ISSA Information Systems Security Association International | Charlotte Chapter

Cybersecurity Risk Management 101

Srinivasan (Mali) Vanamali, CISSP

Principal - Olympus Infotech

OLYMPUS Infotech

Short Bio

- 20+ years practicing information system security
- CISSP (Since 2001)
- Technical and Management Roles - Developer, Systems Security Engineer, Security Architect, Solution Manager
- SME - Identity and Access Management, RBAC
- SME - Cybersecurity Risk Assessment (NIST, HIPAA, PCI, ISO 27005)
- Trusted Adviser, Virtual CISO
- Published Author
  - ✓ Identity Management Framework: Delivering Value for Business (ISACA Journal - 2004)
  - ✓ Role Engineering: Cornerstone of RBAC (ISACA Journal - 2008)

What is Cybersecurity?

Cybersecurity

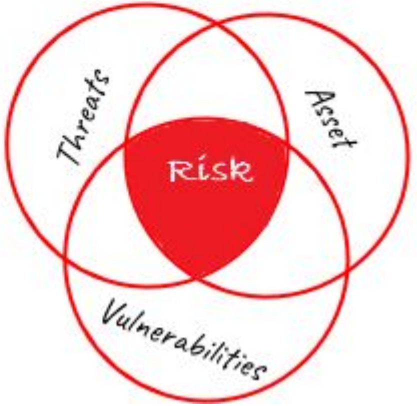
noun cy·ber·se·cu·ri·ty \-si-ˌkyu̇r-ə-tē

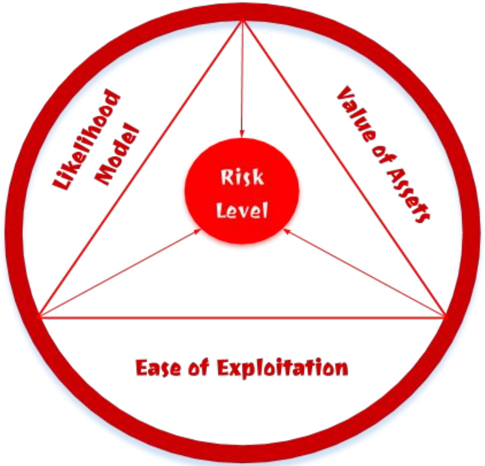
measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

merriam-webster.com

What is Cybersecurity Risk?

Cybersecurity risk is the likelihood of a cyber threat materializing by compromising a vulnerability resulting in loss of confidentiality, integrity or availability of a critical asset, system or an application.





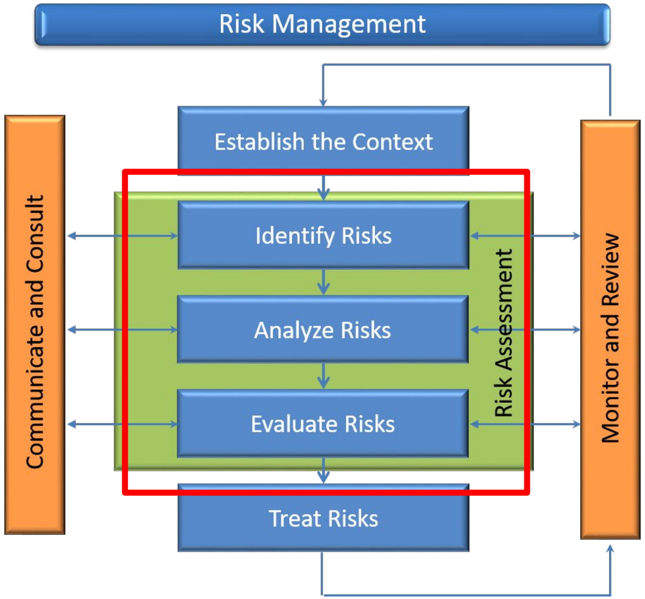
Key Definitions

- **Asset** is anything that has value and therefore requires protection
  - Asset Classification - Public, Internal, Confidential, Restricted
  - Asset Category - Software, Hardware, IP, Data, People, Process, Intangible
- **Threat** has the potential to harm an asset
  - Natural (e.g., floods, earthquakes, storms, tornados);
  - Human (e.g., intentional such as identity thieves, hackers, spyware authors; unintentional such as user error, accidental deletions); or
  - Environmental (e.g., power surges and spikes, hazmat contamination, environmental pollution)
- **Vulnerabilities** is a weakness that can be exploited by a threat to cause harm to an asset

Key Definitions Continued

- **Impact** is a negative quantitative and/or qualitative assessment of a vulnerability compromising the confidentiality, integrity, and availability of an asset
- **Likelihood** is the probability of occurrence in terms of frequency that a threat exploiting a known or unknown vulnerability.
- **Controls** are existing process, policy, systems, applications, practice or other action that mitigate risks or enhance security of an asset.

Cybersecurity Risk Management Framework



ISO 27005: Information Security Risk Management

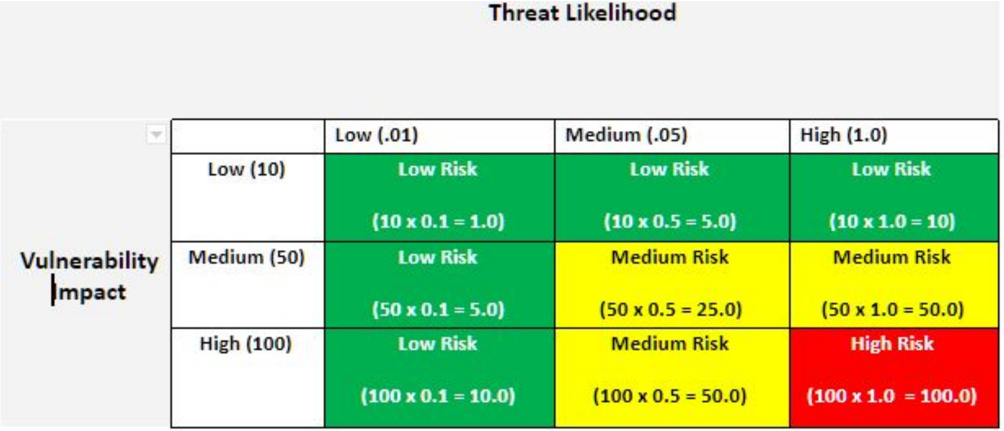
Risk Assessment

Risk Assessment is a well defined process to determine value of critical assets, applicable threats, vulnerabilities that exists or could exist, identifies controls and their effectiveness on identified risks and help prioritize a risk treatment plan to mitigate residual risks.

- Risk Identification
  - Asset Register
  - Identification of Threat
  - Identification of Vulnerabilities
  - Identification of Controls

Risk Assessment ...Contd.

- ➢ Risk Calculation
  - ✧ Quantitative vs Qualitative
  - ✧ Risk = Likelihood x Consequence



		Threat Likelihood		
		Low (.01)	Medium (.05)	High (1.0)
Vulnerability Impact	Low (10)	Low Risk (10 x 0.1 = 1.0)	Low Risk (10 x 0.5 = 5.0)	Low Risk (10 x 1.0 = 10)
	Medium (50)	Low Risk (50 x 0.1 = 5.0)	Medium Risk (50 x 0.5 = 25.0)	Medium Risk (50 x 1.0 = 50.0)
	High (100)	Low Risk (100 x 0.1 = 10.0)	Medium Risk (100 x 0.5 = 50.0)	High Risk (100 x 1.0 = 100.0)

- ➢ High Risk (>50 to 100) - There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
- ➢ Medium Risk (>10 to 50) - Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time as agreed by the asset owner.
- ➢ Low Risk (>0 to 10) - Asset owner should determine if additional compensating controls are needed or accept the risk.

Sample Asset Register

Process Name	Process / Asset Owner	Description of Asset	Asset Type	Storage Location
Patient Onboarding	Customer	Patient Data (EPHI) Class: Restricted Cat: Data	Primary	AWS
User Authentication	Customer	User Credential (EPHI) Class: Restricted Cat: Data	Primary	MongoDB
Data Management	Customer	Patient Data (EPHI) Class: Restricted Cat: Data	Primary	MongoDB

Threat Identification

Asset	Owner	Type	Threat Description	Likelihood		
				Low (0.1)	Medium (0.5)	High (1.0)
Patient Data (EPHI)	Customer	Primary	Breach of contractual requirements	X		
			Cloud Bruteforce Attack		X	
			Damage caused by a third party	X		
User Credential	Customer	Primary	Cloud Bruteforce Attack			X
			Disclosure of Passwords			X
			Leakage of data in the Cloud			X
			Malicious code			X

Vulnerability Identification

Asset	Threat Description	Threat Likelihood	Vulnerability Description	Consequence			Risk Calculation L x C
				Low (10)	Med (50)	High (100)	
Patient Data (EPHI)	Breach of contractual requirements	Low (0.1)	Critical System Vulnerabilities in Host Systems due to insufficient patch management			X	10
			Inadequate protection of cryptographic keys			X	10
			Lack of redundancy			X	10

- Risk Register
  - Asset Specific Threats and Related Vulnerabilities Exposure
  - Each Combination of Threat and Vulnerability Constitutes a Risk
  - Cumulative Qualitative Risk Score per Threat

Control Identification

Asset	Risk Score	Control Description	Control Factor	Residual Risk
Patient Data (EPHI)	30	Addressing security within supplier agreements	27	3
		Identification of applicable legislation and contractual requirements		
		Encryption Key management		

Risk Evaluation Criteria

- Strategic Importance to Business
- Criticality of the Asset
- Compliance, Legal, Contractual Obligation
- Impact on Confidentiality, Integrity and Availability
- Impact on Brand and Reputation

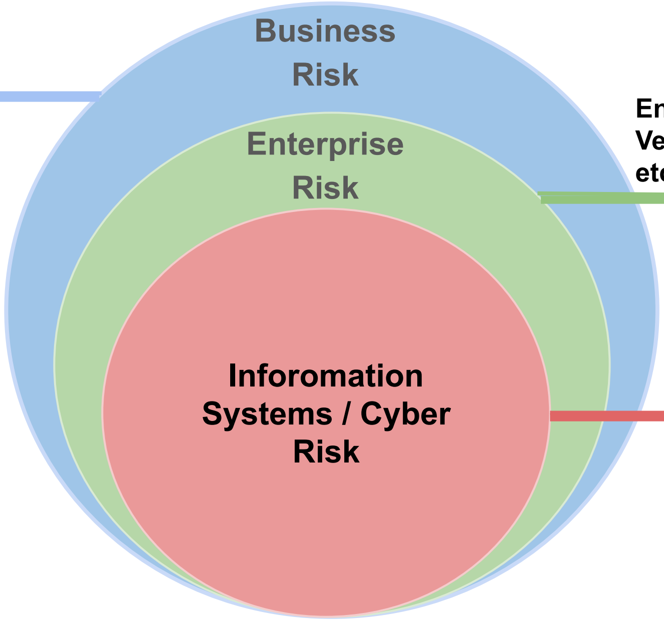
Risk Treatment

- Risk Reduction
  - Additional Controls to Further Mitigate Risks
  - Cost Vs Benefits Analysis
- Risk Acceptance
  - May be Conditional
  - Management buy-in
  - Decision Criteria
- Risk Avoidance
  - Unable to Accept or Mitigate Risks
  - *PANIC MODE*
- Risk Transfer
  - Share Risks
  - Transfer to Third-Party (Insurance)

Why Risk Management?

- Resources are limited ($$)
- Challenges in Prioritizing Risks
- Control Driven Approach is Insufficient
- Compliance (SEC, NY DFS Cybersecurity Regulation)

Risk Management Contexts



Business Risk

Enterprise Risk

Inforomation Systems / Cyber Risk

Supply Chain Risk, Financial Risk, Competition, Operational Risk etc.

Chief Risk Officer (CRO)

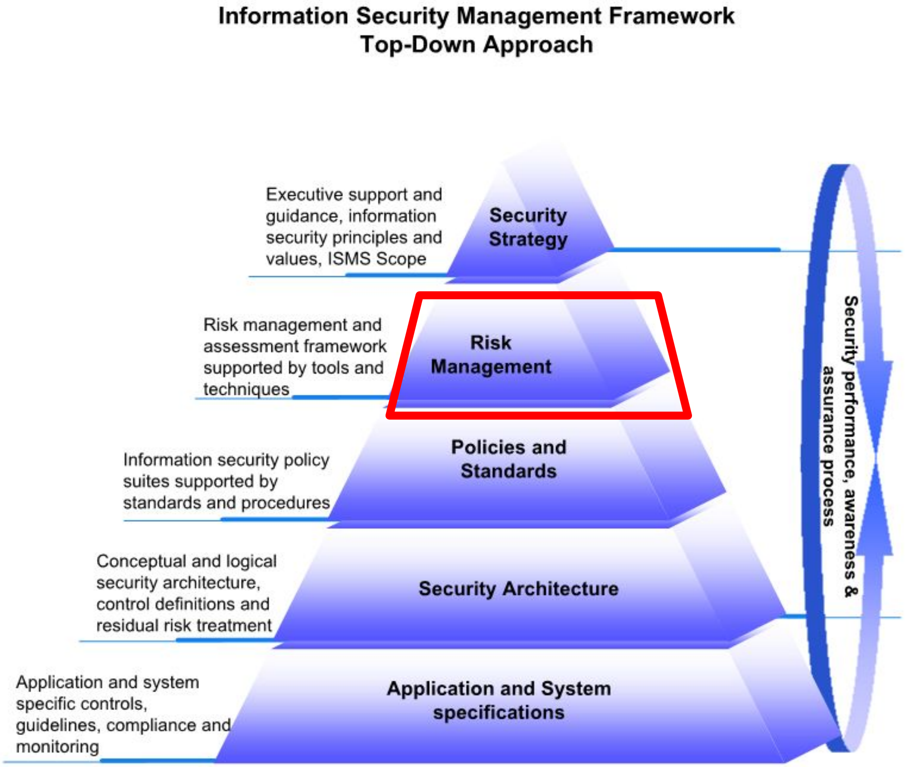
Enterprise Risk Management driven by GRC, Vendor Risk Management, Physical Security etc.

Chief Security Officer (CSO)

Information Systems Security, Cybersecurity Threat Management. Vulnerability Management etc.

Chief Information Security Officer (CISO)

ISMS Framework


Information Security Management Framework
Top-Down Approach
Executive support and guidance, information security principles and values, ISMS Scope
Security Strategy
Risk management and assessment framework supported by tools and techniques
Risk Management
Information security policy suites supported by standards and procedures
Policies and Standards
Conceptual and logical security architecture, control definitions and residual risk treatment
Security Architecture
Application and system specific controls, guidelines, compliance and monitoring
Application and System specifications
Security performance, awareness & assurance process

Questions?

mali@olympus-infotech.com

www.olympus-infotech.com