Top 7 things healthcare institutions must do to remain both HIPAA compliant *and* truly secure

Shahid N. Shah

CEO and Chief Security Architect

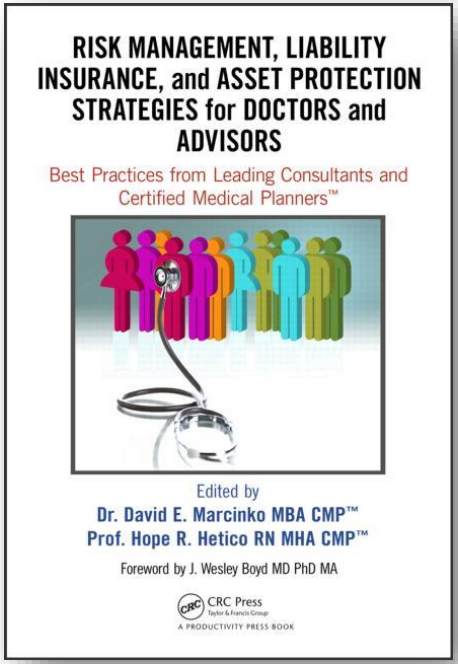
Netspective

EXTENDING THE ENTERPRISE

Who is Shahid?

Cybergeek at Netspective, Gov't Tech & Security Advisor

- 15 years of risk management and cybersecurity expertise (in healthcare, government, and other sectors)
- 15 years of technology management experience (government, non-profit, commercial)
- 18 years of healthcare IT and medical devices experience (blog at http://healthcareguy.com)
- 25 years of software engineering and multi-discipline complex IT implementations (Gov., defense, health, finance, insurance)



Author of two chapters: "Understanding Medical Practice Cybersecurity Risks" and "How to Conduct a Health-Care Environment Electronic Risk Assessment"

What's this talk about?

Background

HIPAA, while a regulatory necessity, is an insufficient framework for modern healthcare risk management cybersecurity.

Most HIPAA compliant institutions have tons of insecure systems because they confuse compliance with security.

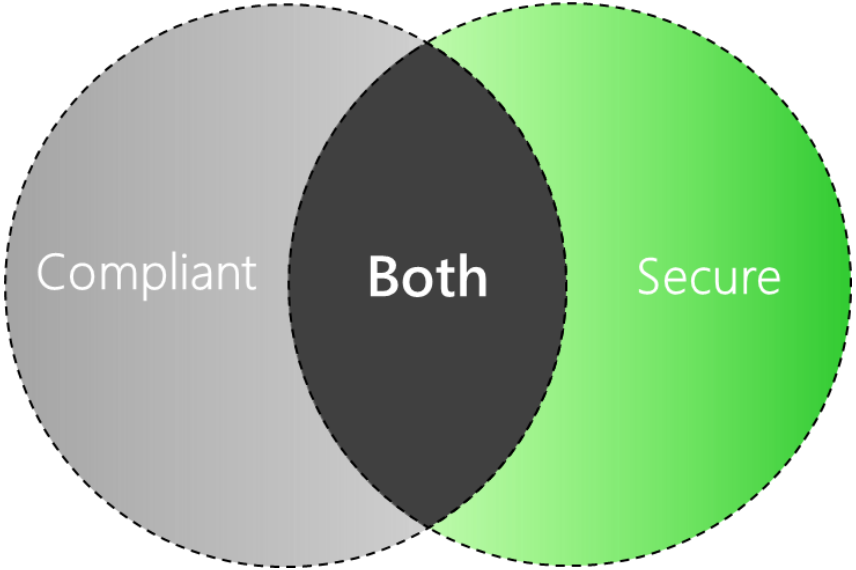
Key takeaways

- Every technology in a modern healthcare enterprise network is becoming more and more healthcare-neutral.
- There's nothing unique about digital health data that justifies complex, expensive, or special cybersecurity technology.
- Healthcare-specific cybersecurity and risk frameworks are going to do more harm than good and the industry should look to major federal government initiatives like DHS CDM for guidance on approach and tools.

The Soapbox

Don’t confuse compliance and security

You can be compliant and not secure, secure but not compliant, or both



☹ Compliant insecurity is pretty common

Compliance: often binary (yes/no)

Security: always continuous

An example of compliant insecurity

Compliance Requirement

- Encrypt all data at FIPS 140 level

Insecure but compliant

- Full disk encryption
  - Encryption keys stored on same disk
- SSL encryption
  - No TLS negotiation or man in the middle monitoring

Secure and compliant

- Full disk encryption
  - Disk-independent key management
- TLS encryption
  - Force SSL → TLS and monitor for MIM threats

This is a common problem in many EHRs, digital health apps, and medical devices.

Another example of compliant insecurity

Compliance Requirement

- Establish procedures for creating, changing, and safeguarding passwords

This is a common problem in many medical devices.

Insecure but compliant

- Default admin password
- Documentation says password should be changed upon initial setup
- Documentation says password should be rotated frequently

Secure and compliant

- When device or software is initially setup, it forces a password change
- Device or software prompts to change password regularly
- Device or software reports, each night, if default passwords aren't changed or rotations haven't occurred

Why does compliant insecurity occur?

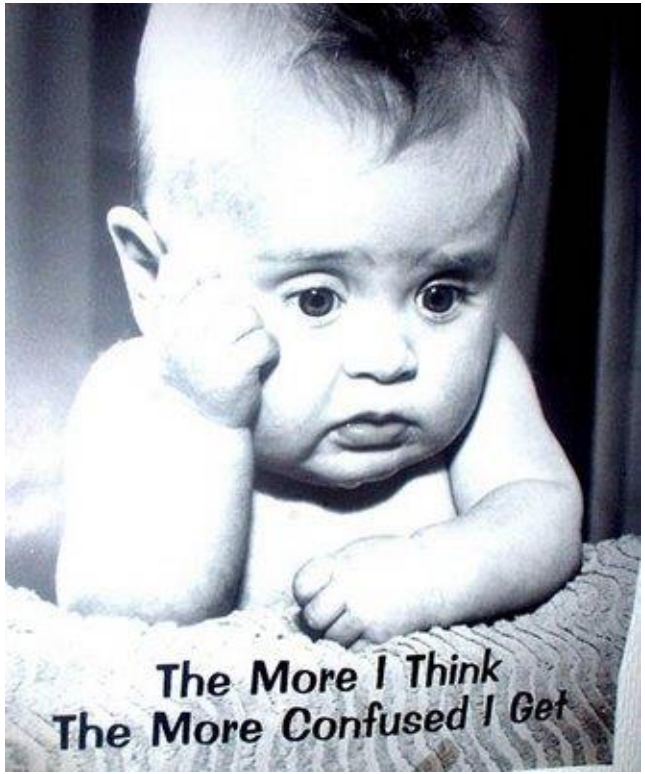
Compliance is focused on…

- Regulations
- Meetings & discussions
- Documentation
- Artifact completion checklists

Instead of…

- Risk management
  - Probability of attacks
  - Impact of successful attacks
- Threat models
  - Attack surfaces
  - Attack vectors
- Bottom-up asset management
  - Full inventory assessment
  - Continuous change management
  - Asset- and risk-specific threat mitigation
- Regular pen testing, user behavior analytics, and data loss prevention activities

Forget compliance…at first



Get your security operations in proper order before concentrating on compliance.

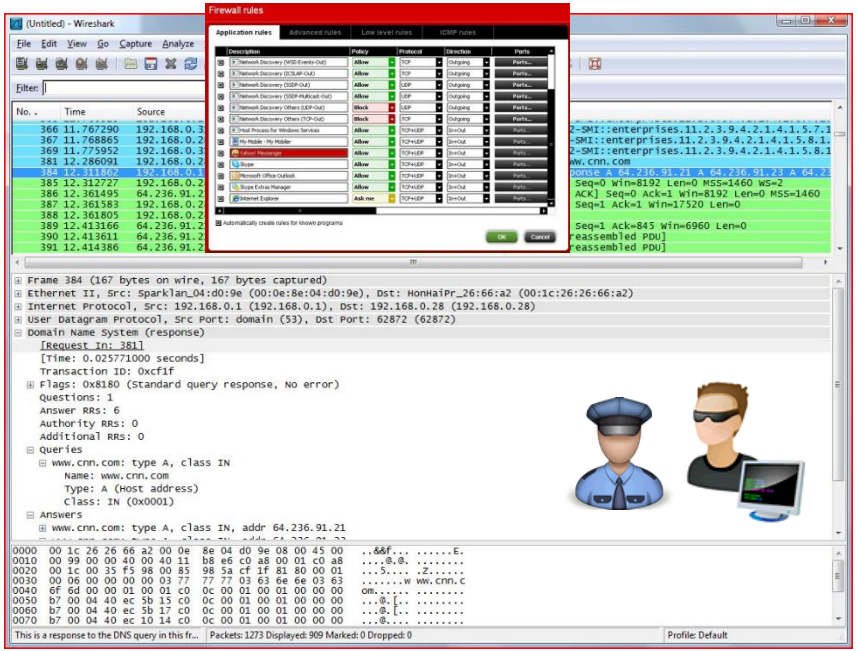
Start sounding like a broken record, ask "is this about security or compliance?" often.

If you're provably and demonstrably secure, it's easier to get to compliance than the other way around

Make sure the right people are in charge

Law: Compliance

Order: Security



Make sure the right people are in charge

Compliance knowledge bases

FISMA

PCI DSS

HIPAA

ONC

FDA

SOX

NIST

CDM

Security knowledge areas

Firewalls & Encryption

User Behavior Analytics

Pen Testing & Access Control

Data Loss Prevention

Continuous Monitoring

Packet Analysis

Understand what's what

Risks

Threats

Privacy

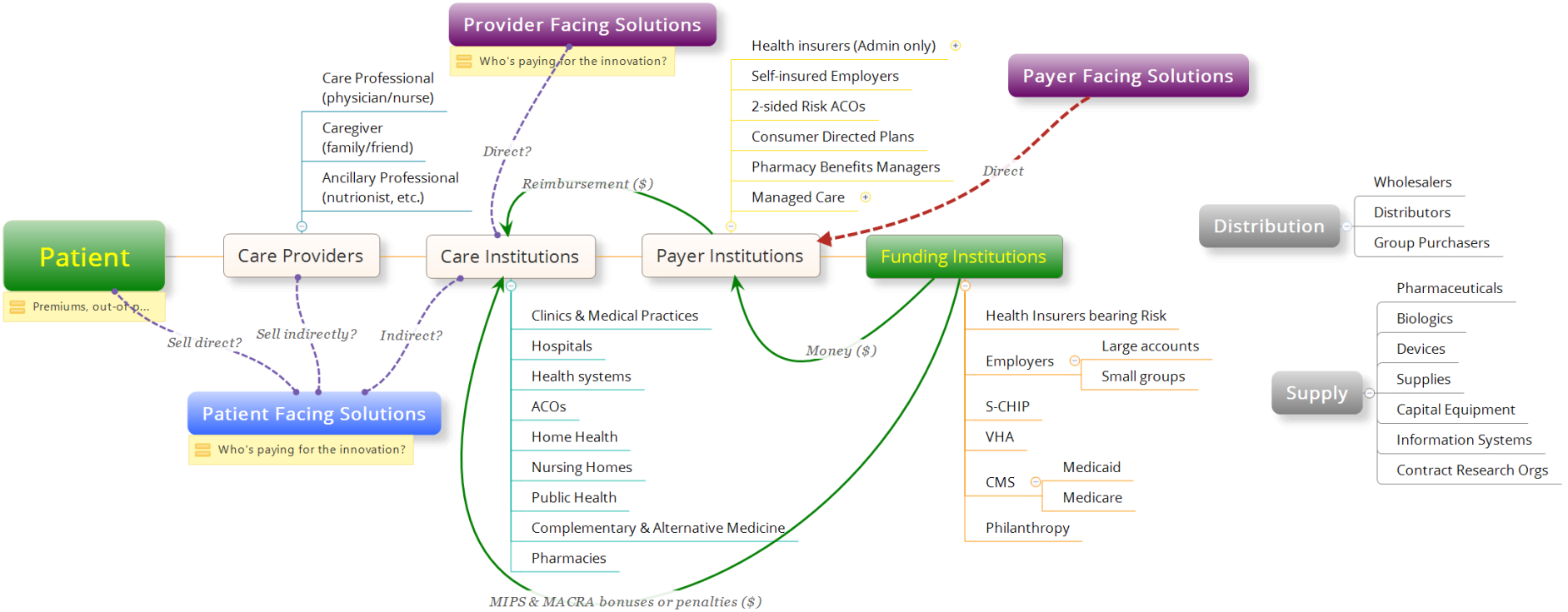
Security

Compliance

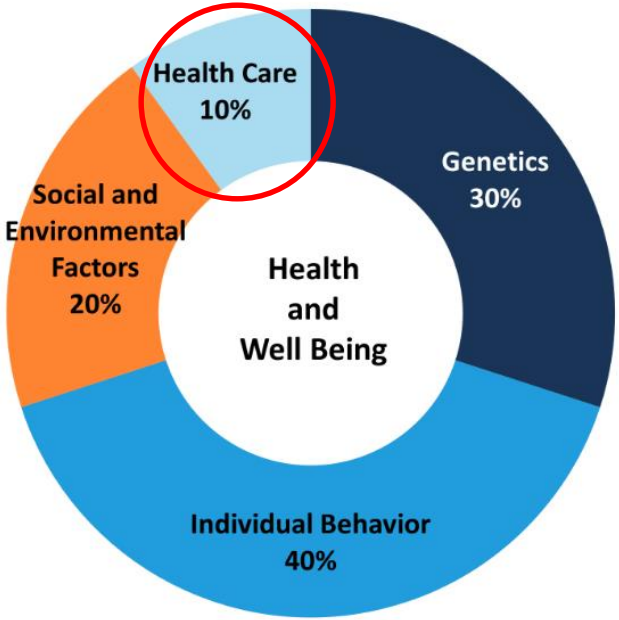
Audits

Remediation

Increased payer / provider collaboration and increases threat surfaces and will drive further data leakage



Huge breaches occur already, what's to come?



Economic Stability	Neighborhood and Physical Environment	Education	Food	Community and Social Context	Health Care System
Employment	Housing	Literacy	Hunger	Social integration	Health coverage
Income	Transportation	Language	Access to healthy options	Support systems	Provider availability
Expenses	Safety	Early childhood education		Community engagement	Provider linguistic and cultural competency
Debt	Parks	Vocational training		Discrimination	Quality of care
Medical bills	Playgrounds	Higher education			
Support	Walkability				

Health Outcomes
Mortality, Morbidity, Life Expectancy, Health Care Expenditures, Health Status, Functional Limitations

Audience Participation

Are your senior executives well versed in the major concepts like compliance vs. security vs. privacy?

- Yes, this is all elementary and our team understands it completely
- No, we understand most of the concepts but some of the nuances aren't clear
- No, we do not understand all the concepts and could use guidance

There is no cybersecurity crisis *specific* to healthcare.

To get the best tools and frameworks with the best support, stay industry-neutral.
Whenever something becomes "healthcare specific" it slows down its innovation.

Risk management, continuous diagnostics & mitigations are a concern.

There is a healthcare data privacy crisis.

Not enough organizations have separated *digital* confidentiality and privacy policies from security policies.

User behavior analytics (UBA) and data loss prevention (DLP) technology isn't as widely deployed as it should be.

Preparing annual controls catalogs and compliance documentation or passing audits doesn't mean you're safe.

Not enough organizations differentiate between point in time assessments versus continuous monitoring.

Only continuous monitoring of each operational asset, from the bottom-up, ensures security.

Things healthcare institutions must do to remain both HIPAA compliant and truly secure

The Top 7 tips for 2017

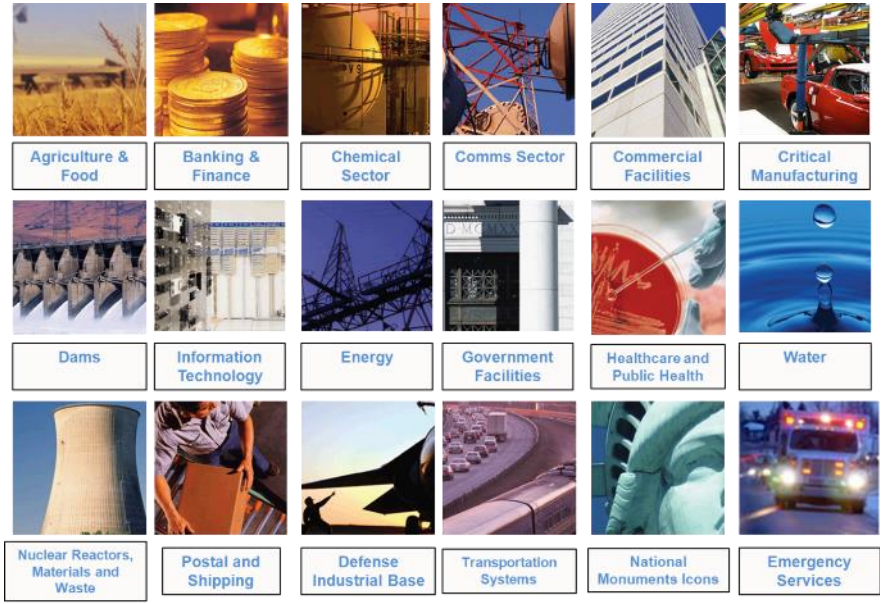
#1

When you have a choice, follow Department of Homeland Security (DHS) guidance; we must *go beyond HIPAA* and healthcare-specific frameworks.

Hackers don't use "healthcare" tools to steal medical records so you shouldn't follow different rules to keep them out.

Learn about the $6 billion DHS Continuous Diagnostic & Mitigation (CDM) Program.

DHS provides advice and alerts to the 16 critical infrastructure areas …



… DHS collaborates with sectors through Sector Coordinating Councils (SCC)

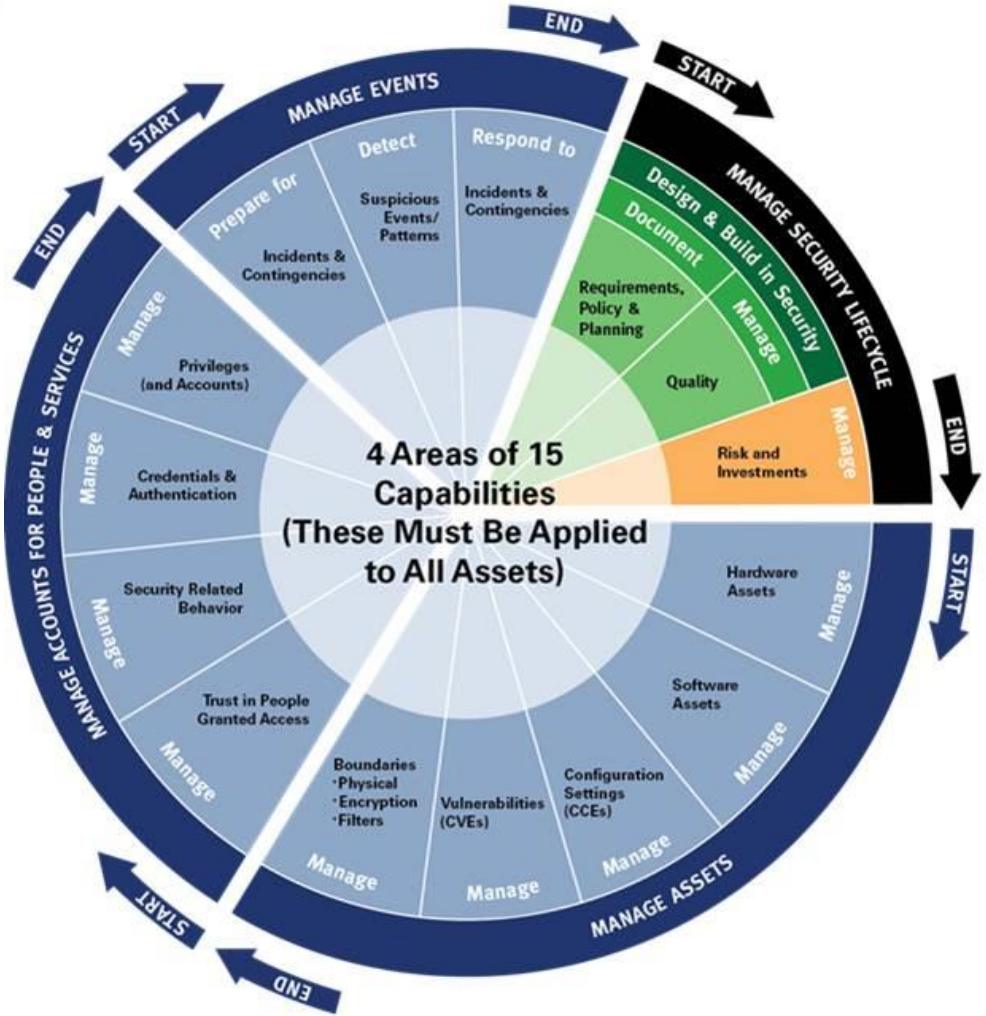
- **Business / Personal**
  - **Shopping & Banking Point of Sale (in store or on line)**
  - **Personnel**
  - **Social Media**
  - **…**

The DHS led CDM Program covers 15 continuous diagnostic capabilities. Your data is not secure unless you understand the entire lifecycle.

Phase 1: Endpoint Integrity
- HWAM – Hardware Asset Management
- SWAM – Software Asset Management
- CSM – Configuration Settings Management
- VUL – Vulnerability Management

Phase 2: Least Privilege and Infrastructure Integrity
- TRUST –Access Control Management (Trust in People Granted Access)
- BEHAVE – Security-Related Behavior Management
- CRED – Credentials and Authentication Management
- PRIV – Privileges

Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle
- Plan for Events
- Respond to Events
- Generic Audit/Monitoring
- Document Requirements, Policy, etc.
- Quality Management
- Risk Management
- Boundary Protection – Network, Physical, Virtual



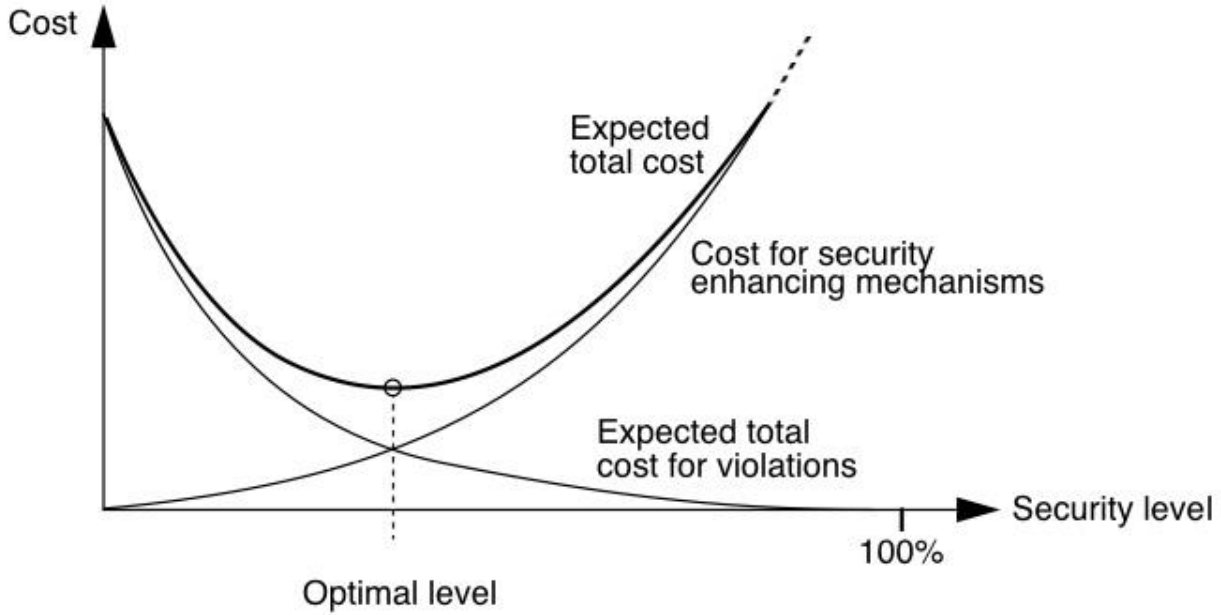
Audience Participation

Is there a reason for healthcare-specific security solutions or should we use industry-neutral tools and technologies?

- No, there's no good reason not to be industry-neutral because our problems in healthcare are the same as everyone else's (medical devices are no different than other IoT devices)
- No, but there are some healthcare-specific problems that we should tell DHS and standards bodies about (like medical devices)
- Yes, there are many good reasons to work on healthcare-specific security solutions because industry-neutral tools are not good enough

#2 Consider costs while planning security

100% security is impossible so compliance driven environments must be slowed by cost drivers



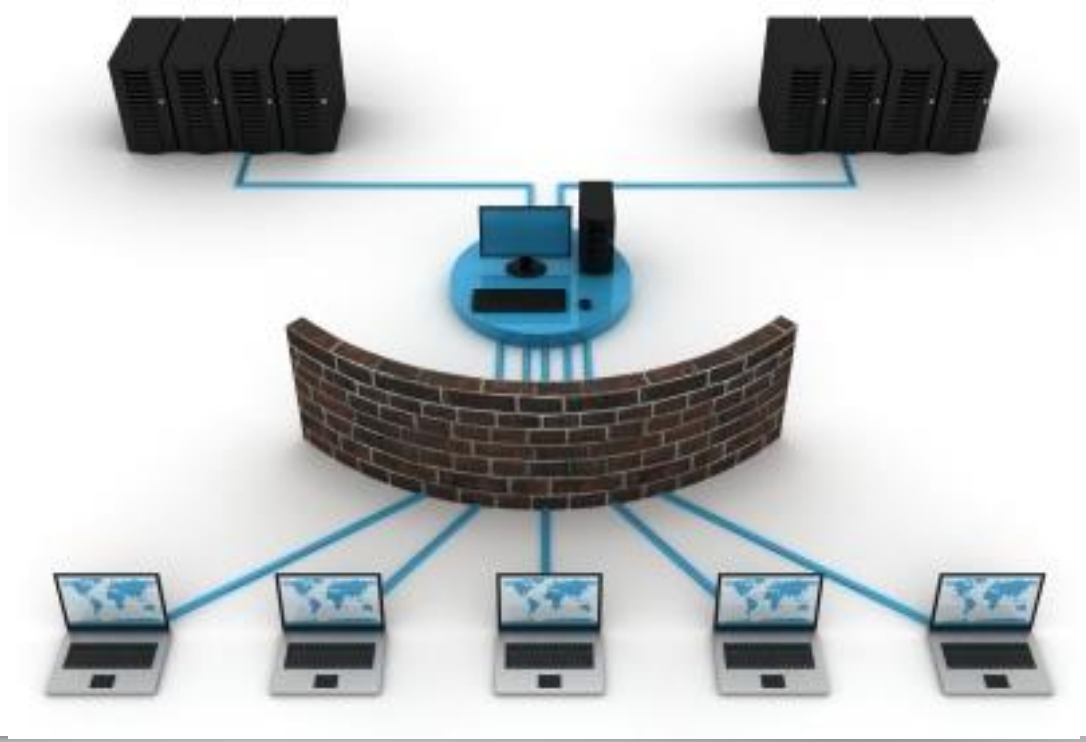
Source: Olovsson 1992, "A structured approach to computer security"

#3 Don’t rely primarily on perimeter defense

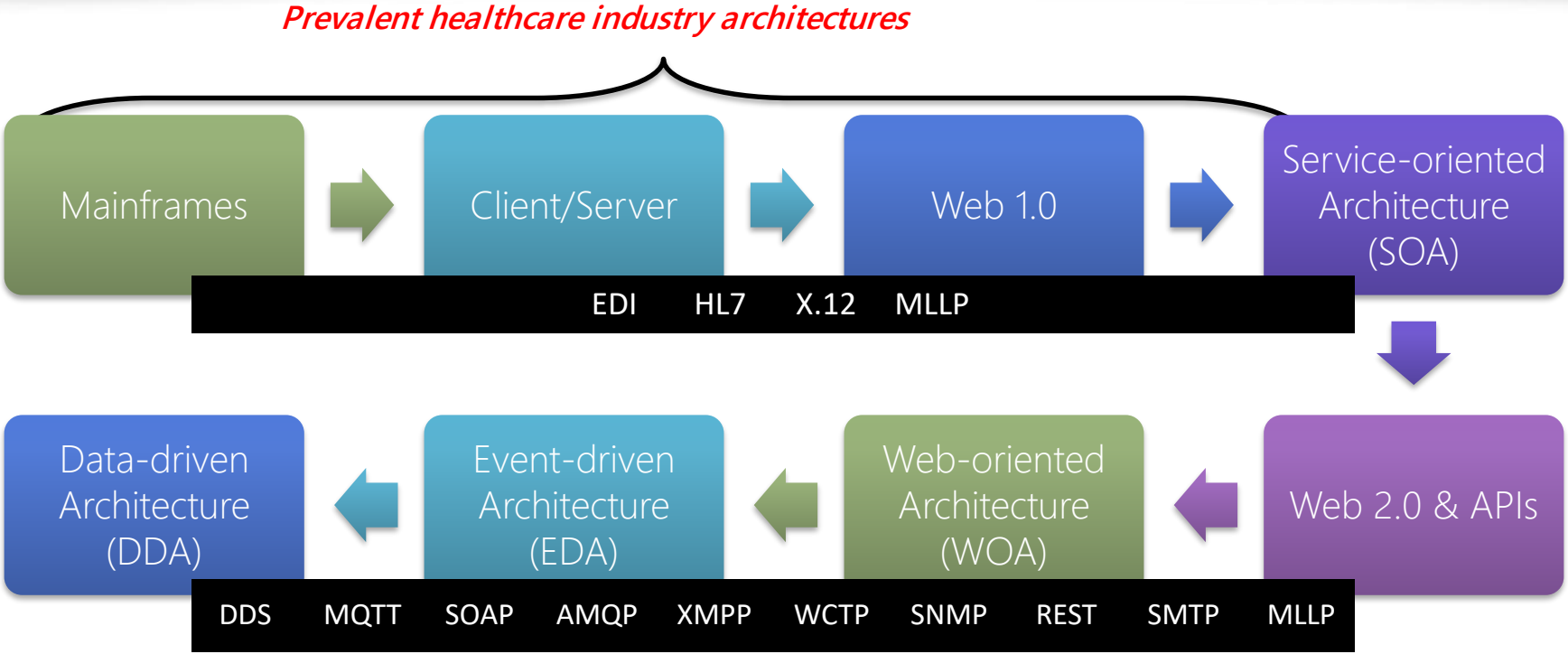
Firewalls and encryption aren’t enough

Many breaches occur by insiders, lots of data disseminated accidentally

Rely on risk-based role-aware user behavior analytics and anomaly detection



#4 Understand architecture transition impacts



#5 Create risk and threat models…and share them widely

He will win who, prepared himself, waits to take the enemy unprepared – Sun Tzu

Define threats

- Capability, for example:
  - Access to the system (how much privilege escalation must occur prior to actualization?)
  - Able to reverse engineer binaries
  - Able to sniff the network
- Skill Level, for example:
  - Experienced hacker
  - Script kiddie
  - Insiders
- Resources and Tools, for example:
  - Simple manual execution
  - Distributed bot army
  - Well-funded organization
  - Access to private information
- Motivation + Skills and Capabilities tells you what you're up against and begins to set tone for defenses

Source: OWASP.org, Microsoft

Create minimal documentation that you will keep up to date

Threat	Layer where mitigation is implemented	Nature of mitigation provided (if specific to Windows Azure)	Application/Service-layer mitigation required	Is this issue higher risk or more complex in cloud deployments?
Spoofing				
Side-channel attacks against VM Guests on the same physical host	Platform	1 VM per core, no communications between different tenants	None Required	Yes
Disclosure of data in transit between client and server			ce of HTTP data is	Yes
Disclosure of SSL Certificates/keys used by Web Roles			e store for SSL e	Yes
Disclosure of arbitrary secrets in blob/table/queue storage			t data prior not store n Windows	Yes

Mitigation is transparent to the customer, no action required.

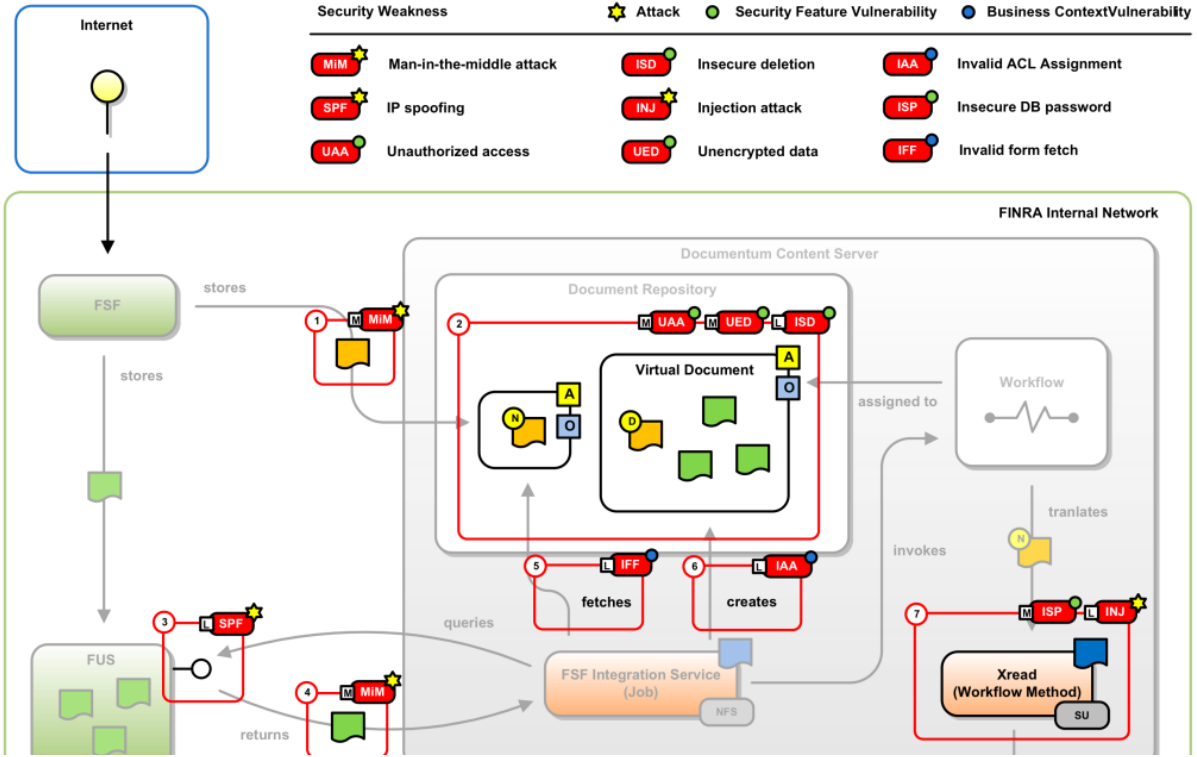
Mitigation is provided by underlying platform/infrastructure and must be utilized by the customer's web application/service; Requires calls to existing/provided APIs.

Mitigation is per-service and is not provided at a lower level; Must be mitigated by the customer's code.

Mitigation is not yet implemented (planned for a future version of Windows Azure) but will be transparent to the customer once complete.

Mitigation is not yet implemented (planned for a future version of Windows Azure) and will require customer code to use Windows Azure APIs once complete.

#6 Visualize attacks / vulnerabilities



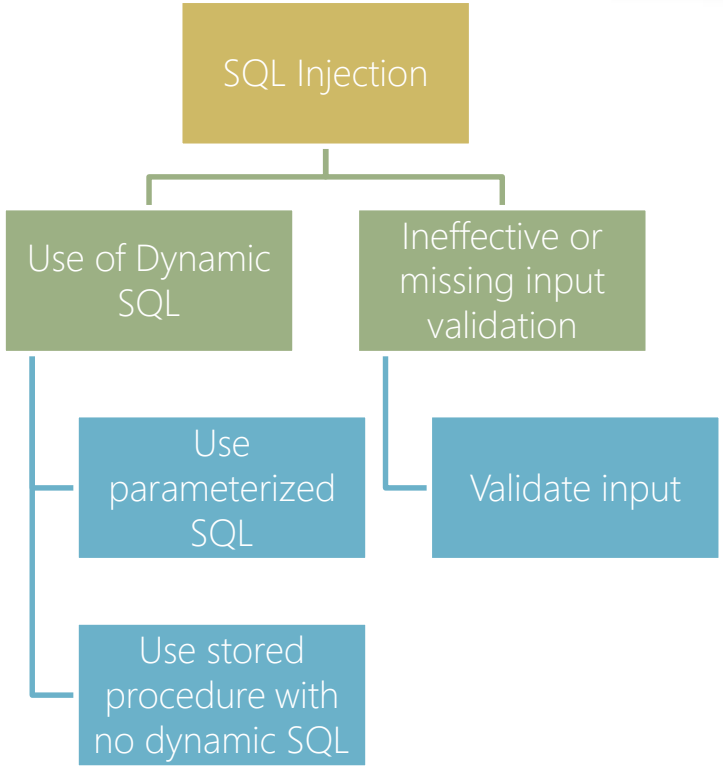
Create an Attack Library…and share it!

- Password Brute Force
- Buffer Overflow
- Canonicalization
- Cross-Site Scripting
- Cryptanalysis Attack
- Denial of Service
- Forceful Browsing
- Format-String Attacks
- HTTP Replay Attacks
- Integer Overflows
- LDAP Injection
- Man-in-the-Middle
- Network Eavesdropping
- One-Click/Session Riding/CSRF
- Repudiation Attack
- Response Splitting
- Server-Side Code Injection
- Session Hijacking
- SQL Injection
- XML Injection

Source: Microsoft

Collect attack causes and mitigations…& share!

- Define the relationship between
- The exploit
- The cause
- The fix



Source: Microsoft

Audience Participation

Are your security threats properly modeled, prioritized, and shared?

- We have a well understood threat assessment process and we have properly documented threat models tied to our risk assessments at the asset level (bottom up)
- We have a well understood threat assessment process and we have properly documented threat models tied to our risk assessments at the security boundaries but not at the asset level (top down)
- We the understand threat assessment process but we have not documented threat models tied to our risk assessments
- No, we haven't done proper threat assessments tied to risks

#7 No security theater! Make risk-based decisions

How you know you're "secure"

- Value of assets to be protected is understood
- Known threats, their occurrence, and how they will impact the business are cataloged
- Kinds of attacks and vulnerabilities have been identified along with estimated costs
- Countermeasures associated with attacks and vulnerabilities, along with the cost of mitigation, are understood
- Real risk-based decisions drive decisions **not security theater**

Bonus! #8 Review security body of knowledge

Everyone

- FIPS Publication 199 (Security Categorization)
- FIPS Publication 200 (Minimum Security Requirements)
- NIST Special Publication 800-60 (Security Category Mapping)

Executives and security ops

- NIST Special Publication 800-18 (Security Planning)
- NIST Special Publication 800-30 (Risk Management)

Security ops and developers

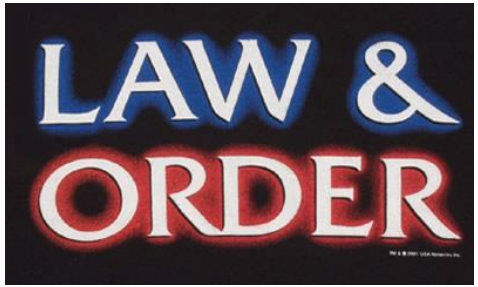
- NIST Special Publication 800-53 (Recommended Security Controls)
- Microsoft Patterns & Practices, Security Engineering
- OWASP
- IEEE Building Code for Medical Devices

Auditors

- NIST Special Publication 800-53 (Recommended Security Controls)
- NIST Special Publication 800-53A Rev 1 (Security Control Assessment)
- NIST Special Publication 800-37 (Certification & Accreditation)

Key Takeaways

- If you have good security operations in place then meeting compliance requirements is easier and more straightforward.
- Even if you have a great compliance track record, it doesn't mean that you have real security.



DHS CDM Deep Dive

The CDM Program BPA Tools Catalog

Continuous Diagnostics & Mitigation (CDM) Product Catalog

As of: 9/11/2015

Homeland Security

GSA

The purpose of the Continuous Diagnostics and Mitigation (CMaaS customers with a comprehensive list of CDM securit CDM CMaaS Blanket Purchase Agreement (BPA). This guide

The Tools/CMaaS BPA Product Catalog lists the tools and se create the Tools/CMaaS Product Catalog includes the CMaa

Over the course of the CDM program, technology-based sol increasingly robust solutions. As new CDM Program capabil accordingly.

The Tools/CMaaS Product Catalog is not intended as an aut support alignment and acquisition of specific products, sup development and refinement. All product categorizations, time, and have not been modified or endorsed by GSA or D

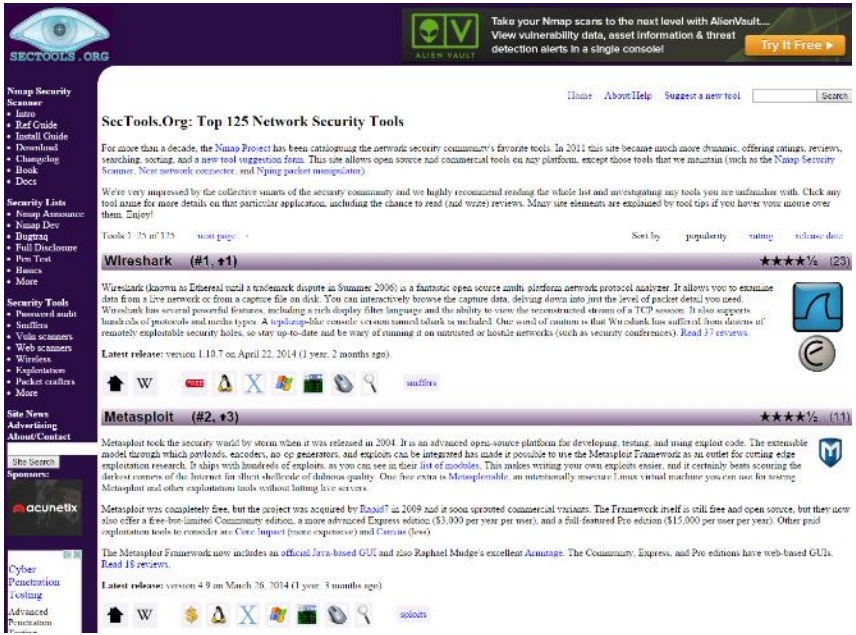
		CDM PHASE 1				CDM PHASE 2				
CDM Product Manufacturer	CDM Product Family	HWAM	SWAM	CSM	VUL	TRUST	BEHAVE	CRED	PRIV	Manufacturer's Product Description
Avecto	DefendPoint Privilege Management								X	Defendpoint provides all the tools you need to suc the right amount of access, with permissions appli themselves. Standard users are highly secure, yet s compromised. By enabling all employees to work environment.
Axiomatics	Axiomatics Data Access Filter					X	X	X	X	The Axiomatics Data Access Filter (ADAF) is an aut purpose of applying policy-based controls in datab according to policy, by modifying SQL statements enables dynamic filtering of database content, cen integrate with multiple database products.
Axiomatics	Axiomatics Policy Server					X	X	X	X	The Axiomatics Policy Server (APS) is a solution av (ABAC). With three different types of authorizatio requirements.
Axiomatics	Axiomatics Reverse Query					X	X	X	X	The Axiomatics Reverse Query (ARQ) is an authori Where the Axiomatics Policy Server responds to in Axiomatics Reverse Query helps automate process
BDNA	BDNA Discover	X	X							BDNA Discover delivers insights into the IT environ and software assets including those not covered b provides advanced application discovery for top v provides complete visibility into the IT environme GRC.
BDNA	BDNA Normalize	X	X							BDNA Normalize is a solution that uses Technoped information about enterprise hardware and softw sources to create a single version of accurate and clean, accurate, and relevant data to drive effecti
BDNA	BDNA Technopedia	X	X							BDNA Technopedia categorizes and aligns hardwa relevant information. With more than 1.2 million

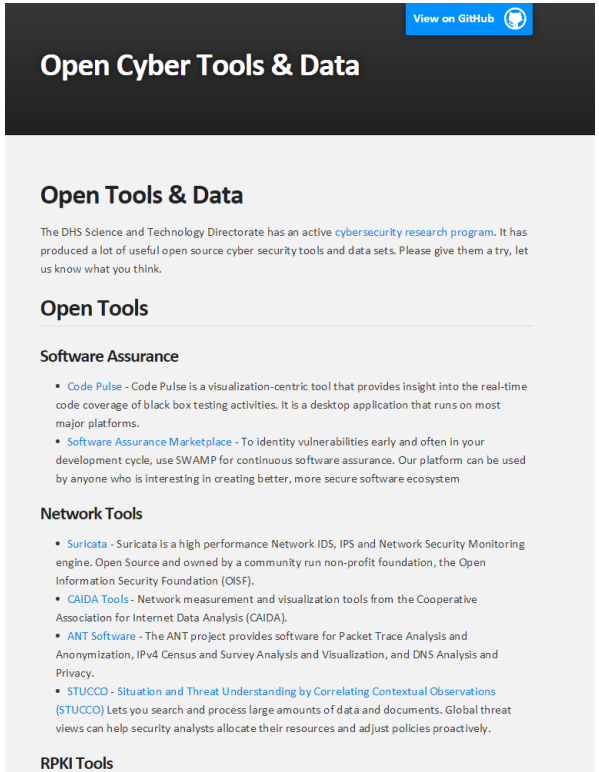
DHS Open Source Cybersecurity Catalog

CATEGORY	APPLICATION(S)
Administration	CFengine, Expect, Process Hacker, Webmin
Anti-spyware	Nixory
Antivirus	ClamAV, ClamWin, Moon Secure Antivirus, Simple Machine Protect
Application Languages & Development Environments	BASH, Clang, Coccinelle, Cygwin, DDD, Eclipse, Emacs, GCC, GDB, Gedit, Java, phpHtmlLib, Python, Qlue, Ruby, Vi, VIM
Browser Add On	Password Maker, Web of Trust
Business Continuity	AMANDA, Areca Backup, Partimage
Cloud Computing	ABIQUO, Cloudstack, Eucalyptus, Juju, Nimbula, Open Nebula, OpenStack
Configuration Management	CFengine, Puppet, Salt
Content Management	Chef, Drupal, Joomla, Juju, Wordpress
Data Backup & Archival	Bacula, Open Nebula, PeaZip, Unison
Database	MariaDB, MySQL, NetDB, Percona, PostgreSQL, SQLite
Data Removal	BleachBit, Darik's Boot and Nuke, Eraser, Wipe
Directory	OpenLDAP
Disk	BleachBit, DBAN, Gparted, Midnight Commander, Parted, Partimage
Email	amavisd-new, ASSP, JAMES Mail, Mozilla Thunderbird, Postfix, Spam Assassin, SquirrelMail, VPOP Email, Zarafa, Zimbra
Email Protection & Anti-Spam	amavisd-new, ASSP, Postgrey, Spam Assassin
Email Services	JAMES Mail, Postfix, SquirrelMail, Zimbra
Encryption	AxCrypt, Crypt, Cryptacular, GNU Privacy Guard, John the Ripper, Mac GNU Privacy Guard, NeoCrypt, Network Security Services (NSS), OpenSSL, TrueCrypt
Enterprise Applications	Open Atrium, Open Source Corporate Management Information Systems (OSCMIS), WorldVistA
File Transfer	CyberDuck, FileZilla, Fugu, Samba, vsftpd, WinSCP
Filtering	DansGuardian, IP Tables, Java EE PDF uXSS Filter, Web Scarab
Firewall	Devil Linux, Endian Firewall Community, ferm, Firestarter, Firewall Builder, IP Cop, m0n0wall, ModSecurity, NetCop UTM, Open WAF, pfSense, Sentry Firewall, Shorewall, Smoothwall, Turtle Firewall, Untangle, Vuurmuur, Wyatta, Zentyal
Forensics	BackTrack, LibHTP, Maltego, Mobius Forensics Toolkit, mod_sslhaf, ODESSA, tcpdump, tcpindex, The Sleuth Kit/Autopsy Browser, WinDump, WinPcap, Wireshark
Geographic Information Systems (GIS)	Falcon View, Open Streetmap, Opticks, PGGIS
Host Based IPS (HIPS)	AFICK (Another File Integrity Checker), Open Source Tripwire, OSSEC
ID Authentication Methods	WiKID
Information Technology Infrastructure	Dradis, OpenCPI
Intrusion Detection & Monitoring	ackack, Kismet, Munin, Open Source Tripwire, OpenVAS, Process Hacker, Suricata, Thicknet, Zabbix

CATEGORY	APPLICATION(S)
Intrusion Detection & Prevention Systems (IDS/IPS)	Fail2Ban, IronBee, OSSEC, QuIDScor, Snort, Suricata
Monitoring Systems	Cacti, ICINGA, Nagios, NetDB, OpenNMS, PandoraFMS, Zabbix, Zenoss
Network	ackack, AFTR, BIND, BIND 10, Bird, BSD Router, ISC DHCP, Munin, Netcat, NetDR, Nmap, Quagga, Samba, Squid
Network Communications Protection	OpenSSH, OpenSSL, Squid
Operating System (OS)	Android, Arch Linux, BackTrack, CentOS, ClearOS, Cygwin, Debian Linux, Devil Linux, Endian Firewall Community, Fedora, FreeBSD, Gentoo, IP Cop, Knoppix, Kubuntu, Lightweight Portable Security (DoD Linux Distro), m0n0wall, Mandriva Linux, NetBSD, NetCop UTM, OpenBSD, openSUSE, Openwall GNU/Linux (OWL), Red Hat Enterprise Linux, Samuri WTF, Sentry Firewall, Slackware, Smoothwall, SUSE Enterprise, Ubuntu, Untangle, Zentyal
OS Hardening	AppArmor, Bastille Unix, Gentoo Hardened Profile, SE Linux
Password Management	KeePass Password Safe, KeePassX, Passkool, Password Maker, Password Safe
Penetration Testing & Vulnerability Assessment	Airoscript-NG, Angry IP Scanner, Auto Scan, BackTrack, batchyDNS, Cacti, Deblaze, Deface, Graudit, inSSIDer, JBoss Autopwn Script, JBroFuzz, JSP Tester, KisMAC, Kismet, Lynis, Metasploit, Nmap, Ophcrack, Peach Fuzzing Platform, QuIDScor, SQL Map, tcpindex, Vega, W3AF, Wireshark
Problem Management	BugZilla, Request Tracker
Program Analysis	AntiSamy, Apparat, Avalanche, BLAST: Berkeley Lazy Abstraction Software Verification Tool, Blind Elephant, Checkstyle, ClamWin, CppCheck, CQUAL, CSRF Guard, Dmalloc, DynInst, FindBugs, Flawfinder, Frama-C, Gendarme, JavaSnoop, Jchord, JSP Tester, LibHTP, Moon Secure Antivirus, Moose, Orizon, Pixy, PMD Copy/Paste Detector, ROSE, RTL-Check, Scrubbr, Simple Machine Protect, Smatch, Sonar, Soot, Sparse, Splint, Squale, Stanse, StyleCop, Valgrind, Yasca
Remote Access Methods Clients	NoMachine, OpenSSH, OpenSSL, PuTTY, PuTTY CAC, TightVNC
Revision Control	CVS, Fossil, git, Mercurial, Subversion
Security Planning Tools	Metasploit, spt (Simple Phishing Toolkit), WebGoat
Storage Tools	DRDB, OCFS 2, Openfiler, Orange FS, Sheepdog, Swift
Virtualization	Cygwin, KeepAlived, KVM, OpenStack Compute, OVM, Packetyzer, VirtualBox, Xen
Visualization	ParaView
VPN	Cacti, OpenVPN
Vulnerability Patch Management	Lynis, Niklo2, OpenVAS, Rogue Scanner
Web Accessibility	Chromium, Konqueror, Mozilla Firefox
Web Server Software	Apache, Apache Tomcat, Drupal, Enterprise Security API, Jboss Autopwn Script, JBoss Enterprise Application Platform, Lucene, mod_sslhaf, NGINX, Nikto2, Open Atrium, Plone, WebFSD, Zimbra, Zope
Web Services	AW Stats, Classic ASP Security Image Generator (CAPTCHA), Django, Joomla, MediaWiki, PIWIK, Plone

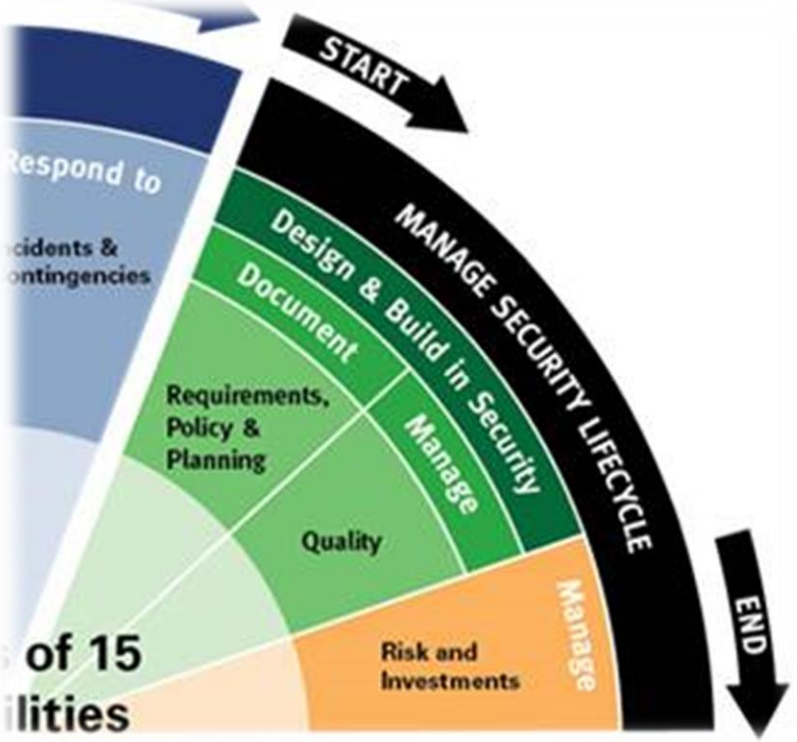
SecTools.org and DHS Research Program





Security Lifecycle challenges and advice

- How do you design and build in security when the software, hardware, and medical devices come from third parties?
- What risk management and investment prioritization frameworks should you use?
- Are you using a bottom-up risk assessment or top-down risk cataloging process?

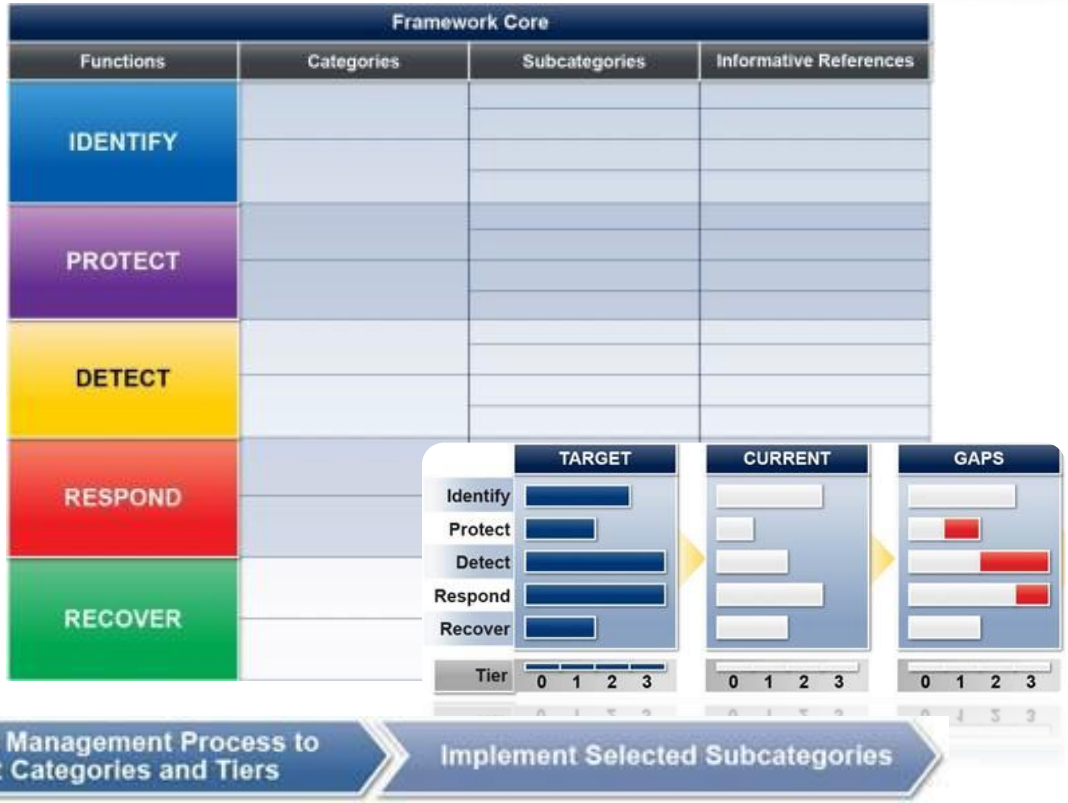


Cybersecurity Framework

- Developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk
- Supports the improvement of cybersecurity for the Nation's Critical Infrastructure using industry-known standards and best practices
- Provides a common language and mechanism for organizations to
  - describe current cybersecurity posture;
  - describe their target state for cybersecurity;
  - identify and prioritize opportunities for improvement within the context of risk management;
  - assess progress toward the target state;
  - Foster communications among internal and external stakeholders.
- Composed of three parts: the Framework Core, the Framework Implementation Tiers, and Framework Profiles

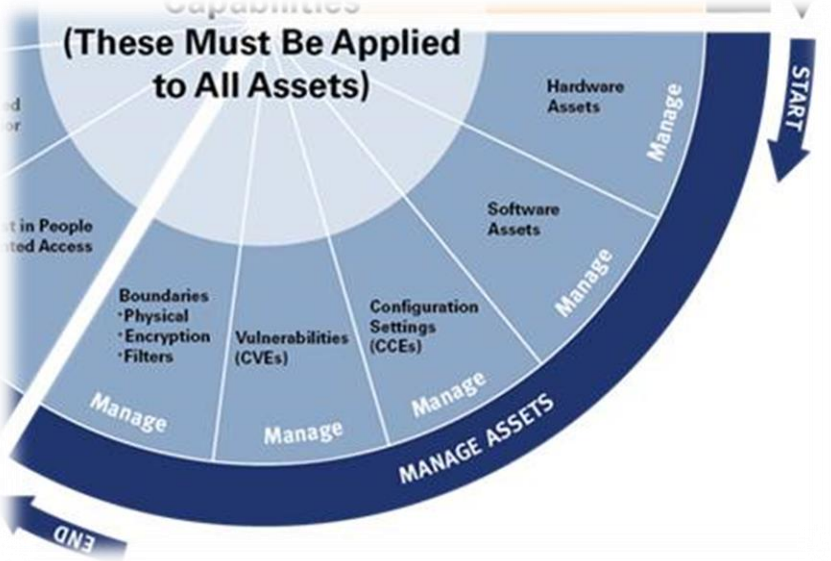
NIST Cybersecurity Framework

Function	Category
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management
PROTECT	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Protective Technology
DETECT	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
RESPOND	Communication
	Analysis
	Mitigation
	Improvements
RECOVER	Recovery Planning
	Improvements
	Communication

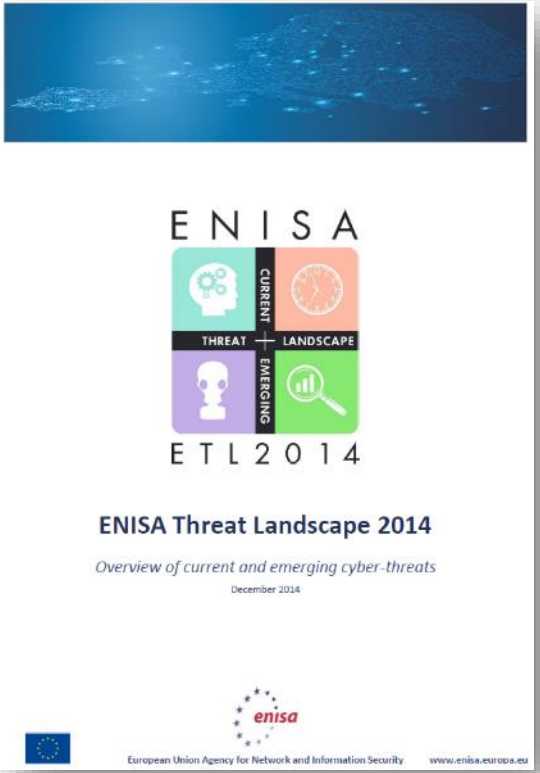


Asset management challenges and advice

- Where is your hardware and software inventory stored?
- How are you tracking configuration settings?
- Who's curating your vulnerabilities?
- How are your boundaries documented?



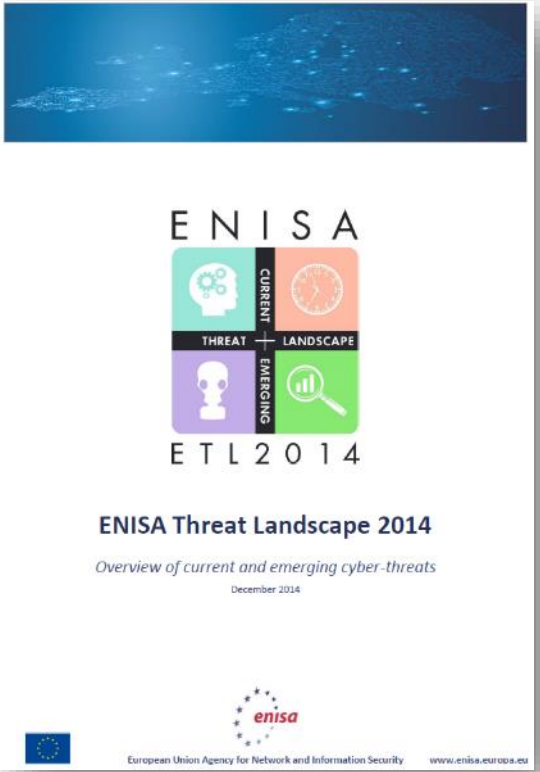
ENISA Threat Landscape



Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

ENISA Threat Agents



	Threat Agents								
	Corporations	Nation States	Hacktivists	Cyber Terrorists	Cyber Criminals	Cyber Fighters	Script Kiddies	Online Social Hackers	Employees
Malicious code: Worms/Trojans	✓	✓	✓	✓	✓	✓			✓
Web-based attacks	✓	✓	✓	✓	✓	✓		✓	
Web application /Injection attacks	✓	✓	✓	✓	✓	✓	✓		
Botnets			✓		✓				
Denial of service	✓	✓	✓	✓	✓	✓			
Spam				✓	✓	✓	✓	✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Exploit kits		✓	✓	✓	✓	✓	✓		✓
Data breaches	✓	✓	✓	✓	✓	✓		✓	✓
Physical damage/theft /loss	✓	✓	✓	✓	✓	✓			✓
Insider threat	✓	✓	✓	✓	✓	✓			✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Identity theft/fraud	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyber espionage	✓	✓							✓
Ransomware/ Rogueware/ Scareware					✓				

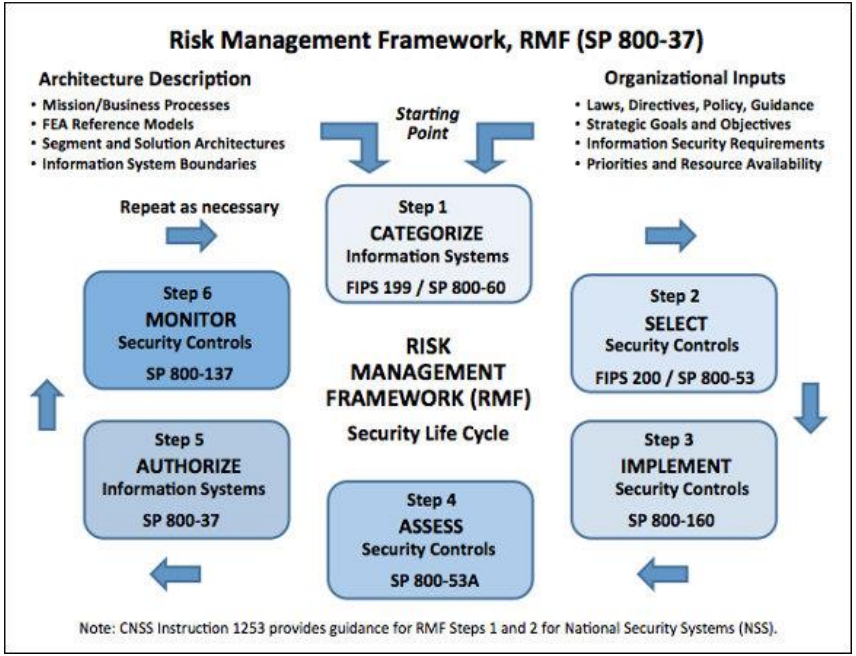
Accounts management challenges & advice

- Do you have identity, credentialing, and access management (ICAM) or just IAM?
- Do you have user behavior analytics (UBA) capabilities?
- Is your training tied to specific risks and assets from a bottom-up perspective?

Event management challenges & advice

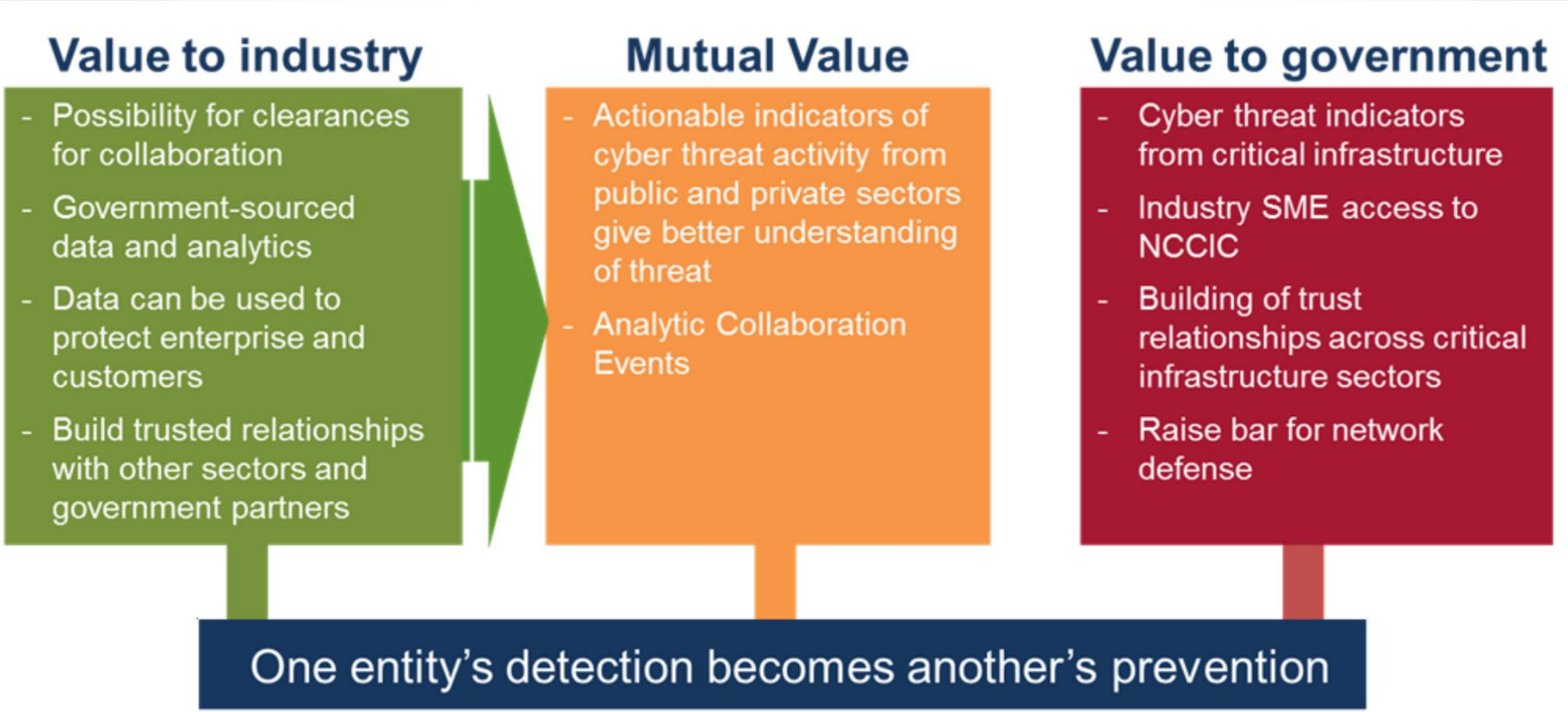
- How sophisticated is your security information and event management (SIEM) infrastructure?
- Do you run breach and incident simulations to help prepare for contingencies?
- Do you have a data spill or other incident response plan documented and ready to execute?

ISAOs as a Model for Regional Cooperation



http://www.dhs.gov/isao

ISAO Value Proposition

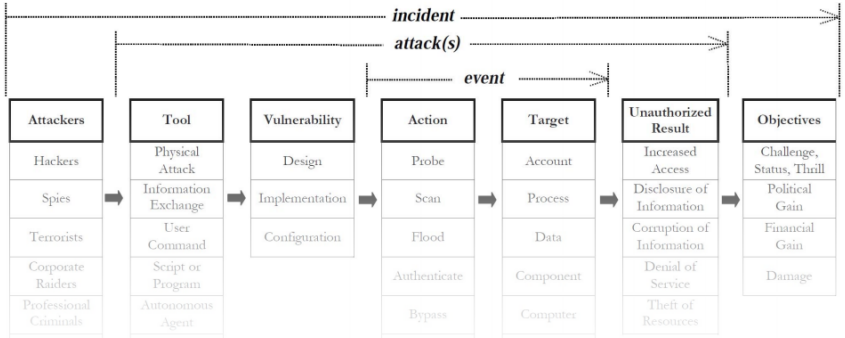


https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf

ISAOs and Coordinating Processes

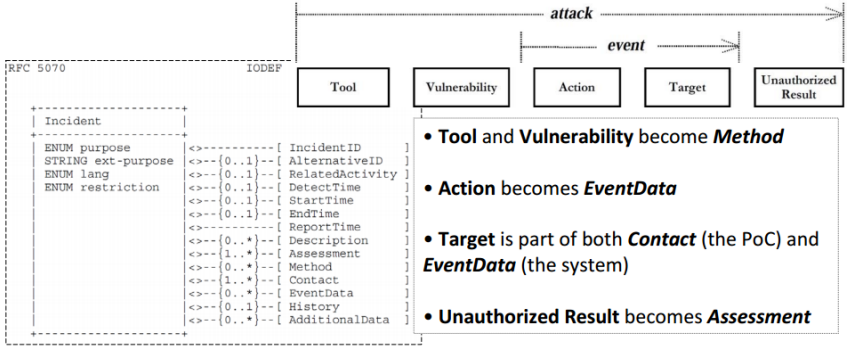
A CSIRT Process Model for Improving Information Sharing & Knowledge Capture in Cybersecurity
https://www.itu.int/dms_pub/itu-t/oth/06/35/T063500000200515PDFE.pdf

Starting Point: Howard & Longstaff



This 7-part taxonomy appears in "A Common Language for Computer Security Incidents" from 1998, by John Howard & Tom Longstaff, published by Sandia National Labs.

One Implementation: The IODEF



5 of the 7 parts from Howard & Longstaff's taxonomy were adopted as data element classes in the IETF's Incident Object Definition Exchange Format, an XML schema for cyber incident reporting.

Security Information Interoperability

- **Standardized Language**
  - Structured Threat Information Expression

STIX™

- **Standardized Exchange Mechanism**
  - Trusted Automated Exchange of Indicator Information

TAXII™

- **Make it easier to express, exchange, consume, and correlate cyber threat intelligence**

- **Large group of contributing parties**
- **Used by real products/communities**
- **Supported by an active community and running code**

http://secure360.org/wp-content/uploads/2014/05/Threat-Intelligence-Sharing-using-STIX-and-TAXII.pdf

Visit http://www.netspective.com
E-mail shahid.shah@netspective.com
Follow @ShahidNShah
Call 202-713-5409

Thank You

Netspective
EXTENDING THE ENTERPRISE