What “REALLY” matters in Cyber?

RE: Internet of things – security

Not sure HOW it can affect you (as it HAS already)?
Hacking of the AP's Twitter account sends the markets plunging (Syrian Electronic Army has claimed responsibility).
The criminal black market is offering Zeus malware under a fraud-as-a-service (FaaS) model.
FTC fines Trendnet over lax security practices… when hackers posted live feeds from its webcam to Web…
AND… what is a “thing” – is that MORE we have to do???

14 Oct, 2013

Mike Davis
mike@sciap.org

ElectEngr/MSEE, CISSP, SysEngr
ISSA / TSN / SOeC… AFCEA / NDIA… IEEE / INCOSE / et al

Bottom line - As in ALL things – it is mostly about your ‘value proposition!’
SO... OK, what does matter in Cyber?
(aka - the “bottom line” up front) *(and who says so?)*

CYBER is fundamentally all about TRUST and DATA

It’s NOT about expensive new “cyber capabilities / toys”
but more about the SoS / I&I “glue” *(distributed trust, resiliency, automation, profiles, etc)*

95% of security incidents are from lack of doing the basics!
*Security baseline* + Security Continuous Monitoring *(SCM / SIEM)* – a MUST DO!
USE enforced: cyber hygiene, enterprise access control, & reduce complexity *(APLs)*

Embrace you Risk Management Plan – *LIVE IT!*
Protect yourself / the business from the unknown risks as well
Employ a due diligence level of security – then transfer the risk!

When in doubt, **do the cyber BASICS well!!!**
An achievable 95+% solution to MOST vulnerabilities – then insure the rest!
The Complexity of Enterprise IT Systems is Increasing
AND so is the associated Cyber Security!

Key challenges in the problem space
- Network-centric, dynamic, very large-scale “systems of systems”
- Stringent simultaneous quality of service (QoS) demands
- Highly diverse & complex problem domains

SO... what is “good enough” in cyber security?

Key challenges in the solution space
- Enormous accidental & inherent complexities (covert channels)
- Continuous evolution & change
- Highly heterogeneous platform, language, & tool environments

Mapping & integrating problem artifacts to solution artifacts is “wickedly” hard

SO.. where is your DATA, who has it – how sure are you?
Cyberspace Characteristics

All of the warfighting - and related business - domains intersect...

Cyberspace Domain is contained within and transcends the others

In relation to other mission areas... run by different Communities Of Interest (COI)

Cyberspace is a blend of exclusive and inclusive ties
Frequently the COI boundaries / MOAs are implicit
These Venn connections / COIs are pervasive

Numerous, dynamic “COIs” dominate relationships - adding Complexity & Comms, & Control overhead - causing “cross domain” DATA sharing effects

Do NOT underestimate this aspect!
What are KEY cyber elements?
(and what can we reasonably expect to influence / affect?)

**Fundamental issues** .... *(givens?)*
- Threats are illusive/morph – so plan/mitigate around consequences *(aka, a fault tree)*
- KISS, as complexity is our enemy – **do the basics well** *(hygiene, anonymity, etc)*
- In a connected world, it’s the shared vulnerabilities that will get you / ALL of us
- “They” have an asymmetrical advantage, plan with it *(and they don’t follow the rules/laws)*
- WE ALL need common homogenous security protection in a heterogeneous world

**Essential gaps / needs**... *(tenets?)*
- Invest in the OSD / NSA R&D / S&T “gap” capabilities, as authoritative sources
- Apply trade-offs / assessments using a common end-state *(an ‘open’ / ubiquitous world)*
- Using an enterprise risk management plan *(RMP)*, and FOCUS on proactive SCM!
- If you can’t integrate “it” into your IT/network environment, then “it” is useless
- Minimize “what you don’t know you don’t know’ “&” get cyber insurance

If you don’t know where you’re headed, **any blind alley will do**
Where the bad actors continue to count on US ALL not being in sync
What’s new in cyber, and what matters?

Sensor + WiFi = device --- Things -> systems, machines, equipment, and devices—connected to the Internet and each other

The Internet of Things
RIFD, Apps, MEMS, WSN, SCADA, PLC, ASIC, API, ETC, etc

Is all this stuff secure? How much is needed?

The “Internet of things (IoT)” is not new… IoT requires ALL the cyber protections we already know - and still need to do
“ALL” the new technologies need to be built with security embedded
Cyber requires *enterprise integration*

Things are only the ‘stuff’ – we need to integrate all IT/IA aspects!

The real value of the Internet of Everything lies in the value of connections among people, process, data, and things, not simply in the sheer number of things that are connected.

Systems / capabilities are characterized by their boundaries
Where interfaces / controlling parameters / PPSM are key

When your car becomes connected to the Internet of Everything...

...more numerous, valuable, and relevant connections with other cars, stop signs, your home, and even the road itself will make your driving experience safer, more fun and informed, and even more efficient.

It’s the *connections* that matter most.

#InternetofEverything
#IoE
“Things” must communicate
paths = n(n-1) = exponential Are *ALL using secure channels*?
Data protected? Adequate Authentication? No covert paths established?

<table>
<thead>
<tr>
<th>Number of Internet Objects</th>
<th>Number of Theoretical Connections (0.001%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>1,000</td>
<td>5</td>
</tr>
<tr>
<td>1,000,000</td>
<td>4,999,995</td>
</tr>
<tr>
<td>1,000,000,000</td>
<td>4,999,999,995</td>
</tr>
<tr>
<td>(Today) 10,000,000,000</td>
<td>499,999,999,950,000</td>
</tr>
<tr>
<td>(By 2020) 51,597,803,520</td>
<td>13,311,666,640,184,600</td>
</tr>
</tbody>
</table>

10,000S of trillions Of communication paths!

Securing low BW channels requires **optimal cryptography** algorithms and **adequate key management** systems, and **security protocols** that connect all these devices.
A cyber end-state stresses encapsulation through a secure virtualized fabric.

What’s a “simple” IA/Cyber vision / end-state look like?
AND what are the “requirements”?

KEY C-I-A entities / touch points

Protected Infrastructure, QOS, COS and Routing Grid

Notional Representation of IA Vulnerabilities and Architectural Approach to Layered Defense in a NetCentric World

Identity, access control and authorization are critical in this environment, significant work on distributed access control systems needs to be completed for High Assurance Solution for ID certification using distributed solutions.

In the Net Centric world data in motion and data at rest become indistinguishable there is a need to protect storage, queues, and memory locations across the grid from information exfiltration.

In the Net Centric world data in motion and data at rest become indistinguishable there is a need to protect storage, queues, and memory locations across the grid from information exfiltration.

Where is your data? Is it assured / with a pedigree? “4Vs” satisfied?

Common Services from Geo Targeting to DNS must be protected at the level required by the highest risk applications using them you cannot consume anything that you do not trust if affects your decision cycle in a way you cannot adapt to. Aggregate risk compounds the protection level required for the components and is seldom accounted for properly.

ALL about TRUST, Rules/MOAs & State

IoT = things + comms

IoT = things + comms

IoT = things + comms

IoT = things + comms

IoT = things + comms

IoT = things + comms
Threat Vectors of Interest

• **Mobile devices ... and wireless** always predicted, *yet proliferates in 2013/4*
  – Starting with *more Android Trojans, digital wallets*, USER provided network services!
  – **Wireless security issues expand** (besides 802.11 & WiMAX, to Zigbee, Z-Wave, ARM, etc.) ...
  – **BYOD** – many hidden costs, legalities and risks than it appears at first *(aka, remember “COTs”)*

• **Cyber crime: easy money, minimal downside and growing (ransomware, etc)**
  – Illicit cyber revenues has essentially equaled all illegal drug trafficking dollars

• **The insider threat is much more “impactful” than given credit for**
  – Considering compromised services and computing devices of all kinds (aka, *supply chain security*). With Improved social engineering attacks... and... stealth exfiltration techniques... etc...

• **Verizon Data Breach Report – MOST breaches avoidable!**
  – 96% attacks not difficult; - 85% took weeks to discover (average is 416 days); - 92% discovered by a third party; 85 - **97% data breaches / security incidents avoidable** through simple or intermediate controls

• **Forbes - The Biggest Cybersecurity Threats of 2013**
  – Social Engineering; APTs; Internal Threats; BYOD; HTML5; Botnets; & Targeted Malware
  - **AND Cloud security -** pretty good, where ISPs / data centers are better than most

... **mobile devices and cloud infrastructure hacking** are two of the biggest rising stars in crime / terrorism in 2013 and beyond...
Threat Vectors of Interest (Cont.)

• SSL/XML/web (HTML5)/browser vulnerabilities will proliferate
  – Browsers remain a major threat vector (as it bypasses the IA suite) – for 80% of all malware
  – JAVA / VM / active code MUST be strictly managed / controlled / under “CM”

• Convergence of data security and privacy regulation worldwide..
  – Compliance gets pervasive (PCI DSS, HIPAA, etc) .. What is “good enough” security?
  – Data security goes to the cloud - where security due diligence is more than SLAs!
  – IPv6 transition will provide threat opportunities... Data Loss Prevention (DLP) is still needed...

• Containment is the new prevention (folks now get the "resilience" aspect...)

• Nation-sponsored hacking: When APT meets industrialization
  – More targeted custom malware (Stuxnet -> Duqu is but one example and now FLAME!)

• Misanthropes and anti-socials / hacktivism morphs – ANYONE can do it now!

• Full time incident responders needed, versus only virtual
  – Monitoring and analysis capability increase, but not enough (re: near real-time forensics &“chain of custody” evidence).... “continuous monitoring” is KEY... (re: SCM / SIEM)

.....MUCH to consider in the “threat” equation... and it’s always changing...
Hence why you must ALSO practice “consequence” risk management
**GAO report on mobile vulnerabilities**

**KEY risks / concerns:**
- Mobile devices often do not have passwords enabled.
- Two-factor authentication is not always used when conducting sensitive transactions.
- Wireless transmissions are not always encrypted.
- Mobile devices may contain malware.
- Mobile devices often do not use security software.
- Operating systems may be out-of-date.
- Software / patches on mobile devices may be out-of-date.
- Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections.
- Mobile devices may have unauthorized modifications. (known as "jailbreaking" or "rooting")
- Communication channels / Bluetooth may be poorly secured.

**Major protection methods:**
Enable user authentication: Enable two-factor authentication for sensitive transactions: Verify the authenticity of downloaded applications: Install antimalware and a firewall: Install security updates: Remotely disable lost or stolen devices: Enable encryption for data on any device or memory card: Enable whitelisting (on phones too!): Establish a mobile device security policy: Provide mobile device security training: Establish a deployment plan: Perform risk assessments: Manage hygiene = configuration control and management:

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
<th>Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>G</td>
<td>We have what we NEED NOW</td>
</tr>
<tr>
<td>Business</td>
<td>Y</td>
<td>Some LSIs resist change</td>
</tr>
<tr>
<td>Policy</td>
<td>Y</td>
<td>Legislation poor Can’t be voluntary</td>
</tr>
<tr>
<td>Procedures / standards</td>
<td>G</td>
<td>NIST done well Need uniform implementation</td>
</tr>
<tr>
<td>Education</td>
<td>G</td>
<td>170+ CAEs (schools) 10,000+ / year</td>
</tr>
<tr>
<td>Leadership</td>
<td>R</td>
<td>Complexity vs CISO C-suite complacency and ability to absorb</td>
</tr>
<tr>
<td>Awareness</td>
<td>G</td>
<td>Education starting earlier, STEM, NICE</td>
</tr>
</tbody>
</table>

We all need to provide an integrated, cyber package that is affordable.
SO just what are we trying to orchestrate?

An integrated “Cyber Defense in Depth / Breadth” EcoSphere using dynamic lead & lag feedback, \textit{establish proactive, dynamic CND / IA Defense}.

\begin{itemize}
  \item \textbf{Cyber “I&W”}
  \item \textbf{“Virtual Storefront”}
  \item \textbf{NMS / Security Management tools}
  \item \textbf{Defensive assessments}
\end{itemize}

- \textit{Incident results}
  \- V&V / C&A
  \- I&W / SCM
  \- CERT / FBI
  \- Red Teams

- \textit{Red Teams}

- \textit{Diagnostic feedback (lagging indicators)}

- Users  
  \textit{predictive feedback (leading indicators)}

- Change  
  \textit{“soft” settings}

- Upgrade  
  \textit{(developed & installed)}

- Predictive feedback (leading indicators)

- Forensic feedback (lagging indicators)

All “IoT” capabilities must be integrated into the cyber ‘system’.
Building a Trusted Cyber Infrastructure

“an adequately assured, affordable, net-centric environment”
(all from disparate heterogeneous capabilities that we must integrate into a homogenous cyber ecosphere!)

Focus on a few core capabilities & devices
= PC, routers, IA suite, Servers, & SANS – all with access control

Standard IA/CND suite
FW, A/V, IDS/IPS, CDS,, etc
Treat as a “SoS”: with high EAL

Make IT security a commodity:
Use IA building blocks = APLs/PPLs -> “NIAP”
Interoperability and Compose-ability are built in upfront and help dramatically reduce complexity and ambiguity
Thus….establishing known risks & pedigrees:
Reduces attack surface, risks / impacts & TOC

<table>
<thead>
<tr>
<th>Eval Assur Level (EAL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

EAL 1 – 2
Secure OS
TSM
HBSS
ZBAC

EAL 3 – 4
Secure OS
TSM
HBSS
ZBAC

EAL 5 – 6
Data centric security
Defensive I&W
Strict access / ZBAC

EAL 6
Secure OS kernel
Secure Virtual Machine
Strict access / ZBAC

ALL OSes (MS, Mac, Unix)
Integration, execution is everything
as if you can’t implement well, it costs you everywhere!!!

The quantitative benefits of systems integration and interoperability (I&I) are:
1. Shorter/reduced steps in business processes
2. Time taken to process one application/record
3. Less complaints from members of the public
4. No. of applications/records processed over a period
5. Less complaints from end-users
6. Reduced number of errors
7. Reduced software development time/effort
8. Reduced maintenance
9. Reduced no. of IT personnel

The qualitative benefits of I&I are:
1. Improved working procedures
2. Better communication with other related organizations
3. Job satisfaction
4. Redefine job specification
5. Improved data accessibility
6. One-stop service
7. More friendly public service

Until the user is happy using / benefitting from the new capability, it has no value

Buying stuff is “easy” getting it to work in your environment is hard...

Plan for “I&I”
- Integration & Interoperability - then double it

The best capability means little, if it stays in the box
SO... what MUST WE ALL DO???

NIST’s “absolutely necessary” Security Protections

NIST - National Institute of Standards and Technology

• Protect information/systems/networks from damage by viruses, spyware, and other malicious code. (IA suite, A/V, encryption, etc)
• Provide security for your Internet connection / ISP
• Install and activate software firewalls on all your business systems
• **Patch** your operating systems & applications (and now “things” too!)
• Make backup copies of important business data/information
• Control physical access to your computers and network components
• Secure your wireless access point and networks
• Train your employees in basic security principles
• Require individual user accounts for each employee on business computers and for business applications
• Limit employee access to data and information, and limit authority to install software

**MUST DO tasks** – consider this your ‘due diligence’ list

Where ALL have “CM / hygiene” aspects
Cyber Security “Best Practices” Overview

(Best practices are not a panacea – just a guide = to DO the basics)

– Quantify your business protection needs – do you have an asset inventory?
– Determine what is “good enough” or minimally acceptable for your business
– Quantify your environment’s threats and vulnerabilities
  • your list should have 10 – 50 or so threats assessed – check out USCERT, others
– Have a security policy that’s useful, complete, CEO/leadership endorsed
  • yes, that’s actually HAVE A POLICY, profiles, access control, BYOD, etc then enforce it!
– Run self-assessments on security measures (use accepted tests, STIGs, PenTests, etc) and compliance (HIPAA, PCI, CFR, SOX, etc)
– Training and awareness programs – much needed, but not a guarantee
– TEST your BCP, COOP, recovery plans, backup – have you ever restored?
– Encrypt where you can - asses where / how you need it : IM, e-mail, file transfer, storage, backup, etc)
– Be familiar with / USE the “NIST” IA/Security series – they are very good!
– DO / check / enforce the cyber basics (re: hygiene, access control, simplify & SCM)
– Reduce complexity – use only approved / preferred products lists (A/PPLs)
– A risk management plan (RMP) - using both threats AND consequences

As, you can somewhat control what you plan,
but you usually ONLY get what you enforce!
## KEY Enabling Technology Areas

### Value / need

<table>
<thead>
<tr>
<th>high</th>
<th>low</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Distributed Trust</strong>&lt;br&gt;• Resilient Architectures</td>
<td>• <strong>Response and Cyber Maneuver</strong>&lt;br&gt;• <strong>Visualization and Decision Support</strong></td>
</tr>
<tr>
<td>• <strong>Component Trust</strong>&lt;br&gt;• Detection and Autonomic Response</td>
<td>• <strong>Recovery and Reconstitution</strong></td>
</tr>
<tr>
<td>• Advanced Cross-Domain Solutions&lt;br&gt;• Advanced Cryptography&lt;br&gt;• Quantum Computing, Comms, and Crypto&lt;br&gt;• Biometrics&lt;br&gt;• Code Verification and Compliance&lt;br&gt;• Correct (Assured) by Construction Software&lt;br&gt;• Deception and Information Hiding</td>
<td>• Human Factors and Training&lt;br&gt;• Malware/Forensics Analysis and Reverse Engineering&lt;br&gt;• Resilient Infrastructure and Comms&lt;br&gt;• Scientific Theory and Measures&lt;br&gt;• Sensing and Data Fusion&lt;br&gt;• Software Pedigree and Provenance</td>
</tr>
</tbody>
</table>

**CYBER is fundamentally about**

distributed trust / assured DATA / secure messaging!
Key cyber capabilities to develop
(think “secure comms / messaging” - here proposed wrt top tier ETAs)

• **Distributed Trust** --- Enable secure distributed interactions by establishing appropriate levels of trust among remote devices, systems, or users …. **supports:** Models and Protocols for Trust Establishment; Infrastructure; Dynamic Evaluation; Out-of-Band and Physical Trust Maintenance

• **Resilient Architectures** --- Enable functional capabilities to continue despite successful disruption or compromise by the adversary …. **supports:** Morphing Engines Generating Unpredictability; Secured Network Storage; System Decomposition for Mission-Tailored Tools; Response and Cyber Maneuver

• **Visualization and Decision Support** --- Enable human decision-makers to quickly understand the security and operational implications of the current situation and to rapidly ascertain the best course of action to pursue …. **supports:** Real-Time Analysis Engines; Common Operational Framework; Holistic Cognitive Environment

• **Response and Cyber Maneuver** --- Enable defenders to perform shaping operations that minimize the attack space and frustrate adversary planning and to take action during attacks to block, disrupt, remove, or counter adversary actions. **supports:** Polymorphic Technologies; Cyber Obfuscation; Network Agility

Internet of things security = SoS and I&I aspects
Detection and Autonomic Response
Technologies that analyze data collected about the ongoing state of networks, hosts, applications, data, or user actions, and evaluate whether it represents known or probable malicious activity. Technologies that select and invoke immediate defensive actuators in real-time in response to a stream of detected events, without the need for human input.
Complex Attack Pattern Recognition, Trustworthy, Intelligent Agents, Game Theoretic Methods

Recovery and Reconstitution
Technologies that restore system trust, capabilities, and reserves to fully functional and normal levels after disruption, damage, or depletion due to cyber attack or effects of a defensive response. Technologies that restore or reconstruct lost or tainted information as closely as possible to its previous undamaged state or to what is current and accurate. Technologies that trace functions, results, or decisions that may have been affected by damaged information and restore or compensate as appropriate.
Bio-inspired self-inoculation, Synchronize repair activities without interrupting ongoing mission progression or priorities, Asymmetric redundancy using distributed trust as a recovery metric/mechanism.

Component Trust
Technologies and methodologies that establish a basis for determining and quantifying the likely trustworthiness of acquired hardware or software products that have been constructed outside an organization’s control, by methods such as external and internal physical examination, execution monitors, and supply chain risk countermeasures.
Hardware/software “DNA” that vouches for a component’s authenticity (re: enhanced TPM), White-listing of trusted hardware/software components, Root of trust, etc

Integration and Interoperability aspects are HUGE
Identified up front "cyber security" capabilities
(1) Distributed IA technologies across consolidated networks (and TRUST)
(2) Computer Adaptive Network Defense in Depth (re: a DiD Functional Ref Arch in work)
(3) Detect and eradicate advanced persistent threats (APTs)(see lack of cyber basics = APT)
(4) Cross Domain/Multi-Level Security Solutions for data and services
(5) Multi domain and multi-level secure information exchange with need-to-know
(6) Technologies for computer network attack and exploitation (e.g., CNA & CNE)

Specific security / cyber details in the report by PMW
130 - (all) Cloud Computing - 160 - Tactical Data Cloud
130 - Integration and synchronization capabilities
130 - Metadata Security - Intelligence Community Information Security Markings (IC-ISM)
130 - Information Operations ("CNO" cyber situational awareness through the real-time collection, analysis, and fusion of telecommunications, network, and maritime information)
130/160 - CDS for Data and Services
130 - CND across networks and multiple security domains; CDS for data sharing

ALL PMWs - Prognostics, Remoted ops and maintenance, IT efficiencies

What small businesses need to know about cyber security before they can offer services to the government

in general, companies must provide a commensurate security level as the government site they are going to do business with... (see NIST & GSA & FISMA web sites below)

This NIST provides a good overview of the government requirements, which in general needs to be met by companies connecting to government sites iso services provided...

Information Security rules by GSA
http://www.gsa.gov/portal/content/104257

FISMA rules / regulations are also representative of items to be assessed
http://csrc.nist.gov/groups/SMA/fisma/index.html

VA has a contract clause that's fairly standard
http://www.iprm.oit.va.gov/docs/Appendix_C.pdf

The education department has a good overview of requirements
http://www2.ed.gov/fund/contract/about/bsp.html

New LAWs - Government Contractors Subject to Cybersecurity Regulations –More are on the Way

Small business security overview (and detailed brief on the major security product details too)
How to find / bid on government contracts

MUST have **DUNS number or Cage Code** (and capability statement/documents)

Central source for SBA
http://www.sba.gov/content/federal-contracting-resources-small-businesses

+++ **System for Award Management**
(“SAM” register here first / asap.. it drives many other processes)
https://www.sam.gov/index.html

FedBizOpps
https://www.fbo.gov/

SPAWAR small business opportunities

Federal Procurement Data System
https://www.fpds.gov/fpdsng_cms/

Dynamic Small Business Search
http://dsbs.sba.gov/dsbs/search/dsp_dsbs.cfm

Interested in the SBIR / STTR programs, See information in the overview offered below
http://www.navysbir.com/overview.htm

You REALLY need an effective business plan to show clients and investors the big picture.
SUMMARY

SO.... What “really” matters in Cyber?

- **OSD / federal S&T activities**
  - Distributed Trust
  - Resilient Architectures
  - Response and Cyber Maneuver
  - Visualization and Decision Support
  - Dynamic policy management (RaDaC)
  - Detection and Autonomic Response
  - Recovery and Reconstitution

- **NSA / agency S&T activities**
  - Mobility, wireless, & secure mobile services
  - Platform integrity / compliance assurance
  - End client security
  - Cyber indications and warning (I&W)
  - Mitigation engineering (affordability)
  - Massive data – (date centric security)
  - Advanced technology.... (targeted)
  - Virtualization – secure capabilities

It’s all about **TRUST and DATA**

It’s NOT all about expensive new “cyber capabilities”

but more about the **SoS / I&I “glue”**

AND doing the **BASICS**:

1. enforced **cyber hygiene**,
2. effective **access control**,
3. reduced **complexity** in IA / cyber (APLs / NIAP / approved products),
4. **IT / IA / Cyber “SCM / SIEM”** (ongoing diagnostics AND mitigations / SIEM)

DO the cyber BASICS well, for things, people & processes

invest in select, KEY new capabilities & follow your RMP!!!

Take **ACTION**: (1) security assessment, (2) SCM/SIEM, & (3) Cyber insurance!

mike@sciap.org
What can you **DO right now?**

*Ready for immediate implementation* = 95+% incident reduction

1. Install tools/scripts to catch **USERS mistakes**.. lock down the end devices, (only allow root admin to install anything..) Use effective access control (*enforce least privilege!*)

2. Manage the **browser as THE threat vector**... *(80% of malware comes through here)*
   Have **ONE secure browser** version (IE9), use the ‘guest’ account (force downloads to one folder), and manage a specific settings profile (to manage active code / Java, etc) Implement a ‘deny all’ access approach, allow URLs using only a controlled white list *(no this is NOT hard to do!)*

3. Run tools / application firewalls to minimize zero-day problems, and **enforce CM/hygiene**, along with "**defensive I&W**" monitoring tools *(re: SCM / SIEM - #5)*

4. **KISS / reduce IA complexity**... only buy cyber products off APLs/PPLs *(they have pedigrees / C&A already!)*... And USE their security features ... like **TPM!!**

5. USE a **security continuous monitor (SCM)** firm for real-time scans for both current vulnerabilities (SQL injection, et al) and new threats... *(where the firm has feeds/data from US CERT, etc, so they are always current on new threats / zero day problems)*

6. **If you make IT stuff, build IA/security in**, there are lots of simple guides
   ![Image](http://www.sans.org/critical-security-controls/guidelines.php)
   ![Image](http://www.sans.org/top25-software-errors/)
   **We’re STILL lax**. Goggle “DarkReading Real-World Developers Still Not Coding Securely”

**Cyber continues to be about “US ALL” doing the basics**
“Overall Way Forward”
(given all the unknowns, variables... this is “one” *approximately correct* path...;-))

**• Company Vision** embedded in **Cyber Plans/RMP**...
  – know where you are going, where the passion is /what the USER values
  – *Hope is Not a Strategy* -re: 2012 Annual DDoS Attack and Impact Survey!

**• Risk Management Plan... RMP**
  – *Use NIST’s RMF!* Have a dynamic, realistic RMP supporting your business success metrics... *as you ARE betting your livelihood on cyber!*

**• Effective, enforced Policy...**
  – Embedded in core business success factors, rules to enforce statutory, legal mandates, key processes, *to enforce behavior* (pos & neg incentives)

**• The Basics, basics, basics...**
  – New toys matter little, if your environment(s) are not managed *(SCM / SIEM!)*
  – *Poor hygiene / CM causes almost ALL security incidents* (80 - 97%)

**SO...** *Quit admiring the “cyber problem / threat” and start DOING something!*
Capabilties Needed for “Information dominance”

Battlefield victory requires dominant position and maneuver
Which require best possible information, before the opposition can: (1) get his own
information; (2) react to your movements or (3) infiltrate your environment…

The best possible info is ID:
A DiD with trusted information systems providing assured / quality data,
facilitating all levels of command decision superiority
“ID” CNO ‘operational’ objectives

Assured Command and Control, Battlespace Awareness, and Integrated Fires, as sets forth the following major goals for the 2013–2017 timeframe:
• Strong and Secure Navy Command and Control;
• Persistent, Predictive Battlespace Awareness;
• Integrated Combat Information;
• Integrated Kinetic and Non-kinetic Fires;
• Information Dominance as a Warfighting Discipline.

Assured C2. The Navy must assure its ability to command and control forces. This requires capabilities that enable commanders to:
• Exchange orders and responses with subordinates;
• Understand the disposition of friendly forces;
• Target and conduct strikes as part of the joint force; and then
• Assess the result of those strikes.

Battlespace Awareness. This is the traditional mission of the Information Dominance Corps and the constituent components of meteorology, oceanography, intelligence, cryptology, communications, networks, space and electronic warfare (EW). It includes:
• Persistent surveillance of the maritime and information battlespace;
• Penetrating knowledge of the capabilities and intent of our adversaries;
• An understanding of when, where, and how our adversaries operate; and
• Expertise within the electromagnetic spectrum.

Integrated Fires. The Navy will use its networks, cyberspace and space capabilities to exploit and attack the vulnerabilities of its adversaries to achieve non-kinetic effects (i.e., fires). Just as importantly, we will expand options for forward-deployed Navy commanders by ensuring that non-kinetic alternatives are considered alongside with kinetic solutions.

WE must translate these into “technical” requirements”
CNO's Unifying Vision and Guiding Principles
(we start with the boss’ direction = ‘operational’ requirements)

First Principles Include:

• Every platform is a sensor
• Every sensor is networked
• Build a little; test a lot
• Spiral development/acquisition
• Plug-n-play sensor payloads
• Reduce afloat/airborne manning
• Transition to remoted, automated
• Collectors dynamically tasked

ID capabilities need to be both prioritized and aligned AND accommodate SoS/I&I factors

• One operator controls multiple platforms (multi-task / multi-mission)
• Emphasize UAS and autonomous platforms
• UAS's increasingly sea-based
• Data discoverable and accessible
• Missions drive requirements
• Commonality in interfaces, data links and control stations
• Every shooter capable of using target data derived from any sensor

* ID is all about TRUST & DATA *
IA / Cyber (and DATA ) must be E2E!

WE have a “natural” hierarchy in our enterprise IT/network environment, where complexities arise in the numerous interfaces and many to many communications paths typically involved in end-to-end (E2E) transactions AND, People and processes TOO!

How does the DATA move about?

Each sub-aggregation is responsible for the data / controls within their boundaries and also inherit the controls of their environment – and need to formalize reciprocity therein!

Thus, the DATA, IA/cyber controls, interfaces and profiles in each element / boundary must be quantified / agreed to upfront!
“Notional” Data Centric Architecture
iso the typical information environment

IA / Security / cyber (e.g., defense in depth (DiD))
Supports quality / assured data (with pedigree / provenance)

Cyber must be preserved in the full data AND capabilities life-cycle
IA controls / inheritance
What IA/security capabilities are needed for the DATA itself?

How does the DATA move about?

Must account for the “four ‘Vs’”
Volume, variety, velocity and veracity

Data is always, either At rest, being processed OR in transit

What of “viscosity and virality”?

ALL must adhere to Standards / profiles!
**DCA major elements**

- **Data-centric architecture (DCA)** decouples designs and simplifies communication while increasing capability and easing system evolution… DCA can link “systems of systems” into a coherent whole, using an open standard — OMG DDS… Transports, operating systems, and other location details do not need to be known, and allowing adaptation to performance, scalability, and fault-tolerance requirements.

- **Define and modularize DCA components** = create specifications (capabilities and profiles)
  - DCPS, DDSI, DataReader, DataWriter, Pub / Sub. Java, mobile code, widgets, storage SW, middleware, services, ESB, etc… these all also have cyber security aspects built in.

  !!!Need to have the data community QA these!!!

- Use **OMG / DSS** as a reference – AND - the data schema / tagging authoritative sources.

---

<table>
<thead>
<tr>
<th>Object-oriented programming</th>
<th>Data-oriented programming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide the data (encapsulation)</td>
<td>Expose the data</td>
</tr>
<tr>
<td>Expose methods – code</td>
<td>Hide the code</td>
</tr>
<tr>
<td>Intermix data and code</td>
<td>Separate data and code</td>
</tr>
<tr>
<td>Define object interfaces</td>
<td>Agree on data labels and schemas</td>
</tr>
<tr>
<td>Invoke/Implement operations on objects</td>
<td>Send/Receive messages</td>
</tr>
<tr>
<td>Combined processing, no restrictions</td>
<td>Strict separation of parser, validator, transformer, and logic</td>
</tr>
<tr>
<td>Changes: Read and change code</td>
<td>Changes: Change declarative data definition</td>
</tr>
<tr>
<td>Tightly coupled</td>
<td>Loosely coupled</td>
</tr>
</tbody>
</table>
Cyber - Begin with the end in mind

It’s clearly important to understand the desired end result, instantiation of your vision - having the image of the vision as your frame of reference to evaluate everything else.

It is also impossible to integrate capability without having a plan and the correct systems in place to run the business.

Vision execution has to do with the "purposes" of capabilities, that have to do with visualization and complete planning! Bundled within personal and business: (a) leadership (what), (b) management (how), and (c) productivity (doing it well)…

You can take the concept further by questioning the vision itself! Challenge assumptions, barriers, limitations, and obstacles…(the five whys?)

Always apply critical thinking (reflective skepticism) to the vision, as that brings New Ideas… Fosters Teamwork… Promotes Options… Uncovers Spinoffs… simulates a Clear Head… and fresh Perspectives emerge….

If you don’t know where you are headed, Seemingly blind alleys won’t cut it either / waste $$$
Cyber - Drive out complexity - KISS

Complexity leads to variation in practice, opportunities for data / operational errors, and increased risk of mission failure.

Reducing complexity is key to improving both risk posture and productivity.

Human engineering and complexity theory teach that WE ALL need to smartly, collaboratively:
- Simplify
- Standardize
- Automate
- Integrate

Reducing complexity is a major competitive factor for ensuring supply chain performance and exceeding customer expectations.

Given an increasing share of work is outsourced, the challenge of handling complexity has become all the more demanding.

Companies that do not master complexity risk experiencing supply chain inefficiencies, resulting in non-competitive working capital structures, lower transparency of cost drivers and difficulties in achieving service levels.

Address complexity in product, processes and organization.. and DATA

Use existing initiative to simplify both objectives and processes:
- Just-In-Time
- Standardization
- Strategic Outsourcing
- Supply-chain management
- Target costing
- Performance Measures

Take the "zero-baseline" approach to complexity
NSPD-54/HSPD-23: CNCI-1 ‘12 Initiatives’
(http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

Establish a front line of defense

Resolve to secure cyberspace / set conditions for long-term success

Shape future environment / secure U.S. advantage / address new threats

Cyber efforts must synchronize with Federal Investments

The HARD part is implementing enterprise integration, interoperability and controlling emergent behavior - that can affect most focus areas
CNCI


There are 12 mutually-reinforcing initiatives that are intended to establish a front line of defense against today’s immediate threats, to defend against the full spectrum of threats, and to strengthen the future cybersecurity environment.

INITIATIVE #1 -- Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections. This is about consolidating our external access points and creating common security solutions across agencies.

INITIATIVE #2 -- Deploy an intrusion detection system of sensors across the Federal enterprise. This is a passive system that watches traffic and helps notify us about unauthorized network intrusions. DHS is deploying signature-based sensors as part of the EINSTEIN-2 (PDF) capability, with notification going to US-CERT.

INITIATIVE #3 -- Pursue deployment of intrusion prevention systems across the Federal enterprise. This takes it up a notch with EINSTEIN-3 (PDF) and not only detects intrusions, but actively prevents intrusions into federal systems. This will have serious zero-day and real-time counter-threat capabilities.

INITIATIVE #4 -- Coordinate and redirect research and development (R&D) efforts. This initiative serves to help us get all of our R&D efforts working together, with a better communications and tasking infrastructure. It's an important part of utilizing our resources and our smartest people to the best of their abilities.

INITIATIVE #5 -- Connect current cyber ops centers to enhance situational awareness. This is our key threat-data sharing initiative.

The National Cybersecurity Center (NCSC) within Homeland Security is helping secure U.S. Government networks and systems under this initiative by coordinating and integrating information from the various centers to provide cross-domain situational awareness, analysis, and reporting on the status of our networks. As a side-effect, it’s also designed to help our various agencies play better with each other.

INITIATIVE #6 -- Develop and implement a government-wide cyber counterintelligence (CI) plan. We're now coordinating activities across all Federal Agencies so we can detect, deter, and mitigate foreign-sponsored cyber intelligence threats to government and private-sector IT.
INITIATIVE #7 -- Increase the security of our classified networks. Our classified networks contain our most valuable and most secret defense and warfighting information. We're continuing to work hard in securing these networks against the changing threat model.

INITIATIVE #8 -- Expand cyber education. This is where the Comprehensive National Cybersecurity Initiative begins to break down, because it's where all modern cyberdefense breaks down -- the people. We're training more and more cyberdefense experts, but we also need to expand that education up and down government, to corporations, and to individuals. We can have the very best-trained cyberdefense expert in a corporation, say, and it'll all break down if the CEO won't allocate the time or funds to conduct that defense. It's all about making everyone know just how real these threats are.

INITIATIVE #9 -- Define and develop enduring "leap-ahead" technology, strategies, and programs. We'll talk more about future directions later, but the idea of leap-ahead is to get 5 to 10 years ahead of the bad guys and explore out-of-the-box thinking in building a better cyberdefense. This is good stuff, and it's the first CNCI initiative that, essentially, opens the door to concepts like Stuxnet (or what The Times claimed the White House called "Olympic Games").

INITIATIVE #10 -- Define and develop enduring deterrence strategies and programs. Put simply, because of the wildly asymmetric nature of the threat, we can't have a mutually-assured destruction option with cyberattack, the way we do with nuclear attack. We're working on developing deterrence strategies, but we're not there yet, a fact which is sadly all too evidenced by constant level of cyberattack, breach, and threat we find ourselves experiencing.

INITIATIVE #11 -- Develop a multi-pronged approach for global supply chain risk management. This area should be one of our biggest concerns. Most Americans get their computers from suppliers who use processors, motherboards, and components made outside the United States -- and often in China. China, as we've seen repeatedly, is one of our most challenging "frenemies". They're clearly important to us financially, but they're also one of the leading sources of cyberattack (and, quite frankly, could be behind the one we're dealing with now). This initiative, though, isn't just about China. Our components and our supplies must be insulated from foreign influence and unapproved modification.

INITIATIVE #12 -- Define the Federal role for extending cybersecurity into critical infrastructure domains. The federal government is relying more and more on private sector services. For example, the Department of Interior is about to start using Google for its email infrastructure. This initiative encourages public/private-sector cooperation to extend Federal-systems cybersecurity into the wider cyber-infrastructure.

A huge sample size! This includes YOUR business category too !!!

855 Incidents, 174 million compromised records, teamed with law enforcement
(an 8 year series, 2000 breaches, one billion compromised records – 36 countries)

WHO
- 98% from ‘external’ agents
- Mostly small business!!!
- Includes ‘internal’ security intrusion activities too – STILL a major concern

HOW
- 81% Hacking
- 69% Malware

COMMON
- 96% attacks not difficult
- 85% took weeks to discover (average is 416 days)
- 92% discovered by a third party
- 97% avoidable through simple or intermediate controls

Mitigations
- Implement a firewall or ACL on remote services
- Change default credentials of POS and internet facing devices
- Ensure essential controls met, regularly check them
- Monitor and mine event logs
- Evaluate threats to prioritize treatments

HYGIENE Factors

We have met the cyber enemy, and they are US
What is Cyber Hygiene?
(and the HUGE percentage of security incidents caused by lack of it)

National Security Agency (NSA) (80-85%)
NSA IAD director “Just improving the “IA Management” aspects of security (aka, hygiene factors) will reduce security incidents by over 80%.

_IA Management = CM, monitoring environment, follow SOPs_


Verizon (2012 Data Breach Investigations Report) (up to 97%)
Report covered 855 incidents, 174 million compromised records

--- Breaches almost entirely avoidable through simple or intermediate controls
Threats: 98% from external agents, 81% from hacking… 69% used malware


Navy (our “red team” / NCDOC) (over 90%)
Poor “accountability” factors = willful misuse, lack of CM (& IAVA / patches), not having / following procedures, weak enforcement of policy, etc
They must spend all their time / resources fixing the “easy” vulnerabilities…

HYGIENE = Maintaining / monitoring your IA / Security / cyber equipment settings
As any incorrectly set cyber capabilities makes them much less effective!
Security Continuous monitoring (SCM)

- **What is SCM anyway?**

  SCM is *ongoing observance with intent to provide warning*. A SCM capability is the ongoing observance and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations.

  SCM is a *risk management approach to Cybersecurity* that maintains a picture of an organization’s security posture, provides visibility into assets, leverages use of automated data feeds, monitors effectiveness of security controls, and enables prioritization of remedies.


- **What good is it?**

  **MANY ‘ROI’ benefits**: Real-time awareness of security posture, cyber benchmarking, complements audit / compliance efforts, improves cyber performance, and reduces risk expose – simples risk management overall.

  Third party IV&V monitors of “hygiene” “AND” potential new threats!


- **WHO does this now, where do I go for help?**

  DISA and DHS have efforts in play already (*DHS is funding continuous monitoring as a service (CMaaS)*).

  State department DID early SCM several years ago, *reduced C&A costs over 90%*


- **SCM is mandated for government entities** (*FISMA / DOD CIO / DHS / others*)

  SCM is a cyber / risk management tool and *provides added due diligence* stopping short of “get out of jail free” – **keeps you from being the low hanging fruit!**
IA/security resources

Main sites
- https://infosec.navy.mil
- https://www.fleetforces.navy.mil/netwarcom/navycanda (?? URL ??)

Other IA/Security sites:
- http://csrc.nist.gov/
- http://www.cerias.purdue.edu/
- http://security.sdsc.edu/

Other IA/Security sites (cont):
- http://www.cert.org/
- http://www.commoncriteriaportal.org/
- https://www.sans.org/about/sans.php

Great ISSE / SSE Site
- This site has almost everything you need
- C&A moved to here