The Consequence-driven Cyber-informed Engineering (CCE) Methodology

Engineering out the cyber risk from things that must not fail

Andy Bochman & Daniel Noyes
Acknowledging the New Realities of Cyberspace

Critique of Cyber Hygiene-Only Approaches

Intro to CCE
Successful strategies must proceed from the premise that cyberspace is \textit{continuously contested territory} in which we can control memory and operating capabilities some of the time but cannot be assured of complete control all of the time or even of any control at any particular time.

\textit{Richard Danzig}

"Surviving on a Diet of Poisoned Fruit"
The New Realities: Beware Tech Monocultures

Recommends a “segmentation of the attack surface ... where optimality and efficiency are traded for robustness and resilience.”

&

“To thwart outcomes that follow sentient opponent actions, diversity of mechanism is required.”

Dan Geer
“A Rubicon”
“Cyber hygiene is helpful for warding off online ankle biters and if done perfectly in a utopian world, might thwart 95% of attackers.” But in the real world virtually all places, “it registers as barely a speed bump for sophisticated attackers aiming at a particular target.”

Michael Assante
Interviewed on CCE
Acknowledging New Realities of Cyberspace

Critique of Cyber Hygiene-Only Approaches

Intro to CCE
What is Hygiene?

SANS Top 20

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises
Cyber Hygiene is Everything We Do in Cyber

- Identify
- Protect
- Detect
- Respond
- Recover

NIST Cybersecurity Framework

NERC CIP Compliance

RSA CONFERENCE

IEEE CYBER SECURITY

* Exception: Active Defense / Hunting
The New Realities: Shortest Form

If targeted, you will be compromised.
Unless ... CCE Takes the Targets off the Table
Acknowledging New Realities of Cyberspace

Critique of Cyber Hygiene-Only Approaches

Intro to CCE
Think like a hacker, but act like an engineer.

- Marty Edwards, former Director, ICS-CERT
CCE – A 4-Step Process

**Consequence Prioritization**
Determine critical functions and high-consequence events; identify what cannot fail through ruthless prioritization based on the consequences.

**System of Systems Analysis**
Examine how the critical function is achieved; identify the key information, access, and actions an attacker must take to produce an effect.

**Consequence-based Targeting**
Illuminate where the control system is vulnerable by thinking like an attacker (networks, supply chain, close-access attacks).

**Mitigation and Protections**
Engineer-out the cyber-risk; interrupt the attacker’s progress with simple and complex engineering controls.
1. Thermisation
2. Raw Milk Storage
3. Pasteurization
4. Separation
5. Cheese Production
6. Shaping, Drying, & Salting
7. Ripening/Ageing
Certain attackers will find ways to create high consequence events.
CCE demands ruthless prioritization
A Variety of Skills are Required

Adversary

- How can I cause the most significant damage to your process?

Analyst

- Is there a cyber-based control system involved?
- Where are the dependencies?

H4XØR

- Where can I attack the system using cyber means?
- Map the ICS Kill Chain

Engineer

- Design out the cyber risk
- This is NOT application of control system cybersecurity!
Mitigation Example

A Modern ICE:

- Digitally controlled
- Mechanically protected
Mitigation Example

Attack Surface Disruptor:

- **Hard-wired safety logic**
- **No software**
- **No comms**

The role of the AD to block a malicious breaker close allows the device to have less restrictive detection thresholds, i.e., no breakers will trip.
What You Can Do Now

I. Keep performing cyber-hygiene across the enterprise

II. Ruthlessly prioritize protection of the systems that support your must-not-fail functions

IV. Change the culture to incorporate cyber-informed security as an engineering principle

III. Mitigate risks with:
- Backstops – analog measures to prevent catastrophic consequences
- Backups – non-identical redundancies
Caution: Good Engineering can be Mistakenly Characterized as Backwards

Senators Want Dumber Tech For Energy Grid Cybersecurity
Thanks !!!