Cyber Security:

The CISO Assessment Level Model CALM

Russell Reynolds ASSOCIATES

What level of CISO do you *have?*

The Cyber Level Model helps individuals and organizations work out where they currently are now and where they want to be in the future. This model uses the widely recognized NIST* framework to help evaluate the leadership of the cyber function.

Level 1 Most cyber functions operate at this level. Typically found in places where cyber is seen as an IT problem. Strong on access controls, less strong on detection and response. Knowledgeable about regulation. Less connected internally and externally. Rarely appears before the main board. Transactional. Suitable for organizations where the likelihood and impact of a cyber attack is low.

Level 2 Cyber seen more broadly than an IT problem. Innovates and transforms. Engages with other functions, e.g., HR. Protects, detects and responds to cyber issues. Weaker on recovery planning. Connected internally and externally. May appear before the main board. Relational and reactionary. Suitable for organizations where the likelihood of a cyber attack is high but the impact minor.

Level 3 As Level 2, stronger relational skills. Comfortable at main board level. Highly change oriented. Influential, innovative, uses data analytics. Shares information with industry peers. Anticipates. Suitable for organizations where the likelihood of a cyber attack is low but the impact severe.

Level 4 As Level 3, more strategic and innovative. Part of the DNA of an organization. Involved in all critical and highly confidential decisions, e.g., M&A. Manages new developments and changes. Suitable for organizations where the likelihood and impact of an attack is high.

What does the CISO do?	Level 1.0	Level 2.0	Level 3.0	Level 4.0
***Identify:** Critical assets and crown jewels	Average	Strong	Strong	Strong
***Protect:** e.g., *Access Control / Training / Data Security*	Strong	Strong	Strong	Strong
***Detect:** e.g., *Continuous Monitoring / Anomalies and Events*	Weak	Average	Average	Strong
***Respond**: e.g., *Communications / Mitigation*	Average	Strong	Strong	Strong
***Recover:** e.g., *Improvements / Recovery Planning*	Weak	Weak	Average	Strong
Automates as much as possible	Weak	Average	Average	Strong
Confidently protects all types of technology	Weak	Average	Average	Strong
Makes connections between physical and logical risk	Weak	Average	Average	Strong
Gets insight from data and analytics	Weak	Average	Average	Strong
Shapes the culture towards cyber	Weak	Average	Average	Strong
Gains control of new developments and changes	Weak	Average	Strong	Strong
Is integral to the digital innovation agenda, e.g., use of cloud	Weak	Average	Strong	Strong
Keeps knowledge current using external sources	Weak	Average	Strong	Strong
Shares information with industry peers	Weak	Average	Strong	Strong
Sets appropriate budget for cyber initiatives	Weak	Average	Strong	Strong
Stays connected with government agencies	Average	Average	Strong	Strong
Innovates with consumer devices and mobility	Average	Strong	Strong	Strong
Stays knowledgeable of the regulatory environment, e.g., GDPR	Strong	Strong	Strong	Strong

What approach does the organization take to cyber risk management?	Partial Approach*	Informed Approach*	Repeatable Approach*	Adaptive Approach*
	▪ Ad hoc cyber risk management	▪ News on cyber risks informally shared ▪ Set approaches to cyber risks in place	▪ Integrated cyber risk practices in place ▪ Organization wide approach to cyber in place ▪ External dependencies understood	▪ Cyber practices continually updated ▪ Cyber risk mgmt is part of the culture ▪ Active info sharing with third parties ▪ Organization anticipates cyber threats

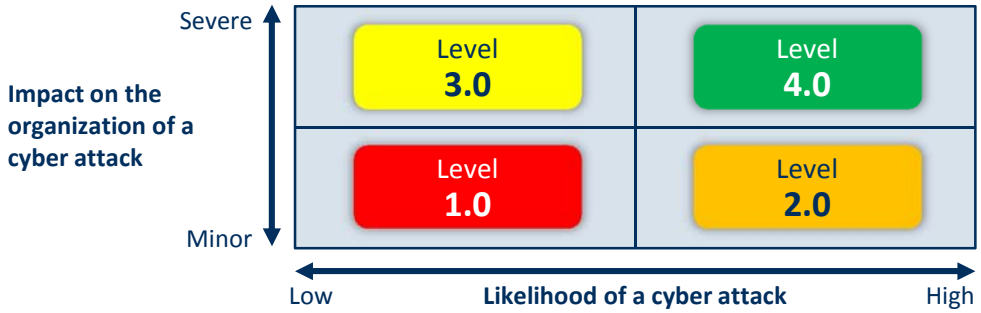
*National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*

Russell Reynolds ASSOCIATES

What level of CISO do you *need?*

What is the organizational attitude towards cyber risk?	Level 1.0	Level 2.0	Level 3.0	Level 4.0
Cyber seen as an IT problem	✓			
Cyber seen as a broader problem than IT		✓	✓	✓
Cyber risks of third party suppliers evaluated	✓	✓	✓	✓
Cyber a regular topic with the audit/risk committee	✓	✓	✓	✓
Organization open to testing, e.g., phishing and penetration testing	✓	✓	✓	✓
Organization open to cyber transformation programs		✓	✓	✓
Innovative approaches encouraged to staff education, e.g., videos		✓	✓	✓
HR engages with CISO, e.g., access controls, "Cyber Insider" and change programs		✓	✓	✓
CISO uses risk metrics to engage business leaders		✓	✓	✓
CISO is consulted widely in the enterprise on cyber issues			✓	✓
CISO trains NEDs in cyber awareness			✓	✓
CISO regularly briefs the main board on cyber and info risk			✓	✓
CISO Involved in confidential situations, e.g., M&A plans				✓
Nature of internal relationships	**Transactional**		**Relational**	
Style of interactions	**Reactionary**		**Anticipatory**	
Compensation	**$**	**$$**	**$$$**	**$$$$**
What level do you need your CISO to influence at internally?	**IT & Operations Level**		**Exco & Board Level**	
Leadership competencies required to operate at this level				
Results orientation	**High**	**High**	**High**	**High**
Team leadership	**High**	**High**	**High**	**High**
Change orientation	**Medium**	**Medium**	**High**	**High**
Influencing and collaboration	**Medium**	**Medium**	**High**	**High**
Strategic capability	**Low**	**Medium**	**Medium**	**High**

Where are CISOs most suitable?



Russell Reynolds Associates

GLOBAL CYBER SECURITY CONTACTS

MATT COMYNS
Stamford
+1 203 905 3353
matt.comyns@russellreynolds.com

TIM COOK
London
+44 20 7830 8045
tim.cook@russellreynolds.com

Russell Reynolds Associates is a global leader in assessment, recruitment and succession planning for boards of directors, chief executive officers and key roles within the C-suite. With more than 370 consultants in 46 offices around the world, we work closely 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, environmental and political trends that are reshaping the global business environment. Find out more at **www.russellreynolds.com.** Follow us on Twitter: **@RRAonLeadership**

GLOBAL OFFICES

Americas

- Atlanta
- Boston
- Buenos Aires
- Calgary
- Chicago
- Dallas
- Houston
- Los Angeles
- Mexico City
- Minneapolis/ St. Paul
- Montréal
- 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
- Seoul
- Shanghai
- Singapore
- Sydney
- Tokyo