SD IEEE Consultants Network
Forum – Enhance Your Practice by Teaching

Monday, September 8, 2014

Mike Davis

Mike.Davis.SD@gmail.com

Cyber Security / Risk Management Consultant (enthusiast)

ElectEngr/MSEE, CISSP & CISO, SysEngr, PM
ISSA / ISC2 / Infragard / SOeC... AFCEA / NDIA... IEEE / INCOSE / et al

Bottom line - As in ALL things
Consulting it is mostly about the ‘value proposition’ “AND” sharing!!!
Points to cover / pontificate on

1). Overview of your career and practice. Include how, why and when you decided to do consulting.

2). How, why and when you decided that teaching would be a good addition to your consulting practice.

3). The best part of teaching as it relates to your practice. (What you feel you have gained the most from teaching).

4). Describe the biggest drawbacks of teaching as it has affected your practice. (What made you think twice about teaching).

5). What you think makes a good candidate for a teacher. What kind of people should avoid teaching.

THEN – show a few cyber education <-> consulting efforts for examples
What MUST we do in Cyber?

Manage **RISK** and DO the **Security BASICS**
(start by managing the top NSA 10 / SANS 20 mitigations!)

**OR..** how about just **DOING** the Cyber Hygiene Campaign top 5 actions!
(e.g., 1 & 2 - Inventory SW & HW, 3 - Secure CM, 4 – SCM/SIEM & 5 - enforce least privileges)

Close the “cyber” barn door first, versus fixing cracks in the wall!

Follow the Hierarchy of Cyber needs – mitigate, manage your way up
RE: Companies / SMBs need “cyber security operators” – not cyber ninjas!

(*) [https://www.cisecurity.org/about/CyberCampaign2014.cfm](https://www.cisecurity.org/about/CyberCampaign2014.cfm)
The Integrated **Business RM** Approach

+ **Making the Risk Management Plan (RMP) work!** +

*(Will teach “Cyber Enabled Business Risk Management” at Webster in fall)*

**Company Vision**
(business success factors)

**Security Policy**
(mobile, social media, etc)

**C&A / V&V**
(effective / automated)

**Known Baseline**
(security architecture)

**Insider Threat**
(Company Intel)
(open source, FB, etc)

**CMMI / Sustainment**
(SoPs / processes)

**SCM / SIEM**
-monitor / track / mitigate

**MSS / CISO**
(3rd party IV&V support)

**Privacy by Design**
(manage PII, HIPAA, **compliance**) )

**Data Centric Security**
(DLP, reputation based methods)

**Cyber insurance**
(broker & legal council)

**Education / Training**
(targeted, JIT, needs based)

**Common Business RMP model** (re: RMF / COBIT & Risk IT)

AND using the **NIST Cybersecurity Framework** (re: CAR / ESA)
Cyber Education triangle
“clarifying the fog of cyber security through targeted training”

(Building a “Cyber Security Operator” course - seed the entry levels (veterans too))

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

MS / BS
Cyber
CISSP / GISP / CISO / etc
forensics / ethical hacker / etc
Firewall / cloud security/
Crypto & Key mgmt / “*”

Security+ “and” Skills development
Awareness Education
STEM (grades 7-12)

Small business security course & practicum

Advanced
Targeted
Foundational

Expands the pool for advanced education
(KEY break point is providing “cyber operators”!)

(“*” = IDS/IPS, anti-virus, wireless, application development, cloud, web/mobile code, mobile, etc…)
Hierarchy of Cyber Needs

(i.e. Maslow Triangle…)

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, comms 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, 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

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

---

**Optimized Value**

**Master**

**Journeyman**

**Apprentice**

ALL topics / areas Need Fixing and training!

---

**KSA / practicum based on small business security**
Cyber Security opportunities
(Cyber can both enhance consulting AND sharing / teaching opportunities = PEST!)

IT / Cyber Global factors – user pull

World-wide B2B
Trust / cloud / sharing

IoT / M2M
Automation / Sensors

Consumerization of IT
Phones / wireless / apps

Privacy / Data
IP / PII / compliance

GAPS / Needs
(from the Federal cyber priority council S&T gaps)

TRUST
Distributed / MLS

Resiliency
SW / apps / APIs / services

Agile operations
BE the vanguard / integration

Effective missions
Business success factors

Vulnerabilities / Threats
(Verizon BDR, Forbes, etc threat reports - what ails us most)

CM / Hygiene
patching / settings

Access control
Authentication is key

Top security mitigations
Whitelist, patch, limit access, etc…

Risk Mgmt
Adhoc / not global

Opportunities that scale

Effective Business Risk Management (BRM) = cybersecurity framework (CMMI / FAR

Focus on reducing business risk… Managed security services (MSS) & cyber insurance…

SIEM / SCM
QA hygiene / sensors
“ESA” / simple tools!

Mobile Security
Poor apps / IOS weak billions users = volume

Mitigate Obsolescence
Minimize patching, legacy vulnerabilities
OA / modularity / APIs & SCRM

Data Security
Predictive analytics
Privacy by design