Cyber Insider Threat
Witting, unwitting and emergent

Rob Hoffman,
Nuclear Cyber Advisor
Idaho National Laboratory, USA

CO-HOSTED BY

insiderthreatmitigation.org

Common definition “Cyber Insider”

INSIDER THREAT MITIGATION

- Type A – Malicious threat actor with trusted access
- Type B – Negligent employee who’s actions enable escalated access

- *2018 Survey by CyberSecurity Insiders and CA Technology* stated that while 47% of companies are concerned about the willful theft of data or sabotage by a malicious cyber actor (Witting), 51% are concerned with data breeches through employee negligence or compromised credentials (Unwitting).

Think about it from the ***computer's perspective***

INSIDER THREAT MITIGATION

- Who or what is a "trusted insider"
- Basically, it's any device that is allowed to communicate with another device at each layer of validation.
- In a network environment it can be literally "anyone" that manages to tap the line, execute a legitimate "handshake" and then "speak" the appropriate language.

Much as we utilize guards and gates in the physical world to protect trusted communities of coworkers, firewalls and authentication protocols are tasked to keep the boarder in a networked environment, but if a device can get "past the gate" trust is implicit.

Human vs Computing “insider interaction”

INSIDER THREAT MITIGATION

	Human	Computer
Authentication	Something we know, have or are (password, badge, bio)	Digital “handshake”
Once inside a controlled area	Relationships build trust over time	Trust is implicit
Continued access	Work assignment, or a “need to know”	Trusted until an action is taken to revoke the trust
Impersonation	Difficult but possible as each interaction risks exposure	“spoofing” a trusted source grants all access of that source
Risk	High in small work circles, much easier in large enterprises	Computers don’t typically consider geographic proximity

Industrial Control Systems

INSIDER THREAT MITIGATION

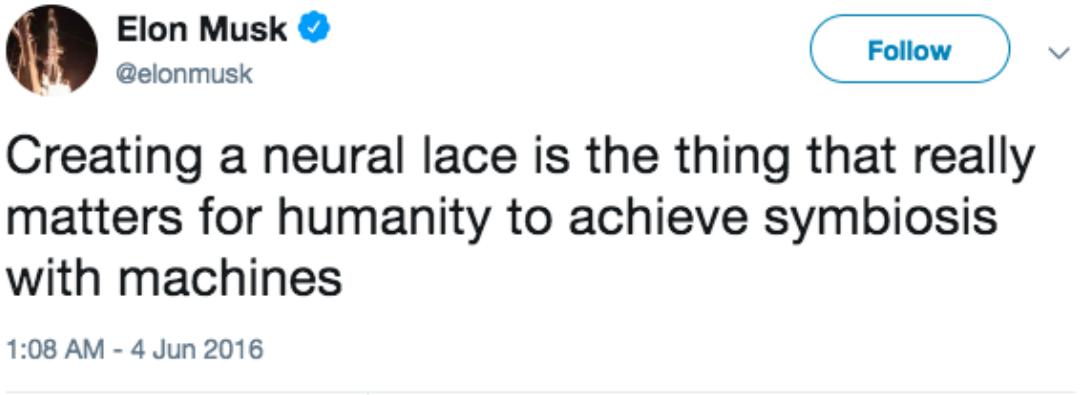
- Inside an industrial process – all devices are typically considered “trusted” unless otherwise stated.
- Be default, any device on the network is there specifically to play a role in the execution of the process that is being automated.
- “Trust” is not earned - “Insider status” is assumed.
- As remote access, process monitoring and control are expanded to support financial efficiencies, *the circle of trust is stretched to unrealistic proportions and ripe for abuse*.

In computing, “Trust” is a luxury we can no longer afford

INSIDER THREAT MITIGATION

- In the expanding “Internet of Things” world view, ***Trust*** is no longer tied to local relationships, ***Insider*** is often difficult to ascertain.
- Every digital device an individual carries or interacts with represents exposure to ***Unwitting*** trust escalation and attack.

Consider – *smart watches, phones, performance clothing, heart monitors, games, home automation, electric fueling stations, navigation systems, and soon, embedded Neural Lace, etc..*



In the near future – interconnected world

INSIDER THREAT MITIGATION

- Ultimately, *as **individuals loose the ability to certify their own digital integrity***, we will need to “Flip” the work related trust model upside down and trust no one, or perhaps rather…

- trust everyone, but verify everything -

Utilize out of band transaction monitoring and validation