Learning

Build processes to learn from real world incidents

Learning · Incidents · Lessons

Standards as a Tool to Manage Risk

- Standards are a good tool to manage risk when it is either well-bounded and understood or when the standard simply codifies well-honed industry practices that are proven to be successful.
- Mandatory cyber standards fail both of these conditions, mainly because advanced cyber threats are not probabilistic in nature, but represent a co-adaptive risk.
- Regulation, although necessary, should be re-evaluated and designed to emphasize learning, enable the development of greater technical capabilities through more qualified staff, and discourage the creation of a predictable and static defense.

Enforcement

- A call for discretion – Challenge for both regulators and entities
- Audit focus on risk and sound practices not administrative issues
- There is a tremendous burden to managing the proof of compliance and staying on top of change control
  - Benefits but it can be taken too far
- Expectations are still not clearly & uniformly being set by audit teams across regions
- Reports are being modified to be audit friendly vice useful for staff responsible for ongoing security risk management
- Methods and practices are still being evaluated for effectiveness

Reporting Models

- FAA/NASA Program

Incidents

Industry observed incidents

Learning · **Incidents**· Lessons

Common Business System Incident Examples

- Global malware
- Botnets
- Webpage hacks
- DoS
- Exploit kits, injection, etc.
  - "under new management"
- Phishing attacks

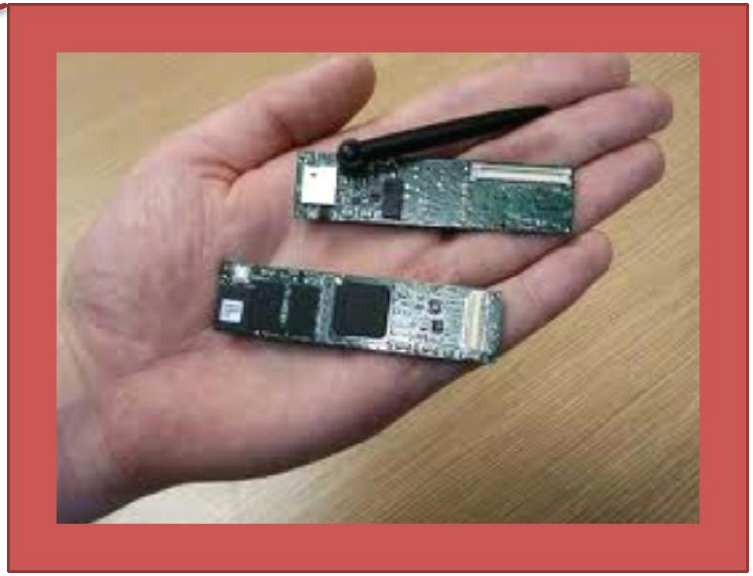
- Standards work best when aligned with this set of attacks, but the electronic security perimeter is quickly becoming an obsolete concept

OT System Incident Examples

- USB Borne malware
- Devices moving into more trusted networks
- Worm propagation
- Web server hacks
- Phishing attacks
- Meter tampering

What are we not seeing/reporting?

- Custom written malware
- Highly directed spear phishing
- Hardware hacks
- Plug-in attacks



The New Threat Landscape

- Sophisticated & High-Consequence Attacks
- Stuxnet dispels conventional thinking that it is just “too hard” for an attacker to assemble the necessary information, gain familiarity with the technology, acquire the knowledge of specific implementations, configurations and accesses, to devise an attack that could disrupt or damage the physical components of an industrial process

Lessons

What do we do

Learning · Incidents · **Lessons**

Lessons

- Incident reporting has been severely impacted by CIP standards
- Supply chain is a successful vector for attacks
- Data collection and analysis tools are lacking
- Forensic capabilities and procedures for ICS do not exist nor exercised across the industry
- Architectures are tired, circumvented, and relaxed as business models are changing
- Programs do not consider embedded systems/firmware
- Vendor involvement in incident response can be critical
- Consider anti-fraud approaches for AMI
- Violations of “know thy self”

Lessons

- Consider economic competition to include supplier/market development (renewable energy plans & procurement)
- Prevention mind set remains – need to transition to contested territory concept
- Pool resources?
- Not keeping up with “ground truth” or adversary TTPs outside of our industry

Defender Goals

Be dynamic, learn, and apply learning