IT/OT Cyber Security

January 19, 2018 | The Langham Luxury Hotel, Chicago, IL

Panel

Riaz Zolfonoon

Sherman Chong

John Bohlmann

Dave Bohlmann

IT/OT = IOT

IT *vis-a-vis* OT

Similarities:

1. **Live in same building**
2. **Not enough people to do job**
3. **Not enough budget**
4. **Use Data and Processes**
5. **Need security**
6. **Must keep C-Level happy**
7. **Do not talk with one another**

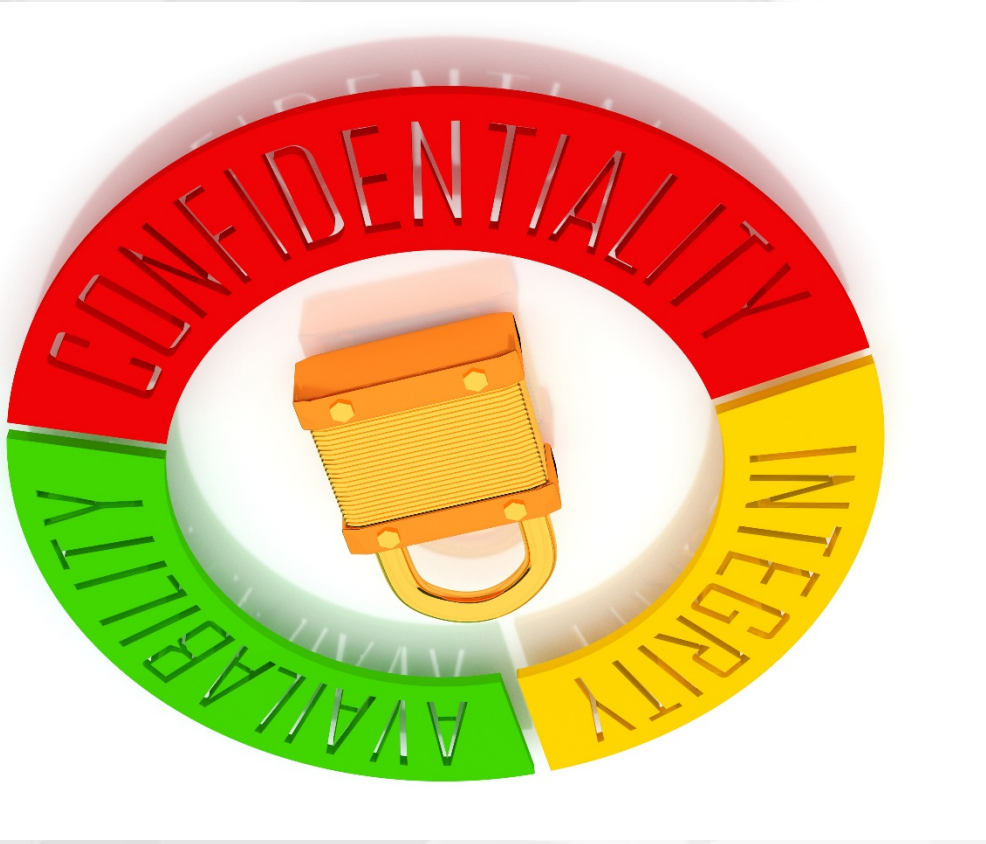
IT *vis-a-vis* OT

Difference in Degree:

1. **IT Data vs OT Processes**
2. **IT Fast vs OT Slow**
3. **IT CIA vs OT AIC**

Security Triad

IT Focus



OT Focus

IT/OT Questions

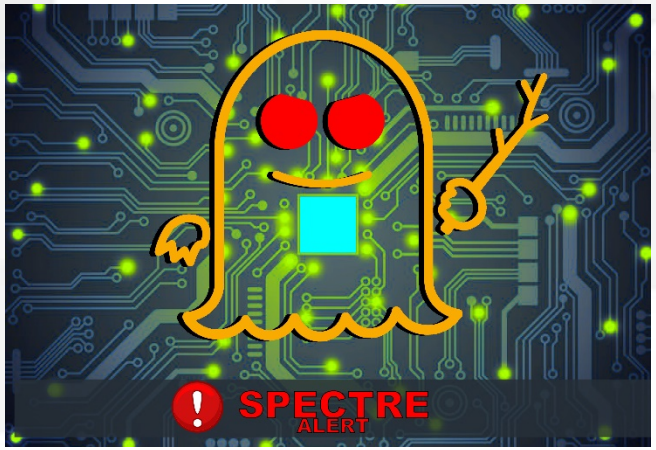
1. When does IT get involved with OT project?
2. Are security requirements clearly written in spec?
3. How to get OT out of IT blind spot?
4. Does OT know IT patch schedule?
5. What IT project can OT help with?
6. How much Mountain Dew does your IT drink? What beer does your OT like?

Security Culture

“Vulnerabilities”

Scope of Problem

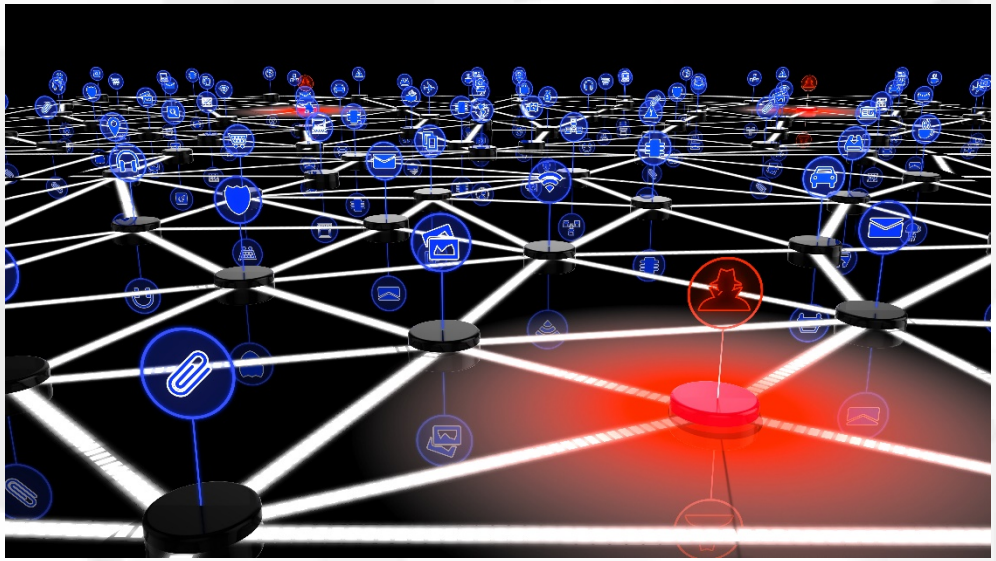
1. 4/5ths successful penetrations via social engineering
2. Avg breach = $7M; cost to repair = $100K
3. 48 States now require some sort of reporting of a breach
4. DDOS servers, malware and ransomware readily available for little cost
5. Privacy laws quickly getting stricter



Get Culturized

Sound Bytes

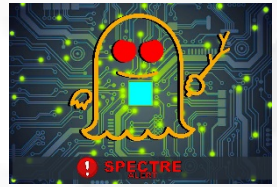
1. Security can't be sprinkled on top – must be baked in
2. Security is basic hygiene
3. 95% of employees seek ways to bypass security policies
4. SSNs used to be $30 on dark web; now are 50¢
5. Most hackers are not ultra smart; take advantage of basic mistakes



“Remedies”

Be Diligent In

1. **Awareness**
2. **Guardedness**
3. **Teamwork**
4. **Planning**
5. **Testing**
6. **Learning**
7. **Diligence**



Knowledge Building

Info and Training

www.stopthinkconnect.org

csrc.nist.gov

ics-cert.us-cert.gov

www.iotprivacyforum.org

www.infragard.org

www.isa.org

ncsc.gov/nittf

www.ge.com/digital/cyber-security

www.isc2.org

Commander Highlights

Commander / Snappy

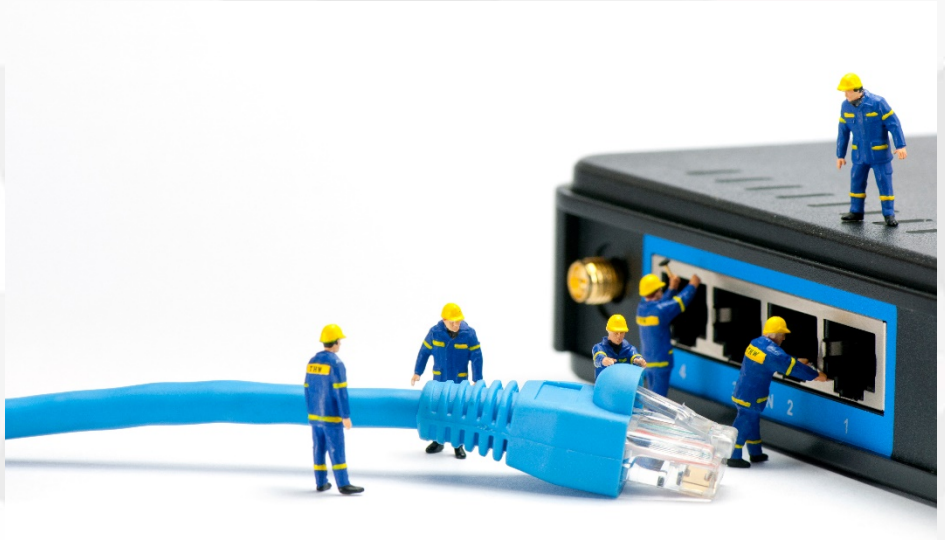
Ubuntu Core / Snappy:

1. **OS kernel read-only**
2. **Code (snaps) ‘dockerized’**
3. **Manual configuration of snap interface with snaps**
4. **Snaps must be Canonical approved for security**
5. **Only pre-configured snaps may execute**

Commander Messaging

Messages:

1. **Initiates all messaging**
2. **Extensive use of TLS**
3. **Configurable LAN/WAN whitelists**
4. **SSH password different for each box**



Fragen?


DANGER
FREE AIR DROP TO
GROUND ON OTHER
SIDE OF DOOR.
FOR ACCESS CONTACT
THE ENGINEERING
DEPT. @ 312.337.1842

Thank you!

Gamification Code: MLA553