Protecting datacenters &
mission critical facilities
- using IP based systems

Presented by: Jeffrey Lam RCDD
Director, Global Accts, Asia
ANIXTER
Agenda

- Industry drivers
- Business trends
- Developing the physical security plan for data centers
  - Physical protection guidelines and strategies
  - Crime Prevention Through Environmental Design (CPTED)
  - TIA-942 standard
- Security technologies for data centers
  - Perimeter layer controls
  - Facility layer controls
  - Computer room layer controls
  - Cabinet-level controls
Industry Drivers for Data Center Security

- **Sensitive data**
  - Medical records
  - Social Security numbers
  - Financial transactions and cardholder data
  - Intellectual property and confidential information

- **Critical infrastructure and key resources**
  - As defined by the Department of Homeland Security:
    “The assets, systems, and networks, whether physical or virtual,
    so vital to the United States
    that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.”
## Data Security Breaches

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 15, 2009</td>
<td>“Police are investigating two incidents in which patients’ medical records - including social security numbers - were stolen from the city’s health department.”</td>
</tr>
<tr>
<td>Dec. 15, 2009</td>
<td>“A stolen laptop exposes applications for study abroad students. Names and Social Security numbers are exposed…”</td>
</tr>
<tr>
<td>Dec. 17, 2009</td>
<td>“Library users at 25 campuses were the victims of a security breach in August. The libraries collect drivers license and Social Security numbers to help identify computer users. The information is stored on a central server…”</td>
</tr>
<tr>
<td>341,900,776</td>
<td>TOTAL number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 (tracked by privacyrights.org)</td>
</tr>
</tbody>
</table>

Source: [http://www.privacyrights.org/ar/ChronDataBreaches.htm#2010](http://www.privacyrights.org/ar/ChronDataBreaches.htm#2010)
Protecting your information!

**Physical Security**
- Tracks people
- Limits access to areas, spaces
- Provides audit of who accessed what
- Integrates with video to provide visual record

**Logical Security**
- Tracks logins
- Limits access to servers, folders and applications
- Provides audit trail of what login accessed what data
Business Trends in Security Systems

- Moving from reactive toward predictive response
- Providing additional operator control
- Preserving existing capital investment
- Regulatory requirements
  - PCI DSS, HIPAA, Sarbanes-Oxley, etc.
Technology Trends in Security Systems

- Analog-to-digital migration
  - Digital allows better image management
    - Record, store, search, retrieve, share, send
- System Integration for greater efficiency
- Standardized structured approach
  - Modular, flexible implementation
  - Easy moves, adds and changes (MAC)
- Anywhere - anytime monitoring
- Video Analytics
Developing the Physical Security Plan

Physical Protection Guidelines & Strategies
Technologies for Data Center Security
Crime Prevention Through Environmental Design (CPTED)

- Awareness of how people use space
  - All space has a designated purpose
  - Social, cultural, legal and physical dimensions affect behavior

- Control physical setting to change behavior
  - Understand and change behavior in relation to physical surroundings
  - Redesign space to encourage legitimate behaviors and discourage illegitimate use
Security Technologies for Data Centers

- **Site Selection**
- **Defense in depth**
  - Implement layers of protection
  - Ensure failure of one element in the system will not create a critical vulnerability in the whole system
  - Delay penetration in event of breaches
TIA-942 Data Center Site Selection Criteria

- Secure all cooling equipment, generators, fuel tanks or access provider equipment outside the customer space
- Computer rooms should not be located near a parking garage
- The building should not be located:
  - In a 100-year flood plain / near an earthquake fault / on a hill subject to slide risk, / downstream from a dam or water tower
  - Within 0.4 km (¼ mile) of an airport, research lab, chemical plant, landfill, river, coastline or dam
  - Within 0.8 km (½ mile) of a military base
  - Within 1.6 km (1 mile) of a nuclear, munitions or defense plant
  - Adjacent to a foreign embassy
  - In high-crime areas
## Locations – EIA/TIA vs China GB Code

<table>
<thead>
<tr>
<th>EIA/TIA 942 TIER</th>
<th>Proximity to airports</th>
<th>GB 50174 CLASS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIER 1</td>
<td>not applicable</td>
<td>GB Class C</td>
</tr>
<tr>
<td>TIER 2</td>
<td>not applicable</td>
<td>GB Class C</td>
</tr>
<tr>
<td>TIER 3</td>
<td>Not less than 1.6 km</td>
<td>GB Class B</td>
</tr>
<tr>
<td>TIER 4</td>
<td>Not less than 8 km</td>
<td>GB Class A</td>
</tr>
<tr>
<td>EIA/TIA 942 TIER</td>
<td>Proximity to major traffic arteries</td>
<td>GB 50174 CLASS</td>
</tr>
<tr>
<td>TIER 1</td>
<td>not applicable</td>
<td>GB Class C</td>
</tr>
<tr>
<td>TIER 2</td>
<td>not applicable</td>
<td>GB Class C</td>
</tr>
<tr>
<td>TIER 3</td>
<td>Not less than 91 m</td>
<td>GB Class B</td>
</tr>
<tr>
<td>TIER 4</td>
<td>Not less than 800 m</td>
<td>GB Class A</td>
</tr>
</tbody>
</table>
# TIA-942 – Data Center Security Tiers

<table>
<thead>
<tr>
<th>Feature</th>
<th>Tier I</th>
<th>Tier II</th>
<th>Tier III</th>
<th>Tier IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bullet resistant walls, windows and doors</td>
<td>n/a</td>
<td>n/a</td>
<td>Level 3 (min)</td>
<td>Level 3 (min)</td>
</tr>
<tr>
<td>Security counter in lobby</td>
<td>n/a</td>
<td>n/a</td>
<td>Level 3 (min)</td>
<td>Level 3 (min)</td>
</tr>
<tr>
<td>Security counter in shipping and receiving</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>Level 3 (min)</td>
</tr>
<tr>
<td>CCTV Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Building perimeter and parking</td>
<td>No requirement</td>
<td>No requirement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Generators</td>
<td>n/a</td>
<td>n/a</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Access controlled doors</td>
<td>No requirement</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Computer room floors</td>
<td>No requirement</td>
<td>No requirement</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Access Control/Monitoring at:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fiber vaults</td>
<td>Industrial grade lock</td>
<td>Intrusion detection</td>
<td>Intrusion detection</td>
<td>Card access</td>
</tr>
<tr>
<td>Emergency exit doors</td>
<td>Industrial grade lock</td>
<td>Monitor</td>
<td>Delay egress per code</td>
<td>Delay egress per code</td>
</tr>
<tr>
<td>Accessible exterior windows/opening</td>
<td>Off-site monitoring</td>
<td>Intrusion detection</td>
<td>Intrusion detection</td>
<td>Intrusion detection</td>
</tr>
<tr>
<td>Security operations center</td>
<td>n/a</td>
<td>n/a</td>
<td>Card access</td>
<td>Card access</td>
</tr>
<tr>
<td>Doors into computer rooms</td>
<td>Industrial grade lock</td>
<td>Intrusion detection</td>
<td>Card or biometric for ingress and egress</td>
<td>Card or biometric for ingress and egress</td>
</tr>
</tbody>
</table>

Source: ANSI/TIA-942
Perimeter Layer Controls

Selection of Site
Site hardening
Video surveillance
Perimeter Layer Controls

- **Goals**
  - Deter, detect and delay
  - Integrate systems
  - Provide layers of protection

- **Security measures**
  - Physical barriers
  - Site hardening
  - Lighting
  - Intrusion detection
  - Video surveillance
  - Physical entry and access control
Site Hardening

- Security walls and gates
- No signage indicating data center purpose
- Parking away from building
- Clear zones
- Psychological impact
- Intimidating doors & hardware
  - Steel doors and heavy-duty locks
Perimeter Video Surveillance

- **Monitor**
  - Parking lots
  - Entry and exit points
  - Garbage bins
  - Power or cooling facilities
  - Building facade and rooftop

- **Detect**
  - Motion detection
    - Sound alarm when triggered
  - Intelligent video analytics
    - Object left behind
    - People counting
    - Wrong way
Impact of the Cabling Infrastructure

- A Category 5e cabling infrastructure’s absence of headroom minimizes the infrastructure’s ability to compensate for marginal electronics.
- A Category 6A cabling infrastructure provides headroom to overcome issues related to the electronics.
Facility Layer Controls

Access Control and Video Analytics
Facility Layer Controls

- **Goals**
  - Secondary layer of protection
  - Further restrict access
  - Redundant power and communications
  - Integrated systems

- **Security measures**
  - Access control
    - **Man-traps**
    - **Turnstiles**
    - **Visitor management**
  - Video surveillance
Access Control

- **Man-traps**
  - Two interlocking doors open only one at a time after presenting authorized credential

- **Turnstiles**
  - Physically allow only one person to pass through at a time
  - Incorporate weight bridge
Visitor Management

- Paper sign-in sheets not secure
  - Incomplete, illegible
  - any visitor can view the log

- Use a driver’s license, passport, photo ID
  - Scanned, recorded in a secure database
  - Customizable

- High-quality badges printed by guard
  - Integrate with access control systems

- Badges can automatically expire
  - “VOID” may appear across the badge
  - Change in color
  - Rendered inactive after a certain time or date
Indoor Video Surveillance

- Monitor exits as well as entrances
- Integrate with access control to monitor internal access
- Use high-resolution cameras for identification purposes
- Configure systems to record on motion or event to save storage requirements
- Consider video compression technology
Detection vs recognition

Enlargement and enhancement

Suitable

Not Suitable

Image courtesy of Scientific Working Group on Imaging Technology & APTA Draft Guidelines for Cameras and Digital Video Recording Systems
Computer Room Layer Controls

Identification
Asset tracking
**Computer Room Layer Controls**

- **Goals**
  - Third layer of protection
  - Further restrict access
  - Monitor all authorized access

- **Security measures**
  - Man-traps and turnstiles
  - Video analytics
  - Biometrics
  - RFID

- **6 wall border**
  - No windows or skylights
  - Secure air-handling systems
Access Control Verification

- **Methods**
  - **Carried**
    - Item carried by the individual:
      - metal keys, proxy cards, mag cards, photo ID, smart cards
  - **Known**
    - Private information:
      - PIN, passwords, code words
  - **Inherent**
    - Biometric features
      - finger and thumb prints, hand geometry, iris scan, speech pattern
Final design

Comms.

MDA
Reserved for future racks

racks

racks

Operating Console
Video Surveillance

Video Analytics
- Incorporate people counting software

Corridor view
- Same resolution and distance
- Different level of details
RFID for the Data Center Environment

- Eliminate manual spreadsheets for tracking
  - Inventory
  - Asset locations
  - Life-cycle data

- RFID technologies can provide instant awareness of data center assets
  - Rack-mounted equipment
  - Mobile equipment such as laptops
  - Employees (e.g., credential tags)
  - Some systems also offer environmental monitoring sensors
Cabinet Layer Controls

Cabinet Level access control
Intelligent Infrastructure Management
Cabinet-Level Controls

- **Goals**
  - Last line of defence
  - Further restrict access
  - Integrated systems for enhanced awareness

- **Security measures**
  - Cabinet-level locking
  - Audit trails
  - Intelligent infrastructure
TZ Praetorian Cabinet Locking System

- Increase security at the cabinet level
- Work with existing enterprise access control systems
- Bring electronic security & audit trail capability to the cabinet level
- Integrate with in-cabinet CCTV camera
Intelligent Infrastructure Monitoring

- Aka “Intelligent cabling solutions”
- Hardware: electronic panels + controller
- Software: server hosted
- 9-pin vs inference technology
- “Intelligent ready”

Security benefits
- Monitors changes in the patch field
- Locates unauthorized devices
Summary

- IP-enabled physical security systems increase reaction time
  - Technology stable & matured
  - Moving toward predictive response
- Develop security plan by leveraging existing security best practices & industry standards
- Different levels of protection for perimeter, facility & computer room and cabinets
Thank you!

Jeffrey Lam, RCDD
jeffrey.lam@anixter.com
+65 97849870