Position Paper on Cyber Security Preparedness

November 2020

Suresh Emmanuel
Chief Information Security Officer
Hatton National Bank PLC

Background

Cyber Security preparedness for a Bank would always be a challenging journey. Managing risks of People, Process and Technology becoming more thought-provoking with today's digitalized Banking context. Banks are becoming more prominent life style partner for customers. Different layers of digital channels have been opened to facilitate demanding customer needs and also to improve customer experience. With digitization, there are set of new technology risks opened for Banks which were not existed before. This risk exposure has resulted in new ways and means for hackers to explore. As a result, Cyber-attacks are becoming more innovative, complex and advance day by day. Hackers always able to find a way out from safeguards in place. A small weakness could be leveraged by an attacker to do a significant damage to an organization. There's a famous saying "An attacker only needs to be successful at occasion". A Bank should have systematical approach to improve its Cyber resilience. Cybersecurity can be an important and amplifying component of a Bank's overall risk management. A Bank shall consider to position itself based on below preparedness principles against its actual implementation.

Any organization should realize that there's no "Silver bullet" for Cyber and Information security while it's a journey of achieving different maturity levels over a period of time. Below systematical approach is prepared to improve Cyber resilience in a Bank. A Bank shall build a strategy to strengthen its Cyber Security preparedness in line to below principles;

- Identify;
- Protect;
- Detect;
- Respond; and
- Recover.

Below is detailed elaboration above principles and what's recommended to be in place.

Identify

01 Setting up Business Environment

- ✓ Establish Cyber security vision, mission and objectives
- ✓ Identify Priorities for Bank's Cyber security mission, objectives, and activities
- ✓ Identify dependencies for Bank's Cyber security mission, objectives, and activities
- ✓ Establish Cyber and Information security strategy
- ✓ Identify regulatory, statutory and contractual obligations
- ✓ Identify critical business processes and their resilience requirements
- ✓ Identify critical success factors for Cyber and Information security

02 Establishing Governance

- ✓ Appointment of Chief Information Security Officer
- ✓ Establishing Information Security Steering Committee
- ✓ Establishing Security Policies, Procedures and Practices
- ✓ Aligning information security practice as per a global standard
- ✓ Establish Information and Cyber security roles and responsibilities
- ✓ Establishing Information and Cyber Security annual activity plan
- ✓ Establishing Information and Cyber Security KPI's

03 Asset Identification

- ✓ Identification of Bank wide physical and systems within
- ✓ Identification of Bank wide software platforms and applications
- ✓ Identification of Bank wide communication channels
- ✓ Identification of Bank wide data flows
- ✓ Identification of Bank wide external connectivity's and systems
- ✓ Identification of Bank wide suppliers and their services
- ✓ Identification of external facing systems and services
- ✓ Identification of Bank wide interested parties
- ✓ Identification of Bank wide user access and their access rights
- ✓ Identification of Bank wide data types

04 Risk Management

- ✓ Establishing Bank wide Cyber and Information Security risk management process
- ✓ Establishing dedicated roles for Technology and Cyber risk management
- ✓ Establishing Board risk committee reporting hierarchy for Cyber and Information security related risks
- ✓ Establishing periodic Information and Cyber risk control assessments
- ✓ Establishing KRIs and related dashboards for Cyber and Information security risks
- ✓ Establishing Bank wide Cyber and Information security Risks tolerance criteria
- ✓ Bank wide Information and Cyber asset based threats, vulnerabilities and risks identified and documented
- ✓ Bank wide Information and Cyber asset based impacts and likelihoods are identified and documented

Protect

01 Identity and Access Management

- ✓ Establishing Bank wide user access matrices for all information assets
- ✓ Bank wide unique and secure user authentication is established
- ✓ Bank wide user access rights are documented and implemented
- ✓ Bank wide physical access is controlled and monitored
- ✓ Bank wide access is granted on least privilege and need to have basis
- ✓ Bank wide information asset access anomalies are tracked and actioned
- ✓ Bank wide remote access is managed
- ✓ Bank wide network access is controlled, authenticated and authorized
- ✓ Bank's privilege access to information assets are tracked and monitored
- ✓ Multi factor authentication is used for all critical information assets logins
- ✓ Bank's information assets Non repudiation is established
- ✓ Periodic user and privilege access review are performed
- ✓ Remote access is secured, controlled and managed
- ✓ Supplier access is secured, controlled and managed
- ✓ All privilege access is controlled through Privilege access management solution

02 Network and Communication Security

- ✓ Availability of next generation firewalls in network perimeter and internal network segments
- ✓ Ensuring threat protection, SSL Offloading, IPS and state full inspection is enabled in firewalls
- ✓ Availability of Next generation malware protection in firewalls
- ✓ Network is segmented into granular level segments and traffic between segments are controlled via firewall
- ✓ Firewall changes are tracked and controlled
- ✓ All web applications are protected with web application firewalls
- ✓ Inbound and outbound communication is encrypted
- ✓ Firewall and network communication security devices are configured alert anomalies
- ✓ Email security gateway is established with malware, phishing and next generation malware protection
- ✓ DOS and DDOS protection is established external facing web applications and network communication channels
- ✓ Periodic firewall rule review and cleansing process is established
- ✓ All network security devices are patched time to time
- ✓ Direct access to network security devices are eliminated controlled via Privilege access management or firewall management solution
- ✓ Controls to detect unsanctioned devices or service to network

03 Data Security

- ✓ Establishing of Bank wide data inventories, flow maps and dictionaries
- ✓ Ensuring Bank wide data at rest and transit are secured
- ✓ Bank wide data is classified and security controls are defined against each classification levels
- ✓ Protections against data leaks are implemented – E.g. Automated data classification, Data leakage prevention, Digital rights management, etc.
- ✓ Bank wide removable media access is controlled, monitored and protected
- ✓ Integrity checking mechanisms are used to verify software, firmware, and information integrity
- ✓ Ensure supplier data sharing is governed, controlled, secured and monitored
- ✓ The development and testing environment(s) are separate from the production environment
- ✓ Integrity checking mechanisms are used to verify hardware integrity
- ✓ Data communication is encrypted in all digital channels
- ✓ User awareness training to protect data, policies, procedures, etc

04 Vulnerability Management & Threat Protection

- ✓ Establishing Bank wide vulnerability management process
- ✓ Establishing all applications, operating systems, platforms, databases, software systems, etc. are patched for security vulnerabilities periodically.
- ✓ Ensure virtual patching solutions and compensative controls are available for systems with limitations
- ✓ Keeping systems that cannot be patched are placed in secure highly controlled network segments
- ✓ Establish Bank wide patch calendar
- ✓ Ensure malware protection is installed for all computer systems in the Bank
- ✓ Ensure group policies are enforced to all computers of the Bank to control execution, services, ports, etc.
- ✓ Ensure approved annual security testing plan in place and executed
- ✓ Ensure software baselining is implemented across the Bank
- ✓ Ensure Bank vendor released patches are tested and applied periodically
- ✓ Ensure all vulnerabilities are documented, classified and tracked for closure

05 Cryptographic controls

- ✓ Ensure all critical databases are encrypted
- ✓ Ensure all laptops are encrypted
- ✓ Ensure all removable media in use are encrypted
- ✓ Ensure confidential data across the Bank is encrypted
- ✓ Ensure all communication channels are encrypted with strong algorithm
- ✓ Data in mobile devices are encrypted
- ✓ API communication is encrypted
- ✓ Data between all web services are encrypted
- ✓ Mobile application data is encrypted
- ✓ All passwords are hashed and hashing iteration count is in line with a standard
- ✓ All Cryptography keys are securely stored, access controlled and managed
- ✓ Availability of Cryptographic key disposal and life cycle management process

Detect

01 Anomalies and Events

- ✓ Establishing Security event and information management system – SIEM and integrating all critical data sources
- ✓ Implementing effective and impactful correlation rules in SIEM
- ✓ Establishing 24*7 monitoring Security Operating Center – SOC
- ✓ Detected events are analyzed to understand attack targets and methods
- ✓ Event data are collected and correlated from multiple sources and sensors
- ✓ Impact of events is determined
- ✓ Incident alert thresholds are established
- ✓ The network is monitored to detect potential cybersecurity events
- ✓ The physical environment is monitored to detect potential cybersecurity events
- ✓ Personnel activity is monitored to detect potential cybersecurity events
- ✓ Malicious code is detected
- ✓ Unauthorized mobile code is detected
- ✓ External service provider activity is monitored to detect potential cybersecurity events
- ✓ Monitoring and detection for unauthorized personnel, connections, devices, and software is performed
- ✓ Vulnerability scans are performed to detect vulnerabilities on periodic manner
- ✓ Roles and responsibilities for detection are well defined to ensure accountability
- ✓ Detection activities comply with all applicable requirements
- ✓ Detection processes are tested – RED team testing, Penetration testing, etc.
- ✓ Event detection information is communicated to relevant stakeholders
- ✓ Detection processes are continuously improved
- ✓ Incident management process is adopted for all detected events which are converted into incidents
- ✓ All detection based intelligence are used for management reporting and analysis
- ✓ Compromise assessments are done based on defined frequency
- ✓ Ensure predictive analysis is conducted on detected cyber security events
- ✓ Deep and dark web analysis to detect any compromised Bank's information assets or data
- ✓ Social media scavenging monitoring performed to detect and compromise.

Respond

01 Analysis, Mitigation and improvements

- ✓ Establishing Cyber security incident response plan
- ✓ Testing Cyber security incident response plan at least annually
- ✓ Forensic investigations are performed
- ✓ Ensure root cause analysis and lessons learnt in place to avoid repetitive incidents
- ✓ Ensure 100% remedial actions for all detection based incidents
- ✓ Incidents are categorized consistent with response plans
- ✓ Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
- ✓ Public and media response procedure in a Cyber-attack are documented and tested
- ✓ Consider analysis output as input to Information security strategy, risk management, security budgeting and prioritization
- ✓ Continual improvement adopted in a systematical approach such PDCA cycle

Recover

01 Analysis, Mitigation and improvements

- ✓ Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
- ✓ Recovery planning and processes are improved by incorporating lessons learned into future activities.
- ✓ Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors
- ✓ Recovery strategies are updated periodically
- ✓ Cyber insurance could be considered as one of risk mitigation and recovery option
- ✓ Emergency contacts and parameters are up to date maintained
- ✓ Public relations are managed

Conclusion

Above parameters would provide a Bank to assess its positioning in identifying their current maturity level. A Bank should start its current state assessment and based on results shall build up a strategy towards a journey to achieve different levels of maturity over a period of time. Above positioning parameters Identify, Protect, Detect, Respond and Recover would cover actions to be taken holistically at ground level for a Bank in implementing effective security parameters. Periodic review and continual improvement should be done in a systematic approach through steering committees and top management to ensure safeguards are in place and effectively functioning. Enterprise level risk management function should include Cyber security and regular discussion item and it's also should be a regular discussion point in Board agenda. Top to bottom, bottom to top and across the organization with effective communication and awareness training are important aspects for a Bank to position itself in a comfortable place.