Can we talk?

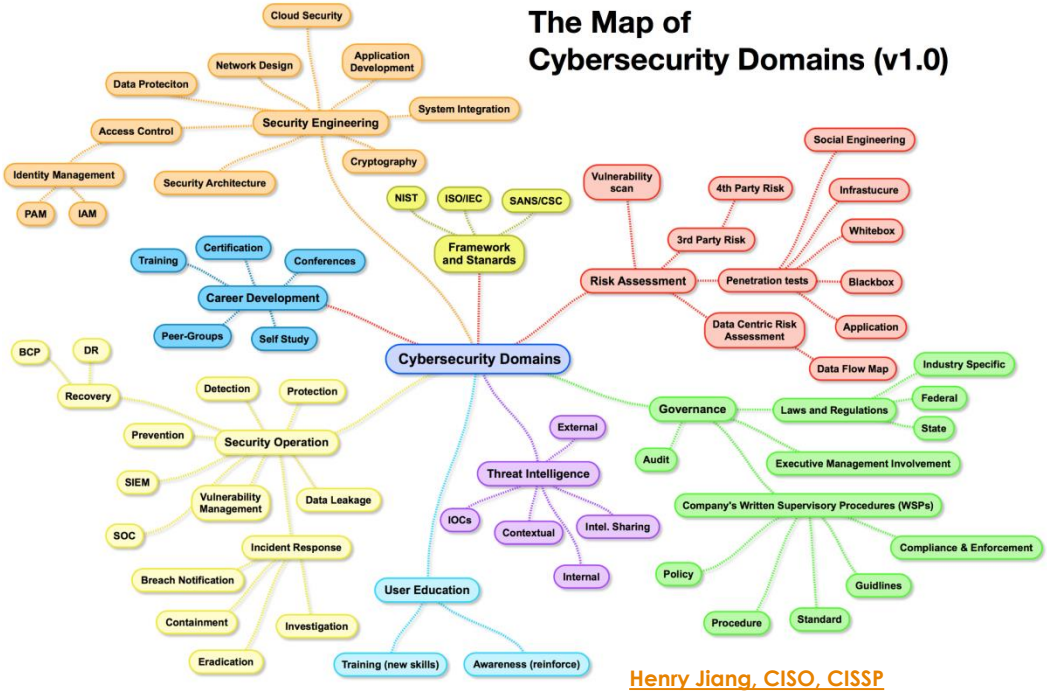
A starting point for a discussion on the topic of Cybersecurity

Braun Tacon, ISO

Introduction & Overview

- The goal of this short deck is to:
  - Share some of my thoughts on what constitutes an effective Cybersecurity Program;
  - while enabling an inclusive conversation;
  - where we can collectively explore and build a viable, palatable, and sustainable Cybersecurity Program

Just what are we talking about?



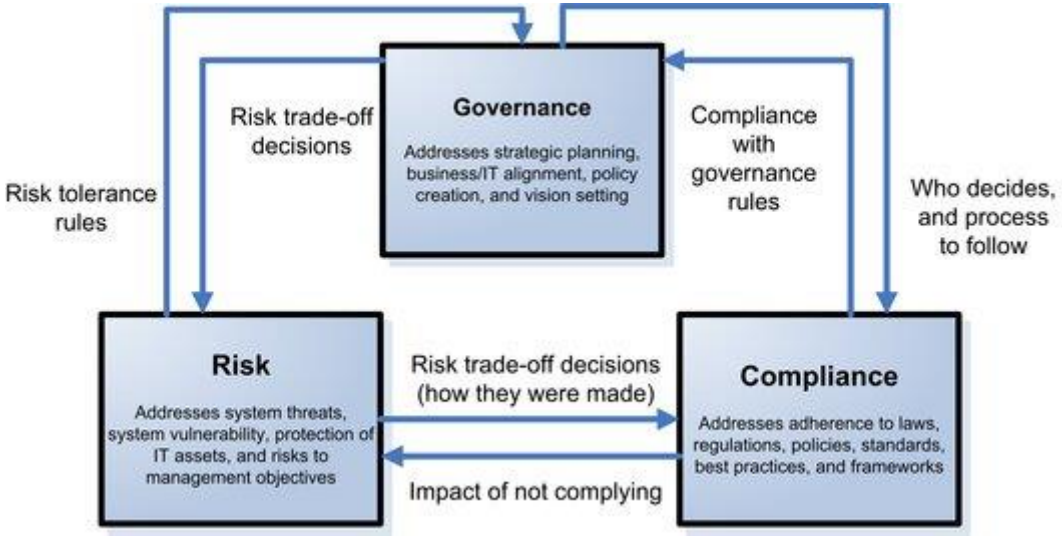
Henry Jiang, CISO, CISSP
CISO and Managing Director at Oppenheimer & Co. Inc.

Why are we talking about it?

- In 2017 there is little in our lives that is not enabled, connected, online and available 24 X 7 via Computers and Computer Systems
- Examples include: Communications including Social Media, Transportation, Government, Finance, Medicine and much more
- These Computer and Computer Systems have become highly complex, inter-connected and inter-dependent organisms
- Managed and maintained appropriately, they provide many useful benefits and advantages
- Managed and maintained inappropriately, they can and will bring all sorts of unneeded threats and risks
- The goal here is to begin a conversation on how we can better manage and maintain those Systems

Begin with the end in mind

- At a minimum our conversations should include the topic of Governance, Risk, and Compliance (GRC)
- Effective GRC is foundational to good Cybersecurity
- The Mind-Map offers additional topics we can add to our conversations

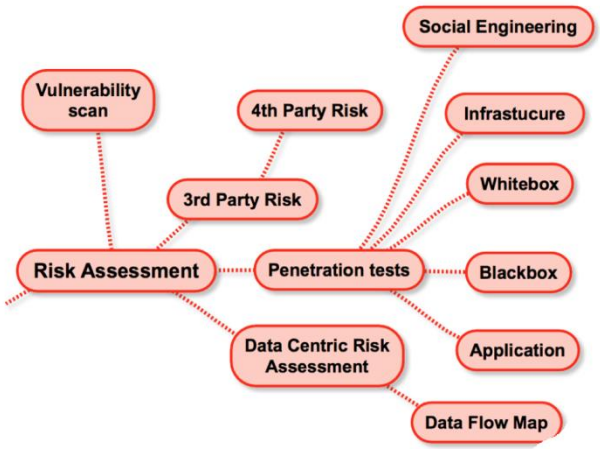


Governance and Compliance

- Governance, which is
  - Informed by Laws and Mandates;
- and directed by Executive Mgmt.;
- ensures Supervision and Control by
  - Compliance & Enforcement of;
  - Written Policy, Procedures, Guidelines and Standards;
- validated by Audit (Trust but Verify)

Risk Assessment

- Where do our Risks live?
- What is the chance of a Risk?
- If a Risk occurs what happens;
  - Loss of Compliance?
  - Loss of Services?
  - Loss of Protected Data?
  - Loss of Reputation?
- Prioritize Risk Mitigation by assessed Risk Impact and Potential

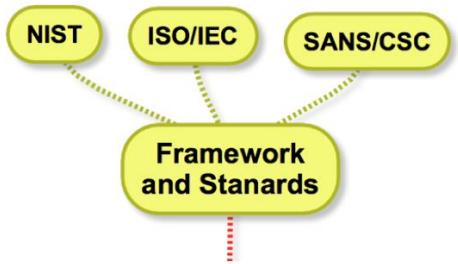


Threat Intelligence

- Understanding Threats is critical
- It is not enough to just look internally
- There are many good sources, many are free
  - https://www.us-cert.gov/ncas/alerts
  - https://ics-cert.us-cert.gov/
  - https://cve.mitre.org/
  - https://www.qualys.com/research/security-alerts/
- Good Threat Intelligence enables Risk Prevention

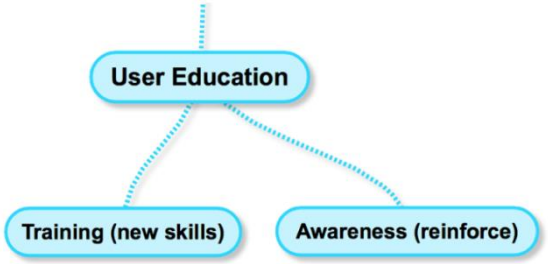
Frameworks & Standards

- Frameworks and Standards offer a documented and proven approach
- The National Institute of Standards and Technology (NIST) has a strong focus on Cybersecurity
- Industry driven Standards such as ISO/IEC are also useful
- For profit consortiums such as SANS and CSC round out the offerings



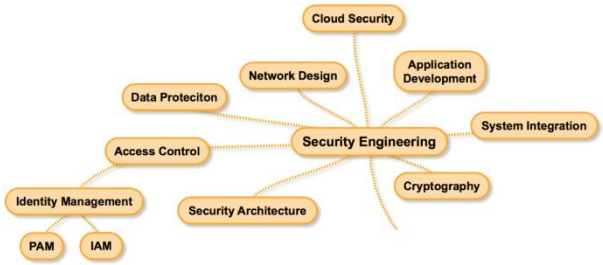
Awareness & Training

- The "User" is often at the front end of a Cybersecurity incident
- Either as the initial recipient or as the cause
- Awareness training is critical in both cases
  - To inform your users how to practice good Cybersecurity
  - Or by teaching them how to recognize poor Cybersecurity and associated failures
- Awareness often has the biggest payoff and is frequently ignored



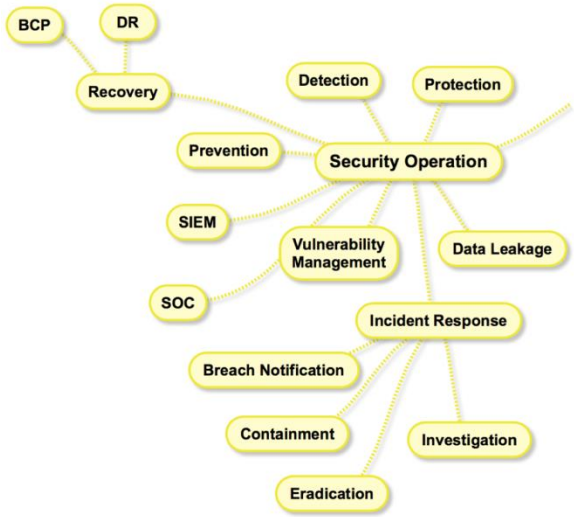
Security Engineering

- Begin with the end in mind
- Focus on desired outcomes, not technologies
- Apply the concept of GRC to all design endeavors
- Assume nothing
  - There are no “failsafe” systems
  - Technology alone is insufficient
  - Design for Human interaction
- If it takes 10 steps to complete a task and 11 steps to complete it securely, **the majority will stop at step 10**



Security Operations

- Begin with the end in mind
- Apply the concept of GRC to all design endeavors
- Policy and Procedures should define and drive all Security Operations
- Focus on desired outcomes, not technologies
- Always consider the human factor
- Plan for the best, Prepare for the worst
  - Major Incident Handling
  - BCP / DR
- Build in redundancy and failover as your first line of defense



Career Development

- Training is important
  - Certifications demonstrate Knowledge
  - Application demonstrates Abilities
  - Peer-Groups provide Validation
- Self Study is equally as important
- A Mature Cybersecurity Program relies on a blend of both

Closing Thoughts

- This is meant to be a starting point
- The foundations provided here are real and solid, but they are only foundations
- There is “No One Standard” for Cybersecurity
- Your own conversations should focus on your needs and gaps