Practice Good Enterprise Security Management

Presented by
Laurence CHAN, MTR Corporation Limited

About Me

- Manager – Information Security
  - Policy formulation and governance
  - Incident response
  - Incident investigation
  - Security advisor

Disclaimer

- The security sharing follows is based on well known security practices in the industry. It has no relations with the security measures in the MTR Corporation Limited.

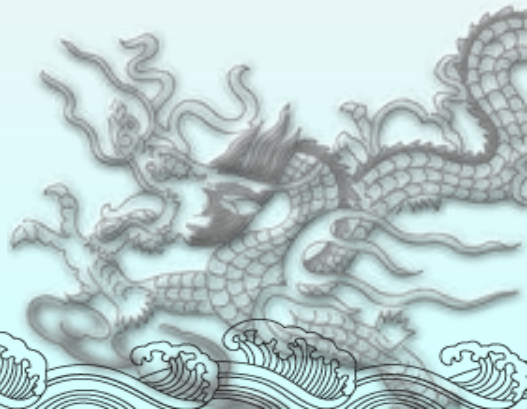
Assets

What aspects of assets are concerned most to an enterprise?

- Information
  - Confidentiality
  - Integrity
  - Availability
- Business service availability
  - System service availability

Threats

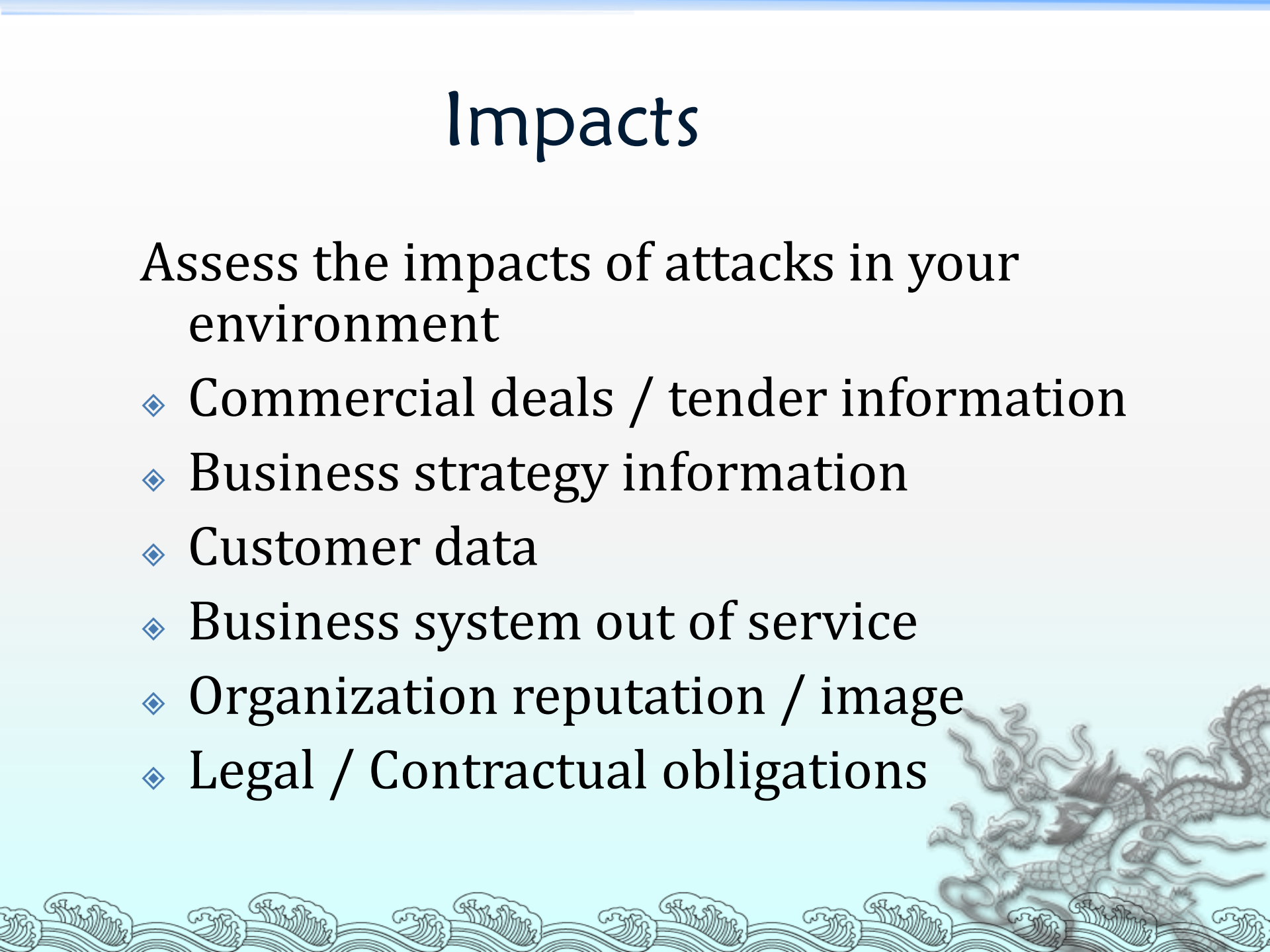
- External threats examples
  - Virus attack
  - APT attack
  - DDoS attack
  - Social engineering (e.g. phising, watering hole)
- Internal threats
  - Intentional data theft
  - Unintentional data leakage/loss



Impacts

Assess the impacts of attacks in your environment

- Commercial deals / tender information
- Business strategy information
- Customer data
- Business system out of service
- Organization reputation / image
- Legal / Contractual obligations

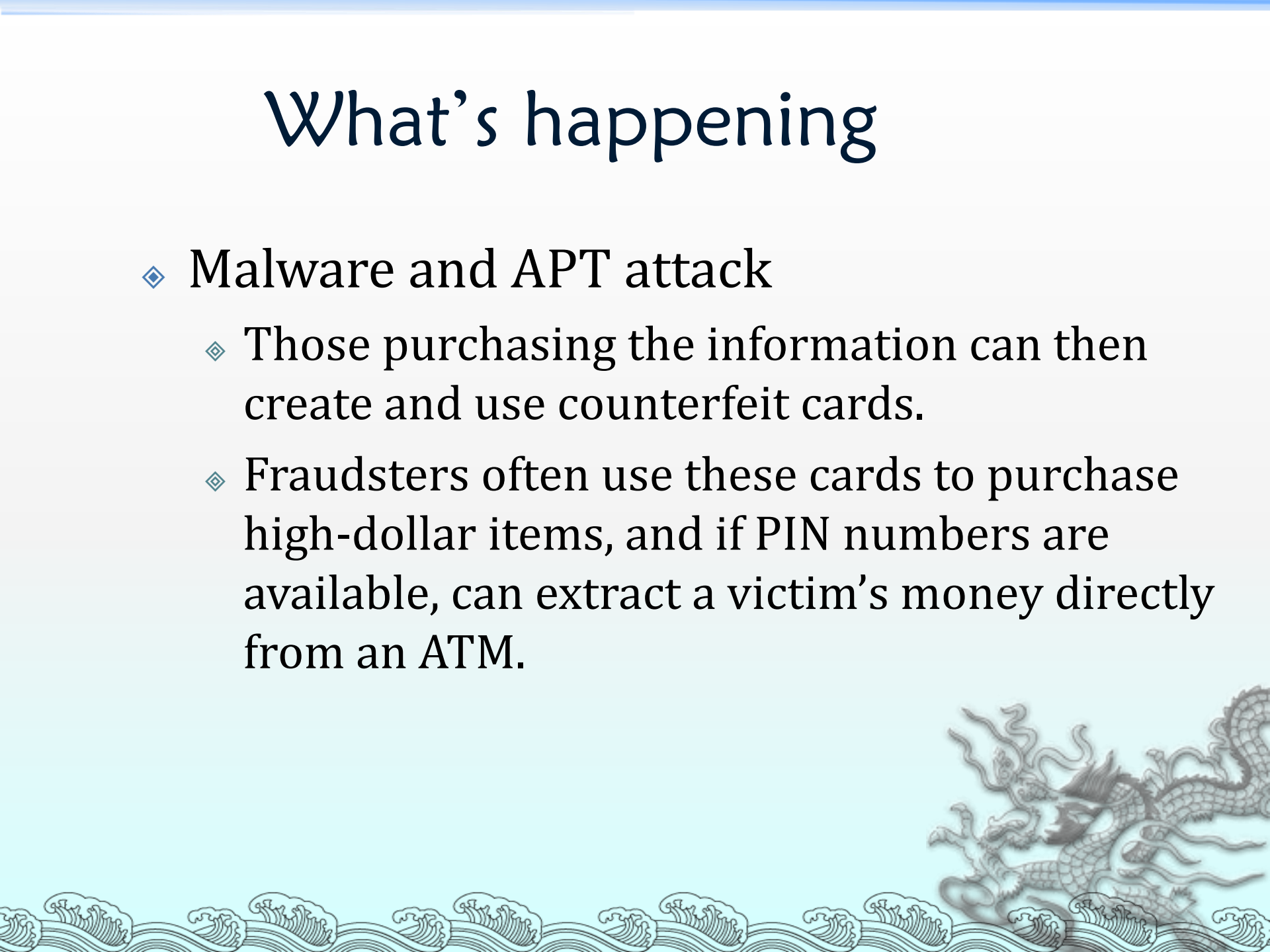


What's happening

- Malware and APT attack
  - On 19 Dec 2013, Target Chief Executive Gregg Steinhafel confirmed that the company's point-of-sale systems had been infected with malware, which led to the theft of 40 million credit and debit card accounts and personally identifiable information for 70 million people.
  - Thieves were able to sell information from these cards via online black market forums.

What's happening

- Malware and APT attack
  - Those purchasing the information can then create and use counterfeit cards.
  - Fraudsters often use these cards to purchase high-dollar items, and if PIN numbers are available, can extract a victim's money directly from an ATM.



What's happening

- Malware and APT attack
  - Malware installed on point of sale (POS) enabled the data theft.
  - This malware utilized a "RAM scraping" attack, which allowed for the collection of unencrypted, plaintext data as it passed through the infected POS machine's memory before transfer to the company's payment processing provider.
  - The malware available on black market cyber crime forums for between USD 1,800 and USD 2,300.

What's happening

- Malware and APT attack
  - Attackers first installed their malware on a small number of POS terminals between November 15 and November 28, with the majority of Target's POS system infected by November 30.
  - Attackers also installed malware, designed to move stolen data through Target's network and the company's firewall, on a Target server. Attackers updated it twice more, during December 2 and December 3

What's happening

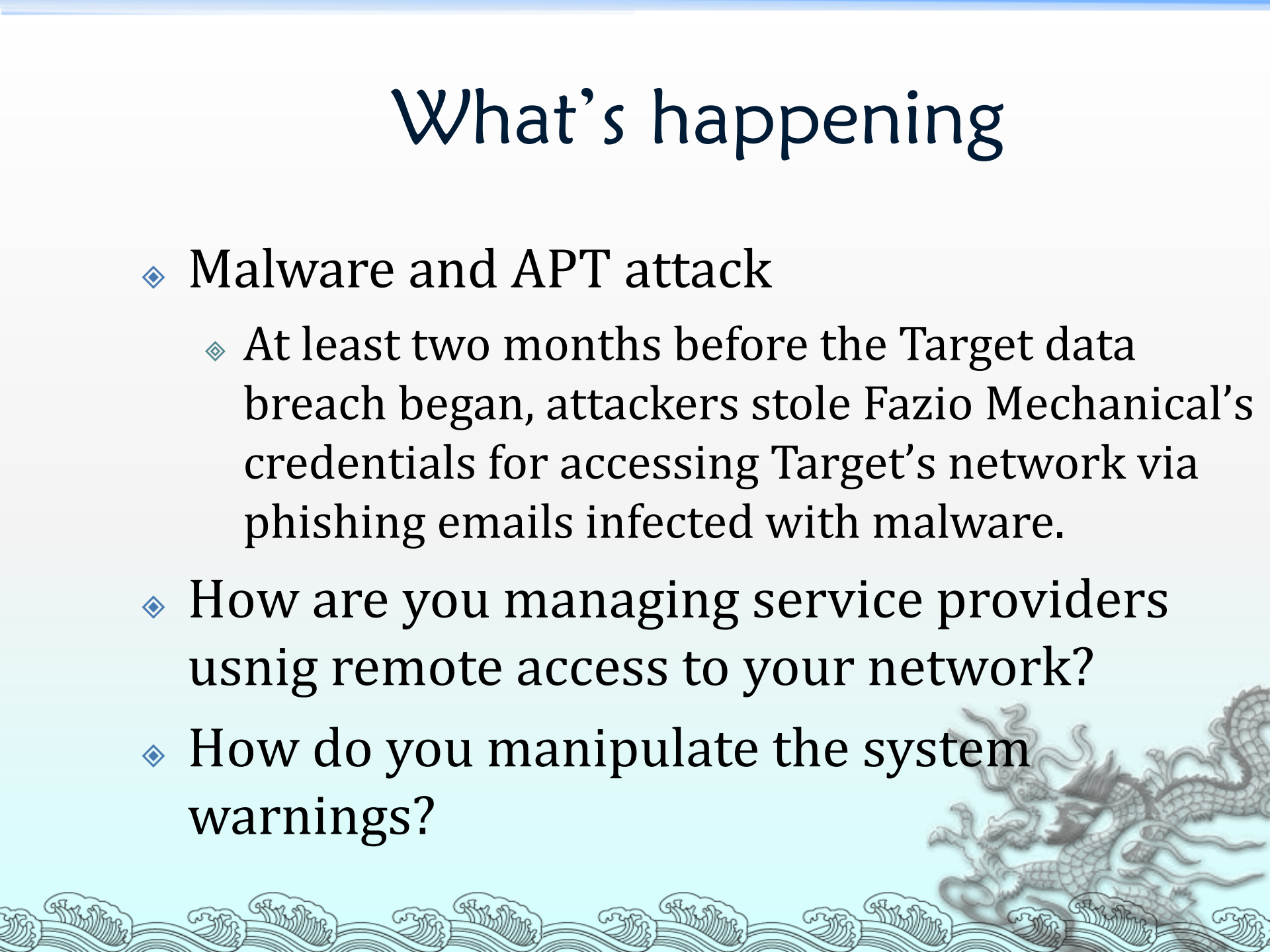
- Malware and APT attack
  - Target's anti-intrusion software showed warnings that the attackers were installing malware on Target's system. Target appeared to have failed to respond to multiple such warnings.
  - Target also failed to respond to multiple warnings from the anti-intrusion software regarding the escape routes the attackers planned to use to exfiltrate data from Target's network.

What's happening

- Malware and APT attack
  - Attackers first gained access to Target's system by stealing credentials from an HVAC and refrigeration company, Fazio Mechanical Services, based in Sharpsburg, Pennsylvania. This company had remote access to Target's network for electronic billing, contract submission, and project management purposes.

What's happening

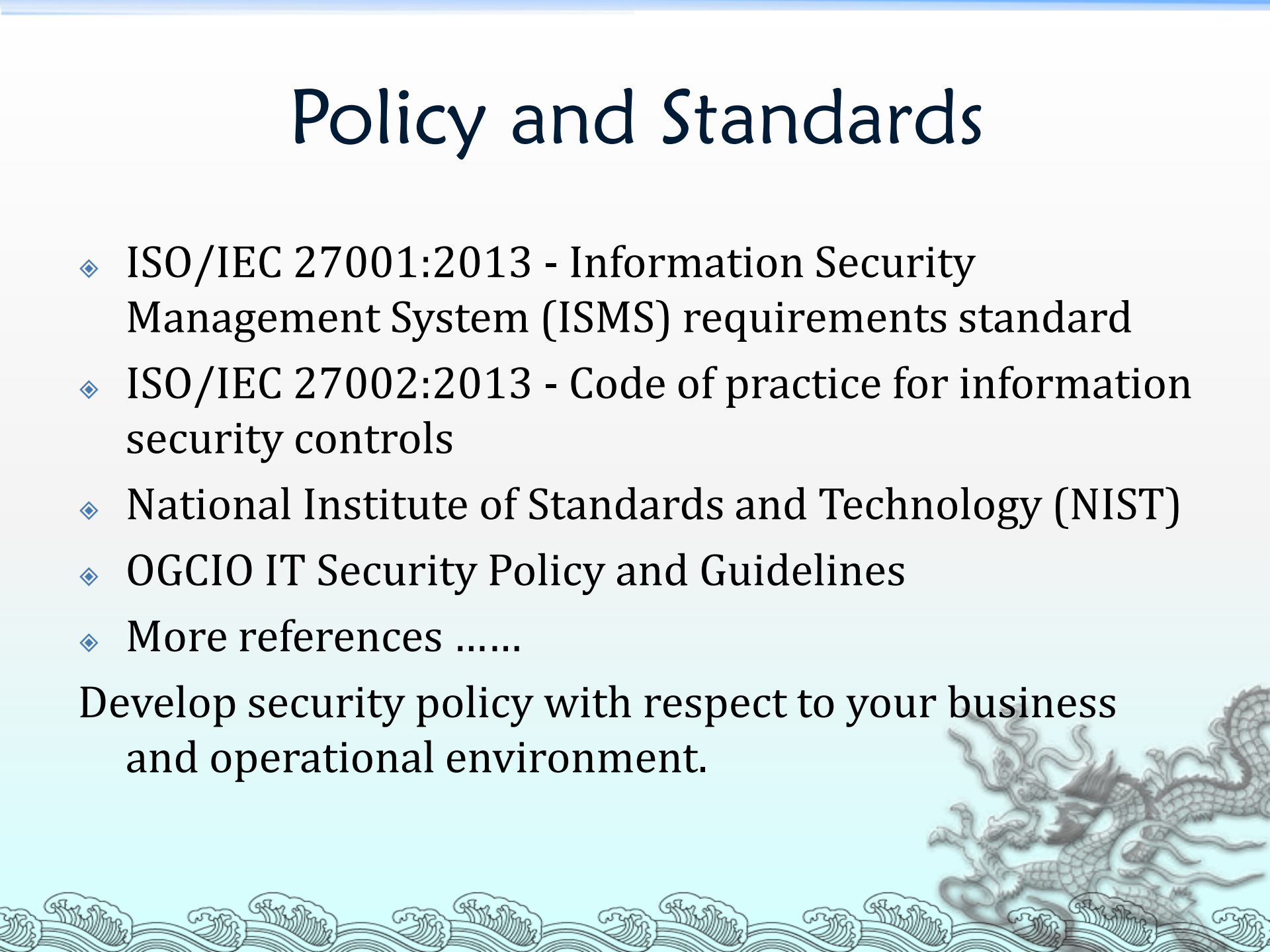
- Malware and APT attack
  - At least two months before the Target data breach began, attackers stole Fazio Mechanical's credentials for accessing Target's network via phishing emails infected with malware.
- How are you managing service providers usnig remote access to your network?
- How do you manipulate the system warnings?



Policy and Standards

- ISO/IEC 27001:2013 - Information Security Management System (ISMS) requirements standard
- ISO/IEC 27002:2013 - Code of practice for information security controls
- National Institute of Standards and Technology (NIST)
- OGCIO IT Security Policy and Guidelines
- More references ……

Develop security policy with respect to your business and operational environment.



Technical Measures

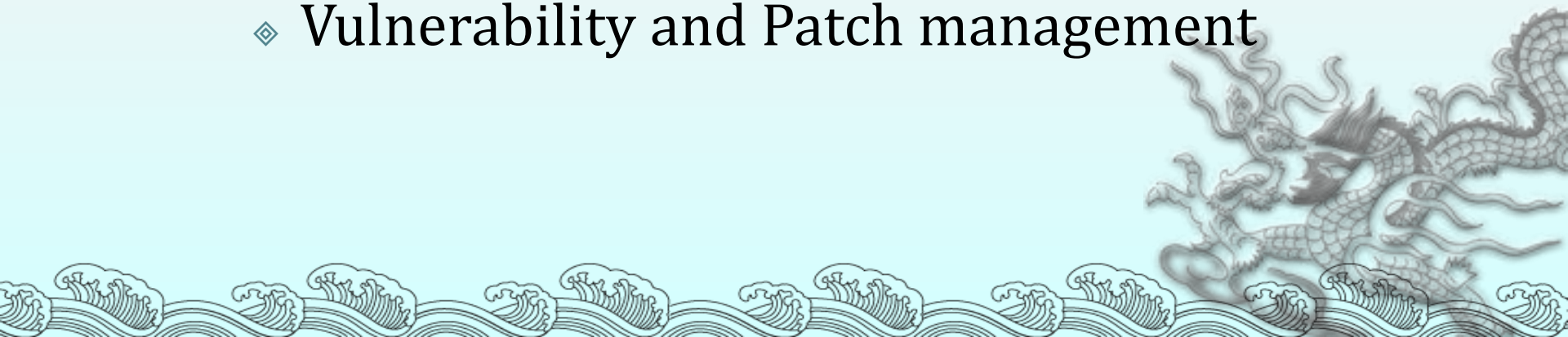
- Network DMZ
  - Firewall
  - Router
  - Proxy
  - Reverse proxy
  - Email gateway
  - Antivirus
  - Authentication

Technical Measures

- Network DMZ
  - IDS and IPS
  - Vulnerability and patch management
  - Data loss prevention
  - Controls over remote access

Technical Measures

- Endpoint device security
  - Antivirus
  - Desktop/personal firewall
  - USB controls
  - Program whitelist
  - Data encryption at storage
  - Vulnerability and Patch management

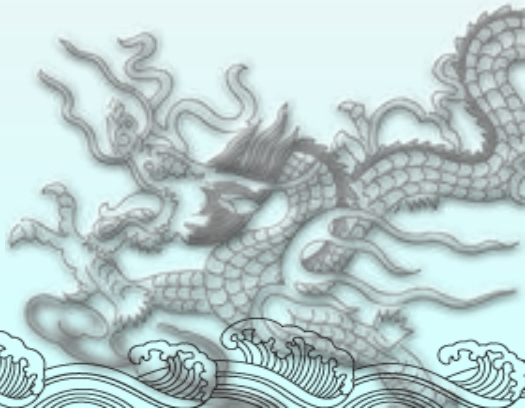


Technical Measures

- Controls to data manipulation
  - Password encrypted in storage
  - Customer data encrypted in storage
  - Logical controls on data access
  - Role-based access permissions

Technical Measures

- Classify your data
- Data access principles
  - Need to Know
  - Need to Hold
  - Grant access permissions according to the above two principles
- Access logging
- Secure printing
- Secure erasure of data

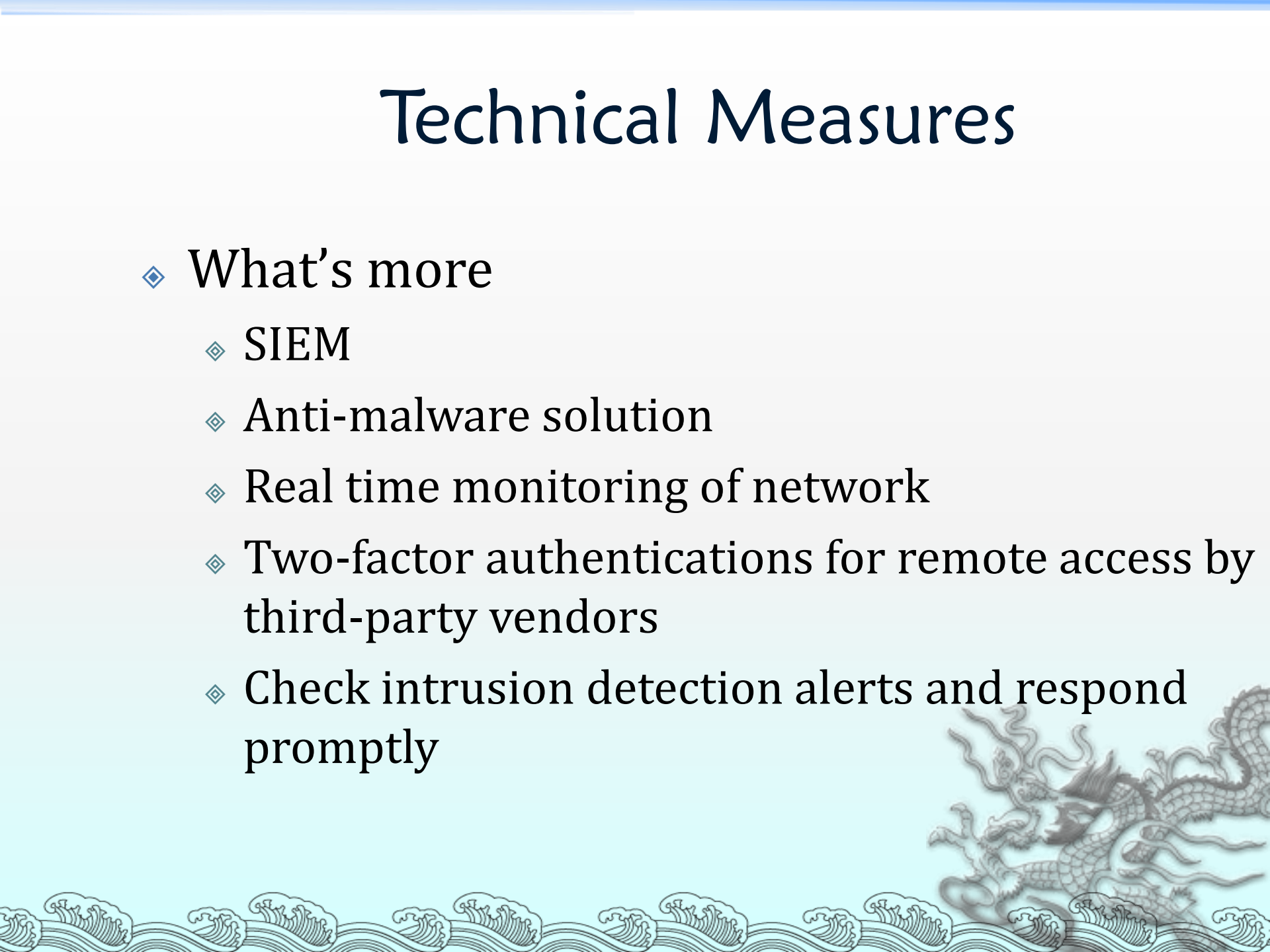


Technical Measures

- Contingency
  - Data backup
  - System backup
  - System resilience
  - Backup site
  - Drill of system and data recovery

Technical Measures

- What's more
  - SIEM
  - Anti-malware solution
  - Real time monitoring of network
  - Two-factor authentications for remote access by third-party vendors
  - Check intrusion detection alerts and respond promptly

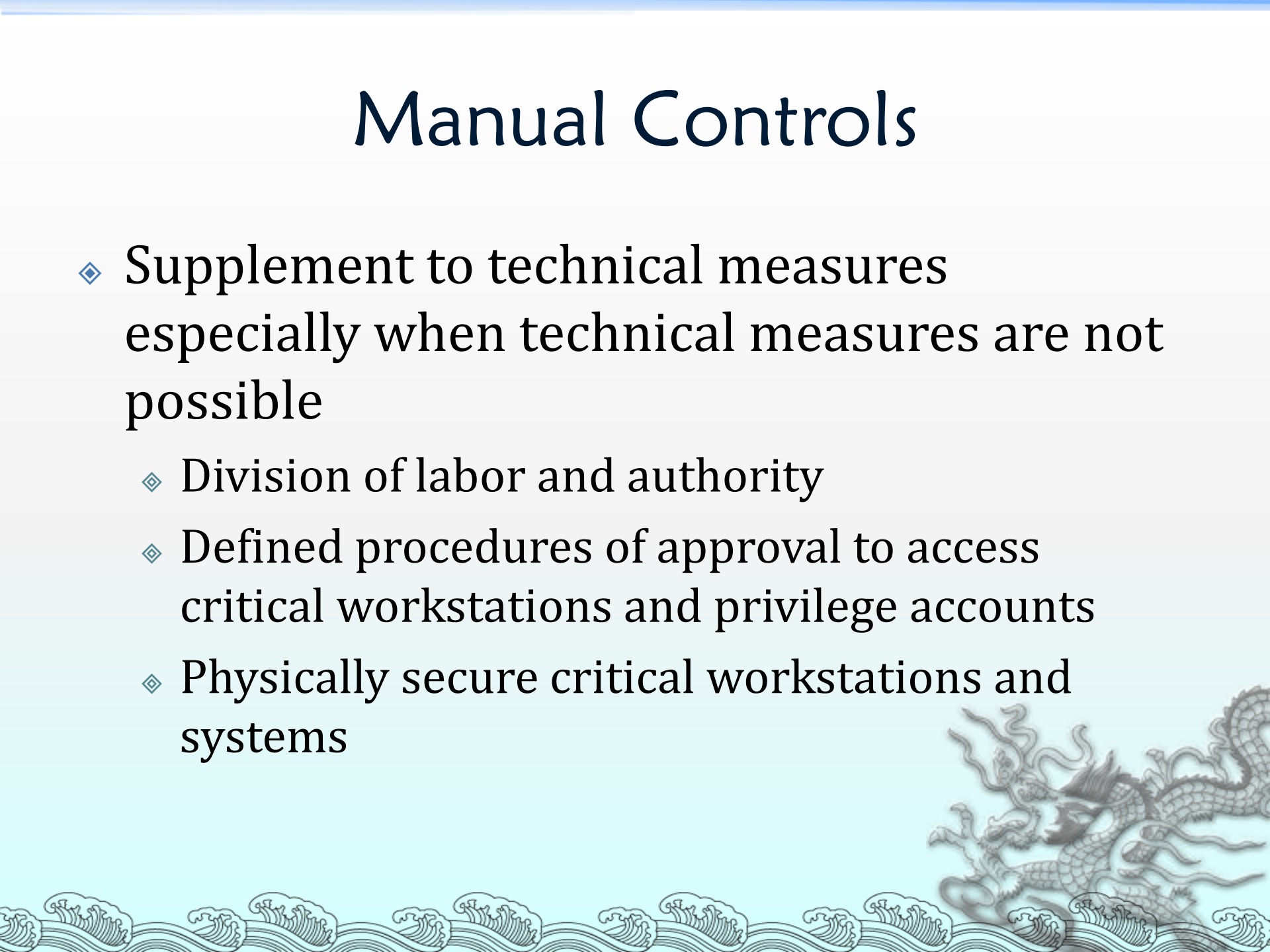


Technical Measures

- What's more
  - Disable guest accounts and change default account password
  - Separate network segments for containment of attacks
  - Separate critical business systems from Internet communications

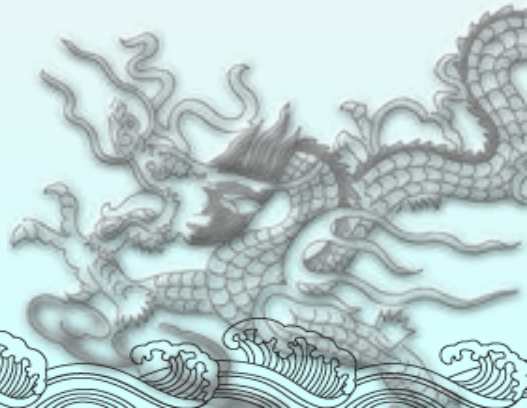
Manual Controls

- Supplement to technical measures especially when technical measures are not possible
  - Division of labor and authority
  - Defined procedures of approval to access critical workstations and privilege accounts
  - Physically secure critical workstations and systems



Human Factor

- Staff awareness
  - Don’t disclose password
  - Don’t share individual accounts
  - Secure use of USB drive
  - Use USB drive of built-in security
  - Emails
  - Internet browsing
  - Mobile devices
  - Secure data disposal



Incident Response

- Handling information security incidents
  - Identification
    - security incident vs operation incident
  - Escalation
  - Containment
    - Limit affected scope
    - Protect critical systems and data
  - Mitigation
    - Patch loophole, remove malware, change passwords, etc.

Incident Response

- Handling information security incidents
  - Recovery of system service and data
  - Aftermath
    - Post-incident analysis
    - Improve security measures
    - Improve incident response procedures and communications
    - Incident Report
- You are not alone: OGCIO and HK Police

Summary

- Technology is changing
- Tactics of cyber attacks are changing
- Keep abreast of new technology, new attacks, and assess how they may impact your assets

Q & A