Physical Security Today and Considerations for the Future

Presented By:
Sean Patton, Sr. Systems Engineer
Frontrunner Network Systems
spatton@frontrunnernetworks.com
(585) 899 - 4474

Agenda

1. **Defining Risks and Threats**
   - **Commonality of Terms**
2. **Physical vs Cyber Security Programs and Planning**
3. **Physical Security Audit**
   - **Multilayer Threats**
4. **Physical Security Audit Review**
5. **Looking at future changes to Physical Security technology and how that impacts Cyber Security**

FRONTRUNNER

Threats and Risks

Threats Facing Enterprise Security Teams

- **Outside Unauthorized Access**
- **Identity Theft**
- **Intellectual Property Theft**
- **Untracked Activity - Eavesdropping**
- **Tampering with Systems and Processes**

FRONTRUNNER

Cyber vs Physical Term Comparisons

Cyber Security

- **Intrusion Detection**
- **Authenticated Access**
  - **Secure Digital Signatures**
- **Phishing**
- **Privilege Escalation**
- **Spoofing**
- **Deep Packet Inspection**

Physical Security

- **Intrusion Detection**
- **Authenticated Access**
  - **Secure Key Formats**
- **Loitering**
- **Tailgating**
- **Key Duplication**
- **Backscatter X-ray**

FRONTRUNNER

Why a Physical Security Audit

- Multiple Layer Approach to Physical Security
- Value of Data driving creativity of hackers
- Outside Access vs Internal Access
  - Electronic Access Control on Ingress Doors
  - Physical Keys or no Access Control on internal offices
    - Next Generation Firewall only using NAT functions
- Physical Security will end up in your purview in the near future anyway

FRONTRUNNER

Looking forward to Cyber and Physical Security Crossover Interests

- Physical Security Manufacturers Leveraging Cloud
  - Hosted Access and Video Management
    - How does this effect Cyber Security Policy?
- Mobility App Based Access Credentials
    - How will this effect MDM?
- Mobility Users accessing Access System Remotely
  - How is your network protected from infected devices?
- Physical Security Manufacturer devices with known Cyber risks
  - Is your organization aware of compromised devices?

Conclusion and Discussion

- Physical Security and Cyber Security Teams need to form an open dialog.
  - Have you assigned an internal liaison between the 2 teams?
  - Have you coordinated a meeting to allow both teams to share their primary focus and concerns with the other?
- All of the Cyber Security Programs put in place can be compromised by a single open door

FRONTRUNNER