RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SBX4-W3

THINK LIKE A HACKER BUT ACT LIKE AN ENGINEER

Marty Edwards

Managing Director
Automation Federation
@ICS_Marty

Stop ignoring the fundamentals

- **PROBLEM:**
  - Cyber attacks on Industrial Control Systems (ICS) and/or Operational Technology (OT) can have significant physical consequences
- **SOLUTION:**
  - Apply sound engineering principles, and consider cyber induced consequences when designing and building systems

Acknowledgement / Disclaimer – This presentation is based upon a series of works entitled “Consequence-Driven, Cyber-Informed Engineering (CCE)” developed by the Idaho National Laboratory (INL). The presenter has collaborated with the INL on this presentation and has obtained their permission to utilize this material.

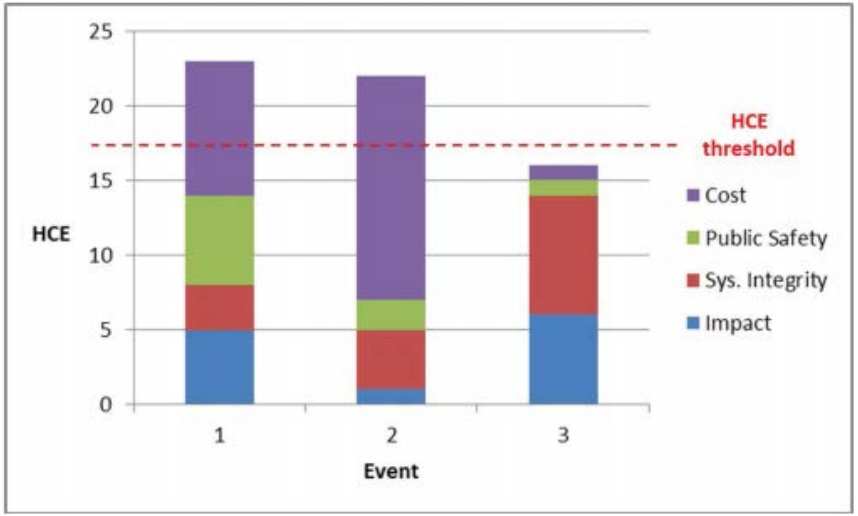
This requires several different skills

- How can I cause the most significant damage to your process?
- Is there a cyber-based control system involved?
- Where are the dependencies?
- Where can I attack the system using cyber means?
- Map the ICS Kill Chain
- Design out the cyber risk
- This is NOT application of control system cybersecurity!

Step 1 - Consequence Prioritization

GOAL

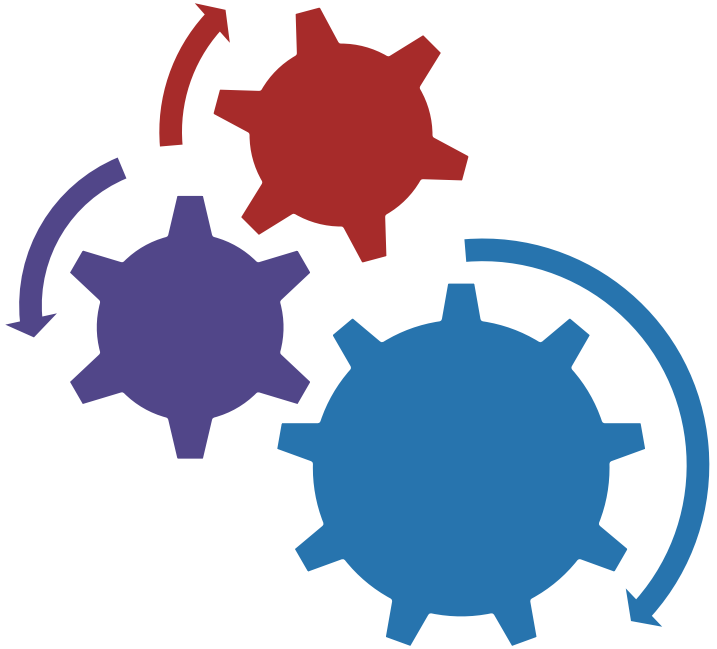
- Generate a list of functions within your business or operation that **“simply must not fail”**
- An adversary intending to do you harm will attempt to find these
- Consider impact measures such as cost, public safety, system integrity
- This list should be extremely short!



Step 2 - System of Systems Breakdown

GOAL

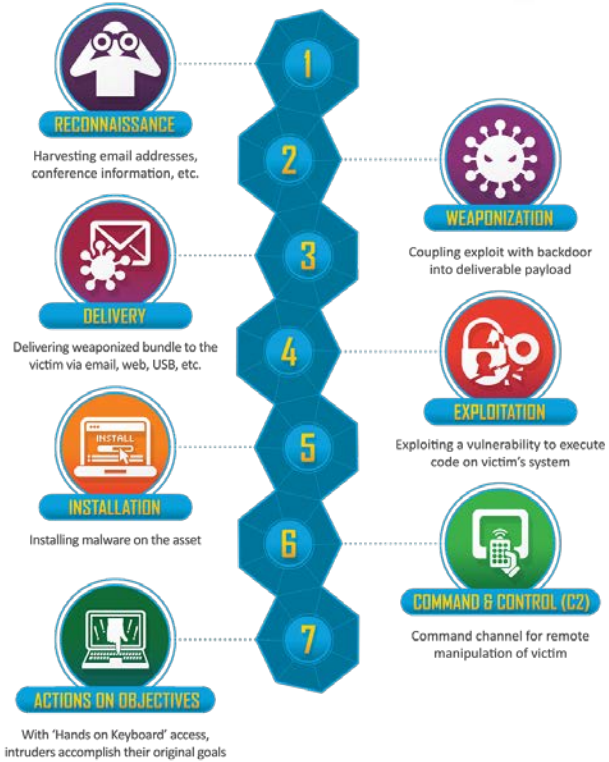
- Understand the multifaceted interdependencies between all components of the system
  - Network connections?
  - Supply Chain?
  - Vendor Remote Support?
- Does equipment require lubrication?
- Where is my weakest link?



Step 3 - Consequence Based Targeting

GOAL

- Identify what an adversary would have to do through cyber means to cause the highest impact effects
- What access do they need?
- What information do they need?
- Adapted from Lockheed Martin by SANS, the ICS Kill Chain is an effective method to walk through these steps



Step 4 – Non Cyber Mitigations & Protections

GOAL

- Develop an engineering based control to eliminate the cyber risk to critical functions -- completely
  - Hardwired interlock
  - Mechanical protection
  - Custom analog and digital circuitry
- No this isn't going "backwards" – this is prudent use of technology

Think like a hacker, but act like an engineer!

- Identify your most critical business or operations function
- Understand what systems, controls or devices support it
- Determine how an attacker would cause the most damage by compromising the cyber integrity of any of that equipment

- Go back to basics – find a way to accomplish the function without relying on a cyber device. After all, it is your most important function!
- Build a culture of security and safety around cyber-physical systems