

Dr. Phil Legg

Associate  
Professor in  
Cyber Security

# Information Risk Management

## 09: Risk Management

Date

**UWE  
Bristol**

University  
of the  
West of  
England

# Today

- What are we going to cover?
- Roles, Responsibilities, and a focus on the CISO
- Cyber Risk Appetite
- Security Culture
- Case studies: Reducing the impact of common cyber attacks

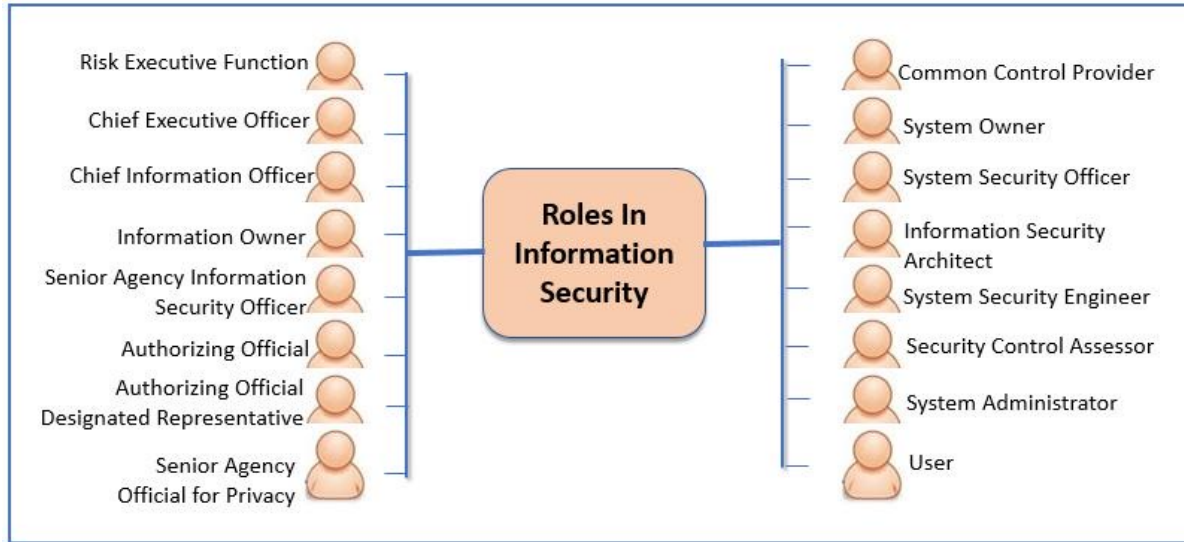
# Roles in Information Security

Information security involves securing information assets, financial information, customer data and other sensitive details. In order to accomplish the Information Security, organization, regardless of size needs to clearly define the roles and responsibilities of their professionals.

For larger organizations, this will support to ensure that no work is ignored and for small organizations & less structured organization, this will support to evenly distribute the workload as the workers may be needed to involve in more than one task.

Here we present the outline of the basic roles and responsibilities involved in the information security with reference to the [NIST special publication 800 – 12 Revision 1](#).

# Roles in Information Security



## 2. Chief Executive Officer (CEO)

This role represents the highest-level senior executive or officials in the enterprise who includes the whole responsibility to offer protection of information security commensurate with the possibilities and influence of the risk, which may result from unauthorized disclosure, access, destruction, and modification.

### **Basic Responsibilities:**

- Integrating the process of information security management with the process of strategic as well as operational planning
- Ensuring that the systems and information used to facilitate organization operation includes the respective information security safeguards
- Approving that the trained personnel are fulfilling with associated information security policies, legislation, instructions, directives, and guidelines

# 3. Chief Information Officer

This role represents the official of the organization who is responsible for designating the senior information security officer, developing as well as maintaining policies, procedures & control techniques of security, supervising personnel with notable responsibilities for security & guaranteeing that personnel is properly trained and supporting senior enterprise officials with their security activities.

## **Basic Responsibilities:**

- Allocating resources for system protections that support the business mission and functions of the organization
- Guaranteeing that systems are shielded by confirming security plans & are permitted to function
- Ensuring that there is an enterprise-wide security program, which is being effectively implemented

# 4. Information Owner

This role represents the official in the enterprise who includes the authority on the operation, management or statutory for certain details.

## **Basic Responsibilities:**

- Establishing the rules for the proper use as well as protection of the sensitive details
- Offering input to the system owners about the security controls and requirements needed to sufficiently protect the sensitive information.
- Creating the policies & procedures supervising its generation, processing, collection, disposal and dissemination

# 5. Chief Information Security Officer (CISO)

This role represents the official in the enterprise who is responsible for serving as the chief contact person between the enterprise chief information officer and the system owners, authorizing officials, system security officers, and common control providers. This role can also be referred as the Senior Agency Information Security Officer (SAISO).

## **Basic Responsibilities:**

- Managing & implementing an enterprise-wide information security program.
- Assuming the responsibility of confirming security control assessor when required.



# 15. System Administrator

This role represents the individual or group who are responsible for forming up and preserving a system / certain component of the system.

## **Basic Responsibilities:**

- Installing, configuring & updating hardware & software.
- Establishing & managing user accounts.
- Supervising backup & recovery tasks.
- Implementing technical controls related to security.

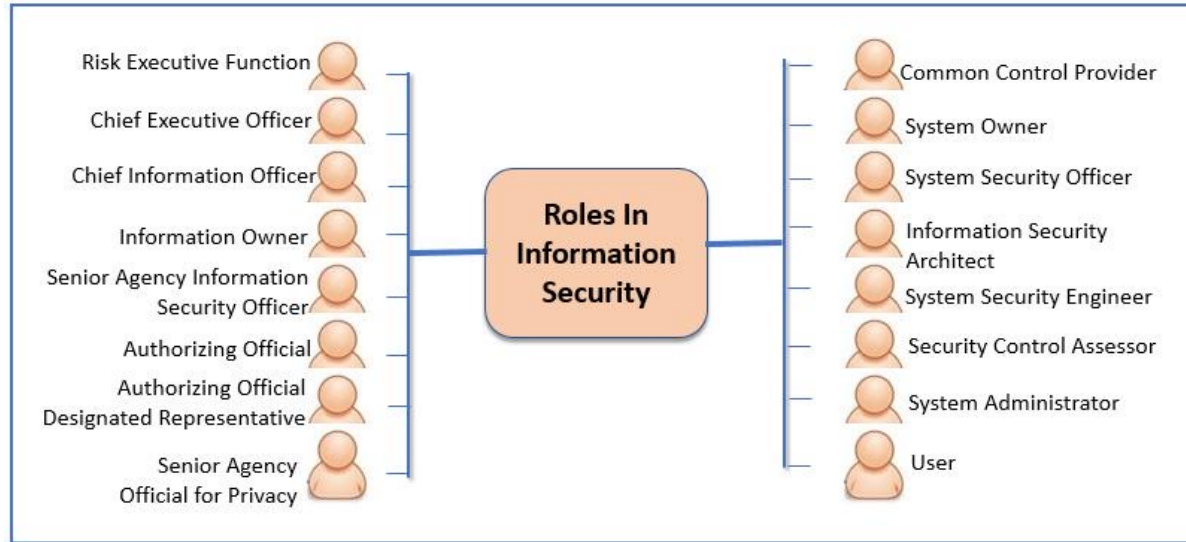
# 16. User

The user is an individual/group / organization who possesses rights to access the data of an organization to perform their assigned duties.

## **Basic Responsibilities:**

- Following to policies, which govern acceptable utilization of systems.
- Employing the enterprise provided resources for certain purposes only
- Reporting suspicious or anomalies system behavior.

# Roles in Information Security



# CISO

## The 7 Qualities of a Great CISO

- *combines great technical skill with great management and great personality*

1. Be Friendly and Approachable
2. Ability to Speak in a Language the Board Understands
3. Ability to Align Security with Business Goals
4. Patience
5. Recruitment and Talent Management
6. Risk Awareness
7. Organization

1. **Assess and prioritize assets that need protecting** – start with a data inventory. Understand how each department works, utilize the necessary tools and communicate both internally and externally. What are the biggest risks? Where do they need to make the biggest changes?
2. **Convey the risks to the board** – they've done a thorough assessment and have all the necessary data to show where the company is most at risk. But how does a CISO translate this into board speak? Find a way to show how the proposed changes will justify the cost it will incur and even better, create more efficiency, productivity and therefore, more revenue for the business.
3. **Implement appropriate controls** – work with a talented team to deliver control to those assets and keep appropriate measures to ensure that they are always monitoring, reporting and improving on the security strategy.
4. **Prepare and respond to incidents** – be ready for anything at any time. Have a well thought out and well documented incident response that every relevant party is not only aware of but knows inside out.
5. **Make it fit for the organization** – every company is different. A great CISO doesn't implement something because they can or because it worked in their last company. They implement it because they know it's the right choice for that company. Create a strategy that moulds to the company's needs; that way it will last longer and work better.

<https://www.itpro.co.uk/careers/28228/ciso-job-description-what-does-a-ciso-do>  
<https://www.cnn.com/2018/07/20/what-is-ciso-chief-information-security-officer.html>

# Cyber Risk Appetite

- *"the fundamental things that organizations undertake in order to drive performance and execute on their business strategies happen to also be the things that actually create cyber risk. This includes globalization, mergers and acquisitions, extension of third-party networks and relationships, outsourcing, adoption of new technologies, movement to the cloud, or mobility. And they are not going to stop doing these things any time soon. Cyber risk is an issue that exists at the intersection of business risk, regulation, and technology. Executive decision-makers should understand the nature and magnitude of those risks, consider them against the benefits a strategic shift would deliver and then make more informed decisions."*
- <https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf>

# Defining Cyber Risk

- **Internal Malicious:** Deliberate acts of sabotage, theft or other malfeasance committed by employees and other insiders. For example, a disgruntled employee deleting key information before they leave the organization.
- **Internal Unintentional:** Acts leading to damage or loss stemming from human error committed by employees and other insiders. For example, in 2013, NASDAQ experienced internal technology issues that caused backup systems to fail.[1](#)
- **External Malicious:** The most publicized cyber risk; pre-meditated attacks from outside parties, including criminal syndicates, hacktivists and nation states. Examples include network infiltration and extraction of intellectual property, and denial-of-service (DoS) attacks that cause system availability issues, business interruptions, or interfere with the proper performance of connected devices such as medical devices or industrial systems.
- **External Unintentional:** Similar to the internal unintentional, these cause loss or damage to business, but are not deliberate. For example, a third party partner experiencing technical issues can impact system availability, as can natural disasters.

# Key Questions for Stakeholders

Cybersecurity is at the top of the board room agenda today because it is well understood that cyber stakes have never been higher. The innovations and strategic advances that organizations make will continue to raise the stakes. It is not a problem that can be solved; cyber risk cannot be completely eradicated, but it can be managed to facilitate the success of a company's drive forward.

Decisions about cyber risk appetite need to be made with the business and communicated throughout the organization. It's important to understand the culture of the company and how the key stakeholders answer the following questions:

- What losses would be catastrophic?
- What can we live without and for how long?
- What information absolutely cannot fall into the wrong hands or be made public?
- What could cause personal harm to employees, customers, partners, visitors?

<https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf>

# Cyber Risk Appetite

- Risk appetite is the level of tolerance that an organization has for risk. One aspect of the definition is understanding how much risk an organization is willing to tolerate, and the other is thinking about how much an organization is willing to invest or spend to manage the risk. Risk appetite sets the boundaries for prioritizing which risks need to be treated.
- Cyber risk appetite should be set by the CEO, CISO and CRO and then shared throughout the organization. Calculating cyber risk through ongoing assessment using defined and proven methodologies and both quantitative metrics and qualitative risk elements is critical to an organization determining how much risk they are willing to accept to achieve specific business goals or objectives. Further, determining cyber risk appetite cannot be a point-in-time exercise. It must become an ongoing process involving constant evaluation and re-evaluation.
- While it seems like setting cyber risk appetite may be just technical, there is more to it than that. There are conversations that need to include non-technical functions. Cyber risk appetite ties together operational risk, cyber risk, and enterprise risk in cross- functional conversations. The strategic conversation is about the risk that the organization is willing to take on and what controls it puts in place to prioritize cyber risk management. Setting the appetite is critical to managing the business effectively and efficiently to help an organization know where to invest time and resources. <https://www.rsa.com/content/dam/en/white-paper/cyber-risk-appetite.pdf>



# Cyber Risk Appetite Challenges

## Exhibit 1: Cyber risk appetite challenges



**Quantification challenge:** The industry has not yet agreed upon a standard approach to quantifying cyber risk (outside of scenario analysis for operational risk more broadly). In addition, institutions have only rudimentary cyber-related data that encompass a limited time-series. This complicates identifying metrics that can be tracked on an ongoing basis supported by historical data to define “normal” ranges.



**Data challenge:** Given the rapidly-evolving nature of cyber risk, the relevance of historical data for the design of a cyber risk appetite is limited. Forward-looking statements and metrics are needed to enable institutions to identify potential issues before they become victims to the next headline-grabbing cyber incident.



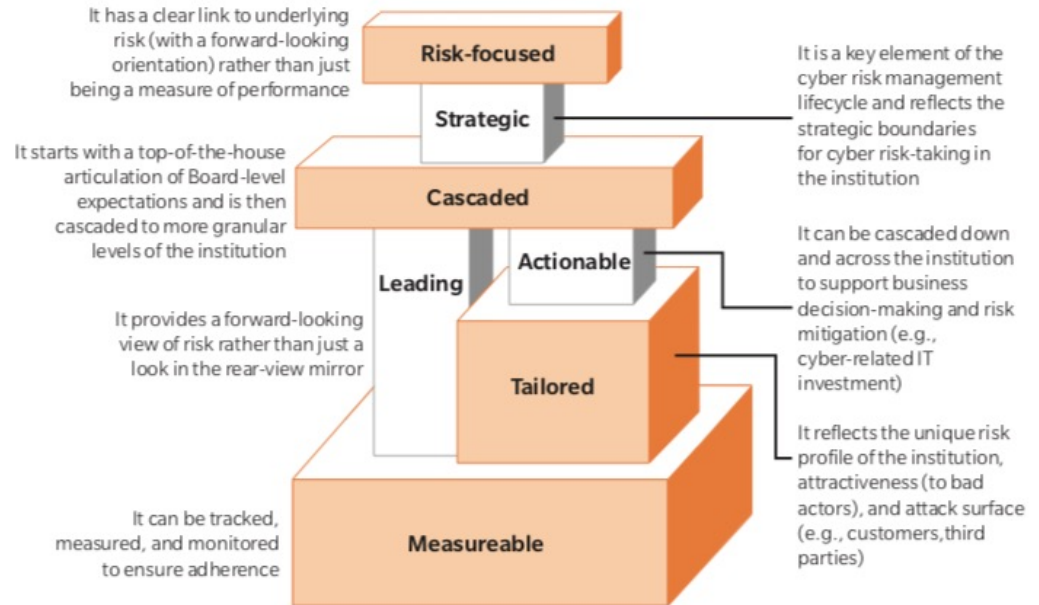
**Communication challenge:** Cyber risk metrics and reporting tend to be very technical and overwhelmingly detailed, especially for the Board. To ensure that cyber risk appetite is actionable, institutions need to strike the right balance between being too technical and too abstract, which is a difficult exercise.



**Embedding challenge:** Cyber risk is far more than an IT problem. It spans people, processes, and technology. Therefore, it is difficult to design top-of-the-house risk appetite statements that are meaningful and communicable, can be cascaded to granular levels of the institutions, and can be translated into actionable business decisions.

# Cyber Risk Appetite Challenges

Exhibit 3: Building blocks for an effective, measurable, and actionable cyber risk appetite



# Cyber Risk Appetite

An example of how a board level risk statement could be established and cascaded to metrics that can be quantified to measure effectiveness

To test this, report delves into modelling (Cyber VaR), trend analysis, industry benchmarks, and internal comparison

Exhibit 4: What a good-practice cyber risk appetite looks like - IT architecture example



## Impact on business decisions

- **Business strategy:** Cyber risk needs to be assessed as part of the due diligence when evaluating strategic business decisions, e.g., acquisitions, market entry. Decision makers need to consider the impact of business decisions on the organization's cyber risk appetite, e.g., does the new business expose the organization as a whole to more or different cyber risk?
- **Product/service strategy:** The new product approval process needs to consider clear criteria to evaluate the impact of new products and services on the cyber risk exposure of the business/organization.
- **IT strategy:** All relevant IT decisions need to consider the cyber risk implications for the organization, e.g., End-of-Life strategy, infrastructure replacement. Additionally, cyber risk needs to be considered an input/driver for the IT strategy, e.g., moving to cloud services to improve cybersecurity capabilities.
- **IT development:** The application and system risk assessment needs to reflect cyber risk assessment criteria. The assessment results need to inform the type and scope of security controls required for detection and protection.

1. Theme identified through the cyber risk identification process

# Security Culture

- “Security culture refers to the set of values, shared by everyone in an organisation, that determine how people are expected to think about and approach security. Getting security culture right will help develop a security conscious workforce, and promote the desired security behaviours you want from staff.”
- The benefits of an effective security culture include;
  - A workforce that are more likely to be engaged with, and take responsibility for, security issues
  - Increased compliance with protective security measures
  - Reduced risk of insider incidents
  - Awareness of the most relevant security threats
  - Employees are more likely to think and act in a security conscious manner

# Security Culture

SeCuRE 4 is a suite of self-assessment survey tools developed by CPNI over years of research and development, conducted in collaboration with our academic partners to ensure a theoretically driven approach to assessing security culture. Secure 4 has been designed to provide new capability for assessing different aspects of security culture. The outputs from the surveys can now be used to:

- Shed light on current and desired strategic approaches to security present in your organisation
- Measure employees' perceptions of how well security is working, and highlight where improvements in security culture are required
- Assess employees understanding of the relevant threats, their security responsibilities and their motivations to be security conscious
- Understand how frequently employees are performing specific security behaviours and what might encourage them to do them more often

# Security Culture

Embedding Security Behaviours using the 5Es

*"An effective protective security regime relies on the successful coordination and integration of **physical**, **cyber** and **people** related security measures to keep critical assets secure."*

- <https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf>



# Security Culture

- Design and validation of information security culture framework

○ <https://www.sciencedirect.com/science/article/pii/S0747563215002447>



Fig. 2. Information security culture change principles (Alhogail & Mirza, 2014a).

STOPE - Strategy; Technology; Organization; People; and Environment


Issues: Human Behavior Diamond	Scope:					Development Tool: Change Management
	S	T	O	P	E	
Preparedness	Prepare employees to behave securely through training, awareness, knowledge acquisition, and change in perception.					Training
Responsibility						Focus groups
						Change agents
	Management	Motivation				
Ensure employees are behaving securely through monitoring and control, reward and deterrence, and applicability		Milestones and measures				
		Involvement				
	Management	Ensure management support by showing management commitment, effective communication and interaction, and facilitation of resources.	Management support			
Resources						
Communication						
Society and Regulations	Consider external factors such as national culture, ethical conduct, government initiatives, and legal and regulations system					Culture analysis
Outcome: behavior (artifacts), values, assumptions and knowledge to enhance information security						
Older State						New State

Fig. 3. Information security culture framework security culture framework.

# NCSC Common cyber attacks: reducing the impact

- Case study 1: Espionage campaign against the UK energy sector
- Case study 2: Hundreds of computers infected by remote access malware
- Case study 3: Spear-phishing attack targets system administrator

***All of the mitigations listed in these case studies are covered in detail in the Cyber Essentials Scheme and the 10 Steps to Cyber Security. To reduce the risk of commodity and bespoke attacks on your business, fully implement a comprehensive suite of cyber security controls.***