KRM22

Best Practices Guide to Cyber Security

BEST PRACTICES GUIDE TO CYBER SECURITY

EXECUTIVE PERSPECTIVE

Cyber Risk has been moving up the board and executive agenda for the last 10 years and this was only accelerated during the COVID-19 pandemic. As traditional modes of office working were swapped for remote working, rapid digitalisation was followed by a significant increase in the level of cyber threats and vulnerabilities faced by many firms. As the pandemic took hold it became increasingly clear that the level of cyber incidents had increased dramatically.

On August 4, 2020 Interpol released a statement, "INTERPOL report shows an alarming rate of cyberattacks during COVID-19" in which they stated that due to COVID-19, cybercrime had seen a significant shift from targeting individuals and small businesses to targeting major corporations, governments and critical infrastructure.

> *"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."*
>
> *Jürgen Stock, INTERPOL Secretary General*

On November 9, 2021, Businesswire reported on the findings from a McFee Enterprise and FireEye research report about cyber security and the pandemic which indicated that 81% of global organizations experienced increased cyber threats with 79% experiencing downtime due to a cyber incident during the pandemic.

At the start of 2022, with firms attempting to return to (a new) normal, many began re-evaluating and reassessing their approach to Cyber Risk Management. At the same time, the cyber threat landscape dramatically changed again as Russian tanks rolled across the borders of Ukraine and launched a major war in Europe. Undoubtedly, firms, including financial services firms, governments, and critical infrastructure, are likely to be targeted directly or suffer the spill over effects as part of this 'cyber warfare'.

REGULATORY PERSPECTIVE

Just as Cyber Risk has moved up the board and executive agenda, so too has it moved up the regulatory agenda.

UK

To understand the UK regulatory perspective on Cyber Risk, we need to start from the statutory objectives of the two regulators: the FCA (protect consumers, protect & enhance market integrity, promote competition) and the PRA (promote the safety and soundness of regulated firms).

The most relevant guiding principles from the FCA Rulebook (https://www.handbook.fca.org.uk/) are;

- Principle 3 of the Principles for Businesses
- Principle 11 of the Principles for Businesses
- SYSC 3.11
- SYSC 3.2.6
- SUP 15.3..1

The most relevant guiding principles (for PRA regulated firms (See PRA Rulebook (https://www.prarulebook.co.uk/) are;

- Fundamental Rule 2
- Fundamental Rule 5
- Fundamental Rule 6

US

The SEC has focused on cybersecurity issues for many years, with particular attention on market systems, customer data protection, disclosure of material cybersecurity risks and incidents, and compliance with legal and regulatory obligations under the federal securities laws.

> *Data collection, storage, analysis, availability, and protection (including security, validation, and recovery) have become fundamental to the function and performance of our capital markets, the individuals and entities that participate in those markets, and the U.S. Securities and Exchange Commission ("Commission" or "SEC"). As a result of these and other developments, the scope and severity of risks that cyber threats present have increased dramatically, and constant vigilance is required to protect against intrusions.* *Jay Clayton, Sept. 2017*

The SEC's focus on Cyber Risk is set to increase with the recent passing of the Strengthening American Cybersecurity Act by the United States Senate which will hand greater powers to the SEC and require greater disclosure of cyber incidents.

BEST PRACTICE GUIDELINES

With the attention of Boards, Executives and Regulators alike, and the heightened cyber threat hanging over the capital markets industry, what is the right approach to managing this risk?

Taking a "Compliance to a Standard" or "Maturity-Based" approach

Faced with the need to improve the approach to Cyber Security, firms may start by focusing on compliance to one of many well established Cyber/Information Security frameworks, such as ISO27001 or the NIST Cybersecurity Framework. Alternatively, they may look to one of the various Cyber Maturity Models, such as the Crest Cybersecurity Maturity Model Certification (CMMC).

While these standards and maturity models do provide some useful guidance, experience shows that taking a "Compliance to a Standard" or "Maturity-Based" approach encourages a one size fits all, where every cyber risk is treated equally.

In an environment where the CISO is under increased pressure to demonstrate how cyber investments are lowering risk and driving a tangible ROI, this approach doesn't work. Rather than delivering a robust, resilient, and secure Cyber environment, it encourages a mindset in which everything must be measured and controlled resulting in an inefficient and costly Cyber Risk practice.

Taking a Risk-Based approach to Cyber Risk

Rather than attempting to address every cyber threat, close every vulnerability and tick every box embedded within standards and maturity models, forward-looking firms are taking a Risk-Based approach to Cyber Risk Management.

Detailed below are eight key steps firms can take to move towards a Risk-Based approach to Cyber Risk Management. In summary, they are:

1. **Embed your Cyber Risk Management framework into your Enterprise Risk Management framework and approach**
2. **Define your business model, strategic objectives, and related risks**
3. **Define and evaluate Enterprise Risks**
4. **Cascade objectives through the firm and align operational processes and change initiatives to the objectives**
5. **Define and evaluate Operational Risks**
6. **Align Information Systems and Assets to deliver strategic and operational objectives**
7. **Use the CIA Triad to prioritise Information Systems and Information Assets**
8. **Define and evaluate Information Risks**

Embed your Cyber Risk Management framework into your Enterprise Risk Management framework and approach

First and foremost, firms should integrate their Cyber Risk Management framework and approach into their overall Enterprise Risk Management framework and approach. It is important that Cyber Risks are reported at the executive level in a way that enables them to be understood, evaluated, and prioritised accordingly alongside other Enterprise Risks.

Ultimately, the firms board and executive decision-makers must be able to evaluate these risks collectively against the firm's risk appetite to determine where there is alignment, and where there is too much (or too little) cyber risk been taken.

Define your business model, strategic objectives, and related risks

For many firms deploying an enterprise risk management framework, the starting point is to ask, "what are our firm's key risks?". Unfortunately, this is the wrong starting point. The right starting point is to ask, "how does our firm create value?".

A firm's business model is paramount to answering this question; how does the firm create, deliver, and capture value? To define this, core value drivers should be identified and clearly specified.

Alongside the business model, firms must define a strategy, with clear strategic objectives for the short-term (typically next 12 months), the medium-term (typically next 3-5 years) and the long-term (typically 5 years plus). These time horizons can vary depending on the firm and industry best practice.

Define and evaluate Enterprise Risks

Getting clarity on the firm's business model and strategic objectives is the critical first step towards building an integrated risk management framework and embedding a risk-based approach to cyber risk management. Once this is complete a firm can then identify enterprise risks.

When defining Enterprise Risks, some firms find it useful to categorise these risks into three categories:

1. **Business Model Risk**

   The risk that the firm has the wrong business model for the current and near-future market? What are the key uncertainties within our business model? Also, could our competitive position or even business be at risk due to business model innovation by a competitor?

2. **Strategic Risk**

   The risk that the firm has made poor strategic choices when defining its strategy.

3. **Strategic Execution Risk**

   The risk that the firm will fail to execute its strategic objectives.

Cascade objectives through the firm and align operational processes and change initiatives to the objectives

Once the firm has a set of strategic objectives defined, the next step is to cascade those objectives through the firm so that each business unit has a set of objectives that are linked directly to the overall firm's objectives.

Objectives should be operationalised through operational processes (the day-to-day activities for the firm) and change initiatives (the change activities within the firm to close performance gaps, bring risk into appetite thresholds or build capabilities for the future).

Define and evaluate Operational Risks

The Basel Committee defines operational risk as the "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". Therefore, getting clarity on the firm's processes and change initiatives are an important step preceding the definition of operational risk.

Additionally, by defining the alignment of processes and change initiatives to strategic objectives, this provides further insights into potential operational risks and the potential strategic impact of those operational risks.

Align Information Systems and Assets to deliver strategic and operational objectives

Alongside people & culture (which is outside of the scope of this document), Information Systems and Information Assets are core enablers for a firm as it seeks to deliver its strategic and operational objectives.

Therefore, firms should create an inventory of all their information systems and the information assets that those systems support.

Use the CIA Triad to prioritise Information Systems and Information Assets

The CIA Triad is a widely used information security tool that is designed to enable firms to prioritise and manage Information Systems and Assets based on their relative value to the firm.

The CIA triad is made up of:

- **CONFIDENTIALITY**

  This relates to who can access and modify systems or information assets.
- **INTEGRITY**

  This relates to how systems and information assets are managed over their lifecycles so that they are not improperly modified either accidentally or maliciously.
- **AVAILABILITY**

  This relates to when systems and information assets are available for users and automated processes.

Define and evaluate Information Risks

With an inventory of Information Systems and Assets, defining and evaluating risks related to these items often begins by developing a comprehensive understanding of the firm's information technology threats and vulnerabilities.

Understanding the attack surface is increasingly important in a post-COVID-19 environment where most staff are working in a hybrid mode (resulting in a less well defined and more fluid attack surface). There has also been a significant increase in the use of cloud computing and SaaS applications, significantly changing the attack surface post-pandemic as compared to pre-pandemic.

Once the risks related to Information Systems and Information Assets have been defined and evaluated, CIA ratings can provide guidance and insights into the potential operational impacts and consequences should those risks materialise.

Whereas, the potential strategic impact and consequences of any information risk can be better understood by linking Information Systems and Assets to strategic objective where applicable.

ABOUT THE RISK COCKPIT

The KRM22 Risk Cockpit is an Integrated Risk Management (IRM) application that enables firms to reduce their use of cumbersome spreadsheets and reduce their reliance on manual risk management processes. In doing so, we deliver a real-time, firm-wide, single version of risk truth with drill-down and drill-across capabilities, covering each of the five domains of risk: Enterprise Risk, Market Risk, Compliance Risk, Operational Risk and Technology Risk.

Within the Cyber Risk domain, we work with CISOs and other senior Cyber Risk professionals who are tasked with building a robust approach to Cyber Risk Management to lower the firm's cyber risk and deliver better, timelier, and more accurate risk-based management information.

Often, they struggle under the burden of multiple spreadsheets, a vast number of cyber security systems to monitor (as many as 30 in some cases), and critical information being sent (and sometimes missed) via email. They are frustrated by the lack of real-time, event-driven risk information which is required to improve the day-to-day management of their cyber risk whilst also making it easier, faster, and less painful to generate operational and executive-level reports which are consistent across the firm.

Visit www.KRM22.com to find out more and sign up for the KRM22 Risk Cockpit, for free.