Case Study related to physical security Cameras to illustrate problems that can be mitigated to help protect against a Breach.

IP camera security and access control are a big part of the buzz about the Internet of Things. There should be more concern about how the industry has possibly left the customer vulnerable. Today, more and more physical security systems are connected to communication networks for security monitoring, safety, and control. These connections leave systems vulnerable to cyberattack. Increasing numbers of attacks on physical security systems and companies' networks deployed in critical infrastructure facilities and corporations must be addressed with a solution that can defend against a broad range of both physical and cyber threats. Surveillance cameras, access control systems, sensors and controllers are connected using ethernet, IP and other technologies, might rely on unsecured communication networks deployed across the site, as well as in the field. The use of these unsecured networks exposes the site to combined cyber and physical threats. With the studies and concern brought about by the IoT, these problems were brought to light. Hardening of devices was not stressed and, in most cases, camera settings were left open to hacking by improper setup. The common factor in most of data breach class-action lawsuits, as well as investigations by regulatory agencies, is the allegation that the breached company failed to implement "reasonable security or protections" to prevent the breach. Logically, then, if you implement "reasonable security and protections," you should be able to confidently defend your security practices and actions.

The release of the malware, known as Mirai, gave cybercriminals with minimal skills a new tool to launch cyberattacks. Camera hacks like the Mirai exposed the threat of unsecured devices being used in an attack that involved the whole group of major websites, including Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times.

I wanted to share a Case Study provided by Axis Communications that highlights vulnerabilities as it relates to the IP Surveillance systems. While this Case Study was done for a University, there could be Vulnerabilities present in all organizations that employ Security Cameras, especially in Legacy systems that have in place for some time. Technological Obsolescence - Legacy IP Surveillance infrastructure can lead to unreliable, untrustworthy systems. Case Study related to physical security Cameras to illustrate problems that can be mitigated to help protect against a Breach.

As a Program member with Axis Communications, we have resources to provide organizations with mitigation strategies. **Please call CSI to provide an evaluation of your security network.**

Cyber Security Integration

Cyber Security Integration

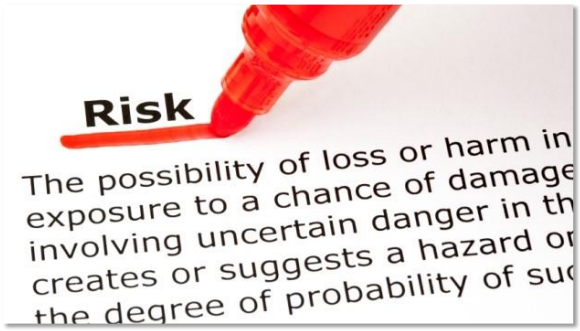
Larry Blumenfeld, President / Security Consultant

AXIS COMMUNICATIONS

Axis A&E Program member

Cyber case study - University

The “Risk”



Case study - University campus

The effect of a cybercrime:

- Identifiable intangible assets
  - Loss of intellectual property
  - Loss of personal and/or sensitive data
  - Damage to a company brand and/or reputation
- Measurable
  - Cost of countermeasures and insurance
  - Cost of mitigation strategies
  - Cost of recovery from cyber attacks

Case study - University campus

Information security

- Registration
  - –Personal data for students, alumni, parents
  - –Financial assistance
    - – Credit / Banking
    - – SSN
    - – Tax / income statements
    - – Medical records
  - –Sponsorship data / Student grades
- Point-of-Sale data
- Intellectual property / cutting-edge research

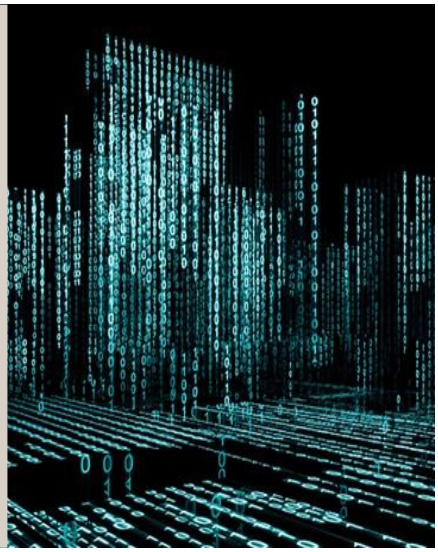
Physical property

- R&D
- University property

Case study - Network

Exploit the camera for malicious activities:

- Remotely gain root access to the camera, potentially gaining access to the rest of the network
- Spoofing the DNS server addresses specified in the camera's settings
- Stealing credentials from camera users
- Hijack devices using just the IP address and without previous access to the camera or its login credentials
- Launch a distributed denial-of-service (DDoS)
  - – Does the Mirai botnet sound familiar?



Case study - Video surveillance platform

Exploit the camera for control:

> Access to live / recorded video and audio feeds
> Execute remote commands against the camera
> Gain access to the video stream
> Ability to freeze streaming
> Control the camera lens motion
> Alter the software of the camera
> Simply rendering the camera entirely useless, leaving the premise at risk
> Add the botnet to the camera(s)

Case study - University campus

Threat to assets:

> DDoS
> Video tampering
> Network penetration

Vulnerabilities present in the environment:

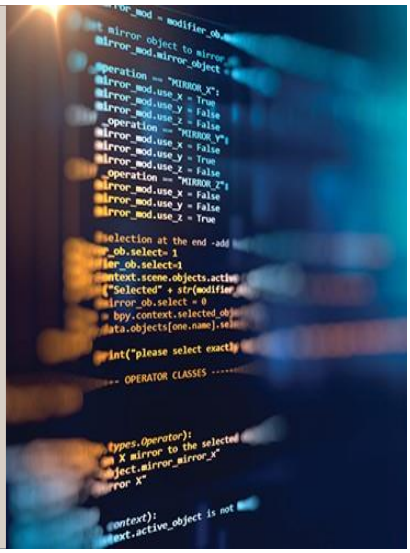
> Technological Obsolescence
> Out-of-date software / firmware
> Poor configuration

Evidence of vulnerabilities:

> Older devices that cannot be patched
> Default PW on devices
> Sporadic encryption

Risk summary:

> Potential exploit of known vulnerability
> Hijacking of camera (streaming, recording, audio, visual clarity)
> Network penetration into information systems



Case study - University campus

Avoid the risk

Transfer the risk

Determine action

Mitigate the risk

Accept the risk

Source: (ISC²)