Lessons Learned in Building and Implementing an Effective Cybersecurity Strategy

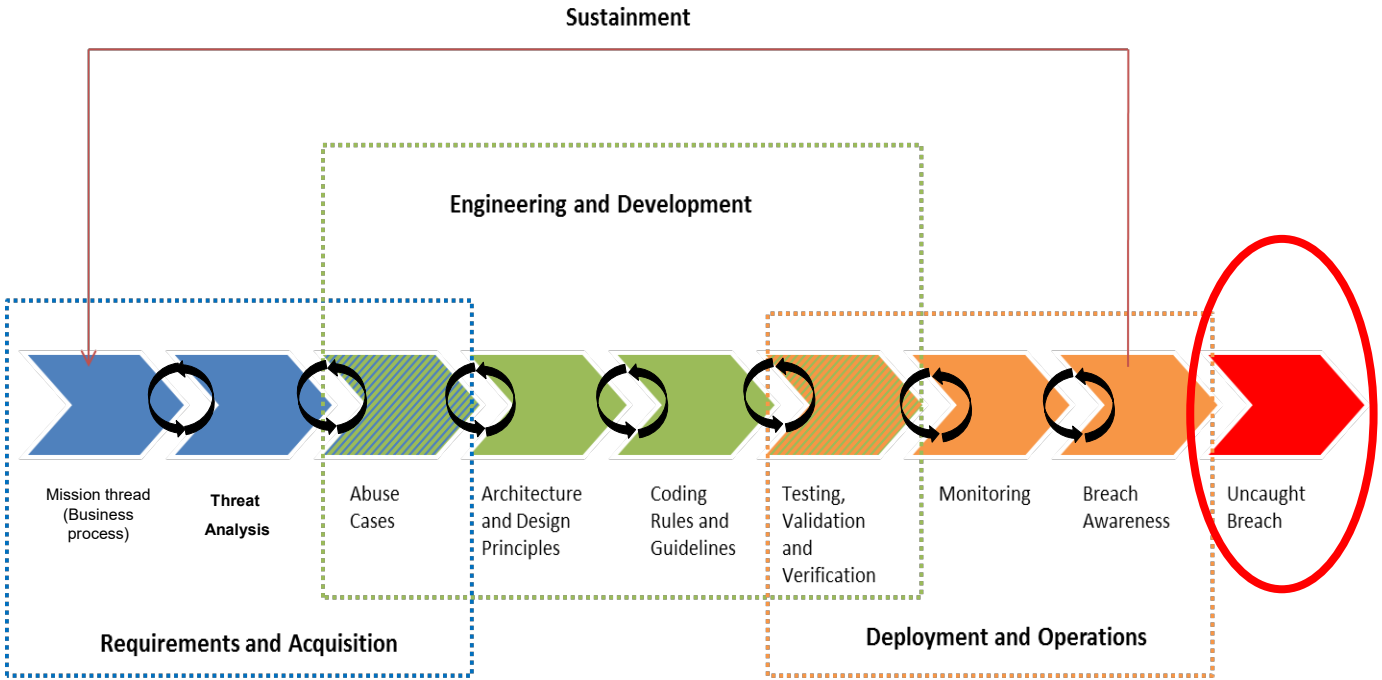
Carol Woody, Ph.D.
Principal Researcher

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0317

Cybersecurity Planning across the Lifecycle is Key to Risk Reduction



Implement an Effective Cybersecurity Strategy

Establish a plan for sufficient system and software cybersecurity engineering to ensure the operational mission(s) continue, even under cyber attack.

- Plan and design trusted relationships.
- Negotiate appropriate security requirements to ensure confidentiality, integrity, and availability with sufficient monitoring in systems and software to identify problems.
- Plan and design a system with sufficient resiliency to be able to recognize, resist, and recover from attacks.
- Plan for operational security under all circumstances, including designed-in methods of denying critical information to an adversary to avoid or minimize mission impact.

Executing the Plan Requires Cybersecurity Engineering

Resources with sufficient understanding of acquisition, development, and security must be involved at the right time in the lifecycle for:

- Determining risk
- Defining and monitoring system and component interactions
- Evaluating trusted dependencies
- Anticipating and planning responses to attacks
- Coordinating security throughout the lifecycle

Executing the Plan Requires Cybersecurity Engineering

Resources with sufficient understanding of acquisition, development, and security must be involved at the right time in the lifecycle for:

- Determining risk
- Defining and monitoring system and component interactions
- Evaluating trusted dependencies
- Anticipating and planning responses to attacks
- Coordinating security throughout the lifecycle

These resources must make tough choices and need to have sufficient understanding of the impact of their decisions. Uninformed choices lead to unexpected outcomes.

Details on Evaluating Trusted Dependencies

What are trusted dependencies?

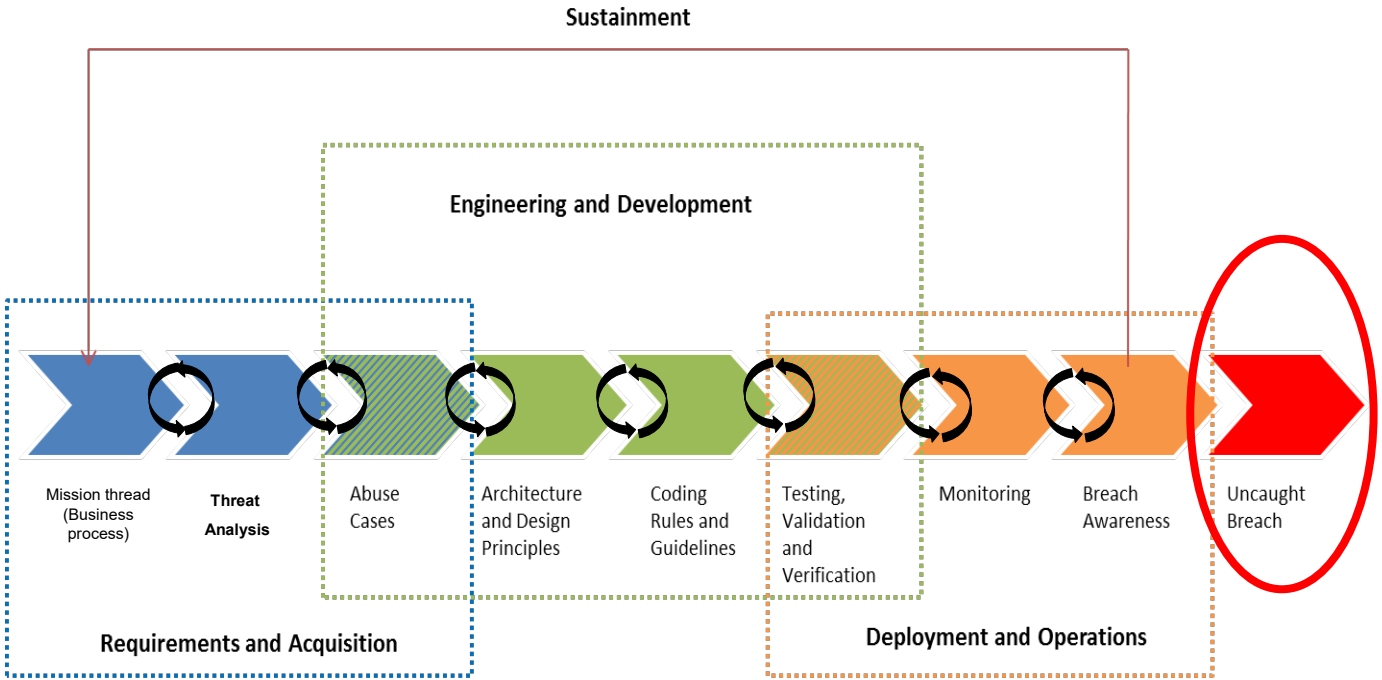
- Reliance on services such as cloud and other shared platforms
- Reuse of code from prior versions, code libraries, open source, etc.
- Integration of 3rd party components into systems

What are the risks?

- Inherited vulnerabilities and limited knowledge of supply chains
- Control of code and patching is outside of the program and must be handled via contract or service level agreement (SLA)
- Insufficient responsiveness to security issues

Programs are trusting dependencies without considering the risk

Planning for Continuous Focus on Cybersecurity Risk Across the Lifecycle is Critical to Operational Mission Success



Contact Information

Carol Woody, Ph.D.

cwoody@cert.org

Web Resources

Building security into application lifecycles

https://sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=48574

CMU SEI Home Page

https://sei.cmu.edu/