Practical Implementation of Cyber Security

August 2021

Suresh Emmanuel
Chief Information Security Officer
Hatton National Bank PLC

Background

Despite many frameworks and standards exist globally, practical implementation of Cyber and Information security is always a major challenge. There are different levels of challenges today's organizations face with the evolving threat landscape. There are overwhelming amount of cyber-attacks are taking place globally, making even difficult for Cyber security professionals to protect organization assts. Cloud computing and borderless infrastructure and software services made Cyber security professionals to be relentless to safeguard organizations.

Below listed are major challenges when it comes to "Practical Cyber Security Implementation"

- Prioritization;
- Budget – Cyber investments are expensive;
- Change resistance;
- Legacy systems;
- Lack of required skills;
- Leveraging of investment;
- Interoperability;
- Complexity; and
- No quick or invisible ROI.

To overcome above challenges and minimize gaps below effective and practical approach to Cyber Security implementation is suggested in this policy paper.

- A governance framework for Cyber Security;
- Preventive Controls;
- Intelligence, monitoring, detection and analysis;
- Reporting, response and mitigation;
- Recovery.

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

01 A governance framework for Cyber Security

- Choose a framework that in line with high security standards
- ISO/IEC 27001;
- NIST Framework;
- CIS Critical Controls;
- PCIDSS, etc.
- Implement and mature
- Awareness and Culture

02 Protect

Threat protection

- Zero day exploits;
- Zero day malware;
- Exploit techniques prevention;
- Cyber kill chain protection;
- Minimal services, applications, ports, etc
- Whitelisting of services.

03 Intelligence, monitoring, detection and analysis

Threat Intelligence

- Threats;
- Techniques;
- Potential campaigns, groups;
- Internal correlation;
- Prioritization.

Monitoring;

- Threats;
- Techniques;
- Potential campaigns, groups;
- Internal correlation;
- Prioritization.

04 Detection and Analysis

- Detection capabilities – Tools – SIEM, Visibility tools, etc.
- Deception
- Threat hunting
  - Reactive threat hunting
  - Proactive threat hunting
  - Indicators
  - IOCs - Compromises
  - IOCs – Concerns
  - IOAs – Attacks
  - TTPs – Tactics, Techniques and Procedures
    - ✓ Process pawning, Behavior, etc.

05 Reporting and response

Incident response and containment process

- Who's doing what
- Call trees
- CERT support
- Contractual agreements with Incident service providers
- Supplier chain arrangements
- Contain threat
- Transfer threat
  - Cyber Insurance
- Drill, Practice and fine tune