Why I Sleep Like a Baby

An Old Academic's View of the State of Cyber Security

Dan Shoemaker, PhD, Professor and Senior Research Scientist
Academic Program Director
Center for Cyber Security
University of Detroit Mercy

It’s Going to Happen to You

- **The current state of cybersecurity is like the parable about the six blind men and the elephant “Though each was partly right – All were entirely wrong.”**

- **And the data makes it clear that it’s getting worse not better So, how do we change that?:**

1. **A Commonly Recognized and Well Defined Body of Knowledge**
2. **Comprehensive Organization-Wide Risk Management**
3. **Trustworthy ICT Product Supply Chains**
4. **Stop Trying to Defend Everything**

A Common Body of Knowledge

- We can't teach it or practice it effectively if we don't know what it is - So a comprehensive and commonly accepted body of knowledge is essential
- The National Initiative for Cyber Security Education, Cybersecurity Workforce Framework is an encouraging first step
- It outlines KSA requirements for seven highly integrated areas of the field:

1. Secure Software/Trusted Acquisition
2. Secure Enterprise Technology Operations
3. Enterprise Network Defense
4. Forensics and Criminal Investigation
5. Threat Intelligence Analysis
6. Threat Intelligence Collection and Operation
7. Governance and Control

Rigorous and Systematic Risk Management

- **Threat identification and categorization and systematic risk analysis and control deployment is a critical cybersecurity function.**
- **The, six stage Risk Management Framework (NIST-RMF) outlines the standard steps to make the risk management process systematic and sustainable:**

1. **Risk identification and Categorization**
2. **Control Selection**
3. **Control Deployment and Implementation**
4. **Control System Performance Assessment**
5. **Control System Authorization/Acceptance**
6. **Control System Monitoring, and Enhancement**

Security of ICT Product Supply Chains

- Organizations purchase their ICT products from global sources that can be easily compromised – a supply chain is only as strong as its weakest link
- That is why control and assurance of sourcing in these five areas is critical:

1. Malicious code
2. Counterfeit components
3. Supplier incapability
4. Supply chain breakdowns
5. Exploitable defects in code

- NIST 800-161 is ane single strategy to uniformly identify, assess, and implement controls up and down a supply chain

Contact – dan.shoemaker@att.net

Cyber Resilience versus Cyber Security

- **Cybersecurity is dead - perimeter based defenses are too expensive to sustain**

- **Cyber-resilience deploys controls for just thost things you can’t afford to lose:**

1. **Categorize business assets – you can’t secure it if you don’t know it exists**
2. **Identify everything that threaten it – not just the “convenient” things**
3. **Designate the “showstoppers” -versus the “nice to haves”**
4. **Ensure reliable protection for each showstopper- develop recovery strategies for the rest**
5. **Evolve– cybersecurity is a continuous state, not a function**

Contact – dan.shoemaker@att.net