Introduction to IT Security and Business Continuity Management

Presented by : Jefferson WAT

Agenda

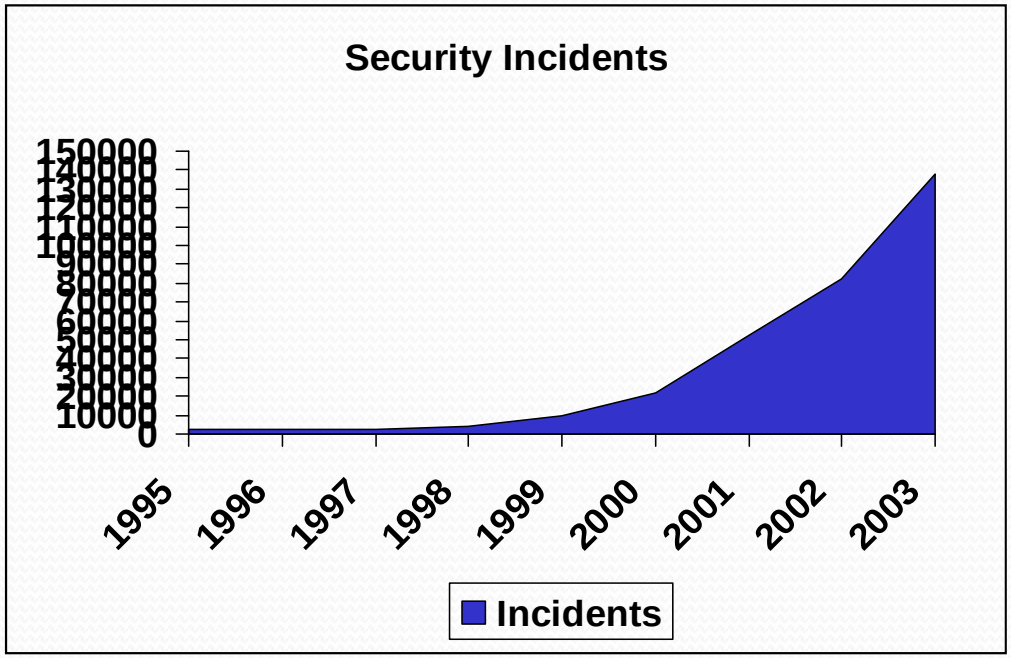
- Protecting our System
- Threat is Real
- Unauthorized Access
- Hacking
- Internet Frauds
- How to Safeguard your System?
- People, Process & Technology
- Business Continuity Management
- Risk Impact Analysis
- Disaster Recovery Planning
- Emergency Response

Protecting our System

- Critical to business operation
- Information is an asset
  - e.g. financials, customer information
- Regulatory requirements
  - e.g. Privacy laws & bank regulations

Threat Is Real

- Vulnerabilities and incidents are growing
- Tech Crime Incidents



Unauthorized Access

- Physical access
- Social engineering
- ID/password in “plain text”
- Phishing
- Pharming

An Oracle White Paper updated August 2006

Hacking

- Who are hackers?
- What harms can be done?
  - get access to sensitive data
  - defacing websites
  - erasing files
  - change programs
  - launching further attacks to other systems
  - steal money

Internet Frauds

- Bogus websites
- E-Stores without goods delivery
- Lottery/ deceased person/ big business

How to Safeguard Your System?

1. Reduce the virus risk
2. Protect automation products
3. Secure our communications
4. Protect the perimeter
5. Increase info security awareness
6. Comply with privacy and regulatory policies

Reduce Virus Risks

- Scan emails for known viruses
- Maintain anti-virus at the desktop
  - Auto download latest anti-virus release
  - Apply OS patches
- Manage the desktop

Protect Automation Products

- Applications are secured
  - Access Control
  - Authorized functions within application
  - Release Control
- Strong Authentication
  - Two factors or more
- Biometrics
  - Sensitive Personal Data

Secure Your Communications

- Ensure safe remote access connections
- e-Certs and encryptions
- Set secure wireless standards

Protect the Perimeter

- Firewalls
- Expand intrusion detection / prevention
- Manage vendor and backdoor connections

Information Security is a Shared Responsibility

- People
- Process
- Technology

People

- Individual employee
- Business partners
- Technical support team

Process

- Consistent Process & Procedure
- Security Policy
  - Policy enforcement
  - Prevent, Detect & Correct
- Communication & Training

Technology

Architecture that promotes policy adherence, network and host-based protection, and seamless updates throughout the organization

- Multi-level security measures
- Enforceable technology
- Ease of Management

Comply with Privacy and Regulatory Policies

- Customer data protection
- .com protection
- International regulations
  - SOX, PCI, HIPAA, etc.

Other Best Practices

- Login Once password in e-mails
- Include images in login process
- Passwords for documents
- Version control
- Backup regularly
- External audit

Business Continuity Management

- Physical Access Control
- Power Failure
- Fire Suppression
- Water Detection
- Contamination Reduction
- Other rare cases

Risk Impact Analysis

- Identifying & Prioritizing Assets & Functions
- Collecting Input from End Users
- A Criticality Spectrum
- Collecting Data on Outage Costs
- Problem with Statistics
- Developing Plan Objectives

Disaster Recovery Planning

- Identification, Classification, & Backup
- Policy-based Data Management
- Storage Consolidation
- Remote Mirroring
- Cost-Justify Off-site Storage
- Implementing the DRP

Emergency Response

- Emergency Decision Making
- Staffing Emergency Response Team
- Emergency Management Flowchart
- Situation Assessment
- Recovery Phase
- Relocation / Reentry Phase