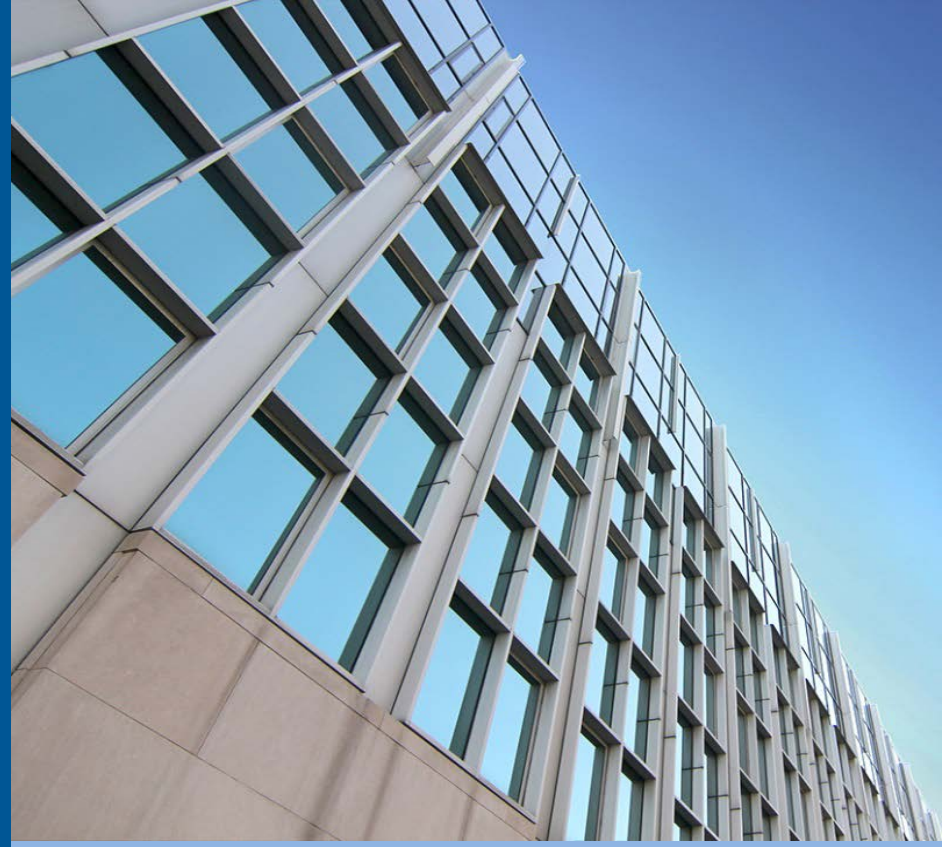
Structuring the Chief Information Security Officer Organization



December 1, 2015

Julia Allen
Nader Mehravari

Cyber Risk and Resilience Management Team
CERT Division
Software Engineering Institute
Carnegie Mellon University
http://www.cert.org/resilience/

Notices

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003092

Topics

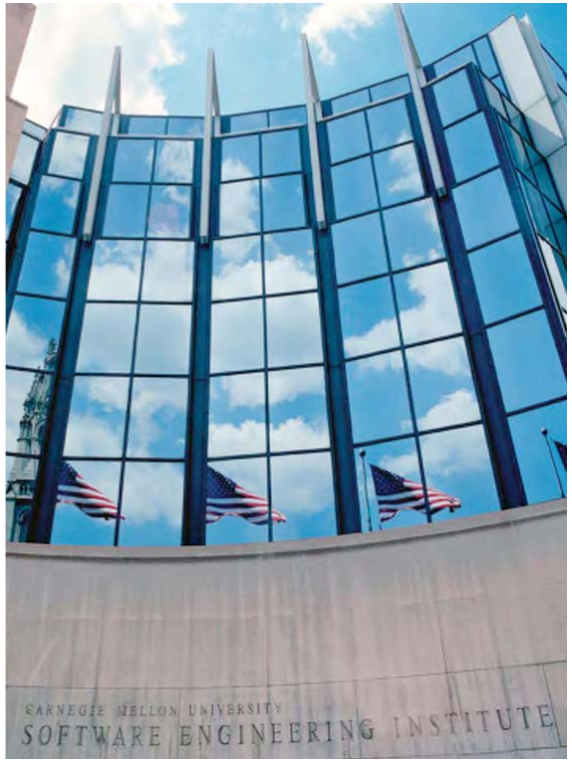
Process for determining a CISO organizational structure

- Four key CISO functions
- Sources of best practices
- Subfunctions, activities, and departments

Candidate CISO organizational structure

Recommended next steps

CERT Division | Software Engineering Institute | Carnegie Mellon University



Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally funded research and development center based at Carnegie Mellon University
- Basic and applied research in partnership with government and private organizations
- Helps organizations improve development, operation, and management of software-intensive and networked systems

CERT Division – *Anticipating and solving our nation's cybersecurity challenges*

- Largest technical program at SEI
- Focused on internet security, secure systems, operational resilience, and coordinated response to security issues

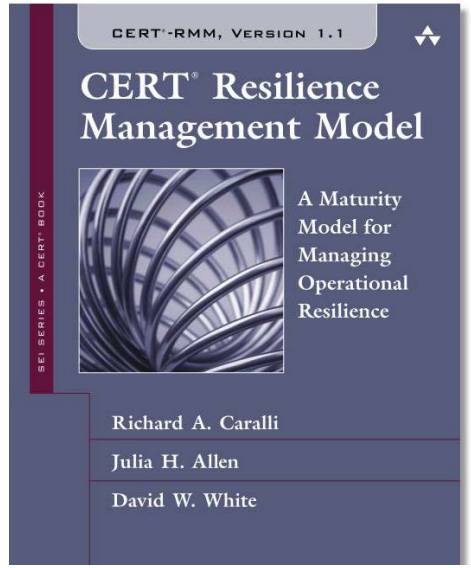
Cyber Risk & Resilience Management Activities

Engaged in

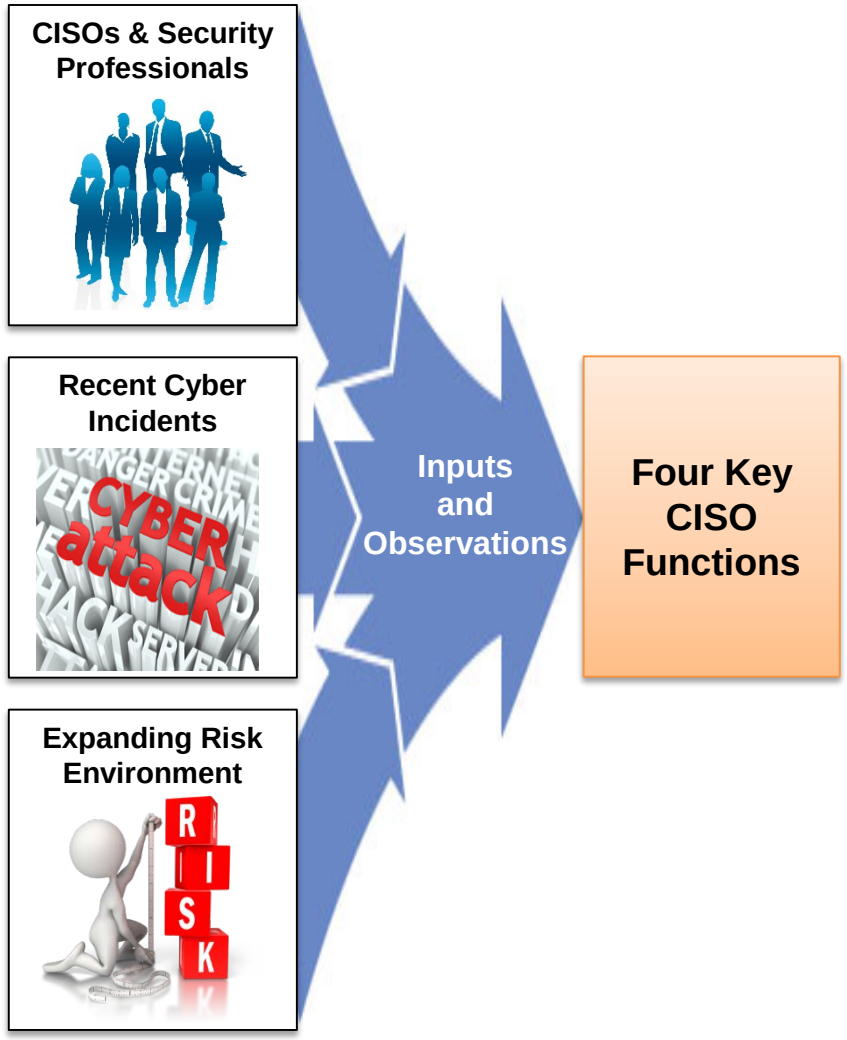
- Applied research
- Education & training
- Putting into practice
- Enabling our federal, state, and commercial partners

In areas dealing with

- Resilience Management
- Operational Risk Management
- Cyber and Resilience Frameworks
- Integration of cybersecurity, business continuity, & disaster recovery



Process for Determining Organizational Structure



Process for Determining Organizational Structure *(cont.)*

Developed the 4-function structure in conversations with CISOs and security professionals

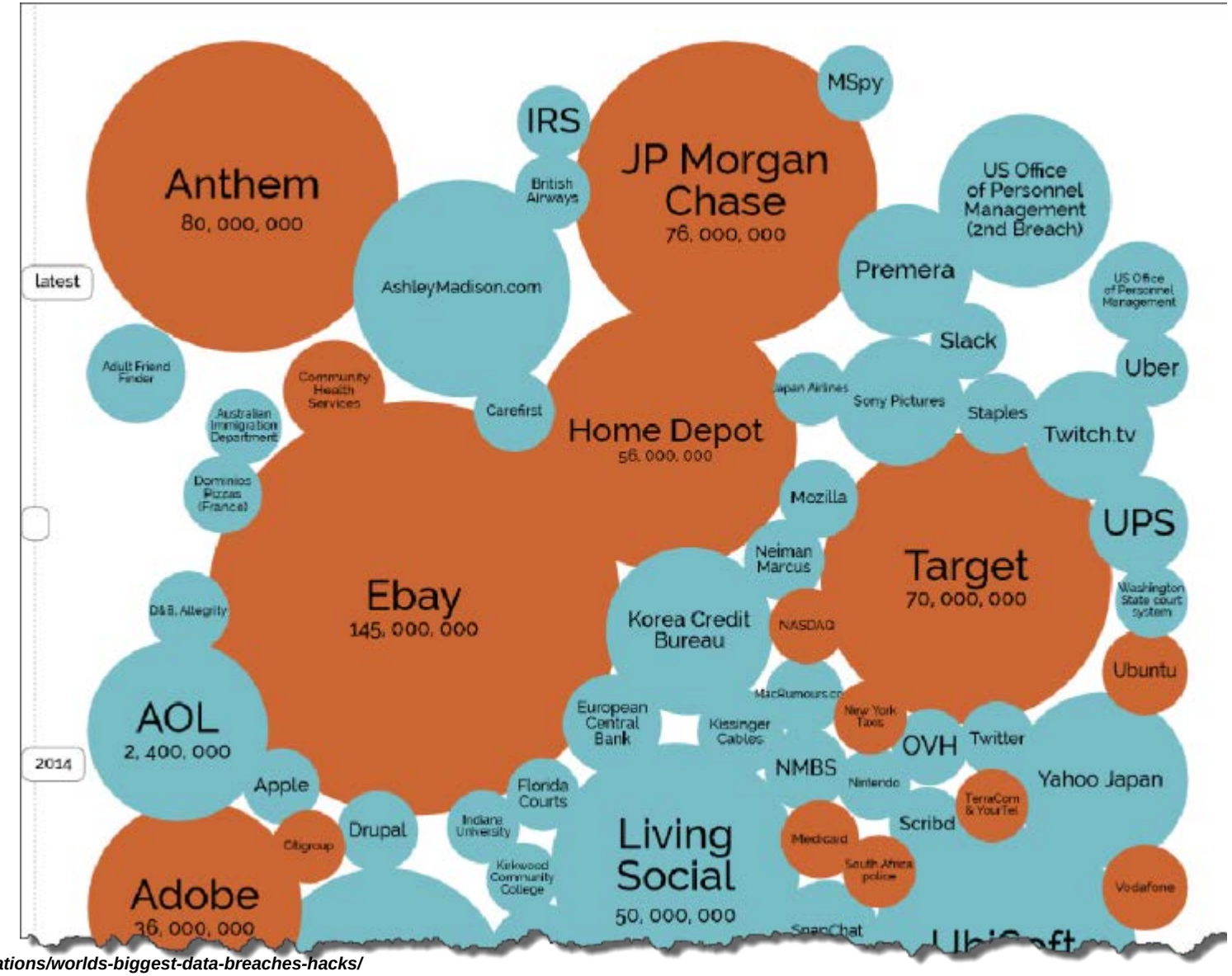
The Four Key Functions of a Modern CISO

Traditional Information Security Function

Protect / Shield / Defend / Prevent

Cyber Intrusions Are a Fact of Life

Cyber Intrusions Are a Fact of Life



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Traditional Information Security Function

Protect / Shield / Defend / Prevent

- Is necessary
- Is not sufficient
- Fails too frequently

Targeted Attacks Are Hard to Detect

How are compromises detected?

69%

of victims were notified by an external entity

How long before the compromises are detected?

205

median number of days before detection

SOURCE: Mandiant® "M-Trends® 2015: A View from the Front Lines" Report

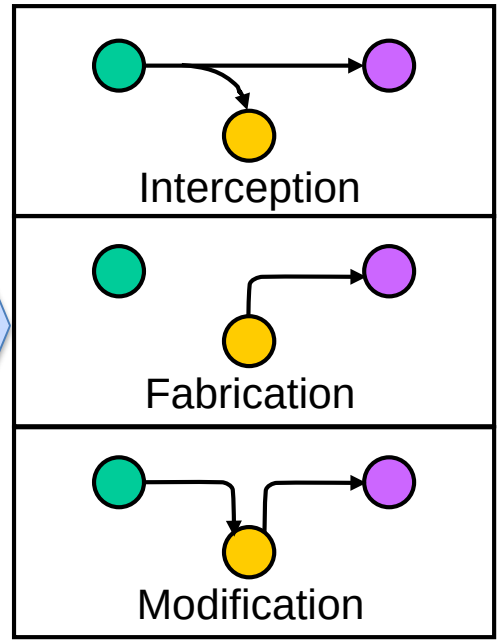
Towards Modern CISO Functions

Protect / Shield / Defend / Prevent	Monitor / Detect / Hunt
	

- Is necessary
- Is not sufficient
- Not immediate
- Takes too long

Most Frequent Cyber Attacks Fallouts

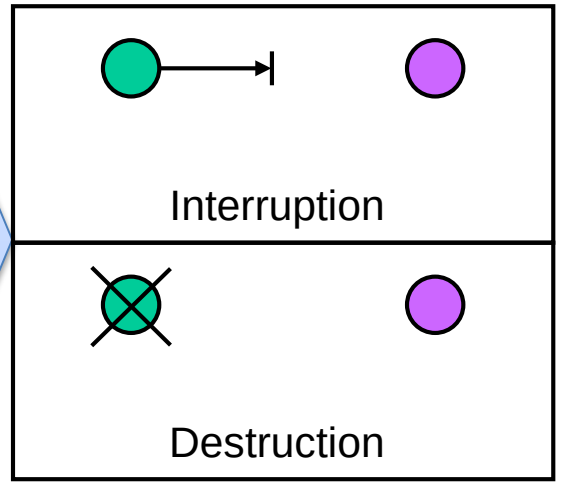
- Disclosure of operationally sensitive information
- Disclosure of privately identifiable information
- Theft of intellectual property
- Theft of user access credentials
- Loss of credit card information
- Disclosure of classified information
- Revealing of company proprietary information
- Exposure of corporate email messages
- Identifying oppositions and enemies
- Leak of trade secrets
- Nuisance
- Reputation damage
- Hacktivism - Delivering political or social message
- Blackmailing



However,

adversaries are interested in more…

- Deleting and destroying data
- Causing operational havoc
- Physical harm to people
- Physical damage to infrastructure
- Destruction of physical goods
- Damaging critical infrastructure
- Affecting delivery of products and services
- Shutting down day-to-day business operations



Example: Sony Pictures Cyber Incident

Reputation

Revenue Loss

Data Exfiltration

- Over 100 terabytes

Business Operations

- Damaged information technology infrastructure
- Hackers implanted and executed malware that destroyed data
- Malware with capability to overwrite master boot records and data files

Legal

- Employees have filed four lawsuits against the company for not protecting their data

Breach Expenses

- In its first quarter financials for 2015, Sony Pictures set aside $15 million to deal with ongoing damages from the hack.

Towards Modern CISO Functions

Protect / Shield / Defend / Prevent	Monitor / Detect / Hunt	Respond/ Recover / Sustain
		

Modern Information Security Functions

Protect / Shield / Defend / Prevent	Monitor / Detect / Hunt	Respond/ Recover / Sustain
		

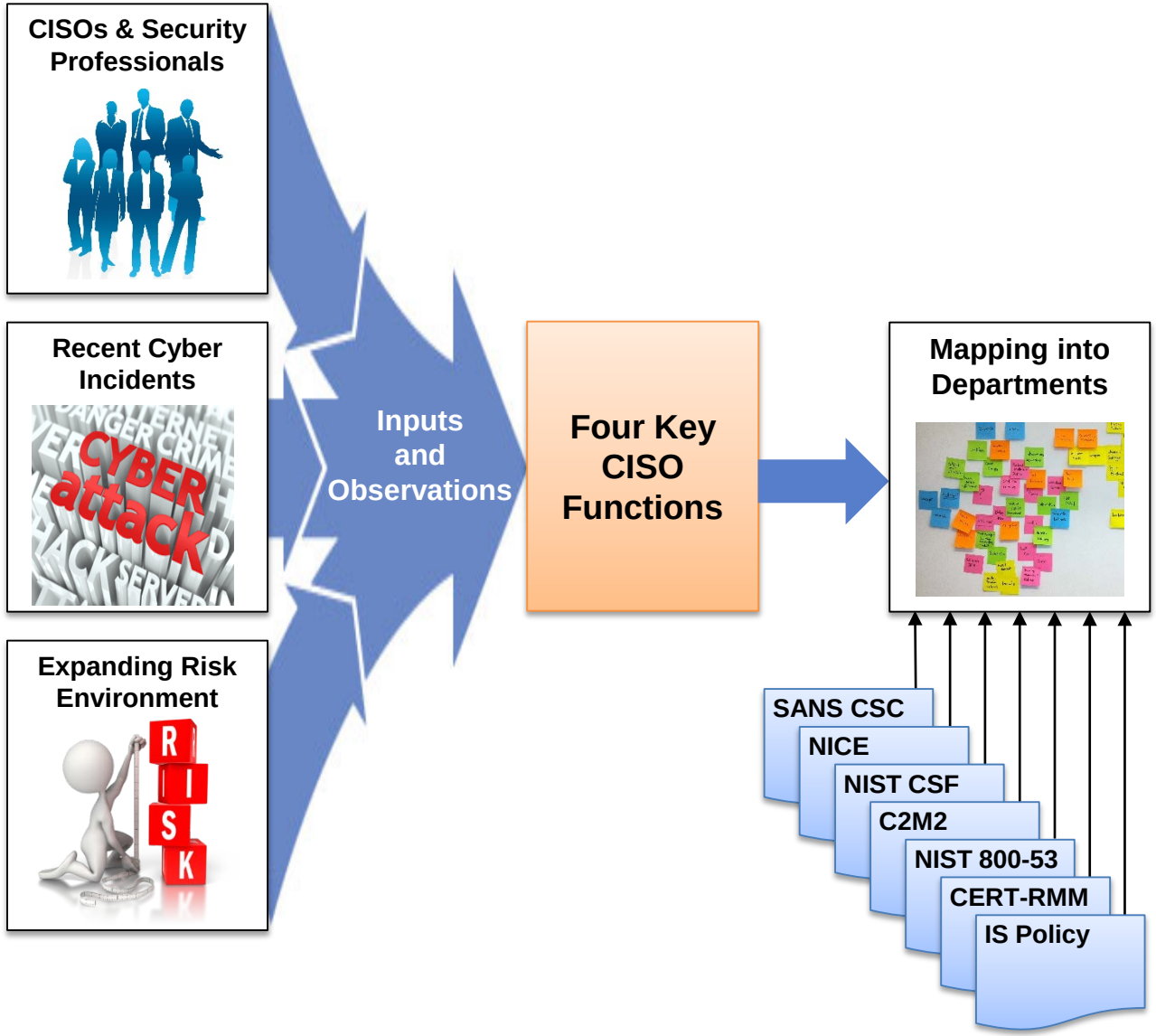
Management,
Governance,
Compliance,
Education,
Risk Management.

Polling Question

Do these four functions cover your current or planned CISO responsibilities?

- ❑ Yes
- ❑ Partially
- ❑ No

Process for Determining Organizational Structure



Process for Determining Organizational Structure *(cont.)*

Developed the 4-function structure in conversations with CISOs and security professionals

Identified relevant sources of best practices for the 4 functions

Sources

- A typical information security policy for a large, diverse organization
- NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- National Initiative for Cybersecurity Education (NICE) The National Cybersecurity Workforce Framework Version 1.0
- SANS Critical Security Controls
- CERT Resilience Management Model, version 1.1
- U.S. Department of Energy Cybersecurity Capability Maturity Model (C2M2)
- Industry-wide research reports

(*) We did not specifically map to the ISO 27001/2 series. All of this content is covered by the combined sources.

Process for Determining Organizational Structure *(cont.)*

Developed the 4-function structure in conversations with CISOs and security professionals

Identified relevant sources of best practices for the 4 functions

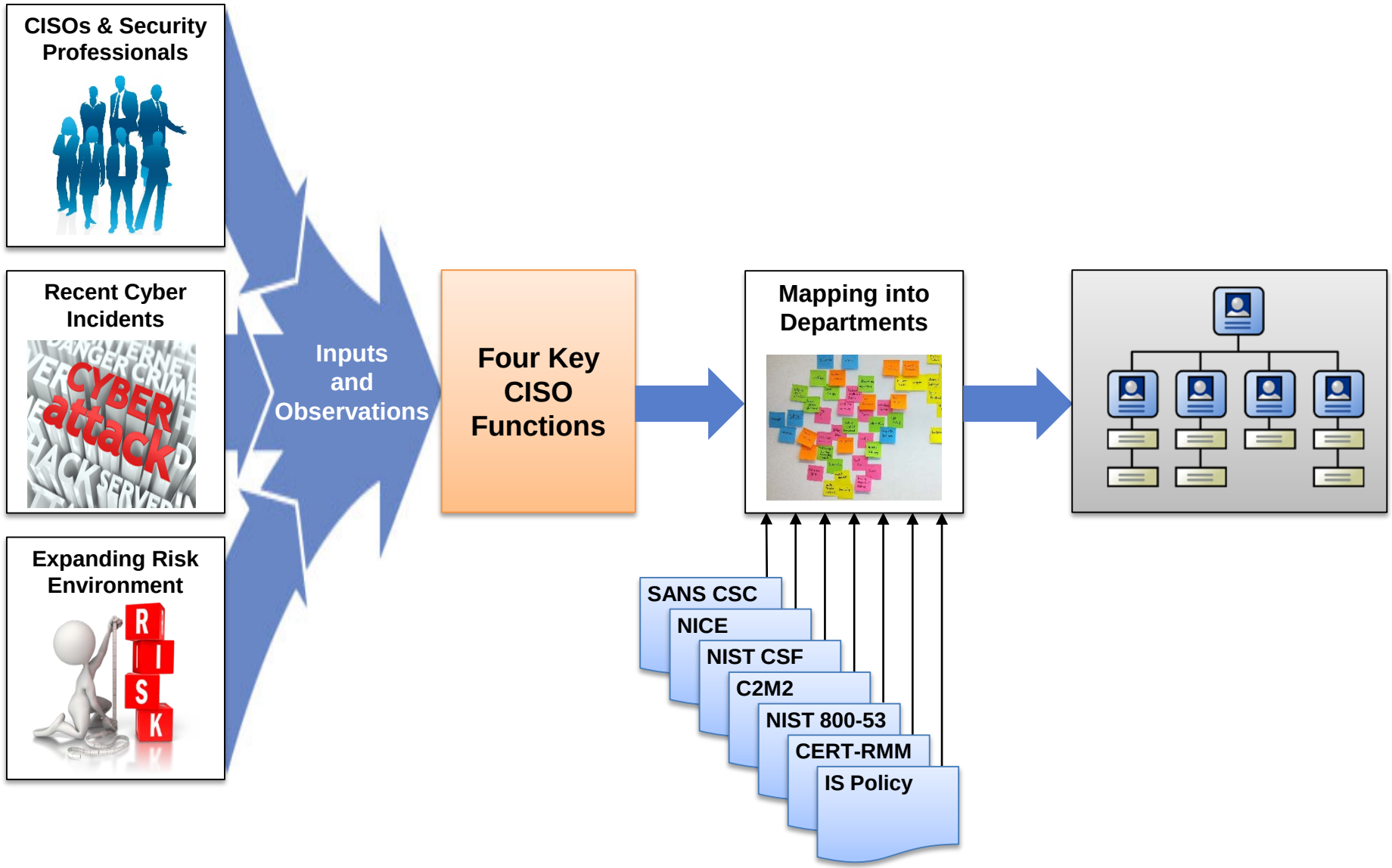
Mapped best practices to one or more of the functions, sub-functions, and departments

Defining CISO Departments

4 Key Functions | **Departments Reporting to CISO** | **Sub-Functions and Activities Performed in Each Department** | **Subcontracted To** | **Policies, Standards, & Codes of Practice**

Function	Department	Sub-Functions	Activities	ubcontracted	IS Policy	RMM	IST 800-5	C2
Protect/Shield	Security Engineering (all asset life cycle relat	Security requirements	Specify and allocate/assign confidentiality, integrity, and availability requirements		3-7, 3-10	KIM, TM, RRD, RI	SA	ACM-1
Protect/Shield	Security Engineering	Security architecture	Develop and maintain a security architecture		8-5	KIM, TM, RRD, RI	PL, PM, SA	CPM
Protect/Shield	Security Engineering	Secure life cycle	Address security throughout the development life cycle	elopment organiz	8-2, 8-3, 10-4	RTSE, TM	CM, SA	CPM
Protect/Shield	Security Engineering	Secure life cycle	Address security throughout the acquisition life cycle	quisition organiz	10-3, 10-4	EXD	SA	CPM-2
Protect/Shield	Security Engineering	Certification and accreditation	Perform certification and accreditation prior to releasing new systems to production	ing/C&A organiz	8-4, 8-5	RTSE, TM	CA, SA, PM	ACM-2
Protect/Shield	Identity Management	Identity and access management	Define and manage identities and access controls based on identities (password management, sin	IT?	3-3, 3-4, 3-5, 3-6	ID, AM	AC, IA	IAM
Protect/Shield	Applications security (operational, not life cycl	Software and applications inventories	Develop and maintain software and applications inventories	IT	10-4	ADM, KIM	CM	ACM-1
Protect/Shield	Applications security	Software and application controls	Define, implement, assess, and maintain controls necessary to protect software and applications l	IT	10-3, 10-4	CTRL, KIM, TM, V	SA	TVM-1
Protect/Shield	Applications security	Configuration management	Manage configurations for software and applications	IT	10-5	KIM, TM	CM	ACM
Protect/Shield	Applications security	Change management	Manage changes for software and applications	IT	10-5	KIM, TM, VAR	CM, MA	ACM-3
Protect/Shield	Host and network security	Host and network inventories	Develop and maintain network, hardware, device, and system inventories (including wireless)	IT	10-4	ADM, TM	CM	ACM-1
Protect/Shield	Host and network security	Host and network controls (mainframes, netwo	Define, implement, assess, and maintain controls necessary to protect networks, hardware, and sy	IT	3-10, 10-2, 10-4, 11-	CTRL, TM, EC, V	SC	TVM-1c
Protect/Shield	Host and network Security	Network controls	Define, implement, assess, and maintain controls necessary to protect the network/Internet perime	IT	11-4, 11-5, 11-6, 11-9	CTRL, TM, EC, E	SC	TVM-1c
Protect/Shield	Host and network security	Configuration management	Manage configurations for networks (including wireless), hardware, and systems	IT	10-5	TM	CM	ACM
Protect/Shield	Host and network security	Change management	Manage changes for networks, hardware, and systems	IT	10-5	TM, VAR	CM, MA	ACM
Protect/Shield	Information asset security	Information asset categorization	Designate and categorize information and vital assets (including PII) (includes privacy requirement	CPO and others	3-2, 3-3, 3-4	ADM, KIM	FIPS 199, 200, RA	
Protect/Shield	Information asset security	Information asset inventories	Develop and maintain information asset inventories	??	10-4	ADM, KIM	FIPS 199, 2	ACM
Protect/Shield	Information asset security	Information asset controls	Define, implement, assess, and maintain controls necessary to protect information and vital assets	IT, CPO	3-5, 3-6, 3-10	CTRL, KIM	MP, SI	TVM-1
Protect/Shield	Physical access control	Access to facilities; access to hosts and netw	Define and enforce access controls for facilities and other physical assets (such as networks and h	CPI/CSO; IT	7-2, 7-3, 7-4	EC, TM	PE	IAM
Monitor/Hunt	Security Operations Center	Intelligence collection & threat management	Collect, analyze, triage, and disposition information from all threat sources		Not present		PM, SI	TVM
Monitor/Hunt	Security Operations Center	Situational Awareness and Common Operatin	Collect, analyze, and report information in (near) real time that provides situational awareness and a common operat		Not present		PM, SI	SA-3
Monitor/Hunt	Security Operations Center	Logging	Perform audit logging (includes review and retention) of users, applications, networks, systems, acc	IT	3-11, 10-7	MON	AU	SA-1
Monitor/Hunt	Security Operations Center	Monitoring	Monitor users, applications, networks, systems, access to physical assets (includes intrusion preve	IT	11-5, 11-10, 14-3	TM, MON	AU	SA
Monitor/Hunt (previously Protect/Shield)	Security Operations Center	Vulnerability management	Scan for, analyze, and disposition vulnerabilities	IT	10-4	VAR	RA, SA, SI	TVM
Monitor/Hunt (previously Protect/Shield)	Security Operations Center	Virus and malicious code management	Detect, analyze, and eliminate viruses and malicious code	IT	10-6	KIM, TM	SC, SI	TVM-1
Monitor/Hunt	Security Operations Center	Information Security Help Desk (a.k.a. CIRT)	Accept, triage, assign, and disposition all reported suspicious events and security incidents		13	IMC	IR, NIST 80	IR-1
Monitor/Hunt	Security Operations Center	Incident management and response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents		13	IMC	IR, NIST 80	IR-1, IR
Recover/Sustain	Emergency Operations and Incident Comman	Incident Management and Response	Detect, triage, analyze, respond to, and recover from suspicious events and security incidents		13	IMC	IR, NIST 80	IR-1, IR
Recover/Sustain	Emergency Operations and Incident Comman	Business Continuity	Plan for business continuity	BC	7-5, 3-3, 12	SC	CP	IR-4, M
Recover/Sustain	Emergency Operations and Incident Comman	IT Disaster Recovery	Plan for disaster recovery	IT DR	7-5, 3-3, 12	SC	CP	IR-4
Recover/Sustain	Emergency Operations and Incident Comman	Test/exercise/drill response plans	Test and exercise BC, DR, and incident management plans (penetration testing, etc.)		12-4	SC, IMC	CP, IR, NIST	IR-3
Recover/Sustain	Emergency Operations and Incident Comman	Problem Management, Root Cause Analysis, a	Perform problem management, analyze root causes, and develop after action reports for high-profi		Not present	TM		IR-3h
Recover/Sustain	Emergency Operations and Incident Comman	Investigations	Perform forensic analysis and support investigations (includes interfaces with law enforcement)		Not present	IMC	IR, NIST 80	IR-3i
Govern/Manage	Program Management Office	Information security program/plan	Develop, implement, and maintain an information security program and plan		Not present	GP2	PL, PM	CPM
Govern/Manage	Program Management Office	Information security program/plan	Define, implement, maintain, and improve information security processes			OPD, OPF	PL, PM	
Govern/Manage	Program Management Office	Information security program/plan	Define information security roles/responsibilities		2-2	GP4	PL, PM	WM-1
Govern/Manage	Program Management Office	Information security program/plan	Allocate adequate trained/skilled resources to implement the information security program and pl		Not present	GP3	PL, PM	CPM-2
Govern/Manage	Program Management Office	Information security program/plan	Identify, manage, and maintain all of the work products required to implement the information secur		Not present	GP6	PL, PM	CPM
Govern/Manage	Program Management Office	Information security program/plan	Reporting and communications		Not present	COMM	PL, PM	SA-2
Govern/Manage	Program Management Office	Information security program/plan	Allocate and manage funding for the information security activities		Not present	FRM	PL, PM	Man
Govern/Manage	Program Management Office	Information security program/plan	Measure and monitor cost, schedule, performance		Not present	MA, GP8	PL, PM	CP
Govern/Manage	Program Management Office	Information security program/plan	Identify and involve relevant stakeholders (internal and external)		Not present	GP7	PL, PM	Ma
Govern/Manage	Program Management Office	Information security program/plan	Review the status of the security program with higher level managers		Not present	GP10	PL, PM	CPM-1
Govern/Manage	Program Management Office	Information security program/plan	Identify, review, assess, and enable business services/functions that rely on/impact information sec		Not present	EF	PM, SA	CPM
Govern/Manage	Governance, Risk, and Compliance	Information security program/plan	Define, implement, and enforce information security policies		2-1, 3-1, 4-1, etc.	EF, GP1	PL, PM	Man
Govern/Manage	Governance, Risk, and Compliance	Risk Management	Establish an information security risk management strategy, process, and program		4	RISK	RA, NIST 80	RM
Govern/Manage	Governance, Risk, and Compliance	Governance and Compliance	Govern/oversee the information security program & plan (includes CCB and other oversight boards		Not present	EF, GP1	PM	CP
Govern/Manage	Governance, Risk, and Compliance	Governance and Compliance	Ensure that controls are adequate to meet legal, regulatory, policy, standards, and security requir		14-2	COMP, TM, VAR	AU	IAM-5
Govern/Manage	Governance, Risk, and Compliance	Governance and Compliance	Ensure that controls are adequate to meet privacy requirements	CPO	2-2, 3-3, 3-5	KIM	AP, AR, DI, DM	
Govern/Manage	Governance, Risk, and Compliance	Governance and Compliance	Conduct audits		14-4	COMP, GP3	AU	TV
Govern/Manage	Personnel and External Relationships	External relationship management	Manage relationships with third parties (vendors, suppliers, contractors, partners, critical infrastru		7-6	EXD	PS, SA	EI
Govern/Manage	Personnel and External Relationships	External relationship management	Manage relationships with [illegible]		Not pre			M

Process for Determining Organizational Structure



Process for Determining Organizational Structure *(cont.)*

Developed the 4-function structure in conversations with CISOs and security professionals

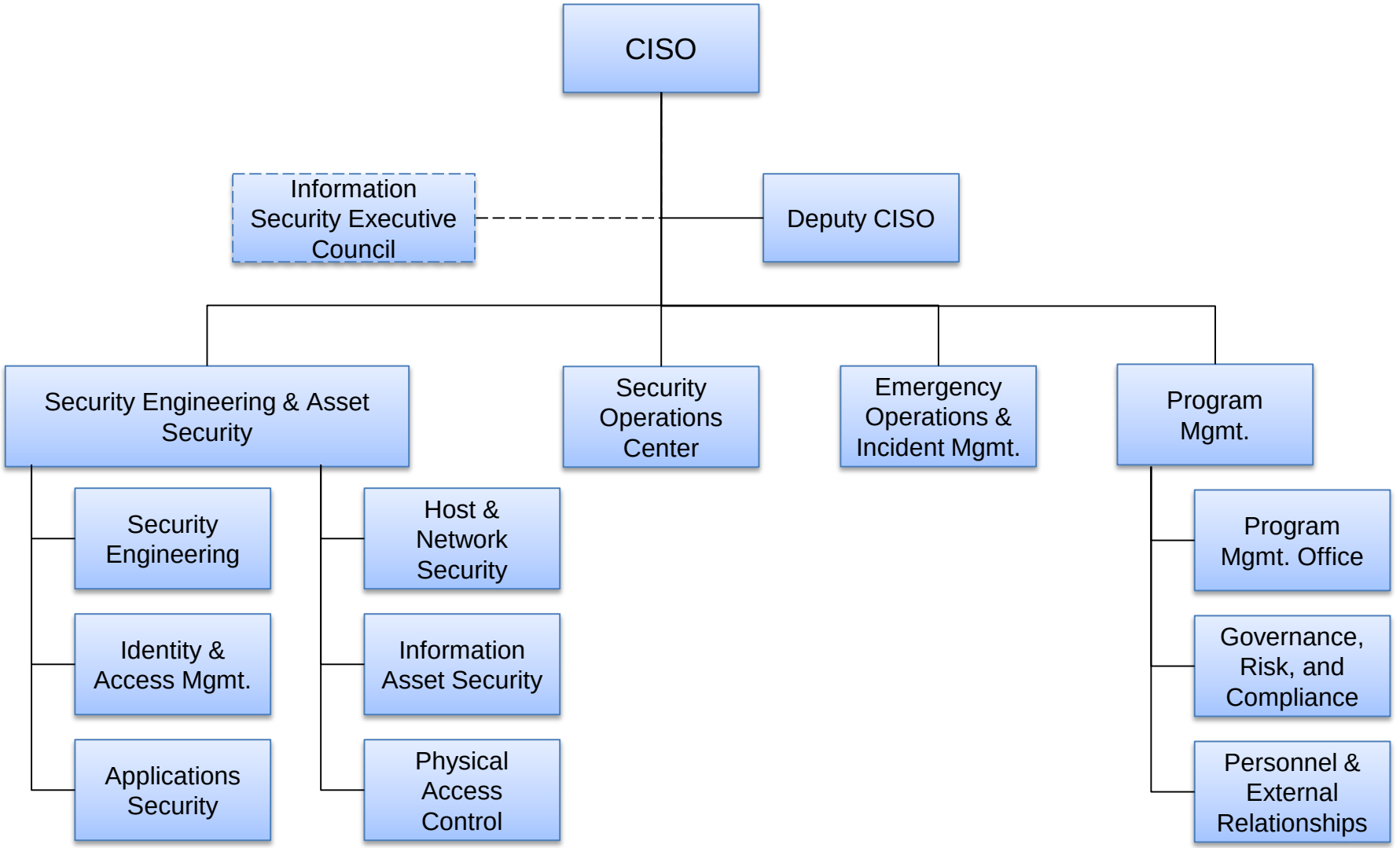
Identified relevant sources of best practices for the 4 functions

Mapped best practices to one or more of the functions, sub-functions, and departments

Developed a candidate organizational structure derived from departments and sub-functions

Candidate CISO Organizational Structure

Candidate CISO Organizational Structure



Program Management Office

Implement Information Security Program/Plan

- Develop, implement, and maintain an information security program, plan, and processes
- Define information security roles/responsibilities
- Allocate adequate trained/skilled resources to implement the information security program and plan
- Identify, manage, and maintain all of the work products required to implement the information security program and plan
- Reporting and communications
- Allocate and manage funding for the information security activities
- Measure and monitor cost, schedule, performance
- Identify and involve relevant stakeholders (internal and external)
- Review the status of the security program with higher level managers
- Identify, review, assess, and enable business functions that impact information security (SAAS, cloud, mobile, etc.)

Governance, Risk, and Compliance

Information Security Program/Plan

- Define, implement, and enforce information security policies

Risk Management

- Establish information security risk management strategy, process, and program

Governance and Compliance

- Govern/oversee the information security program and plan (includes CCB and other oversight boards/groups)
- Ensure that controls are adequate to meet security requirements
- Conduct audits

Personnel and External Relationships

External Relationship Management

- Manage relationships with third parties (vendors, suppliers, contractors, partners)
- Manage relationships with external stakeholders (for example, NCCIC, NSA, DHS, US-CERT, FBI, the press)

Personnel Management

- Manage the employment life cycle and performance of personnel IAW security requirements (background checks, succession planning, disciplinary action, termination, etc.)
- Manage knowledge, skills, capabilities, and availability of the information security team
- Implement enterprise-wide role-based information security awareness and training program
- Define and enforce acceptable use

Security Operations Center

Intelligence Collection and Threat Management

Situational Awareness and Common Operating Picture

Logging (users, applications, networks, systems, access to physical assets)

Monitoring (users, applications, networks, systems, access to physical assets)

Vulnerability Management

Virus and Malicious Code Management

Information Security Help Desk (a.k.a. CIRT, CSIRT)

Incident Management and Response

Emergency Operations and Incident Management

Incident Management and Response

Business Continuity

IT Disaster Recovery

Test, Exercise, and Conduct Drills of Response Plans

Problem Management, Root Cause Analysis, and After Action Reports

Investigations

Security Engineering

Security Requirements

- Specify and allocate/assign confidentiality, integrity, and availability requirements

Security Architecture

- Develop and maintain a security architecture

Secure Lifecycle

- Address security throughout the development and acquisition life cycles

Certification and Accreditation

- Perform certification and accreditation prior to releasing new systems to production

Identity and Access Management

Define and manage identities and access controls based on identities.

Including

- Active Directory
- Passwords
- PINs
- Digital signatures
- Smart cards
- Biometrics
- etc.

Applications Security

Software and Applications Inventories

- Develop and maintain software and applications inventories

Software and Application Controls

- Define, implement, assess, and maintain controls necessary to protect software and applications IAW security requirements

Configuration Management

- Manage configurations for software and applications

Change Management

- Manage changes for software and applications

Host and Network Security

Host and Network Inventories

- Develop and maintain network, hardware, system, and mobile device inventories (including wireless)

Host and Network Controls

- Define, implement, assess, and maintain controls necessary to protect networks, hardware, systems, and mobile devices IAW security requirements (intrusion prevention/detection, etc.)

Network Controls

- Define, implement, assess, and maintain controls necessary to protect the network/Internet perimeter IAW security requirements (firewalls, VPNs, etc.)

Configuration Management

- Manage configurations for networks (including wireless), hardware, systems, and mobile devices

Change Management

- Manage changes for networks, hardware, systems, and mobile devices

Information Asset Security

Information Asset Categorization

- Designate and categorize information and vital assets

Information Asset Inventories

- Develop and maintain information asset inventories

Information Asset Controls

- Define, implement, assess, and maintain controls necessary to protect information and vital assets (including media) IAW security requirements

Physical Access Control

Access to facilities; access to hosts and networks

- Define and enforce access controls for facilities and other physical assets (such as networks and hosts)

Information Security Executive Council

Purpose

- Advising the CISO (not on day-to-day activities)
- Ensuing alignment with business and strategic objectives

Sample Membership

- Chief Operating Officer
- Chief Information Officer
- Chief Financial Officer
- Legal / Privacy
- Human Resources
- Communications / Marketing
- Business Unit VPs
- Engineering VP
- Information Technology VP

Polling Question

Does this candidate organizational structure cover your current or planned CISO responsibilities?

- ❑ Yes
- ❑ Partially
- ❑ No

Recommended Next Steps

Recommended Next Steps

Map your current CISO (and supporting) structure to this candidate structure, departments, sub-functions and activities.

Determine which organizational units can continue as is, which ones need to change (expand, contract), and what new ones need to be created

Develop an implementation roadmap

- based on, for example, defined maturity indicator levels derived from CERT-RMM; used in DOE C2M2 and DHS Cyber Resilience Review
  - Incomplete, performed, planned, managed, measured, defined, shared

Additional Resources

SEI Technical Note documenting this work

Slides from this presentation

List of references on the next slide

CERT's Podcast Series: Security for Business Leaders *(late December/early January)*

CMU Heinz School Chief Information Security Officer (CISO) Executive Training Program

References

- Allen, Julia et al. *Structuring the Chief Information Security Officer Organization.* Software Engineering Institute, Carnegie Mellon University. 2015. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=446186
- Allen, Julia & Mehravari, Nader. Structuring the Chief Information Security Officer Organization podcast. To be published at http://www.cert.org/podcasts.
- Caralli, Richard A.; Allen, Julia H.; White, David W. CERT® Resilience Management Model: A Maturity Model for Managing Operational Resilience. Addison-Wesley, 2011.
- U.S. Department of Homeland Security US-CERT Cyber Resilience Review website: https://www.us-cert.gov/ccubedvp/self-service-crr
- U. S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2) Version 1.1. U. S. Department of Energy and U. S. Department of Homeland Security, February 2014. http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014
- U. S. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. U. S. National Institute of Standards and Technology, February 2014. http://nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- Joint Task Force Transformation Initiative. Security and Privacy Controls for Federal Information Systems and Organizations NIST Special Publication 800-53 Revision 4. U. S. National Institute of Standards and Technology, January 2015. http://csrc.nist.gov/publications/PubsSPs.html
- SANS. “Critical Security Controls Version 5.0.” SANS, 2015. http://www.sans.org/critical-security-controls/

Contact Information

Julia Allen

Principal Member of Technical Staff
Cyber Risk and Resilience Management Team
CERT Division
Software Engineering Institute
Carnegie Mellon University

jha@sei.cmu.edu

Dr. Nader Mehravari, MBCP, MBCI

Principal Member of Technical Staff
Cyber Risk and Resilience Management Team
CERT Division
Software Engineering Institute
Carnegie Mellon University

nmehrvari@sei.cmu.edu