Cyber Education triangle
“clarifying the fog of cyber security through targeted training”

Curriculum & Resources
Linked / leveraged (on-line, companies, colleges, etc)

Education levels
Advanced

Targeted

Foundational

Expands the pool for advanced education

MS / BS Cyber
CISSP / GISP / CISO / etc
forensics / ethical hacker / etc

Firewall / cloud security / Crypto & Key mgmt / “*”

Security +
Awareness Education
STEM (grades 7-12)

(KEY break point ->)

Small business security course & practicum

("*" = IDS/IPS, anti-virus, wireless, application development / management, web/mobile code, mobile, etc…)
Notional Cyber education roadmap

(Authoritative sources, categorized, mapped to CSF)

NICE
Levels & methods

NSA CAE
Accreditation
Focus areas

NIST
SPs & ‘must do’ + requirements

SANS top 20
Top 35 Mitigations
OWASP top 10
Top 25 SW errors

Customer
Awareness
AND Demand

CERT areas / KSAs
Grouped & aligned
Support key IA needs

Align Needs / Areas
Clarify / map certs to specific demand areas

Target environment

Curriculum MAP
Objectives
Quantified KSAs

Cyber Needs Paper
Center & align KSAs with security needs to also educate leaders

Cybersecurity framework (CSF)

foundation
Inputs / factors
Key artifacts
outcome
Cyber capabilities – KSA decomposition

(Objective = Business Risk Management – prioritized vulnerability reductions)

Overall Cyber Security Factors

---

Main functional Areas / buckets

- people
- processes
- products
- policy

(1) Provision
(2) requirements analysis

From NICE framework = (1) functions... (2) cyber skills (KSAs)

(1) Provision Analyze O&M / support Collect Investigate Protect & defend
(2) requirements analysis Assessment Security testing Pen testing C&A Security design

KEY capabilities / products / processes / methods = KSAs

- Compliance
- IA/CND
- IA&A
- Mobile / wireless
- Tools
- Policy
- Network (client / server / router)
- SW/apps services
- Web / active code
- Data
- O&M/support
- Threats
- C&A RISK (V&V) Assessment

ALL geared to specific positions / types (manager, project lead, Cyber SME / ISSE)
And with some aspect of technical level (apprentice, journeyman, master)
Hierarchy of Cyber Needs (i.e.…..Maslow…)

Where if you don’t take care of the level before the one you are operating in, focusing on, then your efforts are for the most part mute, as you are in a higher risk status until the earlier level is satisfied!

1 – **Resiliency** - Survival / recovery
   + Secure backup (Types / methods, various sites / levels)
   + Incident responses (company processes, comm with LE / FBI, etc)
   + Recovery Plan - COOP / BCP (phases of recovery, hot / mirror site, etc)

2 – **Cyber foundation**
   + Access control (PW, CAC, enforce least privilege, separate / rotate duties, etc)
   + Layered Defense - IA/CND strategy – WHAT capabilities are needed
   + Security Policy (privacy, social media, PI, etc) - enforcement aspects too
   + Monitoring / Know your baseline – SCM / SIEM.
   + Business Risk Management / Assessment (RMF / COBIT) / requirements analysis with an AoA

3 – **Cyber Maintenance** - security Hygiene / CM / SoPs
   + Manage Policy - social media - content & settings... restrict sharing / privileges = proactive monitoring
   + Maintain Cyber Security Suite – patches, upgrades, etc.. control system settings... & dashboard!
   + Standard operating procedures (SOPs). USE / enforce them
   + Security training / education awareness – ALL levels – reinforce / Incentivize – pos & neg

4 – **Applied cyber security** (IA / CND / security capabilities best practices)
Given the below best practices, cyber protections approach, then distill the key attributes for each IA/CND capability, while following and tailoring for the company’s environment the install instructions of the products... specific equipment settings for ‘secure’ sustainment / operations
= Firewall, A/V suite, IDS/IPS, Crypto, Key mgmt., Mobile, wireless, ‘Network, apps, data security, etc

5 – **Cyber actualization** - compliance / assessment / analytics
   + V&V / TE&C / C&A – formal proof -> residual risks -> cyber value proposition
   + KEY compliance activities – PII, PCI, HIPAA, etc... + Forensics / ethical hacker
   + Big data / predictive analytics (integrate SCM / SIEM, IA/CND reports, etc...)
   + Pen / security testing (of all cyber capabilities, backup, PW, etc)

**KSA / practicum based on small business security**

**NSA IAD top ten tasks**
**Top 20 security controls**
**Top 35 mitigations**
The Cyber Integrated Package

Structured “bottom up” / needs approach to effective cyber education!