NTT Security

NTT Communications
Transform. Transcend.

Embracing The New Security Normal

Why Cybersecurity Fortification Initiative (CFI) Changes Your Security Equation

Luke Ma
Head of Consulting, Asia
NTT Security

THE STARTING POINT

Massive ransomware threats, organized cybercrimes, cloud-based botnet intrusions and frequent DDoS attacks – You can be forgiven to think that we are under siege of an ongoing cyberwar. The real truth is that the global economy is becoming more digitally connected. Network attacks, mobile malware and intrusions are no longer an IT concern but a business one.

The financial services industry (FSI) is no different. As many digitalize for operational efficiency, market agility and innovation, hackers are exploiting loopholes and the weak links within the interconnected platforms to stage an attack. For FSI players, the damage is multifold, including business data loss, disrupted operations, and unrecoverable trust of end-customers and regulatory bodies. The threat to banks can also continue after the attack, as hackers use stolen data for ransomware or to sell on the lucrative black market for other malicious uses.

There are global security governance frameworks that address this, offering a good starting point for firms to understand gaps in their current cybersecurity strategy. But in a highly regulated industry like FSI, where local regulations are becoming more clinical, a more practical and localized approach is needed.

Enter **Cybersecurity Fortification Initiative (CFI)**. Launched in May 2016 by the Hong Kong Monetary Authority (HKMA), the initiative aims to raise the level of cybersecurity of banks and better equip banking professionals to face emerging cybersecurity challenges.

CFI IN A NUTSHELL

In essence, CFI addresses three key concerns of cybersecurity: **governance, training and resilience**. For governance, CFI proposed the Cyber Resilience Assessment Framework (C-RAF), a common risk-based framework for all Authorized Institutions (AIs) in Hong Kong (i.e. the banks) to assess their maturity of cybersecurity protection, detection and resilience measures, as well as applying appropriate measures to close the gaps in cybersecurity controls.

C-RAF covers three stages:

- Inherent Risk Assessment that will examine the bank's risk exposures based on the business complexity and operations;
- Cyber Maturity Assessment, a comprehensive control assessment program covering seven cyber domains; and
- Intelligence-led Cyber Attack Simulation Testing (iCAST) for banks with inherent risk level assessed to be 'medium' or 'high' level.

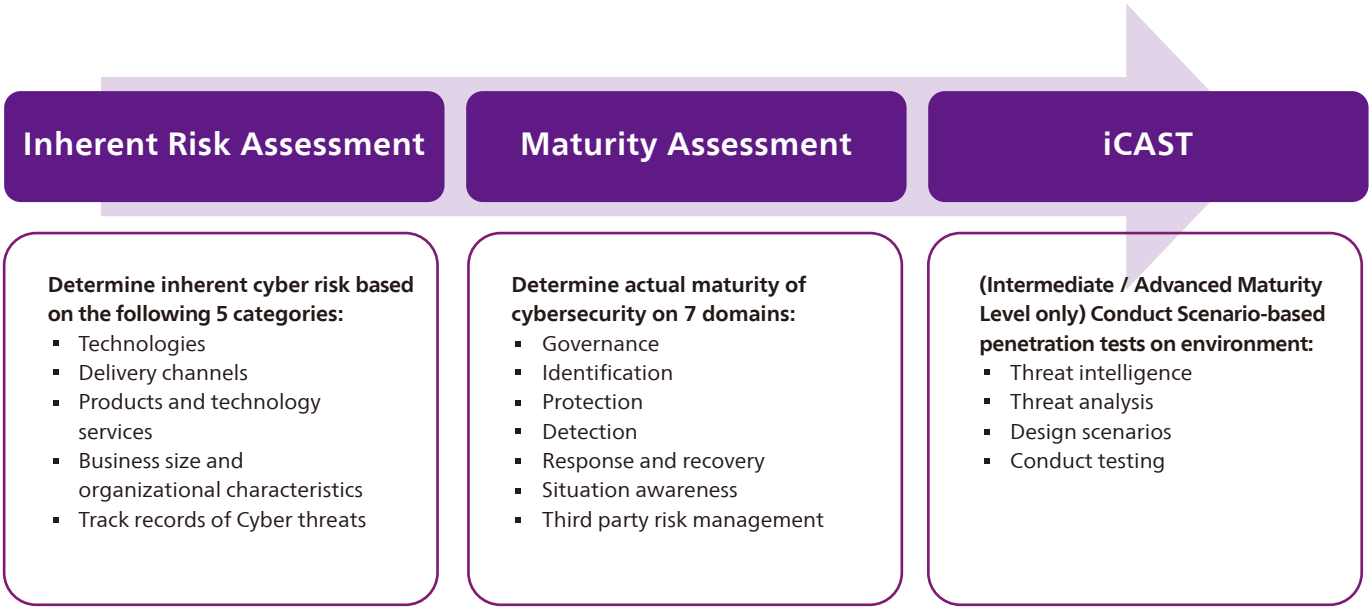
For training, CFI is launching the Professional Development Program (PDP). To be developed together with Hong Kong Applied Science and Technology Research Institute (ASTRI) and Hong Kong Institute of Bankers (HKIB), PDP will offer a certification program for cybersecurity professionals in banking.

The Cyber Intelligence Sharing Platform (CISP), which addresses resilience, underscores the importance of sharing threat intelligence across the industry. Established together with ASTRI and Hong Kong Association of Banks (HKAB), the platform aims to lay the foundation for cybersecurity intelligence exchange among critical infrastructure entities, enabling timely information sharing to allow precautionary measures to be taken in combating cyber attacks.

The framework is meant to be exhaustive and covers various departments in banks, including the board and senior management, compliance, risk management, information security, IT and even legal. It aims to reinforce Hong Kong SAR's role as a regional financial services hub, and acknowledges that an industry-led approach is needed to protect data and reinforce the trust of its end-customers.

CFI continues efforts by other regulators to shore up cybersecurity. UK has CBEST, led by the Bank of England. In China, the new cybersecurity law will shape how data is collected, protected and used. In Singapore, the Cyber Security Agency was formed to manage cyber incidents and raise standards across all industries. Meanwhile, Australia launched its own Cyber Security Strategy that closely aligns with the US's Center of Strategic and International Studies (CSIS) recommendations for the US Government.

For global and regional banks, meeting the regulations and compliance in different countries can be a huge challenge and requires a lot of manpower as well as collaboration of internal and external resources. For many, outsourcing to professional cybersecurity services firms with a global presence is an option worth considering.



KEY TAKEAWAY

1. Start Preparing Today

CFI is already here. Key timelines to remember:

- **End of Sep 2017**: 30 major local and multi-national banks, selected by HKMA for the first phase of implementation to complete Inherent Risk Assessment and Cybersecurity Maturity Assessment.
- **End of Jun 2018**: iCAST, applicable to banks with inherent risk level assessed to be 'medium' or 'high' level, to be completed.
- **Late 2018**: The second phase covering all remaining banks, expected to complete the assessments and submit the reports to HKMA.

Although there seems to be ample time for most banks to adopt a "wait and see" stance, it takes a considerable amount of effort and time in planning, budgeting, allocating resources, and implementing measures on "People, Process and Technology" to ensure that banks are cyber-resilient. The best advice is to start preparing for it now.

2. In-house vs Outsource

Maintaining CFI is a bank's responsibility, and it requires a lot of resources, including the right solutions and talents. This could mean significant investment. A clear understanding of whether there are gaps in the infrastructure and talent pool can help decide what to pursue in-house and outsource. In addition, outsourcing security consulting and Managed Security Services (MSS) may be a viable option.

3. People, Processes and Partners

Building a strong cybersecurity governance architecture that is holistic and not dependent on point solutions is important. It also needs to cover people, processes and partners. In an increasingly interconnected environment, governance should also be extended to all stakeholders.

4. Invest in Intelligence

Subscribing to the right threat intelligence service providers or leveraging threat intelligence from MSS providers can enhance the banks' "situational awareness" against emerging cybersecurity threats, and promptly prepare for appropriate security measures in advance. By proactively sharing these information, banks will be able to take timely precautions, and coordinated decisions around risk management and cybersecurity.

5. Leverage Your IT Partner

Preparing to comply with CFI can be daunting for those unprepared – especially when banks work with many third-party service providers. The C-RAF itself includes clear expectations in managing and assessing the security risk of third-party service providers exchanging and processing a bank's data. Banks can leverage a reputable vendor's infrastructure, network connectivity and facilities that are proven to be cyber resilient. It allows you to take advantage of the vendor's continual investment in cybersecurity and pool of expertise, while ensuring compliance to current security and privacy regulations across your different areas of operations.

6. Prepare for the Long Haul

Security does not end with CFI. Cyber threats are always evolving. By keeping close communications with regulators, professional bodies, and security services providers, banks keep themselves informed of emerging cybersecurity trends enhancing their cyber resiliency.

OTHER SECURITY REGULATIONS

Securities & Futures Commission (SFC) of Hong Kong

Mar 2016 – Circular to All Licensed Corporations on Cybersecurity

Focuses on cybersecurity controls including risk assessment against SFC regulated corporations, risk assessment against service providers, awareness training, incident management processes and data protection programs.

Oct 2016 - Commencement of Cybersecurity Review on Internet & Mobile Trading Systems

Covers a questionnaire to SFC regulated corporations for cybersecurity assessment against internet /mobile trading systems, SFC's on-site inspection of selected brokers, and benchmarking of SFC regulatory requirements.

SWIFT

Mandatory Customer Security Requirements

Covers 3 objectives, 8 principles and 27 controls. The final control descriptions are now available, with SWIFT requiring mandatory enforcements in January 2018.

WHY NTT GROUP COMPANIES?

NTT Security is the specialized security company of NTT Group. With embedded security, we enable Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of consulting and managed services for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world.

More importantly, NTT Security adopts a full security life cycle approach to address cybersecurity concerns. Many aspects are already mirrored in the CFI requirements. It begins with understanding your business, current risks and existing solutions before developing the right programs and controls. It offers a natural first step toward complying with CFI.

In all, through the wide partnership network and working closely with NTT Group Companies especially NTT Communications, together we enable your cyber resilience using a combination of consulting, managed, cloud, and hybrid services.

NTT Com Asia Limited

Tel: (852) 3793 0288 | Fax: (852) 2521 0081
Email : marketing@ntt.com.hk
Website: www.ntt.com.hk