INL/MIS-24-80768-Revision-0

Cyber Informed Engineering (CIE) Principles Slide Presentation

June 2024

Benjamin Ruhlig Lampe, Virginia L Wright

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-24-80768-Revision-0

Cyber Informed Engineering (CIE) Principles Slide Presentation

Benjamin Ruhlig Lampe, Virginia L Wright

June 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

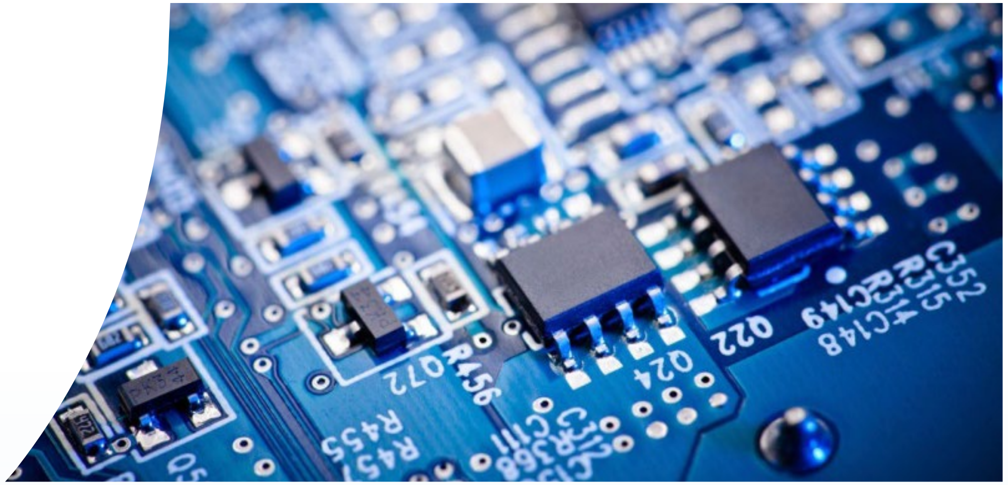
Cyber-Informed Engineering

What is CIE?

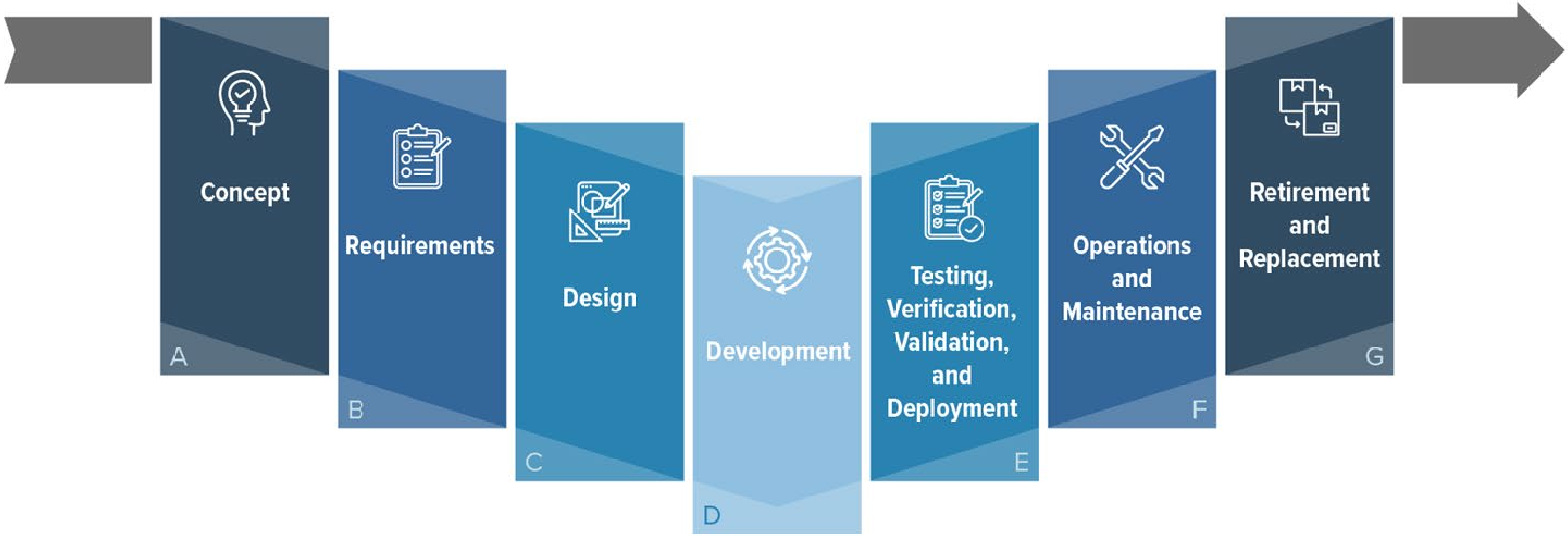
June 27, 2024

Cyber-Informed Engineering (CIE)

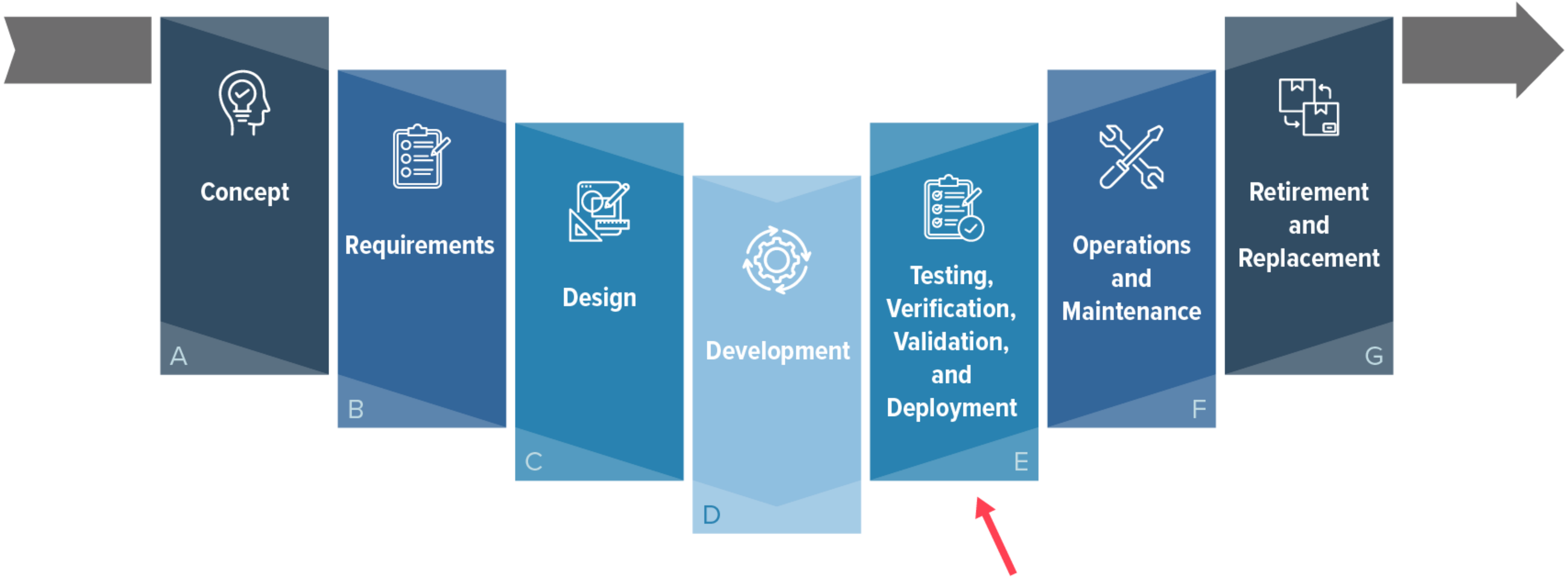
- CIE uses **design decisions and engineering controls** to eliminate or mitigate avenues for cyber-enabled attack.
- CIE offers the **opportunity to use engineering to eliminate specific harmful consequences** throughout the design and operation lifecycle in addition to traditional cybersecurity controls.
- Focused on **engineers and technicians**, CIE provides a framework for cyber education, awareness, and accountability.
- CIE aims to build **a culture of cybersecurity** aligned with the existing industry safety culture.



CIE and the Systems Engineering Lifecycle

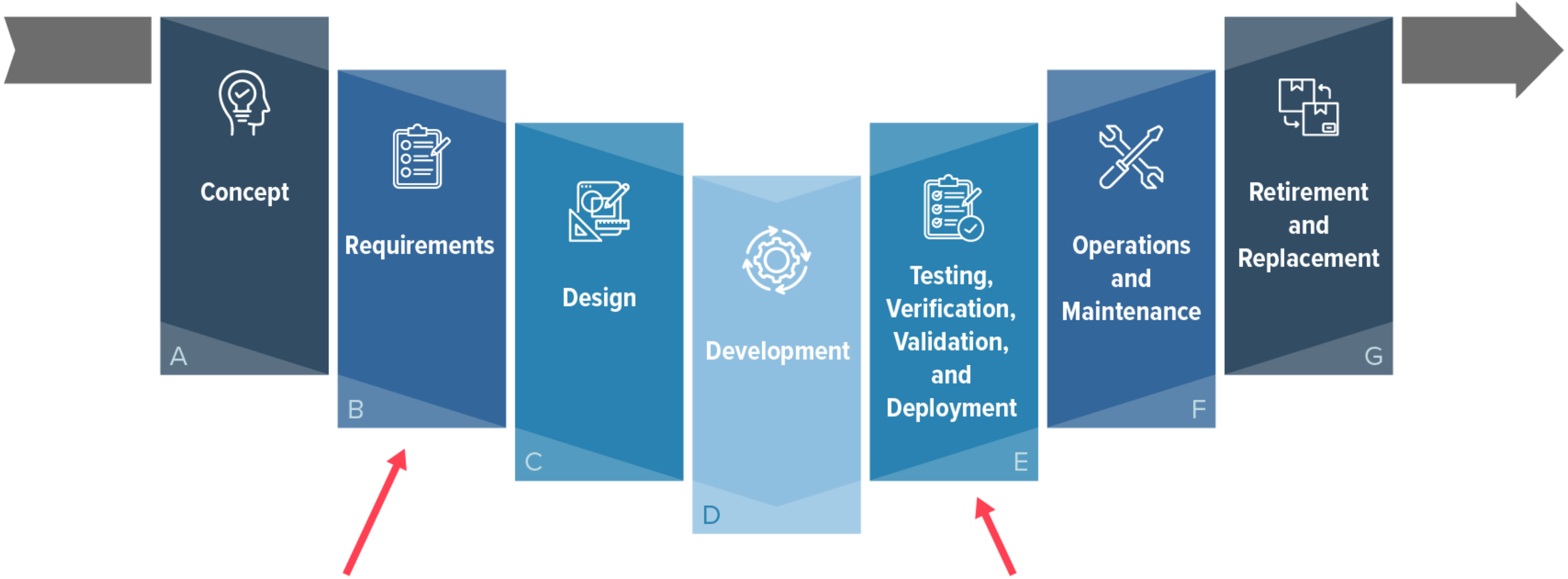

Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

CIE and the Systems Engineering Lifecycle


Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

OT Cybersecurity risk mitigations are usually applied here…

CIE and the Systems Engineering Lifecycle


Concept
A
Requirements
B
Design
C
Development
D
Testing, Verification, Validation, and Deployment
E
Operations and Maintenance
F
Retirement and Replacement
G

...but they are more effective and efficient when applied here.

OT Cybersecurity risk mitigations are usually applied here...

Cyber-Informed Engineering

CIE Principles

PRINCIPLE	KEY QUESTION
Consequence-Focused Design	How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?
Engineered Controls	How do I select and implement controls to minimize avenues for attack or the damage that could result?
Secure Information Architecture	How do I prevent undesired manipulation of important data?
Design Simplification	How do I determine what features of my system are not absolutely necessary to achieve the critical functions?
Layered Defenses	How do I create the best compilation of system defenses?
Active Defense	How do I proactively prepare to defend my system from any threat?
Interdependency Evaluation	How do I understand where my system can impact others or be impacted by others?
Digital Asset Awareness	How do I understand where digital assets are used, what functions they are capable of, and what our assumptions are about how they work?
Cyber-Secure Supply Chain Controls	How do I ensure my providers deliver the security the system needs?
Planned Resilience	How do I turn “what ifs” into “even ifs”?
Engineering Information Control	How do I manage knowledge about my system? How do I keep it out of the wrong hands?
Organizational Culture	How do I ensure that everyone’s behaviors and decisions align with our security goals?

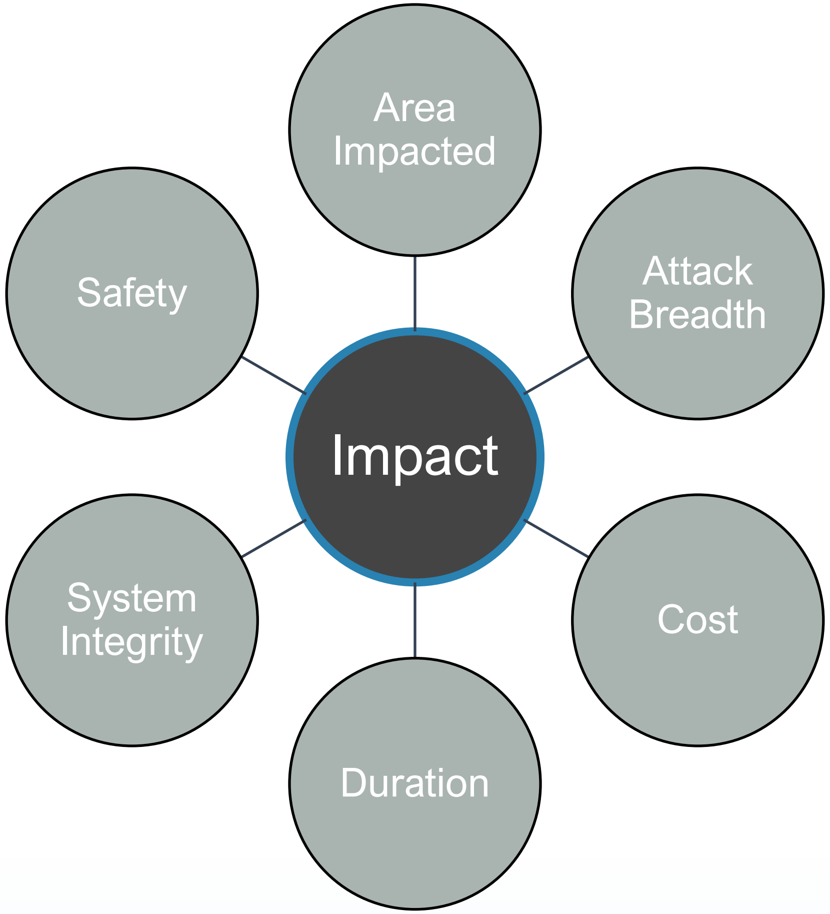
CIE Principles Deeper Dive

Consequence-Focused Design

KEY QUESTION

How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?

- What is normal operation?
- What is the worst consequence of this operation?
- What are the system's critical functions?
- What is my risk appetite?

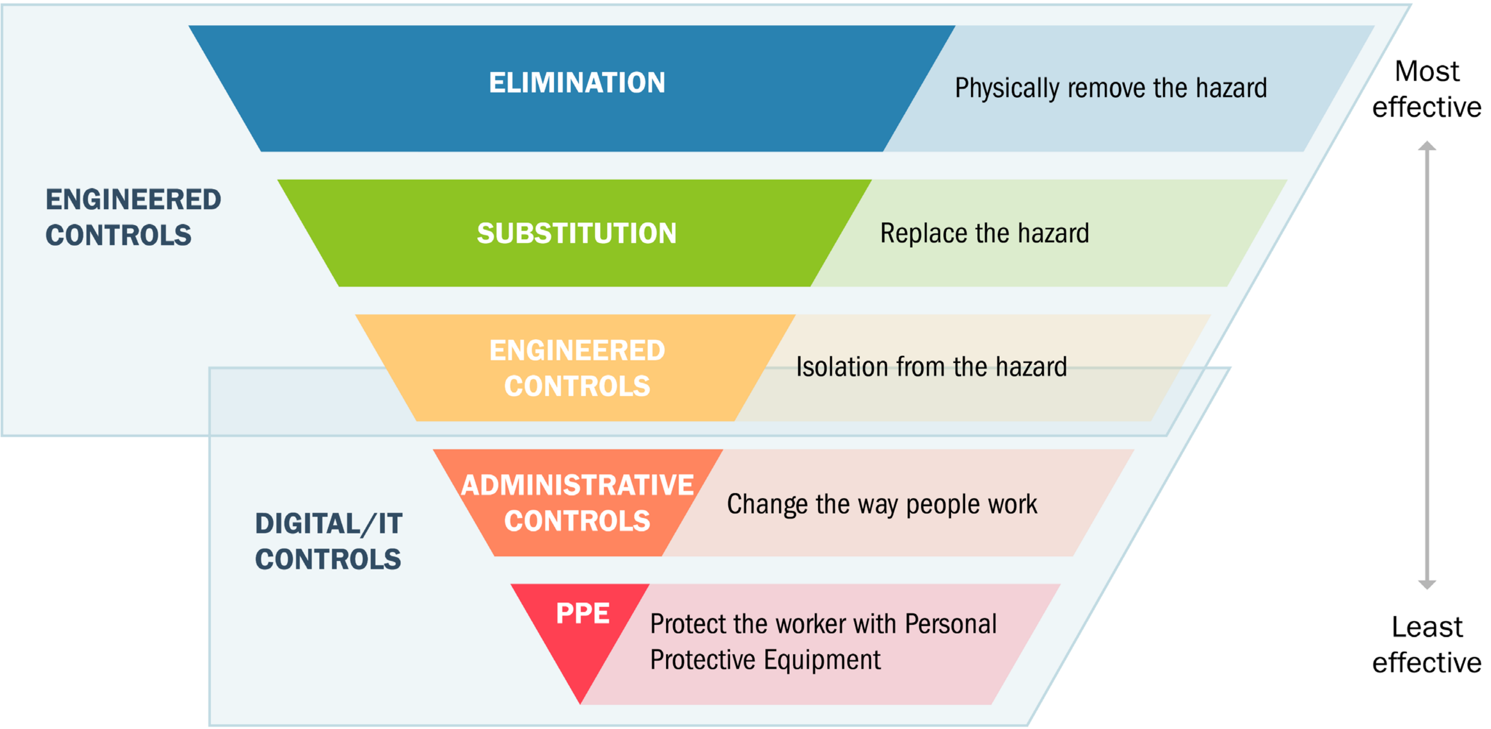


Engineered Controls

KEY QUESTION

How do I select and implement controls to reduce avenues for attack or the damage that could result?

Hierarchy of Controls



Graphic adapted from: CDC NIOSH - https://www.cdc.gov/niosh/topics/hierarchy/default.html

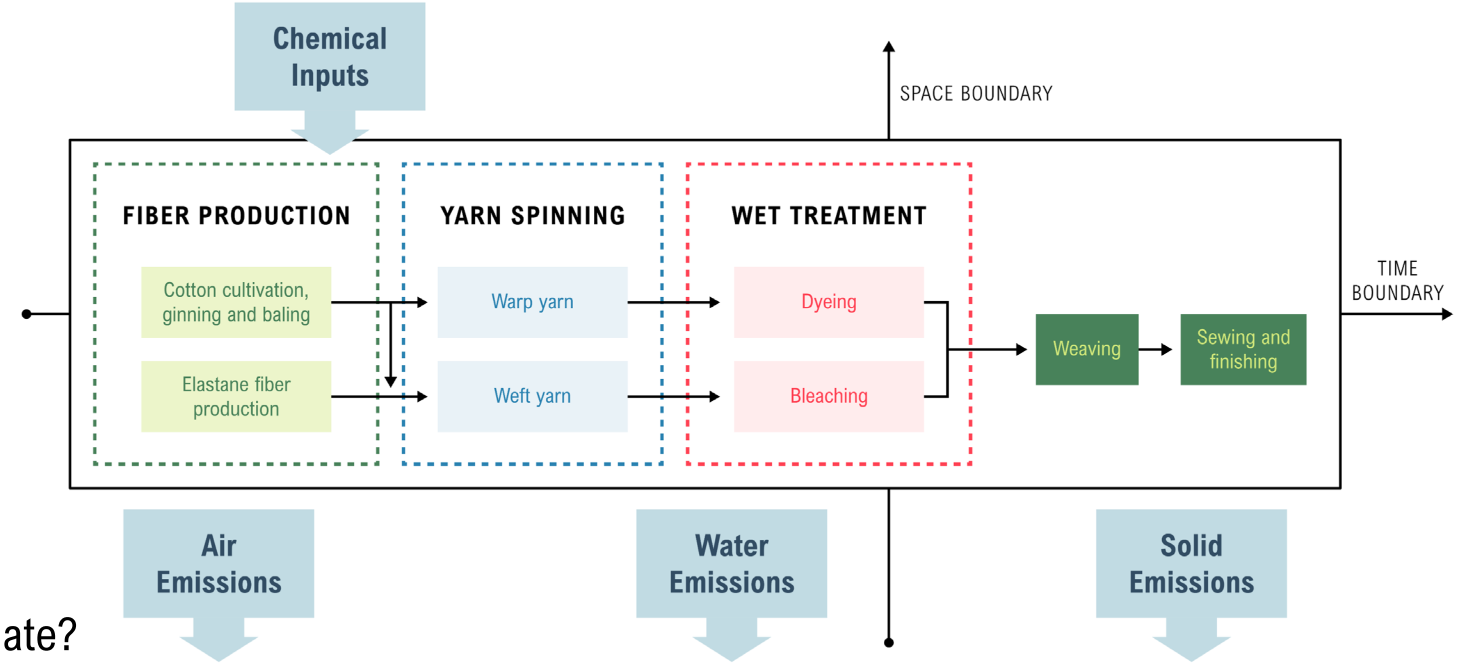
Secure Information Architecture

KEY QUESTION

How do I prevent undesired manipulation of important data?

For our critical functions:

- What is the critical data?
- What systems originate, change, and validate?
- How will data flow?
- How should we group the data flows and data?
- How can we create monitorable boundaries?
- Where are areas of implicit trust?

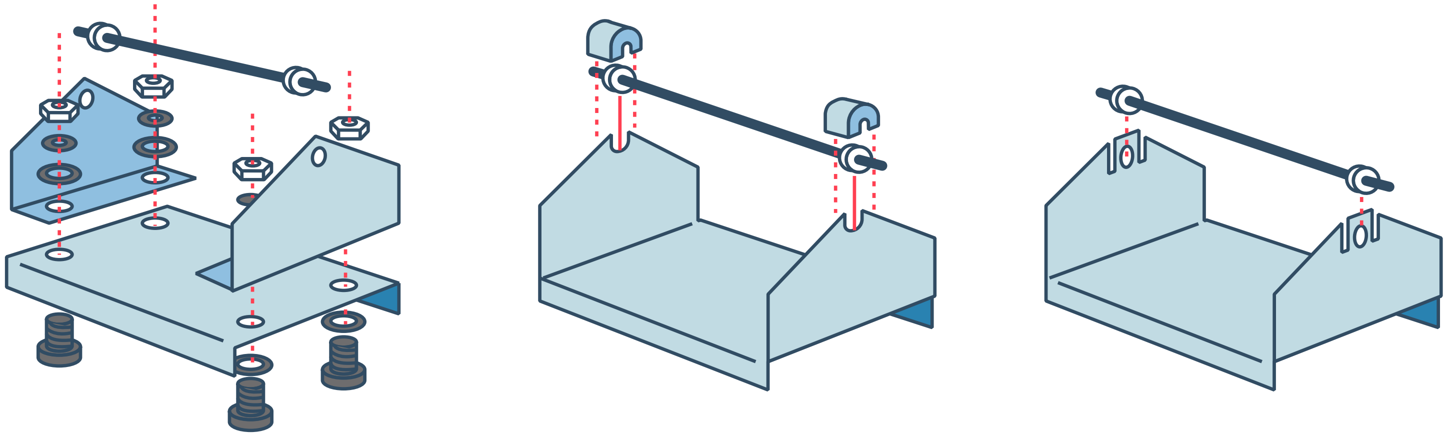


Design Simplification

KEY QUESTION

How do I determine what features of my system are not absolutely necessary to achieve the critical functions?

- Are all of the elements of my design actually required?
- How do I reduce complication?
- What do I lose by simplifying?

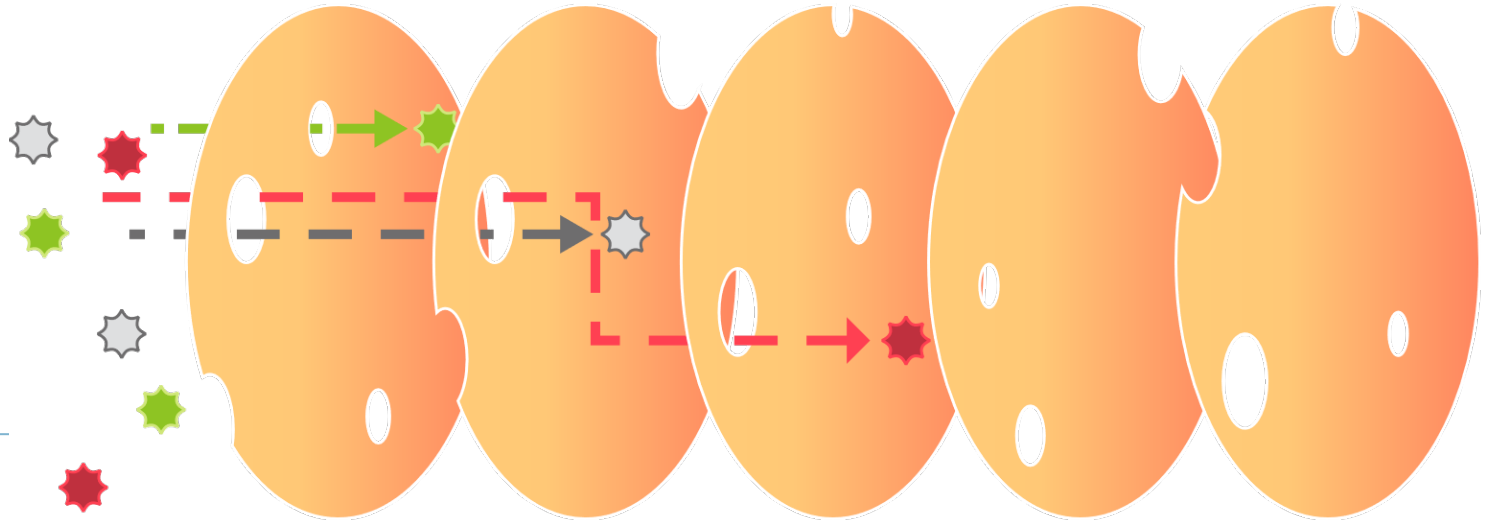


Graphic adapted from: http://www.slideshare.net/BabasabPatil/product-design-ppt-doms

Layered Defenses

KEY QUESTION

How do I create the best compilation of system defenses?



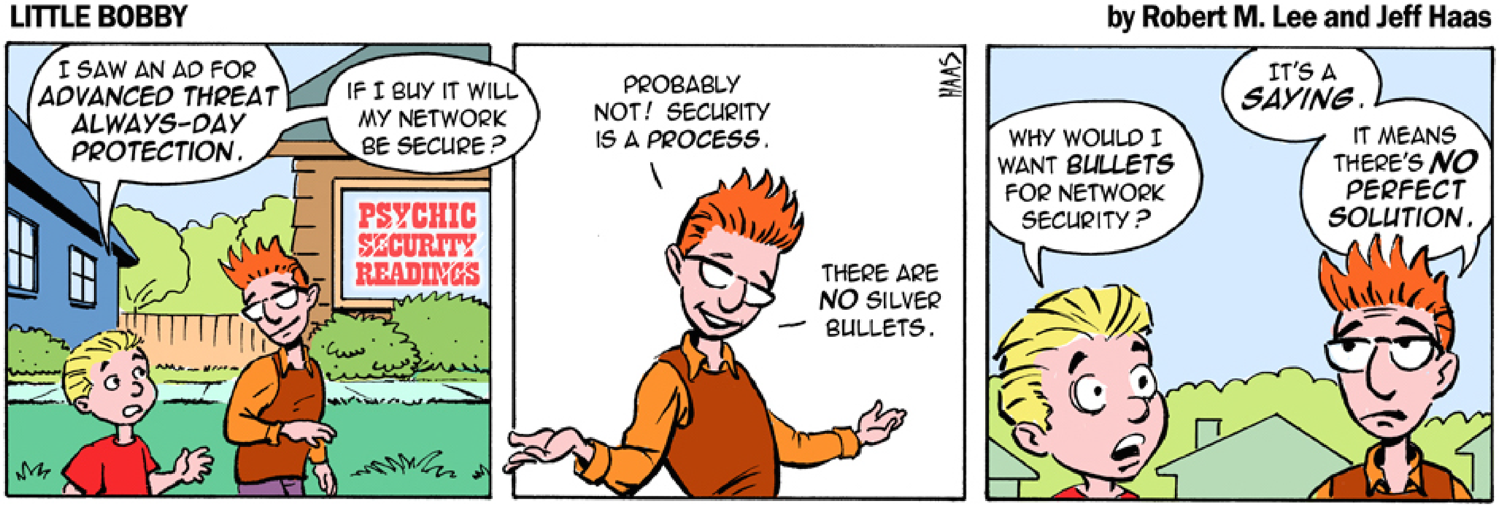
Reason's Swiss Cheese Model adapted from: https://skybrary.aero/articles/james-reason-hf-model

Active Defense

KEY QUESTION

How do I proactively prepare to defend my system from any threat?

- How do I protect what I designed?
- How can engineers and IT collaborate in defense?
- How do we exercise/practice defense?
- Have we developed policies and procedures?


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
I SAW AN AD FOR ADVANCED THREAT ALWAYS-DAY PROTECTION.
IF I BUY IT WILL MY NETWORK BE SECURE?
PSYCHIC SECURITY READINGS
PROBABLY NOT! SECURITY IS A PROCESS.
THERE ARE NO SILVER BULLETS.
HAAS
WHY WOULD I WANT BULLETS FOR NETWORK SECURITY?
IT'S A SAYING.
IT MEANS THERE'S NO PERFECT SOLUTION.

Used with permission from: https://www.recordedfuture.com/active-cyber-defense-part-2/

Interdependency Evaluation

KEY QUESTION

How do I understand where my system can impact others or be impacted by others?

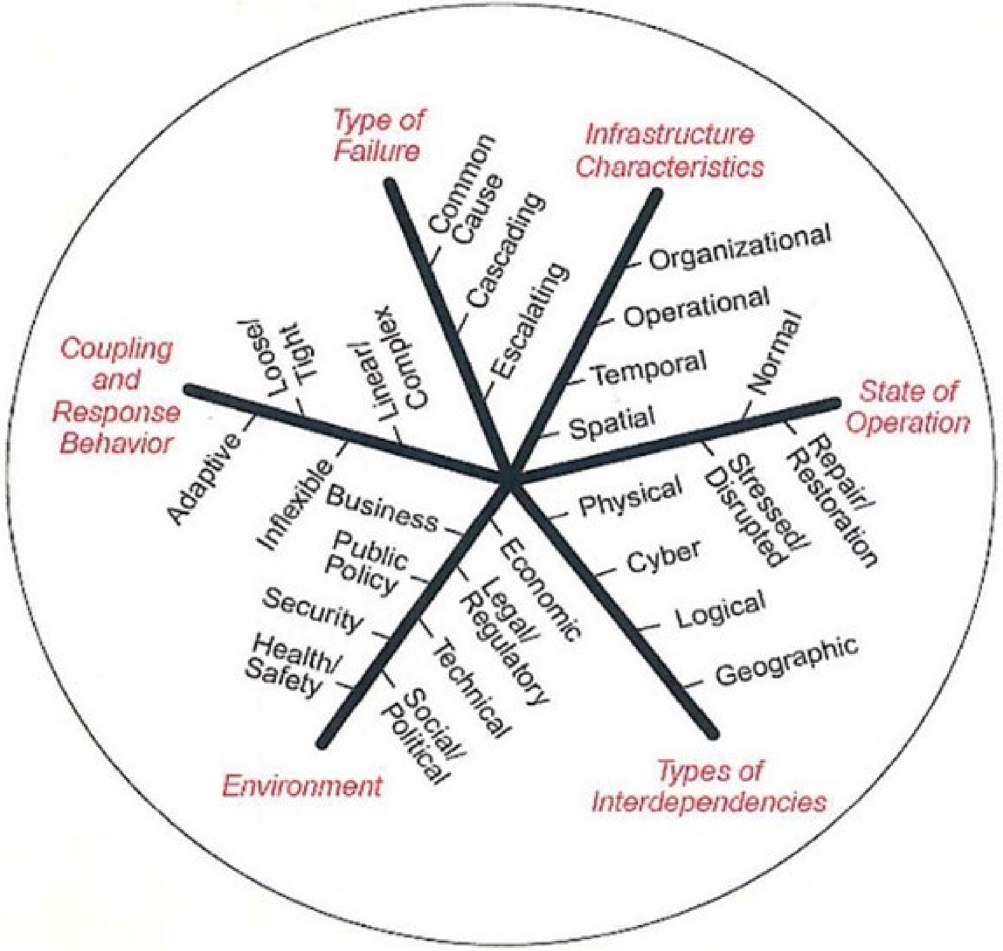


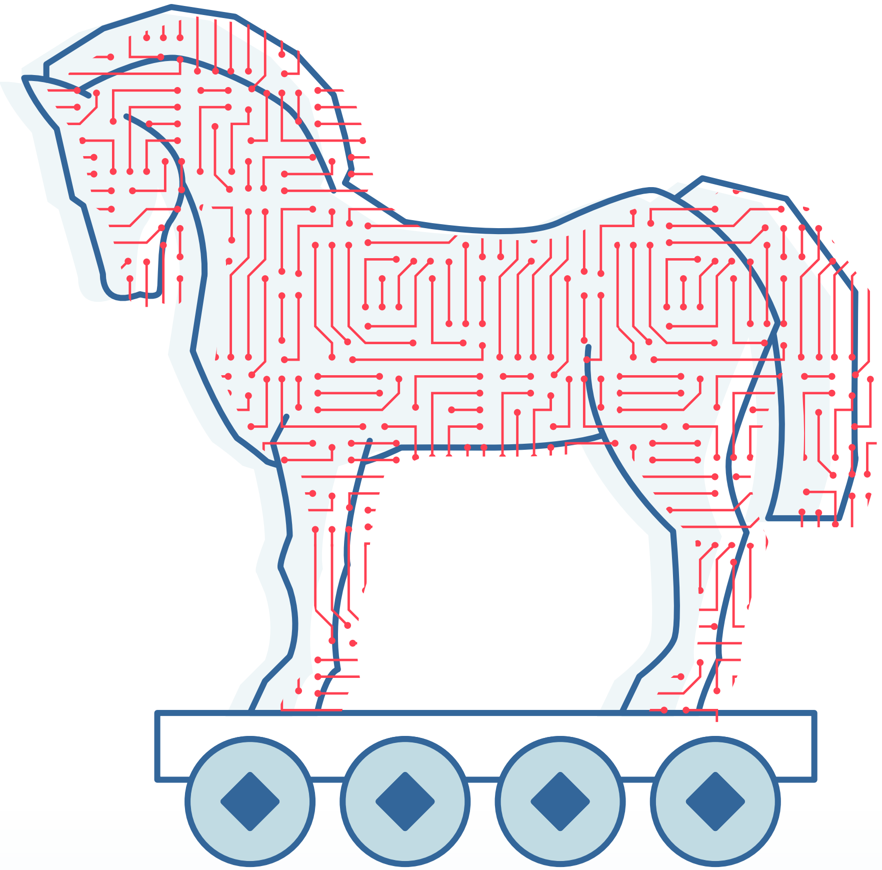
Image adapted from:
http://witandwisdomofanengineer.blogspot.com/2010/11/infrastructure-interdependencies.html

Digital Asset Awareness

KEY QUESTION

How do I understand where digital assets are used, what functions they are capable of, and our assumptions about how they work?

- Digital systems are different from their analog counterparts
  - Turning off features doesn't remove them
  - Digital features area a source of different risks
- One way of tracking risk is keeping an inventory of digital assets
  - Simple? Maintaining accuracy is not simple
- How do you protect this information?

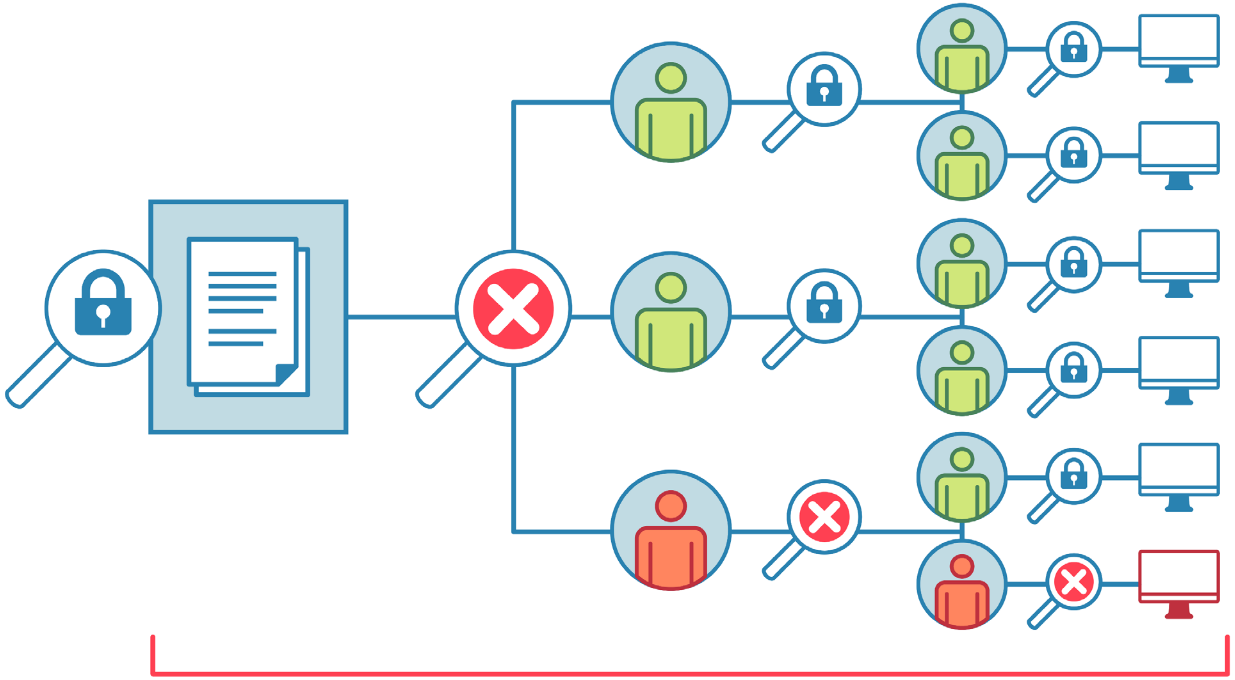


Cyber-Secure Supply Chain Controls

KEY QUESTION

How do I ensure my providers deliver the security the system needs?

- How do cyber security requirements flow to vendors, integrators, and third-party contractors?
    - What assumptions are we making?
- Does procurement language must specify the exact requirements a vendor must comply with as part of the system design, build, integration, or support?
- How do we verify compliance?



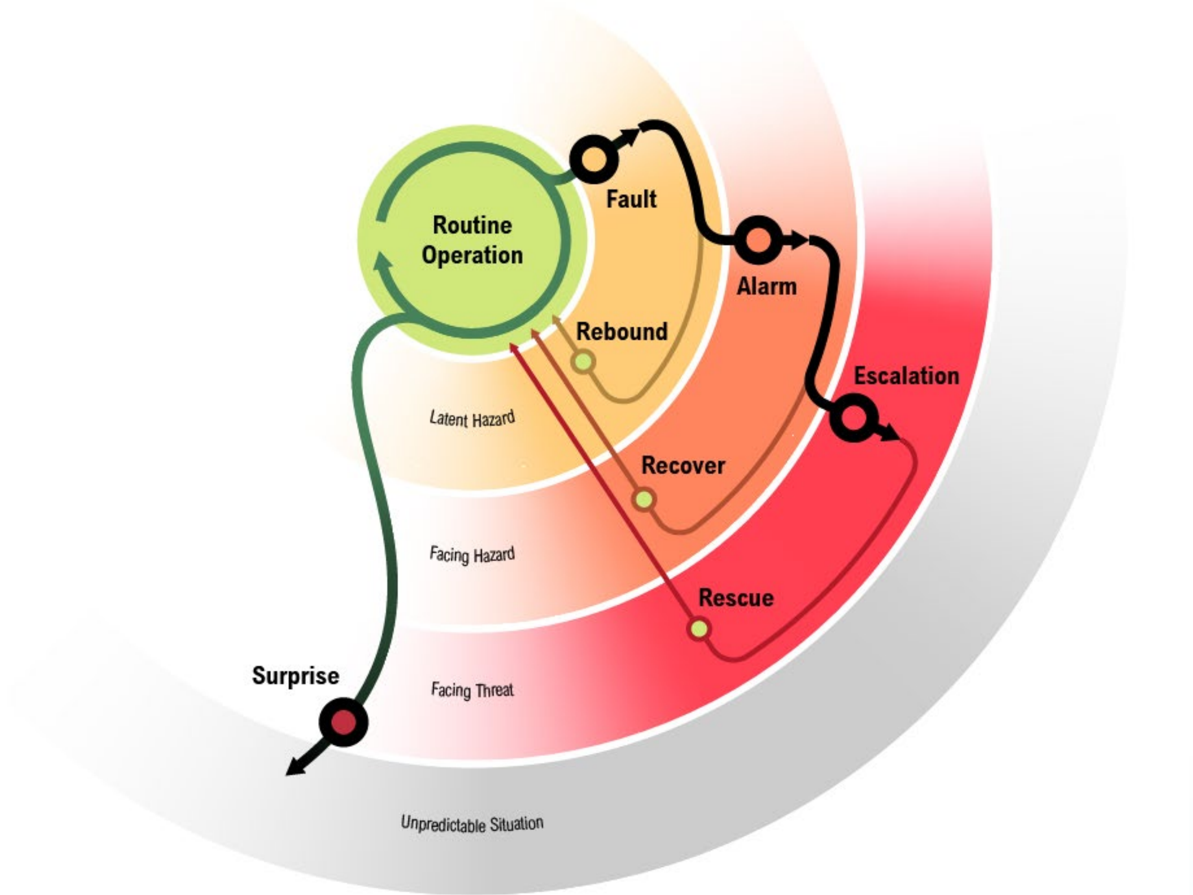
You are only as secure as your least secure vendor

Planned Resilience

KEY QUESTION

How do I turn “what ifs” into “even ifs”?

- What are the limits of acceptable degradation for critical system functions and what alternate operating modes would protect and maintain those critical system functions within acceptable limits?
- How does the organization maintain business continuity and critical function delivery through incident response and recovery?
- How will resilience measures be validated?



Cyber-Informed Engineering

Engineering Information Control

KEY QUESTION

How do I manage knowledge about my system? How do I keep it out of the wrong hands?

- **What** information should we protect?
- **Who** has and should have it?
- **How** do we protect it?

Image from: https://www.uscomputer.com/2016/02/16/employee-education-thwarts-social-engineering-threat/

Organizational Culture

KEY QUESTION

How do I ensure that everyone's behavior and decisions align with our security goals?

- Include cyber security into engineering and engineering into cyber security
- Ensure entire staff is enlisted and endorses cyber security
- Ensure staff understand and follow processes and procedures
  - All it takes is one user to lower security posture
- How do we encourage a questioning attitude?
- How can we provide the same rigor for cybersecurity as physical protection security and safety?

Conversations

Explicit Assumptions

Collaboration on Projects

Assessments

Scenarios

Exercises

Questions?