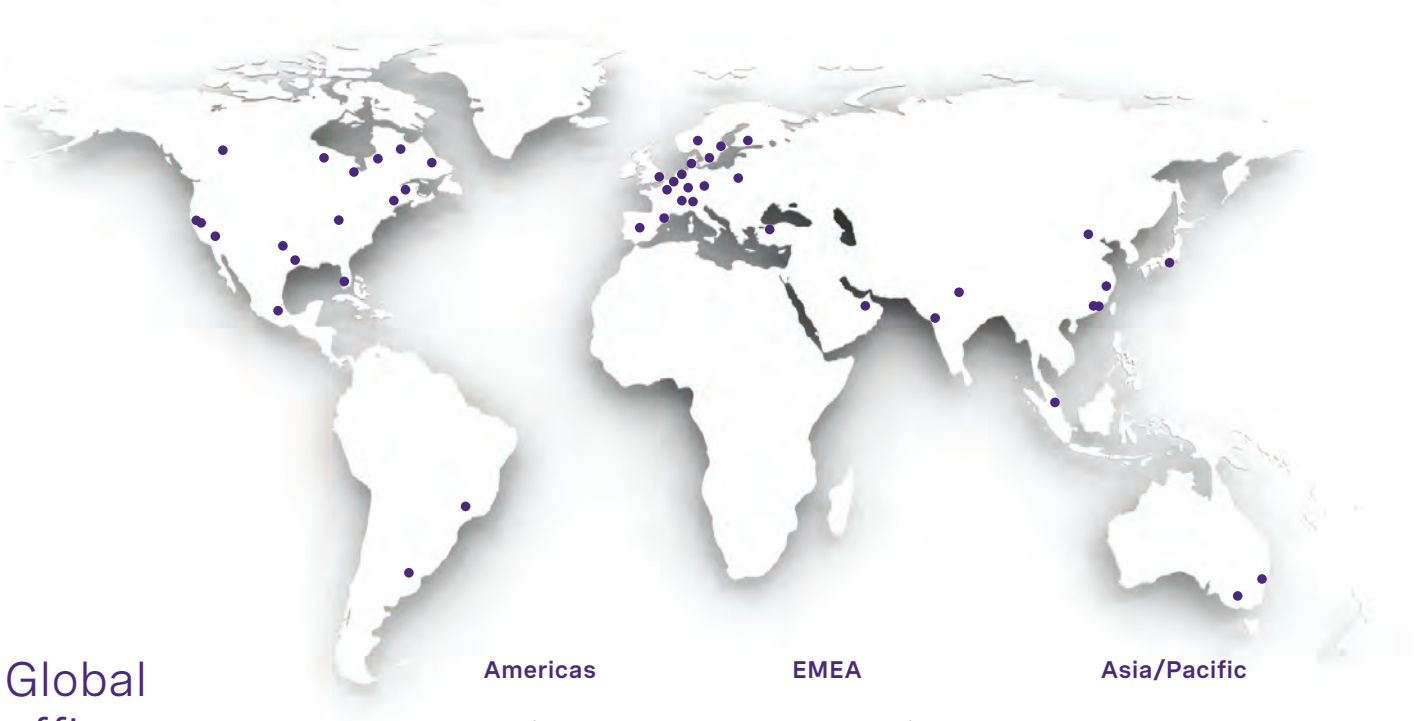
1. "Russell Reynolds Associates Global Leadership Monitor"

2. "NIST Cybersecurity Framework"

About Russell Reynolds Associates

Russell Reynolds Associates is a global leadership advisory firm. Our 600+ consultants in 47 offices work with public, private and nonprofit organizations across all industries and regions. We help our clients build teams of transformational leaders who can meet today's challenges and anticipate the digital, economic and political trends that are reshaping the global business environment. From helping boards with their structure, culture and effectiveness to identifying, assessing and defining the best leadership for organizations, our teams bring their decades of expertise to help clients address their most complex leadership issues. We exist to improve the way the world is led.

www.russellreynolds.com



Global offices

Americas

- Atlanta
- Boston
- Buenos Aires
- Calgary
- Chicago
- Dallas
- Houston
- Los Angeles
- Mexico City
- Miami
- Minneapolis/St.Paul
- Montreal
- New York
- Palo Alto
- San Francisco
- São Paulo
- Stamford
- Toronto
- Washington, D.C.

EMEA

- Amsterdam
- Barcelona
- Brussels
- Copenhagen
- Dubai
- Frankfurt
- Hamburg
- Helsinki
- Istanbul
- London
- Madrid
- Milan
- Munich
- Oslo
- Paris
- Stockholm
- Warsaw
- Zürich

Asia/Pacific

- Beijing
- Hong Kong
- Melbourne
- Mumbai
- New Delhi
- Shanghai
- Shenzhen
- Singapore
- Sydney
- Tokyo