20th ACG Cross Training Seminar

Wednesday, October 24, 2018

Cyber Resilience

Muhammad Imran

Central Depository Company of Pakistan Limited (CDCPL)

Contents

- Introduction
- Five Pillars
- Key Points
- CDCPL Vision/Mission
- Five Pillars @ CDCPL

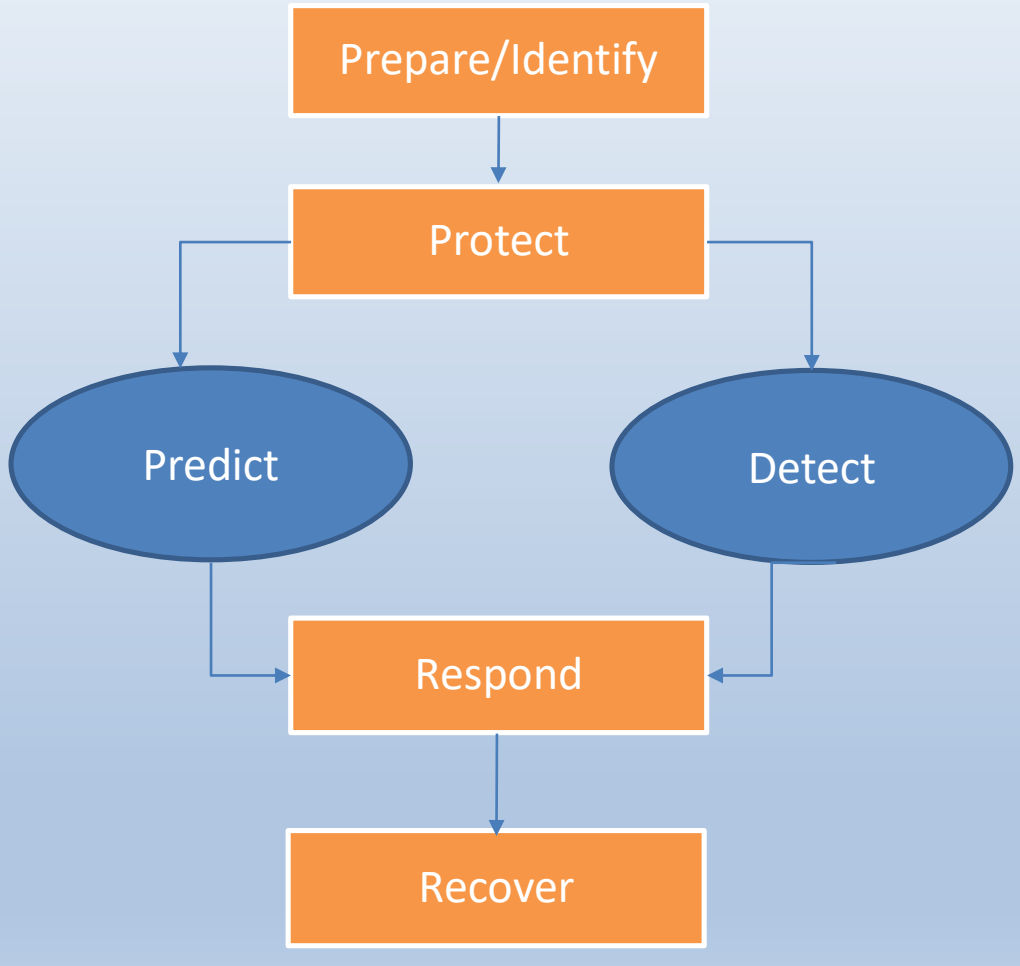
Cyber Resilience

- Cyber Resilience is the ability for an organisation to resist, respond and recover from incidents that will impact the information they require to do business.

Five Pillars of Cyber Resilience

- Pillar 1: Prepare/Identify
- Pillar 2: Protect
- Pillar 3: Detect
- Pillar 4: Respond
- Pillar 5: Recover

Five Pillars of Cyber Resilience



Pillar 1: Prepare/Identify (What is the impact?)

Risk Identification:

- Aggregated set of typical risks associated with cyber risk.

Risk Events:

- Scenarios that could impact the organization and are specific to cyber threats.

Pillar 2: Protect (How do we organize?)

Operating Model:

- Specifying the structure with people, organization, roles, tools and processes to govern.

Business & IT Controls:

- Continuous review of controls and their testing programs.

Pillar 3: Detect (How do we monitor?)

Operational Monitoring:

- Aligning the tools to identify and detect threats along with their escalation and management.

Detection & Identification:

- Tools & Systems to identify and logs, helping manage operations.

Pillar 4: Respond (How do we respond?)

Incident Response Plan:

- Structure to identify and manage action plans against use cases/different scenarios.

Crisis Management:

- Well defined process to handle incidents and notify impacted parties.

Pillar 5: Recover (How do we Recover?)

- This stage involves developing and implementing the appropriate systems and plans to restore any data and services that may have been impacted during a cyber attack.

Key Points of Cyber Resilience

Three key points were stressed when it came to developing a cyber resilience strategy:

- Consider the broader business objectives and how this cyber resilience strategy does its part in achieving the overall objective.

- Take the onus away from IT and engage leaders across the business. Cyber Resilience isn't just an IT problem, it's a business problem.

Key Points of Cyber Resilience

- Communicate planning to all staff, ensuring that they are well educated and engaged with on a regular basis – educating staff is especially important to ensure that employees are able to identify and deal with potential attacks when they do come through.

CDCPL Vision / Mission

- Provide secure, reliable and innovative solutions that systematically reduce risk, enable transparency and bring efficiencies to Capital & Financial markets.

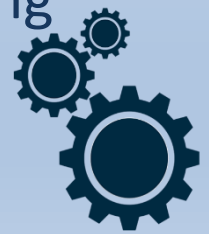
- Stimulating business growth and maximizing benefits for all stakeholders.

Pillar 1: Prepare/Identify @ CDCPL

- Humans are the weakest links. Modern day attacks are mostly driven by social engineering. So it is imperative to educate and train the users.

- CDCPL conducts regular security awareness trainings of all staffs including clients, third party contractors and vendors to ensure that users using CDCPL system(s) are well aware of the threats CDCPL is facing.

- To make awareness more effective, CDCPL has an eLearning portal to ensure all the staff can easily login to eLearning portal to get the security related content anytime.



Pillar 2: Protect @ CDCPL

- Protection is an essential component of cyber resiliency. CDCPL has taken various measures to protect its information assets.
- For protection, CDCPL conducts vulnerability scans of all its production and testing systems on a daily and weekly basis.
- In this vulnerability management program, including scanning to find vulnerabilities, reporting for patching and escalating the risk in case of any acceptance.

Pillar 2: Protect @ CDCPL

- All internet exposed web applications are protected with cloud based application firewalls.
- CDCPL has deployed state of the art technology to ensure protection of customers and at the same time preventing malicious actors to intrude the system.
- CDCPL also conducts third party penetration testing by engaging expert firms.

Pillar 3: Detect @ CDCPL

- Detection is really essential and without detection, prevention is never possible.
- CDCPL has deployed state-of-the-art SIEM solution, IPS, Firewalls and Anti-virus solutions.
- SIEM collects security logs from all servers and devices for event correlation and generate alerts on offenses and anomalies.

Pillar 4: Respond @ CDCPL

- CDCPL is ISO/IEC 27001:2013 certified for Information Security Management and is Pakistan's first company to receive ISO 22301 certification for its Business Continuity Management Program.
- CDCPL has a central incident response program. It has a forum where all the incidents are reported, assessed, prioritized, investigated and resolved.
- Intelligence built in Centralized monitoring solution that automatically respond to a service failure and takes action accordingly.

Pillar 5: Recover @ CDCPL

- CDCPL has appropriate Business Continuity (BCP) arrangements. Its primary Disaster Recovery (DR) site has been outsourced to a third party in recent past.
- CDCPL ensures Data replication is performed in real time to its Business Continuity / Disaster Recovery site.
- Regular DR Drills are conducted to ensure staff and system readiness.
- CDCPL has the tested capability to resume its operations from its Business Continuity / Disaster Recovery site in case of disaster.

It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.

– Stephane Nappo

Thanks

For feedback and suggestions: muhammad_imran@cdcpak.com