Cybersecurity 101: Hardening the Physical Network

“I know you know this stuff, but do you practice it?”

Michael Mann CPP, PSP, CISSP
Partner / Sr. Systems Design Consultant
Network Geek Question?
What’s Layer 1 of the Open Systems Interconnection (OSI) Model?
Network Geek Question?
What’s Layer 1 of the Open Systems Interconnection (OSI) Model?

Physical: Transmission and reception of raw bit streams over a physical medium.

At the base of all communications systems something needs to connect A to B.

AKA the Wire!
What’s the easiest way to crash a network?
What's the easiest way to crash a network?

Attack, Attack, Attack!!!!

Steal Passwords?
Eavesdropping?
Launch Denial of Service?
SQL Injection?
Trojan Horse?
Send in the Worms?
What’s the easiest way to crash a network?

How about we unplug it!
Without the Physical there would be no Logical.

Hardening your Physical Network

- Data Communications Facilities
- Redundancy
- Cabling Infrastructure
- Network Equipment
- Devices and Connections
Look Goldilocks, the doors unlocked, and no one's home.
Communications Spaces

Data Communications Facilities:
Data Center, MDF / IDF, Communications Closets

Lock the door, and make sure you know who has the key! (Better yet, don’t use a key.)

Implement Electronic Access Control on all access point to critical infrastructure. (audit who, when, and where.)

Implement Video Surveillance in communications nodes.
( I see you 😊 )

The Insider will always be your Biggest Threat.
Redundancy

It’s technically a Tropical Storm not a Hurricane. Does it really matter?

What are Rolling Blackouts?

Lightning, what lightning?

Who turned off the lights?

And the worst of the worst “I can’t check my Facebook!” The internet is down!
Redundancy

Power will go out, make sure your network doesn’t.

Provide appropriate UPS, Surge Protection, and Generator Power to your network and equipment.

If you live in the “Cloud” or have remote resources via the internet, your only as good as your provider, consider having a back-up plan.
Is that a Network Switch in the staff break room?

“Yeah, it seemed like a good idea at the time.”
Secure your equipment. Keep it accessible only to individuals who need access.

Put your equipment in appropriate locations.
LOCK YOUR CABINETS!
Cabling Infrastructure

I can’t ping that video camera?

“That’s because someone cut the wire.”
Cabling Infrastructure

Ensure your critical infrastructure and device deployment is appropriately hardened.

Protect your structured cabling from the elements and sabotage.

Cable Management, Network Monitoring Systems
Wow, I just plugged my Laptop into this network drop and I can see the “World”.

Network Devices and Connections
Network Devices and Connections

Keep rouge devices off your network. Practice network port security. Remember, if someone can plug it in, they will.
Thank You.

Questions?