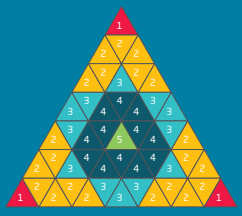
The CISO & Information Risk Officer Model (CIRO)

Balancing cyber defence with risk appetite and digital innovation



KAFUE

Does your organisation balance cyber defence with digital innovation and risk appetite?

How exposed are you and how do you balance digital innovation and cyber risk?

Minimal risk

What is your current exposure to digital risk?

- **Least Risk:** Limited use of technology, few computer applications. No external connections.
- **Minimal Risk:** Low complexity; low variety of products, some in-house and outsourced systems. Some connections to 3rd parties.
- **Moderate Risk:** greater transaction volume more sophisticated systems. Diversity of channels and products. Some IOT and more outsourcing.
- **Significant Risk:** complex & sophisticated technology used, including IOT. Complex supply chain and substantial connections to 3rd parties. Emerging technologies used.
- **Highest Risk:** extremely complex technology and myriad of products & services offered. Hyper connected. Widespread use of emerging technologies. Dependence on sophisticated 3rd parties.

Highly damaging

What would be the financial impact on you of cyber attacks?

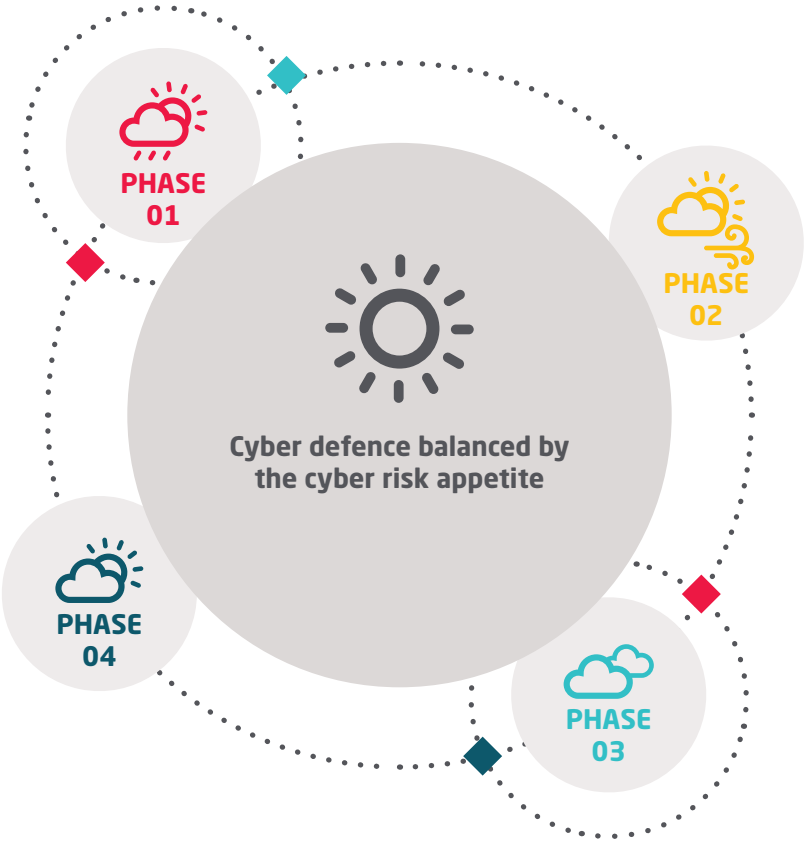
- **Hygiene factor only:** The financial losses we would incur will not affect our trading.
- **Irritation:** The financial losses we would incur would impact the current quarter only.
- **Short term impact:** The financial losses we would incur would have an impact in this fiscal year.
- **Highly damaging:** The financial losses we would incur would have a financial impact beyond this fiscal year.
- **Terminal:** The financial losses we would incur would be catastrophic for the business.

Balanced approach

How do you balance digital innovation & cyber risk?

- No appetite for cyber risk from digital innovation
- Cautious approach to innovation taken within strict cyber risk parameters.
- Balanced approach taken to innovation and cyber risk.
- Innovation a key business driver, within looser cyber risk parameters.
- Digital innovation a strategic business imperative any cyber risks will be managed as they arise.

How is your cyber defence plan influenced by your cyber risk appetite?



Phase 01
Evaluate inherent exposure to cyber risk.

Phase 02
Assess scope and effectiveness of cyber risk controls.

Phase 03
Develop cyber improvement plan.

Phase 04
Monitor operational performance and progress against the plan.

Introducing the CISO & Information Risk Officer (CIRO) Model

Not all cyber risk appetites are the same, and neither are CISOs. The CIRO model helps to clarify what good looks like in the function that manages cyber and information risk.

The model shows five levels of CISO and Information Risk Officers: Level 1 (the lowest level) represents about 50% of the market and Level 5 represents the top 1% of CISOs worldwide, many of whom are in the US. As CISOs progress through the maturity levels they become increasingly involved in balancing cyber defence and information protection decisions with the appetite for risk in their organisations and the strategic importance of digital innovation.

The CIRO Levels

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. Less connected internally and externally. Rarely appears before the main board. Transactional. Reactive and audit Led. Best suited in less complex organisations where there is no appetite for risk from digital innovation and the financial impact of a cyber attack is not expected to impact trading.

2

As Level 1 but cyber seen more broadly than an IT problem. Engages with other functions, e.g., HR. Weaker on recovery planning. Connected internally and externally. May appear before the main board. Relational and reactionary. Best suited in more complex organizations with some diversity of products and channels, where the financial impact of a cyber attack would only last for a trading quarter, and a cautious approach to innovation is taken with a limited appetite for risk. Knowledgeable about regulation. Technology focused.

3

As Level 2, but with stronger relational skills. Comfortable at main board level. Change oriented. Has influence, will be innovative. Shares some information with industry peers. Anticipates. Is aware of risk appetites. Suitable for organizations where there is complex and sophisticated technology in use, including IOT, and substantial connections to 3rd parties, where the financial impact of a cyber attack may last for a fiscal year, and a balanced approach is taken to digital innovation and risk.

4

As Level 3, more strategic, innovative and influential. Part of the DNA of an organization. Involved in all critical and highly confidential decisions, e.g., M&A. Starting to use the language of risk appetite in decision making. Suitable for organizations where there is extremely complex technology in use, eg process control networks, and a myriad of critical connections to 3rd parties, where the financial impact of a cyber attack could last beyond a fiscal year, and where digital innovation is important but takes place within a risk appetite framework.

5

As Level 4 but a trusted advisor at executive and Main Board level, and a regular attendee at the board meetings of other companies especially those in the same ecosystem. Will frame all cyber investment decisions through the lens of business risk appetite, could make a good Non Executive Director. Suitable for large scale sophisticated global organizations that are hyper connected, where the impact of a cyber attack could be terminal on the business but where digital innovation is a strategic imperative and the appetite for risk is high.

Cultural behaviors

Nature of internal relationships	Somewhat Transactional	Mostly Relational	Always Trusted
Style of interactions	Often Reactionary	Usually Anticipatory	Always Advisory
Influential at	IT Level / Ops Level	Internal EXCO & Board Level	Internal & External EXCO and Board Level

Leadership competencies required to operate at this level

Cyber & Information Risk Leadership Competencies	1	2	3	4	5
Results orientation & fast execution	Low	Medium	Medium	High	High
Agile Team leadership	Low	Medium	Medium	High	High
Change orientation & Adaptability	Low	Medium	Medium	High	High
Influencing and constant collaboration with stakeholders	Low	Low	Medium	Medium	High
Data driven strategic insight and clear vision	Low	Low	Medium	Medium	High

What level of CISO do you need?

Where are you in your journey to a comprehensive cyber risk management strategy?

START

Stage 1

Cyber risks partially understood*

Level 1 often found here but Level 2 needed to continue the journey

Stage 2

Informed understanding of cyber risk*

- Business units own identification of cyber risk activities
- CISO presents to exco and main board
- Audit looks at broader business impact of cyber
- Informal information sharing in sector
- Awareness of supply chain cyber risks
- No formalised policies in place

Level 2 and 3 are well suited here

Repeatable approach to risk*

Stage 3

ONWARDS

Stage 4

Adaptive approach to cyber risks in place*

- Comprehensive cyber risk management strategy in place
- Audit assesses whether cyber risk management strategy is appropriate
- CISO drives execution of cyber risk management strategy across enterprise
- CISO identifies measures and manages cyber risk at business unit level
- Culture of continuous improvement from lessons learned
- Cyber information actively and regularly shared with partners
- Real time understanding of supply chain cyber risks
- Strong relationships in place with partners affected by supply chain cyber risk

If this is as far as you are going to travel then Level 3s work well. If you are continuing to build then Level 4 and 5 are good

Level 5 often found here but a good development option for a Level 3

*NIST Cyber Security Framework

How effective are your leaders?

This is an important part of your journey. Go through the table below and see at what level you believe your CISO functions are currently at and where you want them to get to. This will then help you map out the development journey ahead to create a really effective CISO function.

Increasing maturity →

	How aware are CISO leaders in these areas:	1	2	3	4	5
Identify*	• Understand the business context • Understand critical Resources & related Risks • Identify Key assets & crown jewels and how they are managed • Be aware of critical business events • Identify governance gaps • Influence the cyber management strategy	Limited awareness	Limited awareness	Some awareness	Some awareness	Strong awareness
Protect*	Limit or contain the importance of a cyber event by: • Access control • Awareness & training • Data security & information protection • Maintenance & protective technology	Some awareness	Some awareness	Some awareness	Strong awareness	Strong awareness
Detect*	Timely discovery of cyber & information intrusions by: • Identifying anomalies & events • Continuous security monitoring • Detection processes	Limited awareness	Some awareness	Strong awareness	Strong awareness	Strong awareness
Respond*	Contains the impact of a cyber and information breach by: • Responsive planning • Good communications • Root cause analysis • Mitigation and improvement	Some awareness	Some awareness	Some awareness	Strong awareness	Strong awareness
Recover*	Restore impaired capabilities and services by: • Good recovery planning • Implementing improvements	Limited awareness	Some awareness	Strong awareness	Strong awareness	Strong awareness

How often does the CISO Leader do these things:	1	2	3	4	5
Uses risk metrics to engage business leaders	Seldom	Often	Often	Frequently	Frequently
Automates as much as possible	Seldom	Often	Frequently	Frequently	Frequently
Utilizes critical security controls e.g. NIST to enable cost effective cyber defense	Seldom	Often	Frequently	Frequently	Frequently
Consults widely in the business, e.g. engaging HR on Access Controls, Insider threats and change programs	Seldom	Seldom	Often	Frequently	Frequently
Shapes the culture towards cyber	Seldom	Seldom	Often	Frequently	Frequently
Is integral to digitization initiatives	Seldom	Seldom	Seldom	Often	Frequently
Gets appropriate budgets for cyber	Seldom	Often	Often	Frequently	Frequently
Develops unique innovative techniques to gain an advantage over adversaries	Seldom	Seldom	Seldom	Frequently	Frequently
Trains Main Board Members in cyber awareness	Seldom	Seldom	Often	Often	Frequently
Briefs the Main Board on the cyber situation	Seldom	Often	Frequently	Frequently	Frequently
CISO briefs other company boards and/or Govt Agencies on all aspects of cyber	Seldom	Seldom	Often	Frequently	Frequently

*NIST Cyber Security Framework

Background

In carrying out cyber search assignments for clients it was clear that whilst there had been considerable progress on defining standards and approaches for dealing with Cyber Security, including the widely adopted NIST* Cyber Security Framework, there was little clarity on understanding what good looked like in the leadership of the cyber function itself. We therefore set ourselves the task of seeing whether we could define a maturity model for CISOs that also included the NIST* Cyber Security Framework. We tested the first version of this at the RSA conference in San Francisco in February 2016, and received good feedback but there was plenty missing. Over the next several months we had numerous conversations with CISOs, CIOs, consultancies (including the Big 4), main board members and officials dealing with cyber and information risk including in the national security sector. With their feedback we iterated the model and improved it. We used the model in workshops where we got CISOs to evaluate themselves against it, and we presented it to numerous clients to help define what they were looking for in the leadership of the cyber function. The first version of the model was accessible on the NIST* website in 2016, and an updated version called the Cyber Leader Assurance Model (CLAM) came out in 2017.

However, it has become increasingly urgent that cyber cannot be seen in isolation from the pace of digital innovation and appetite for risk in an organisation. We have therefore launched a completely overhauled model that aims to clarify what good looks like for CISOs trying to balance cyber protection with digital innovation and various risk appetites in their organisations. We have called this the CIRO Model which now has five maturity levels within it.

Next steps

The CIRO Model is a framework to help organisations, and individuals, understand where they are in balancing cyber defence with risk appetite and digital innovation. If you are interested in learning more, or asking us to assess and develop your own cyber and information risk functions, please contact Tim Cook on tim.cook@kafue.io

Kafue

Careers in a digital age are like riding a river in full flow: each day will be very different to the day before; collapsing timeframes for decision making, creating new opportunities and threats that we had not seen before. Trust and reputation in the digital age can be catastrophically and rapidly lost through a breach of information security. In these conditions executives face profound challenges in assuring security, sustaining operations, acquiring insurance cover, maintaining confidence, and building the resilience necessary to restore capability and confidence. Kafue is a multi-disciplinary consultancy with a sharp focus on leadership resilience and capability of individuals and teams in digital roles that encounter a high degree of ambiguity. Every service that Kafue offers is focused on strengthening your executive teams and reducing risk:

- Headhunting of cyber leaders and those roles at the interface of digital transformation and technical risk including CISOs, CIOs and CTOs
- Comprehensive executive assessment, development and succession planning
- Psychometrics and benchmarking against cyber leadership maturity models
- Building resilience and agility in executive teams
- Managing the Insider Risk

Kafue will donate 5% of its profits for conservation, clean water and coaching initiatives in the Zambezi River Basin, an ecosystem under extreme threat, but also an area of outstanding beauty and opportunity flowing through not only the world's largest conservation area, but also the world's largest waterfall: Victoria Falls.

For more information or a discussion on how to benchmark your own cyber function contact:

Tim Cook
t: +44 207 873 2477 e: tim.cook@kafue.io

KAFUE