2020 Executive Report for Information Security Rick Management

Presenter : Perkins/ Date: 2020.10.26

Information System Security Management

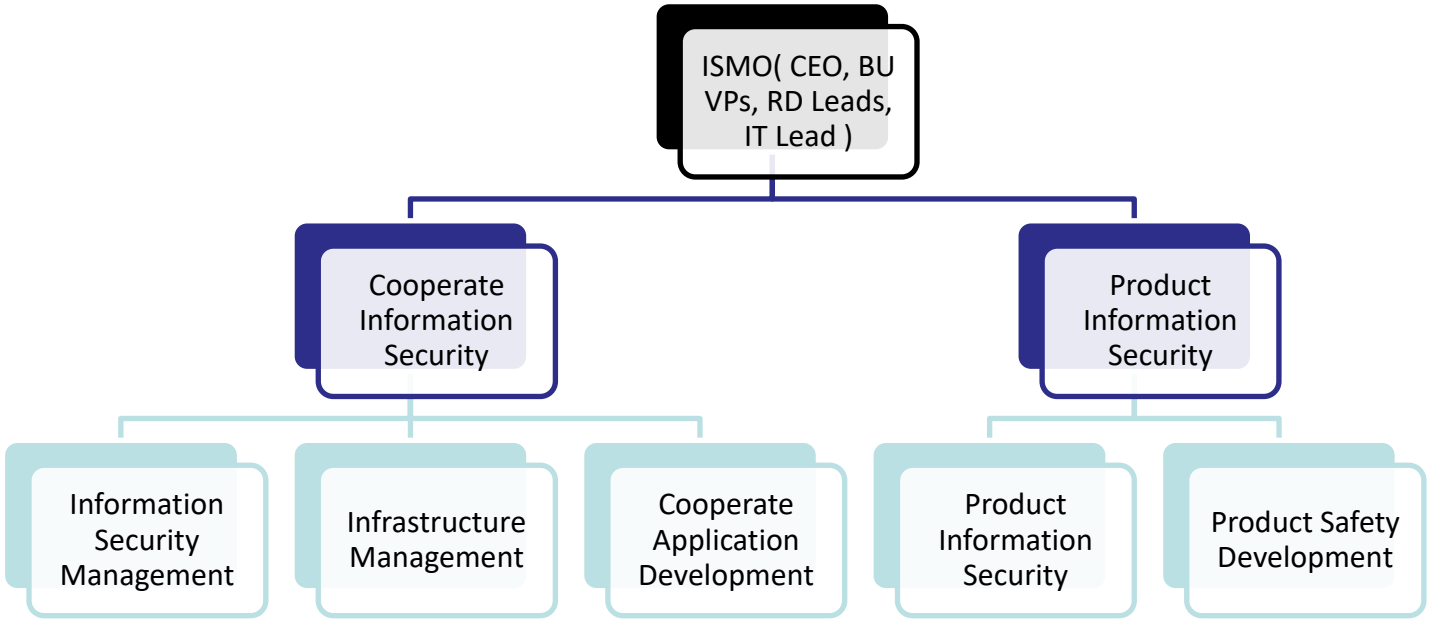
- Overview
  - Continuously improve and optimize information technology and information infrastructure
  - Establish information security policies based on international standard and Delta group regulation.
  - Protect important assets and equipment.
  - Form information security management team to handle information threat and keep improving.

Information System Security Management

- 2020 Challenges
  - COVID-19 malicious email attack
    - Publish a remote working guide to remind users
    - Upgrade server side e-mail protection
  - Malicious and phishing mails
    - Enable server side e-mail protection
    - Education users
    - Periodic drill for phishing mail.

Information System Security Management

- Policy
  - Reinforce information security organization
    - Form information security management team, the members as below. The first meeting hold on 2020 November, and regular meeting per half year.
      - The first meeting discuss: ISO 27001 certification, network security policy and abandon private own servers.



Information System Security Management

- Policy
  - Information Security Policy Execution
    - All employees have the responsibility to “Protect customers data privacy, and secure sales information data”
    - Review security policy on half year meeting and update if needed
    - ITD division head will report to board the yearly execution plan and review of previous year’s.
    - This slides has been reported to board on 2020.10.26
  - Integrate all servers
    - Though MIS has only limit resource, all information related system should be mamaged by MIS
    - System manager should not manage data and normal user should not touch system management.
    - More integration will let normal users touch less underlying data, the system will be more secure.

Information System Security Management

- 2020 execution status
  - Enhance Information Infrastructure and Business system
    - Take back private setup servers' management right
      - Linux、Source code control system、CI server、Working process server、KM server
    - Virtualized all server to make management easier – on going
    - Setup information asset management system
      - Will setup access white list base on the collection in this server to enhance LAN security.
    - Information equipment status visualization
      - locating problem quicker and lower down the period of system failure.
      - All network equipment joins LibreNMS this September
    - Fihish one time of vulnerability scanning
      - Ensure intranet safety

資訊系統安全風險管理

- 2020 execution status
  - Product and network security
    - Help product security design and flaws processing - on going
    - Help product to pass TAICS security certification - done
    - Upgrade all server to use HTTPS - done
  - Customer data security
    - Ensure product to be GDPR compliant - done
    - Prepare to certify with ISO27001 - on going

資訊系統安全風險管理

- 2020 Highlights
  - Network bandwidth management center - on going
  - Network system monitoring center - done
  - Invading detection and logging - on going
  - Vulnerability scanning - done
  - E-mail and information system protection - done
  - Important information asset remote backup - done

- Future works
  - Standardize the information security management and improve the efficiency.
  - Apply international information security standard
    - Pass ISO27001 certification on 2021 Q1
  - Establish Cyber Security Incident Response mechanism

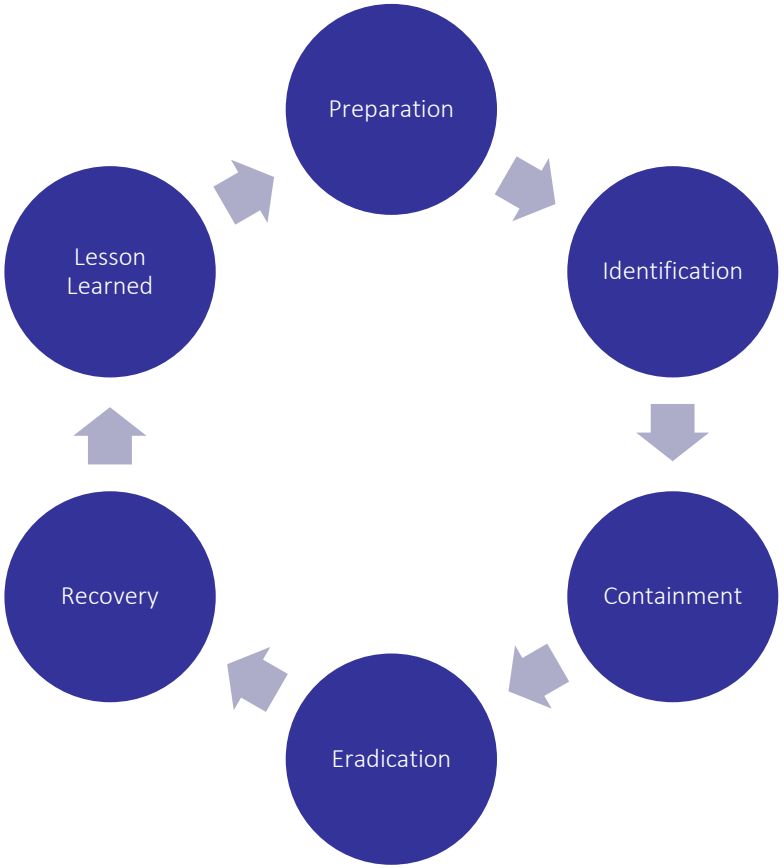
Cyber Security Incident Response

Draft for VIVOTEK.com Cyber Incident Response

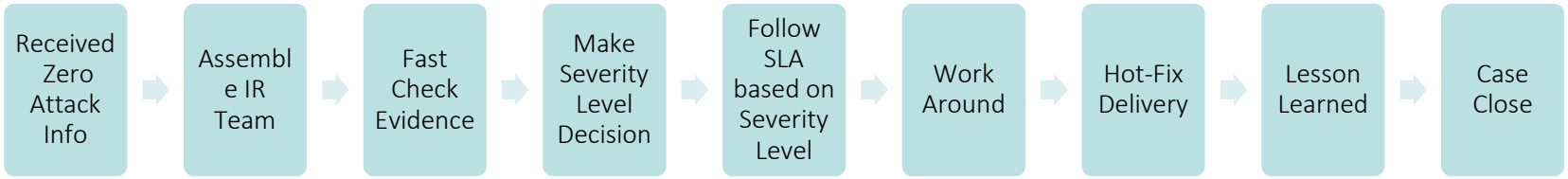
CSIRT and PSIRT

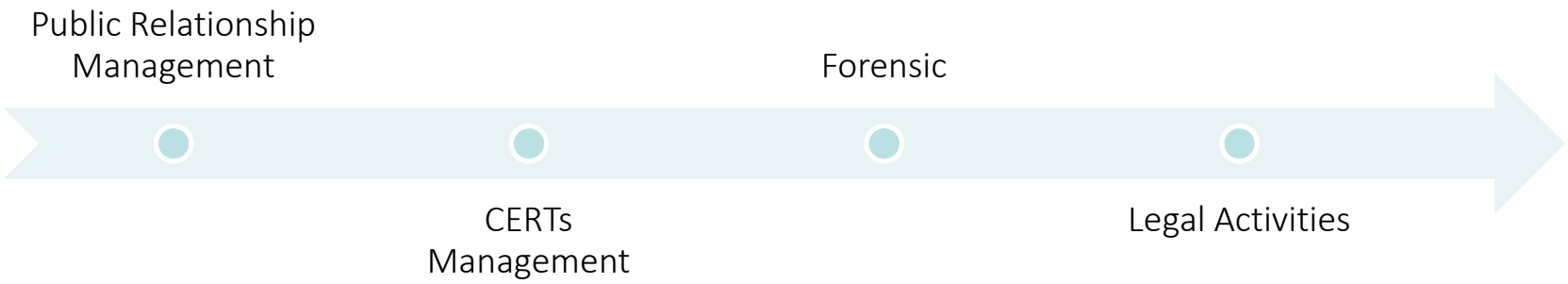
- VIVOTEK Information and Cyber Security Incident Response Team
  - CSIRT
    - Computer Security Incident Response Team
    - ISMS ISO Standard Plan and Execution
    - ITIL / ISO 20000 Incident / Problem / Change Monitoring
  - PSIRT
    - Product Security Incident Response Team
    - https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.0

STANDARD PROCESS FOR CYBER-SECURITY RESPONSE



Incident Response Process (High Level View)





Incident Response Team and Responsibilities Group A

FAE	Work with Security Partners on Vulnerabilities Monitoring Key Stakeholders / High Profile and Impact Clients Monitor and Management Work-Arounds Delivery
PM and Dev Team	Analyze System Defects to decide Severity Level Work with Software and Security Partners on Hot-fix or Patch according to Severity Level

Incident Response Team and Responsibilities Group B

ISMS / Cybersecurity Professional

Coordinate Cyber Security Issues

Organize IR team

Manage CERTs

Infra Team Member

Monitor Inbound and Outbound Traffic and Behaviors

FW (Firewall) / IPS / WAF (Web Application Firewall) Rules and Modification Readiness

Patch Delivery System Readiness and Resource Adjustment

Incident Response Team and Responsibilities Group C

Public Relationship Personnel

Media Relationship Management

PR Announcement and Information Point of Contact for outside of the company

Legal

Management with Law Enforcement

Legal Actions

Thank you

for your attention