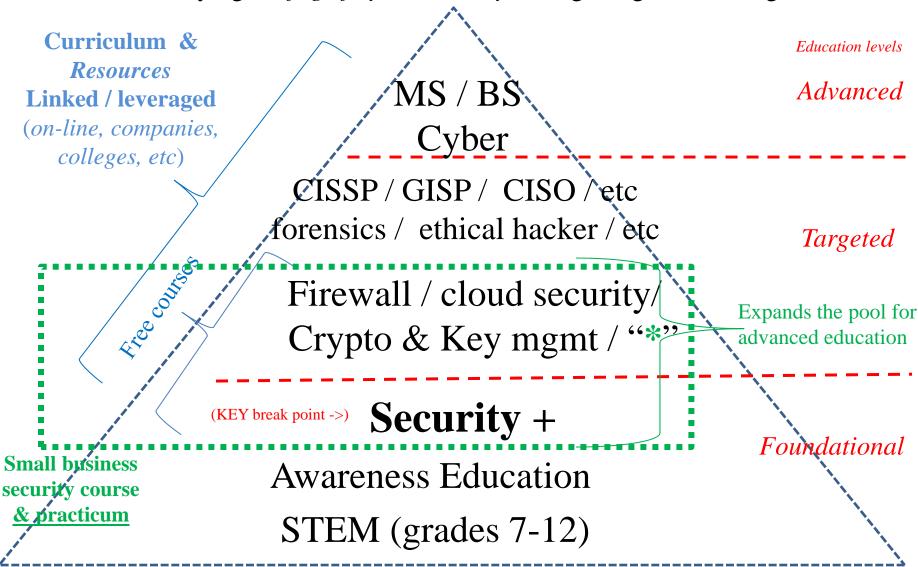
Cyber Education triangle

"clarifying the fog of cyber security through targeted training"



("*" = IDS/IPS, anti-virus, wireless, application development / management, web/mobile code, mobile, etc...)

Notional Cyber education roadmap

(Authoritative sources, categorized, mapped to CSF)

NI	С
IVI	匚

Levels & methods Customer

Awareness

AND Demand

NSA CAE

Accreditation

+ requirements

Focus areas

CERT areas / KSAs

NIST Grouped & aligned

Support key IA needs SPs & 'must do'

Align Needs / Areas

SANS top 20 Clarify / map certs to Top 35 Mitigations specific demand areas

OWASP top 10 Top 25 SW errors Target environment

Curriculum MAP

Objectives

Quantified KSAs

Targeted / focused

Trained / proven KSA

Cyber Workforce

Cyber Needs Paper

Center & align KSAs

with security needs

to also educate leaders

NIST / Whitehouse

Cybersecurity framework (CSF)

foundation Inputs / factors Key artifacts outcome

Cyber capabilities – KSA decomposition

(Objective = <u>Business Risk Management</u> – prioritized vulnerability reductions)

Overall Cyber Security Factors

Main functional Areas / buckets products policy processes people Analyze O&M / support Collect Investigate Protect & defend (1) Provision From NICE framework = (1) functions... (2) cyber skills (KSAs) (2) requirements analysis C&A Assessment Pen testing Security design Security testing KEY capabilities / products / processes / methods = **KSAs** Compliance IA/CND IA&A Mobile / wireless Tools Policy Network & crypto/key mgmt (client / server / router) SW/apps Web / active code Data O&M/support C&A **RISK** Threats services Sys Admin & CM/hygiene (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!

Master

Optimized Value

Journeyman

Operations

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...l)
- + Pen / security testing (of all cyber capabilities, backup, PW, etc)

NSA IAD top ten tasks Top 20 security controls **Top 35 mitigations**

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

- **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

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, PII, etc) enforcement aspects too
- + Monitoring / Know your baseline SCM / SIEM.. + Tools selection and integration
- + Business Risk Management / Assessment (RMF / COBIT) / requirements analysis with an AoA

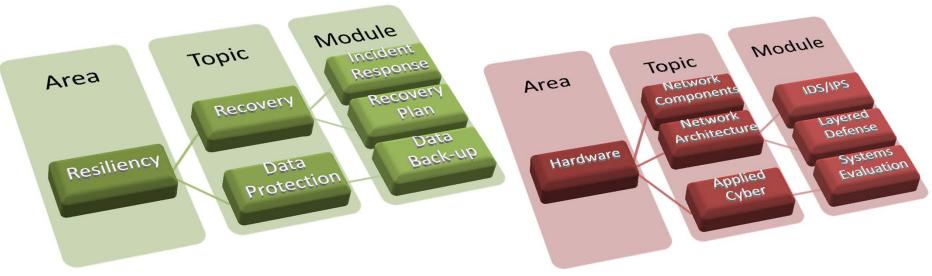
1 - Resiliency - Survival / recovery

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

Apprentice BASICs

KSA / practicum based on small business security

The Cyber Integrated Package



Structured "bottom up" / needs approach to effective cyber education!

