Agenda

• Overview
• Physical Access Control
• Common Applications
• Physical Threats to Data
• Attack Scenario
• Physical Access Control Systems (PACS)
• Healthcare Impacts
• GhostExodus
• Internet-of-Things (IoT) Devices
• Crime Prevention Through Environmental Design (CPTED)
• Environmental Threats
• Security Assessment
• Supplemental Guidance

Slides Key:

- Non-Technical: managerial, strategic and high-level (general audience)
- Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Overview

- The protection of physical computer systems, organizational assets, infrastructure, and personnel are all under the scope of physical security.
- Physical security represents a part of an overall cybersecurity approach that is just as important as technical elements.
- Physical access control incorporates numerous capabilities to prevent, detect, or correct unwanted intrusions into an organization.
- Using simple techniques such as theft or accessing an on-site workstation, cybercriminals can potentially steal private data residing on enterprise systems.
- Physical access control systems which are commonly used to secure businesses, have commonly seen risks associated with the integrated technology.
- In healthcare, the rise of IoT systems vulnerable to proximity-based attacks highlights the need for physical security standards.
- A number of examples of physical security impacts to healthcare systems exist, including multiple instances of computer theft per year, and highly sophisticated attacks done in close proximity to medical devices.
- Similar to auditing computer systems and networks in an organization, a physical assessment of an organization’s physical security can identify risk areas in which to incorporate best practices.
Physical Access Control

- Physical Access Control (Physical Security Control) – focuses on the physical protection of information, buildings, personnel, installations, and other resources.
  - Restricts physical access by unauthorized personnel
  - The physical attack vector regarding cybersecurity is often overlooked compared to more technical vectors.

**Used to mitigate a variety of threat types:**
- Sabotage, vandalism, theft
- Eavesdropping (key loggers, cameras, shoulder surfing)
- Natural disasters – tornadoes, earthquakes, floods, tsunamis
- Man-made disasters – terrorism, arson, bombings
- Loss of access to electricity, air, and water.

Although physical access control is used as a tool to mitigate a broad category of threats, its linkage to cybersecurity is highly important.

Physical Access control represents one of the three fundamental security controls that make up computer security.

Source: Infosec Institute

<table>
<thead>
<tr>
<th>CONTROL TYPES</th>
<th>PREVENTATIVE</th>
<th>DETECTIVE</th>
<th>CORRECTIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Fences, gates, locks</td>
<td>CCTV and surveillance camera logs</td>
<td>Repair physical damage, reissue access cards</td>
</tr>
<tr>
<td>Technical</td>
<td>Firewall, IPS, MFA solution, antivirus software</td>
<td>Intrusion detection systems, honeypots</td>
<td>Patch a system, terminate a process, reboot a system, quarantine a virus</td>
</tr>
<tr>
<td>Administrative</td>
<td>Hiring and termination policies, separation of duties, data classification</td>
<td>Review access rights, audit logs, and unauthorized changes</td>
<td>Implement a business continuity plan or incident response plan</td>
</tr>
</tbody>
</table>
Common Applications

- A number of capabilities exist to strengthen physical security
- Security controls and the capabilities within them are often divided into separate functional categories
  - Preventative – stops unauthorized activity from occurring
  - Detective – detects and alerts to unwanted or unauthorized activity in progress
  - Corrective – repairs damage or restores resources and capabilities to their prior state following an unauthorized or unwanted activity.

**Common Physical Security Applications**

<table>
<thead>
<tr>
<th>Preventative</th>
<th>Detection</th>
<th>Corrective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badges</td>
<td>Motion Sensors</td>
<td>Physical Repairs</td>
</tr>
<tr>
<td>Mantraps</td>
<td>Intrusion Alarms</td>
<td>Administrative Unlocks</td>
</tr>
<tr>
<td>Fences</td>
<td>Cameras/CCTV</td>
<td>Re-issuing access cards</td>
</tr>
<tr>
<td>Locks</td>
<td>Lights</td>
<td></td>
</tr>
<tr>
<td>Guards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Image Source: [Trend Micro](#)
Physical Threats to Data

- Cyber threats to an organization's computer systems are often mistakenly thought of as being solely technical.
  - There are a number of physical threats, malicious and unintentional, that can negatively impact an enterprise system.
  - A number of cyberattack campaigns have incorporated a physical element into an overall operation.

**Stolen Devices**
Unsecure devices that are stolen can potentially contain sensitive data that can be extracted by the cybercriminals.

**Proximity scanning**
Improperly Encrypted IoT Devices such as nurse stations and imaging devices can be accessed with small computing devices, if close enough, and potentially used to attack other devices on the same network.

**Manual Malware upload**
Physically accessible systems can be easily infected with malware via USB or optical disk.

**Physical Destruction**
Malicious outsiders, disgruntled employees, or environmental factors can damage accessible equipment, risking data loss and disrupting operations.
Malicious actors can infect networks and/or gain admin privileges through physically accessible devices in an organization.

Example Attack Scenario

Attacker

Locates Admin User

Admin Access

Attacks Admin User

Workstation

User Access To Software
Physical Access Control Systems (PACs) are used as an electronic security counter measure that can control access to a facility within controlled interior areas.

- Commonly made up of many software and hardware components such as software applications, servers, databases, panels, door controllers, and workstations.
- Typically interoperates with an Intrusion Detection system, Video management system, and a visitor management system.
- Often issues PIV ID Cards supported by a certificate validation system and hardware infrastructure.

- Although PACs are recommended as a physical security practice, they are not without flaws.
  - PAC software is susceptible to hardware/software vulnerabilities.

**Common issues with PACs systems**

- Vendor solutions implemented without testing
- PACs using outdated software/hardware
- No maintenance or support after installation
- Lack of strong encryption on devices
- Heavily reliant on IT but may lack understanding

---

**Real-world PAC Vulnerability Example**

- On January 2019, multiple Zero-day vulnerabilities were discovered in a PACs technology suite developed by IDenticard®
  - When exploited, the vulnerabilities would give attackers unrestricted access to the badge system database, allowing them to enter buildings by creating fraudulent badges and disabling building locks.
  - According to the IDenticard website, IDenticard has tens of thousands of customers around the world, including Fortune 500 companies, K-12 schools, universities, medical centers and government agencies.

Source: [Security Boulevard](https://www.securityboulevard.com), [Globenewswire](https://www.globenewswire.com)
Stolen laptop puts health information of 7,000 Texas hospital patients at risk

By Andrew S. Williams, Esq. on March 21, 2016
Posted in Fiduciary Matters, Welfare Benefit Plans

Recent Examples of Physical threats in Healthcare

March 2019 – 1,221 patients were notified their information may have been accessed after four desktop computers were stolen from an Oklahoma hospital.

September 2019 – Texas Hospital learned a laptop that stored patient information of 7,358 individuals was stolen.

March 2018 – A laptop containing PHI of 289,904 individuals was stolen from a Minnesota hospital, resulting in a 1.55 million-dollar HIPPA violation fine.

January 2018 – Stolen computer at Philadelphia medical practice compromised roughly 1,000 patient records.

January 2018 – A Chicago hospital was contacted by a man residing in the Philippines inquiring how to unlock a stolen computer belonging to the hospital.

Data of 43,000 patients breached after theft of unencrypted laptop

- Physical Security is particularly important in the healthcare industry due to:
  - PHI data that resides in hardware devices must be secured.
  - The accessible nature of hospitals and healthcare facilities further drives the need for physical security protections.
  - Many modern medical devices incorporate Internet of things/network technology that can be exploited to steal data or access networks.
  - The pervasive use of mobile devices in healthcare increases the likelihood of stolen devices with PHI data.
Jesse William McGraw, aka “GhostExodus”, former leader of the Electronic Tribulation Army, was sentenced to 9 years and 2 months in prison for installing malware on computers at a Texas hospital.

Caught FBI attention after posting a YouTube video of himself “staging an infiltration mission” at an office building, in which he installs a RxBot on a desktop computer.

- Part of the Electronic Tribulation Army's plan was to build a botnet to attack a rival hacking group
- Also posted another video displaying his collection of infiltration gear, including lock picks, a cellphone jammer, and fake FBI credentials.

McGraw’s employment as a security guard at the Texas hospital enabled him greater access to the facilities assets.

- Dozens of hospital systems with PHI data, including nurses’ station with PHI data, and the hospital HVAC system controller were compromised with malware.

Source: Wired
Internet-of-Things (IoT)

- The rise of IoT device usage in healthcare has led many hackers to focus on exploiting these devices.
  - Research indicates cyberattacks on IoT devices increased 300% in 2019.
  - Further research estimates that 161 million IoT devices will be in hospitals, clinics, and medical offices by 2020.

- Although hacking an IoT device remotely can prove difficult for cybercriminals, several researchers have demonstrated the ability to easily hack IoT devices with a small computing device within close proximity of healthcare related systems.

- June 2019, Israeli researchers used a raspberry PI in close proximity to manipulate CT and MRI scanning equipment, changing medical images at will.

- In 2018, researchers at DEF CON demonstrated the ability to exploit a protocol vulnerability used for devices that monitor patient's conditions and vital signs.
  - Using the exploit, they could take information on heart rates, blood pressure, blood oxygen levels, and various other points of data.
  - Researchers were able to demonstrate the ability to manipulate the data feed of the devices, displaying false information.

Source: Threatpost, Forbes, Forbes
Crime prevention through environmental design (CPTED): a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.

- Developed in the 1960s and has been expanded upon as environments and crime have evolved.
- Focuses on an organization’s physical layout; from large-scale facilities, to microenvironments, such as offices and restaurants.

Comprised of Three principles

- **Natural surveillance**
  Use and placement of physical environment features in ways that maximize visibility (e.g., walkways, activity areas, lighting)

- **Natural access control**
  Guidance of people entering and leaving a space by the placement of doors, fences, lighting, and landscaping

- **Territorial reinforcement**
  Creates physical design that emphasizes or extends the organization’s physical sphere of influence so legitimate users feel a sense ownership of the space.

Proper maintenance and management is sometimes cited as a “fourth principle.”
Environmental Threats

- Environmental threats can negatively impact an organization’s enterprise systems, damaging data assets and disrupting operations.
- Organizations should understand what types of environmental threats can affect data assets and incorporate mitigation best practices.

Fire

Fires present a danger to both personnel and critical data assets
- Organizations should understand basic fire prevention methodologies, as well as understand options for fire detection and fire suppression
- It is important to understand the different classes of fires along with the corresponding suppression method.

<table>
<thead>
<tr>
<th>Fire Class/type</th>
<th>Suppression Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A: Common Combustibles</td>
<td>Water, Foam</td>
</tr>
<tr>
<td>Class B: Liquid</td>
<td>Gas, CO2, foam, dry powders</td>
</tr>
<tr>
<td>Class C: Electrical</td>
<td>Gas, CO2, dry powders</td>
</tr>
<tr>
<td>Class D: Combustible Metals</td>
<td>Dry powders</td>
</tr>
</tbody>
</table>

Fire suppression systems come in a variety of forms:
- Wet pipe: Always contain water, discharged by temperature control
- Dry pipe: Water is held in a “holding tank” until released. Used for colder climates.
- Preaction: Water is released when pressurized air within the pipes is reduced. Used to prevent false alarms.
- Deluge: Allows greater volume of water to be released upon dispersal.

Water

Water can cause extensive damage to equipment, infrastructure, and computers
- Mold and mildew can also be a factor when unwanted water is introduced into an environment.
- Organizations should be able to detect leaks and unwanted water
  - Water detectors are an available option that should be utilized for large facilities.
  - Water detectors should be positioned under raised floors or on dropped ceilings.

Atmosphere

Proper atmospheric conditions must be maintained for the proper maintenance of data assets
- High humidity levels (<60%) risk causing corrosion to equipment.
- Low humidity levels (>20%) risk building static electricity, potential harming equipment.

Damaging Temperature levels
Computer systems and peripheral devices <175°F, >35°F
Magnetic storage devices: 100°F
Paper products: 350°F
Security Assessment

• Like auditing computer systems and networks that make up an enterprise systems, physical security should also be audited to reveal threats or gaps that may exist in the organization.

• A typical security assessment should focus on:
  - Assessing the physical security risk level
  - Planning an appropriate control to mitigate the risk
  - Devising the security and administration processes
  - Implementing the controls according to the laid down processes
  - Managing the controls as per the security administration policy
  - Auditing and evaluating the security level regularly after the defined period
  - Taking the corrective action if issues are discovered

Significant issues revealed by a physical security assessment

- Lack of leadership buy-in to the security strategy in place.
- Poor management and/or direction of security personnel within the organizations.
- Failure to identify important resources in an organization (i.e. personal computers, furniture, office equipment, workstations, processes and many other assets).
- Staff are not aware and trained about the security strategy, approaches to the resources, working with the resources, and resources leaving the organization.
- Poor visitor control system/management in place.
- Screening of contractors and temporary workers is not adequately addressed.
- The absence of a secure provisioning of the archives inside and outside the organization premises.
- Improper testing and maintenance of security equipment.
- Inadequate lighting inside and outside the facility.
- Proper physical security capabilities (i.e. intrusion detection, fire prevention systems, CCTV) not being implemented.
- Intrusion recognition frameworks, fire caution frameworks, CCTV observing frameworks and other frameworks are not appropriately used according to the security policy to keep them fully effective.
Supplemental Guidance

DHS Physical Access Control Systems

GSA – Physical Access Control Systems Customer Ordering Guide

Securicon – Physical Access Control System Security Checklist

Cybersecurity Act of 2015, Section 405(d) Task Group - Health Industry
Cybersecurity Practices: Managing Threats and Protecting Patients


Questions

Upcoming Briefs
• Remote Desktop Protocol Exploitation
• BlueKeep Update

Product Evaluations
Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information
Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.