4/25/2017

CISO Playbook

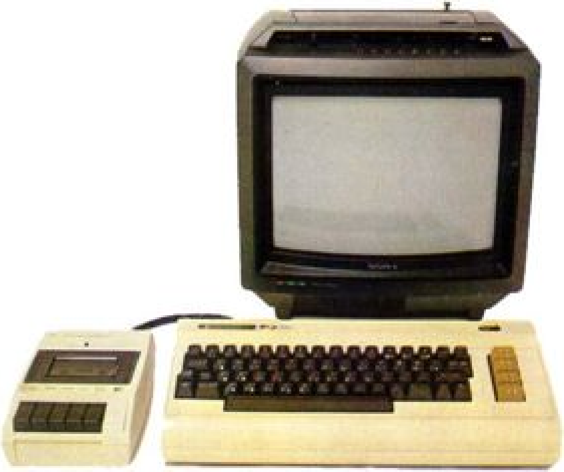
John McLeod, AlienVault

Breaking News

- DISCLAIMER: The opinions expressed in this presentation are my own and may not reflect the opinions of my company.

whoami

- AlienVault Chief Information Security Officer
- Mandiant, Guidance Software, Halliburton and National Oilwell Varco
- Retired AFOSI computer crime investigator
- 20+ years of computer security experience
- First computer:



State of the Hack

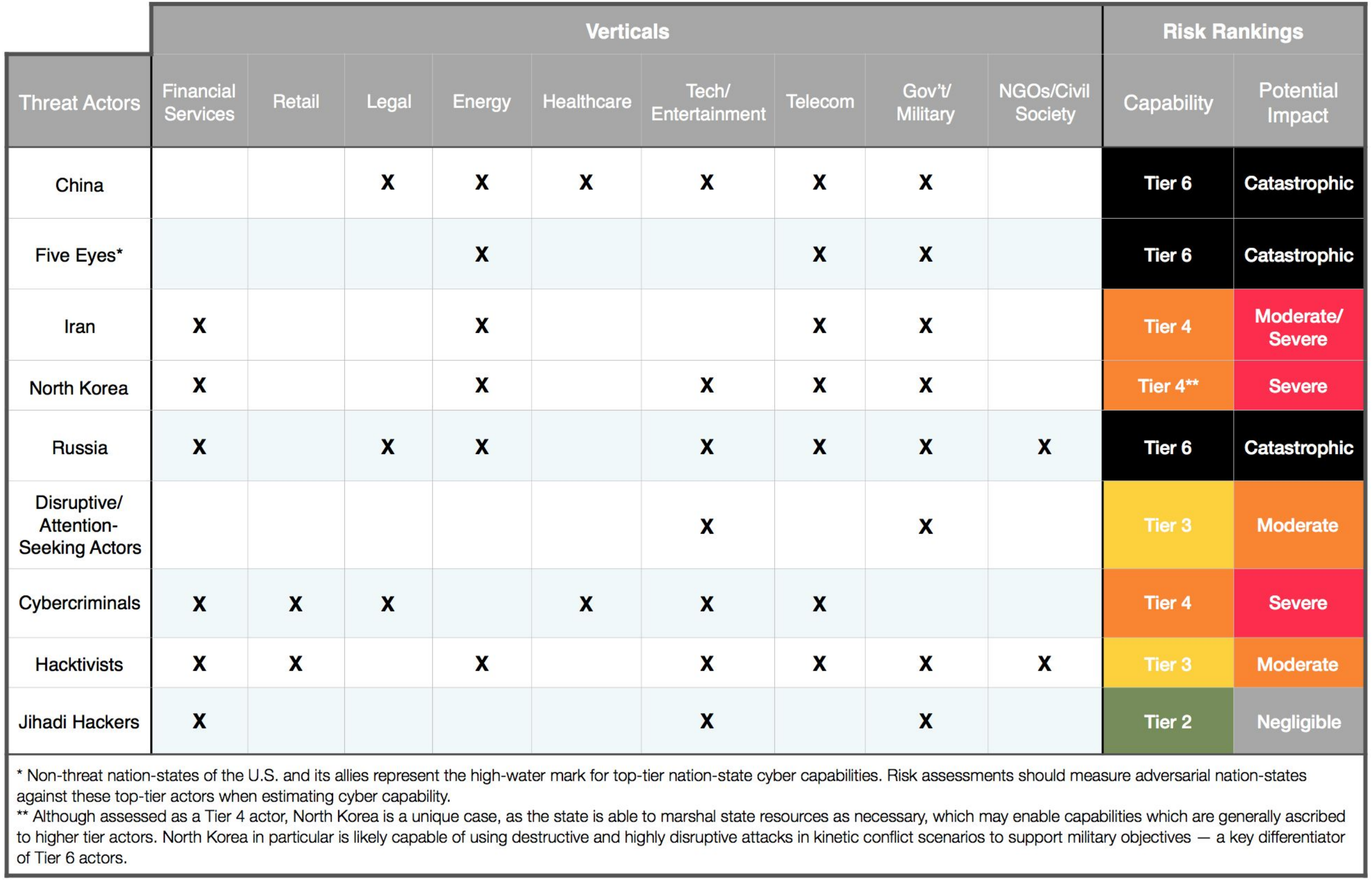
- Mandiant
  - Attackers are calling their targets directly
  - Nation-state-sponsored APTs continued to harvest systems for PII
  - Global median time from compromise to discovery has dropped significantly from from <u>146</u> days in 2015 to <u>99</u> days 2016, but it is still not good enough

- Crowdstrike
  - The use of anti-forensic tools to cover the attacker's tracks
  - Third-party trust relationships introduce significant risks
  - Malware-free intrusions have become the norm

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
https://www.crowdstrike.com/resources/reports/crowdstrike-cyber-intrusion-services-casebook-2016

State of the Hack

FLASHPOINT



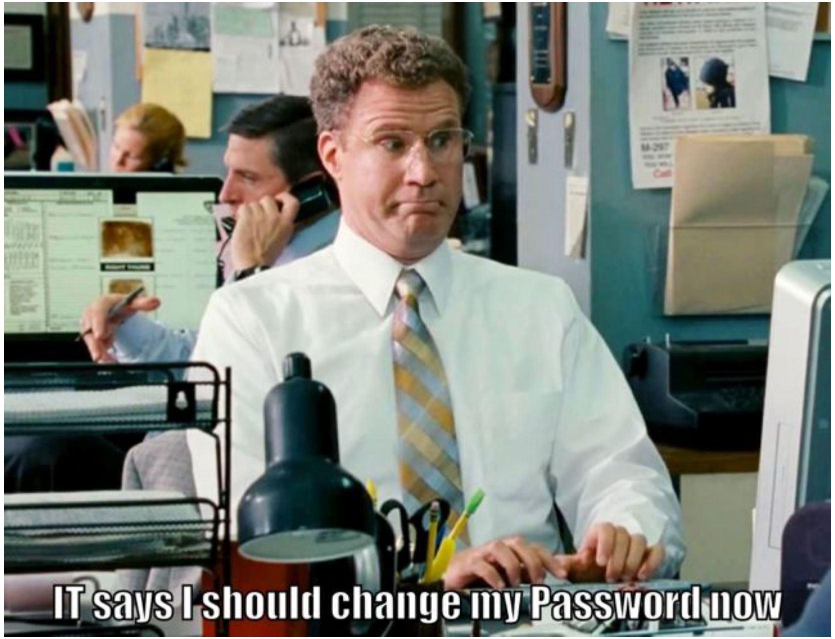
	Verticals									Risk Rankings	
Threat Actors	Financial Services	Retail	Legal	Energy	Healthcare	Tech/ Entertainment	Telecom	Gov't/ Military	NGOs/Civil Society	Capability	Potential Impact
China			X	X	X	X	X	X		Tier 6	Catastrophic
Five Eyes*				X			X	X		Tier 6	Catastrophic
Iran	X			X			X	X		Tier 4	Moderate/ Severe
North Korea	X			X		X	X	X		Tier 4**	Severe
Russia	X		X	X		X	X	X	X	Tier 6	Catastrophic
Disruptive/ Attention-Seeking Actors						X		X		Tier 3	Moderate
Cybercriminals	X	X	X		X	X	X			Tier 4	Severe
Hacktivists	X	X		X		X	X	X	X	Tier 3	Moderate
Jihadi Hackers	X					X		X		Tier 2	Negligible

* Non-threat nation-states of the U.S. and its allies represent the high-water mark for top-tier nation-state cyber capabilities. Risk assessments should measure adversarial nation-states against these top-tier actors when estimating cyber capability.

** Although assessed as a Tier 4 actor, North Korea is a unique case, as the state is able to marshal state resources as necessary, which may enable capabilities which are generally ascribed to higher tier actors. North Korea in particular is likely capable of using destructive and highly disruptive attacks in kinetic conflict scenarios to support military objectives — a key differentiator of Tier 6 actors.

State of the Hack – Matter of Fact!

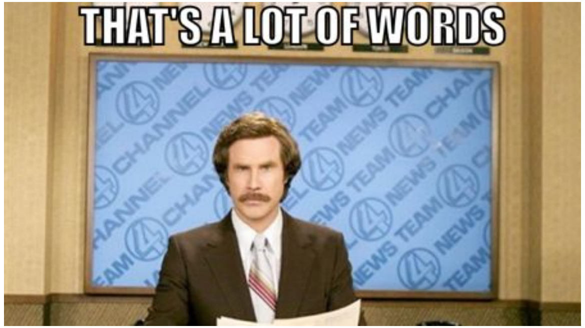
- Every company has at least one person who will click on anything



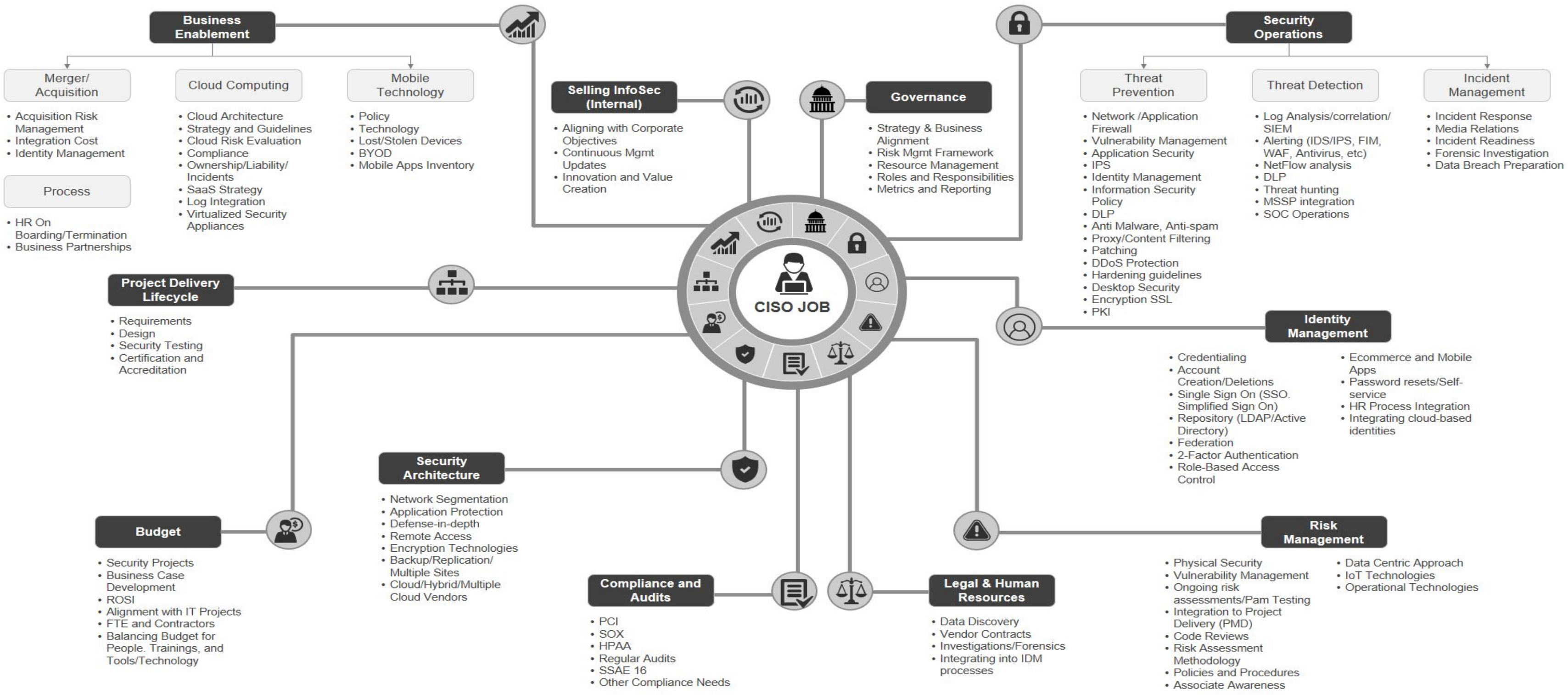
WHAT IS A CISO?

According to Wikipedia

- A chief information security officer (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and information technology (IT) risks. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures.



CISO Mind Map



CISO JOB

Business Enablement

Merger/ Acquisition
- Acquisition Risk Management
- Integration Cost
- Identity Management

Cloud Computing
- Cloud Architecture
- Strategy and Guidelines
- Cloud Risk Evaluation
- Compliance
- Ownership/Liability/ Incidents
- SaaS Strategy
- Log Integration
- Virtualized Security Appliances

Mobile Technology
- Policy
- Technology
- Lost/Stolen Devices
- BYOD
- Mobile Apps Inventory

Process
- HR On Boarding/Termination
- Business Partnerships

Selling InfoSec (Internal)
- Aligning with Corporate Objectives
- Continuous Mgmt Updates
- Innovation and Value Creation

Governance
- Strategy & Business Alignment
- Risk Mgmt Framework
- Resource Management
- Roles and Responsibilities
- Metrics and Reporting

Security Operations

Threat Prevention
- Network /Application Firewall
- Vulnerability Management
- Application Security
- IPS
- Identity Management
- Information Security Policy
- DLP
- Anti Malware, Anti-spam
- Proxy/Content Filtering
- Patching
- DDoS Protection
- Hardening guidelines
- Desktop Security
- Encryption SSL
- PKI

Threat Detection
- Log Analysis/correlation/ SIEM
- Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
- NetFlow analysis
- DLP
- Threat hunting
- MSSP integration
- SOC Operations

Incident Management
- Incident Response
- Media Relations
- Incident Readiness
- Forensic Investigation
- Data Breach Preparation

Project Delivery Lifecycle
- Requirements
- Design
- Security Testing
- Certification and Accreditation

Identity Management
- Credentialing
- Account Creation/Deletions
- Single Sign On (SSO. Simplified Sign On)
- Repository (LDAP/Active Directory)
- Federation
- 2-Factor Authentication
- Role-Based Access Control
- Ecommerce and Mobile Apps
- Password resets/Self-service
- HR Process Integration
- Integrating cloud-based identities

Security Architecture
- Network Segmentation
- Application Protection
- Defense-in-depth
- Remote Access
- Encryption Technologies
- Backup/Replication/ Multiple Sites
- Cloud/Hybrid/Multiple Cloud Vendors

Budget
- Security Projects
- Business Case Development
- ROSI
- Alignment with IT Projects
- FTE and Contractors
- Balancing Budget for People. Trainings, and Tools/Technology

Compliance and Audits
- PCI
- SOX
- HPAA
- Regular Audits
- SSAE 16
- Other Compliance Needs

Legal & Human Resources
- Data Discovery
- Vendor Contracts
- Investigations/Forensics
- Integrating into IDM processes

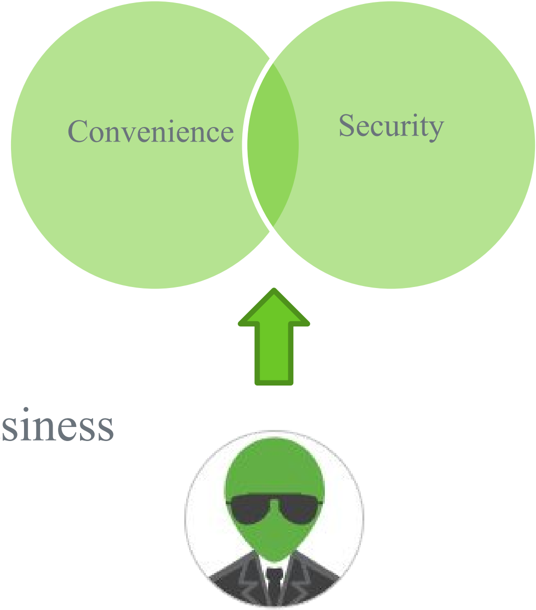
Risk Management
- Physical Security
- Vulnerability Management
- Ongoing risk assessments/Pam Testing
- Integration to Project Delivery (PMD)
- Code Reviews
- Risk Assessment Methodology
- Policies and Procedures
- Associate Awareness
- Data Centric Approach
- IoT Technologies
- Operational Technologies

Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

An Overview of The Responsibilities and Ever Expanding Role of The CISO

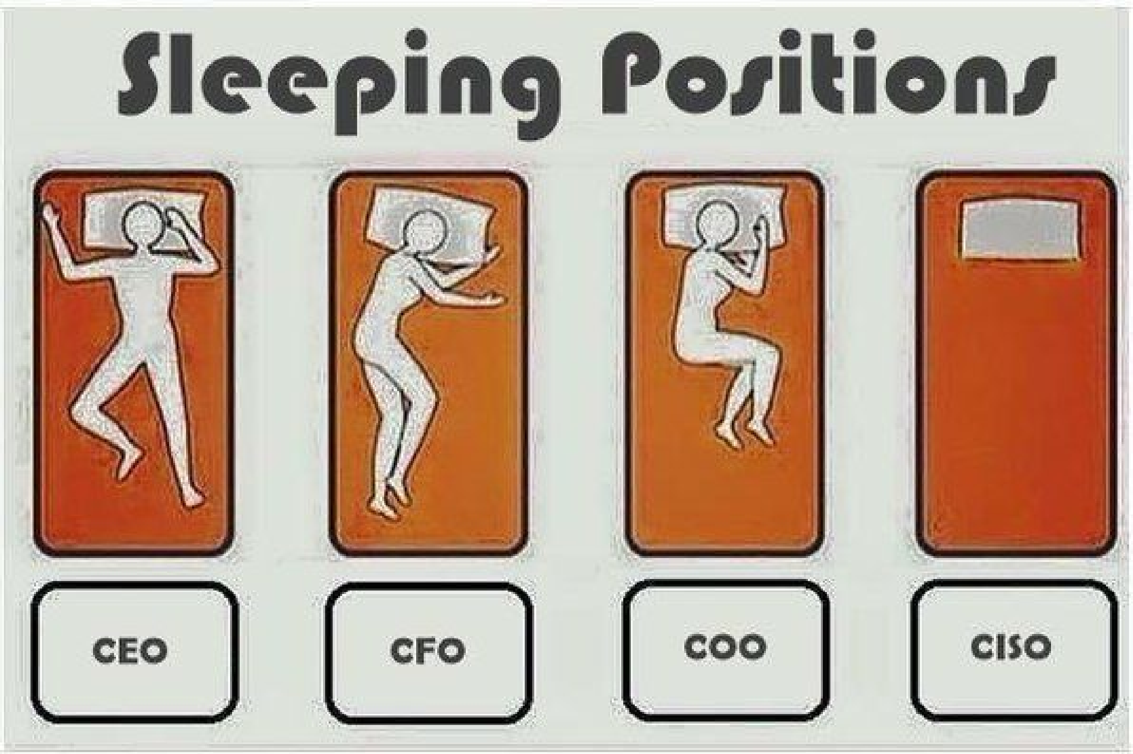
CISO Four focus areas

- Guardian
  - Protect business assets
- Strategist
  - Drive business and cyber risk alignment
- Advisor
  - Educate business on cyber risk
- Technologist
  - Find and implement the right technology for the business



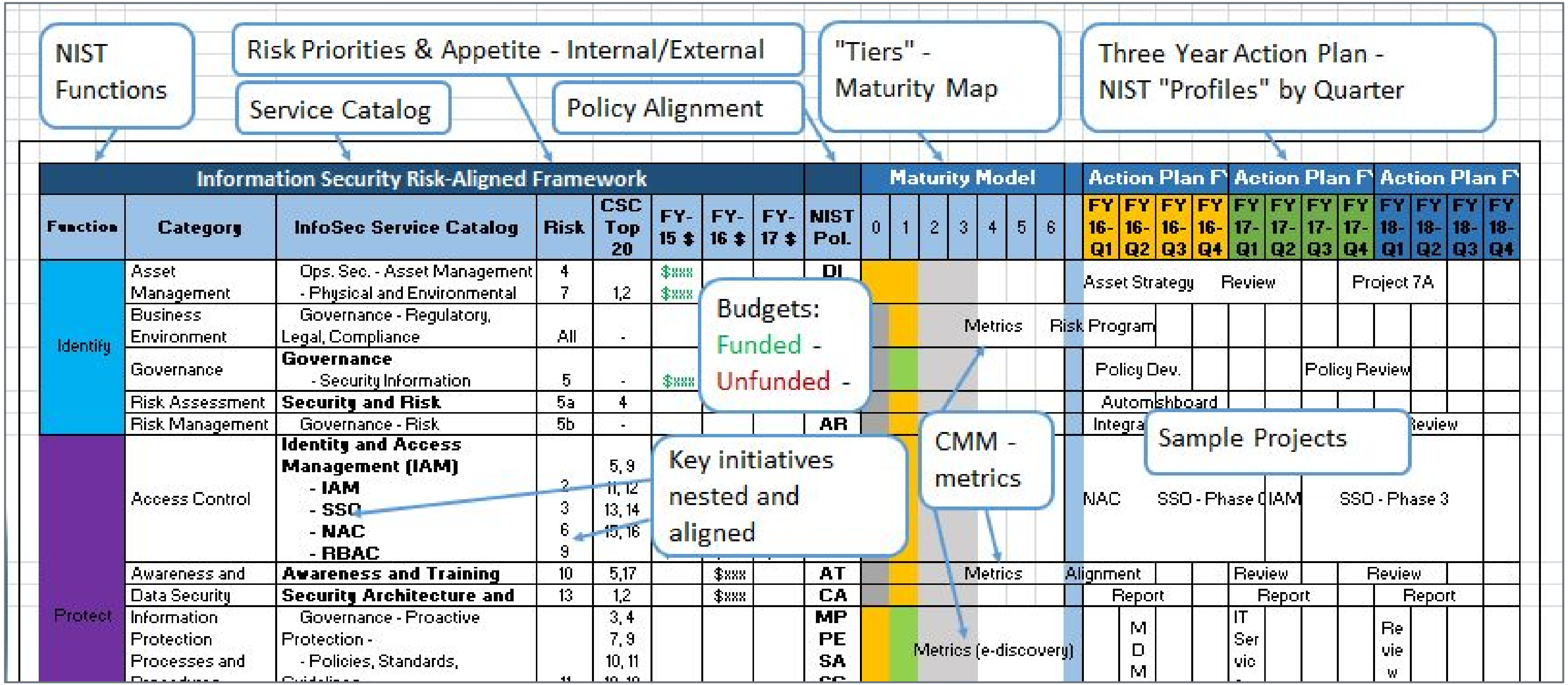
THAT MIND MAP LOOKED EXHAUSTING, HOW ARE YOU SLEEPING?

And how are you sleeping?



SEEMS LIKE A LOT, IS THERE A CISO ROADMAP?

Planning Tool – NIST CSF



NIST Functions

Risk Priorities & Appetite - Internal/External

Service Catalog

Policy Alignment

"Tiers" - Maturity Map

Three Year Action Plan - NIST "Profiles" by Quarter

Budgets: Funded - Unfunded -

Key initiatives nested and aligned

CMM - metrics

Sample Projects

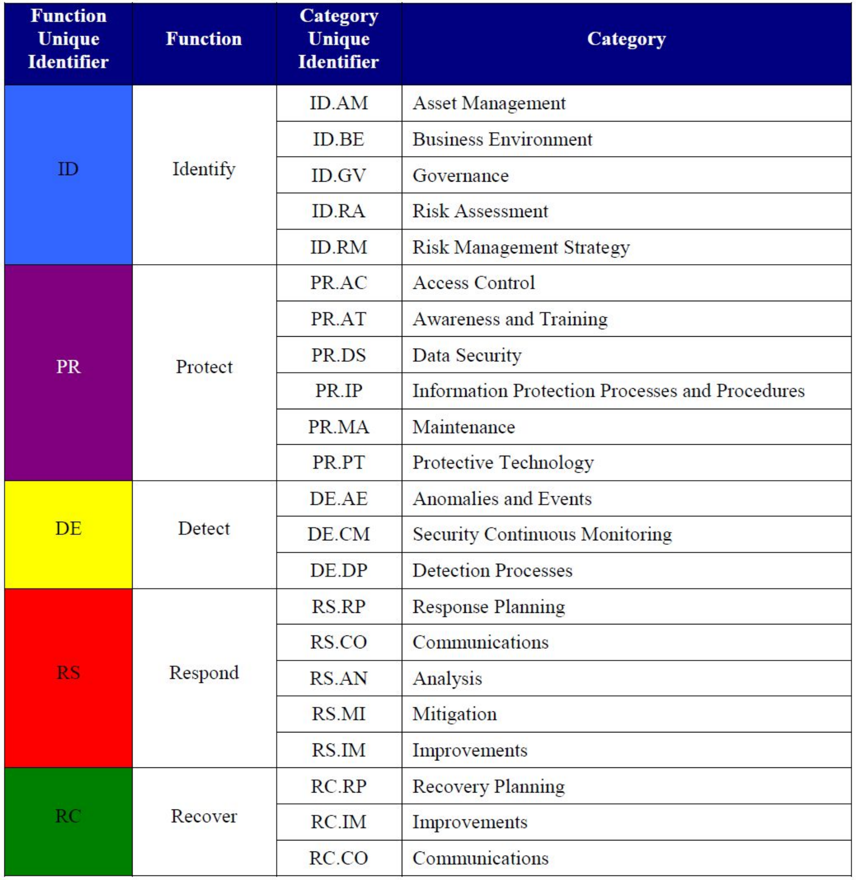
Information Security Risk-Aligned Framework

Function	Category	InfoSec Service Catalog	Risk	CSC Top 20	FY-15 $	FY-16 $	FY-17 $	NIST Pol.
Identify	Asset Management	Ops. Sec. - Asset Management - Physical and Environmental	4 7	1,2	$xxx $xxx			DI
	Business Environment	Governance - Regulatory, Legal, Compliance	All	-				
	Governance	**Governance** - Security Information	5	-	$xxx			
	Risk Assessment	**Security and Risk**	5a	4				
	Risk Management	Governance - Risk	5b	-				AR
Protect	Access Control	**Identity and Access Management (IAM)** **- IAM** **- SSO** **- NAC** **- RBAC**	2 3 6 9	5, 9 11, 12 13, 14 15, 16				
	Awareness and	**Awareness and Training**	10	5,17		$xxx		AT
	Data Security	**Security Architecture and**	13	1,2		$xxx		CA
	Information Protection Processes and	Governance - Proactive Protection - - Policies, Standards,		3, 4 7, 9 10, 11				MP PE SA

NIST Pol.	Maturity Model 0	1	2	3	4	5	6		Action Plan FY FY 16-Q1	FY 16-Q2	FY 16-Q3	FY 16-Q4	Action Plan FY FY 17-Q1	FY 17-Q2	FY 17-Q3	FY 17-Q4	Action Plan FY FY 18-Q1	FY 18-Q2	FY 18-Q3	FY 18-Q4
DI									Asset Strategy			Review				Project 7A				
				Metrics		Risk Program														
									Policy Dev.						Policy Review					
									Automshboard											
AR									Integra								eview			
									NAC		SSO - Phase		IAM			SSO - Phase 3				
AT				Metrics					Alignment				Review			Review				
CA									Report				Report				Report			
MP PE SA			Metrics (e-discovery)							M D M			IT Ser vic				Re vie w			

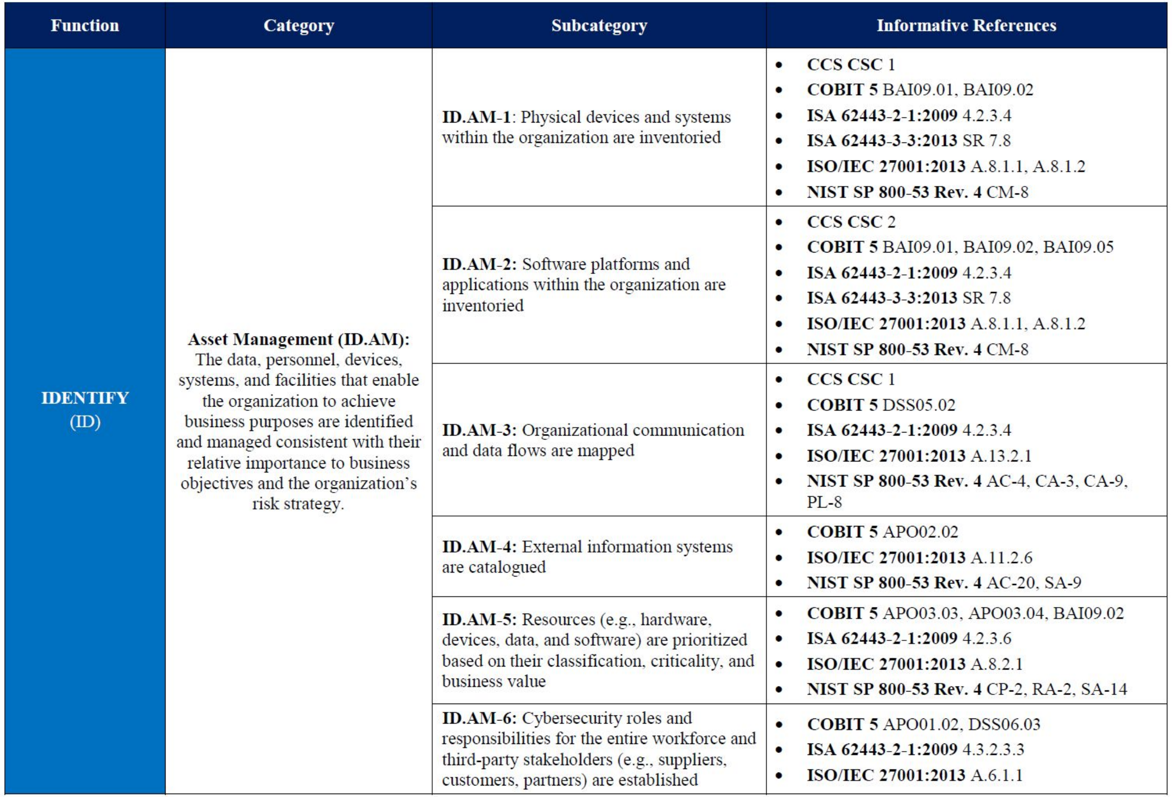
Christopher Paidhrin, City of Portland, OR – Planning tool
http://www.tenable.com/whitepapers/nist-csf-implementation-planning-tool

NIST Cyber Security Framework



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Map Security Controls to the Framewor



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

HOW MANY SECURITY CONTROLS ARE THERE?

Cyber Security Standards

- Each standard has a set of security controls:
  - Sarbanes-Oxley
  - NERC
  - PCI DSS
  - HIPAA
  - COBIT
  - ISO 27001
  - ISA/IEC-62443
  - FISMA
  - GDRP
  - ETC…

Thousands of security controls but many overlap

Is Security, Compliance?

- Security is not Compliance and Compliance is not Security
- Security is a Journey
    - If you do security right, compliance is easy

WHERE DO WE START?

Top 20 Critical Security Controls

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports

0. Data Recovery Capability

11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.cisecurity.org/critical-controls.cfm

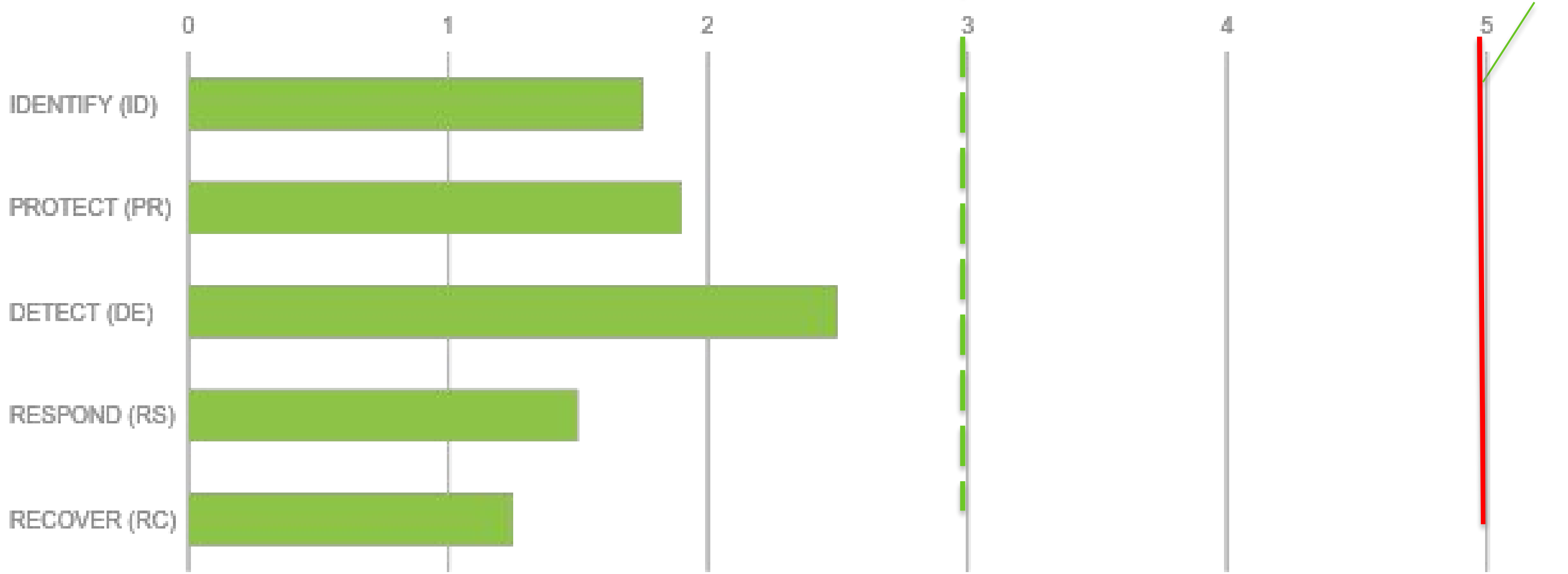
WE HAVE CONTROLS… NOW WHAT?

Cyber Security Maturity Level - example

Where you should be

Department of Defense

Today



Take Away

- Balance risk and cost
- Prioritize work based on risk
- Establish top-notch security incident management
- Use resources and knowledge outside my team effectively
- Must have a roadmap
- Incidents expected, must have a controlled response

Questions