TACKLING CYBER THREATS HEAD-ON:
CYBERSECURITY BEST PRACTICES FOR FINANCIAL INSTITUTIONS

GROWING CYBER THREATS TO FINANCIAL INSTITUTIONS

Hong Kong's ranking of Internet threat in Asia-Pacific was 58th in 2014

http://www.singpao.com.hk/index.php?fi=history&id=16763

Banking sector is **300%** more likely to face cyber-attacks than any other sector

Source: Hong Kong Institute of Bankers (HKIB)
HKMA Guide to Enhanced Competency Framework on Cybersecurity

The global average annualised cost of cybercrimes per year amounted to **HK$59.73 million**

Source: HKMA Guide to Enhanced Competency Framework on Cybersecurity

140% increase in the total volume of malware detected in the finance sector since 2014

2016 NTT Group Global Threat Intelligence Report

More than **12%** of vulnerabilities were over 5 years old, and over 5% were more than 10 years old

2016 NTT Group Global Threat Intelligence Report

Average of **23%** organizations are capable of responding effectively to a cyber incident

77% have no capability to respond to critical incidents and often purchase incident response support services post the incident

2016 NTT Group Global Threat Intelligence Report

CYBERSECURITY FORTIFICATION INITIATIVE

- The **Cyber Resilience Assessment Framework (C-RAF)** is one of the three pillars of the Cybersecurity Fortification Initiative (CFI) undertaken by the Hong Kong Monetary Authority in collaboration with the banking industry
  - It is an **assessment tool for evaluating cyber risk exposure and resilience** and **helps to improve the best practices** on cyber resilience
- The assessment framework comprises the following three elements:

Inherent Risk Assessment

- Assess financial institution's level of current risk exposure
- Existing cybersecurity risks are categorized into 'low', 'medium' or 'high' in accordance to the outcome

Maturity Assessment

- Measurable process by mapping each inherent risk level to an expected maturity level of cyber resilience
- Roadmap to improve gaps between the expected level of resilience and actual level of resilience

Intelligence-led Cyber Attack Simulation Testing (iCAST)

- Simulation test scenarios designed to replicate real life cyber attacks based on latest threat intelligence.
- Financial institutions with inherent risk level assessed to be 'medium' or 'high' level, are expected to conduct iCAST

KEY STEPS TOWARDS C-RAF

Security Operations Services

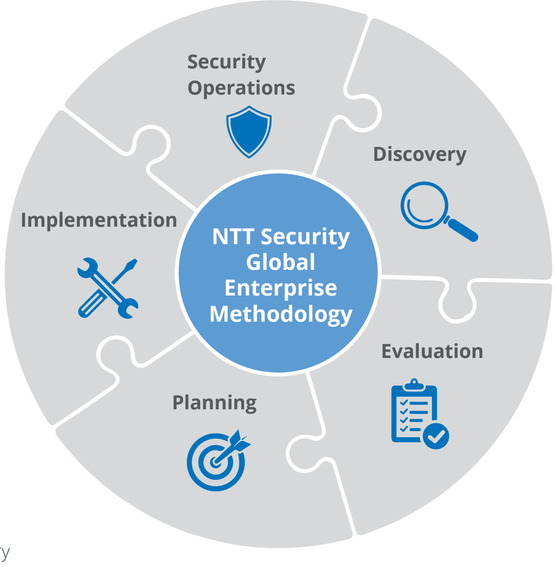
- Managed Security Services
- Regular Penetration Testing
- Incident Response Services
- Security Awareness Training

Technology Implementation Services

- To ensure client implement technology controls (eg. SIEM, UBA, IPS, NG-FW, DLP, NAC, etc.)
- Technology optimization

Architecture Planning and Design Services

- To assist client to design technology solutions
- Technology selection advisory



Cyber Resilience Assessment Services

- To discover & determine current Cyber risk exposure
- To evaluate the Cyber control effectiveness against HKMA C-RAF
- To prioritize identified gaps
- Inherent Risk Assessment
- Maturity Assessment
- iCAST Assessment

Strategic Security Consulting Services

- To develop actionable and practical security improvement roadmap

Should you have any questions on NTT Security Global Enterprise Methodology, please contact **Marketing-APAC@nttsecurity.com**