UNIVERSITY OF Southampton

Foundations of Cyber Security Risk Management

By Dr. Nawfal Fadhel

Contributor

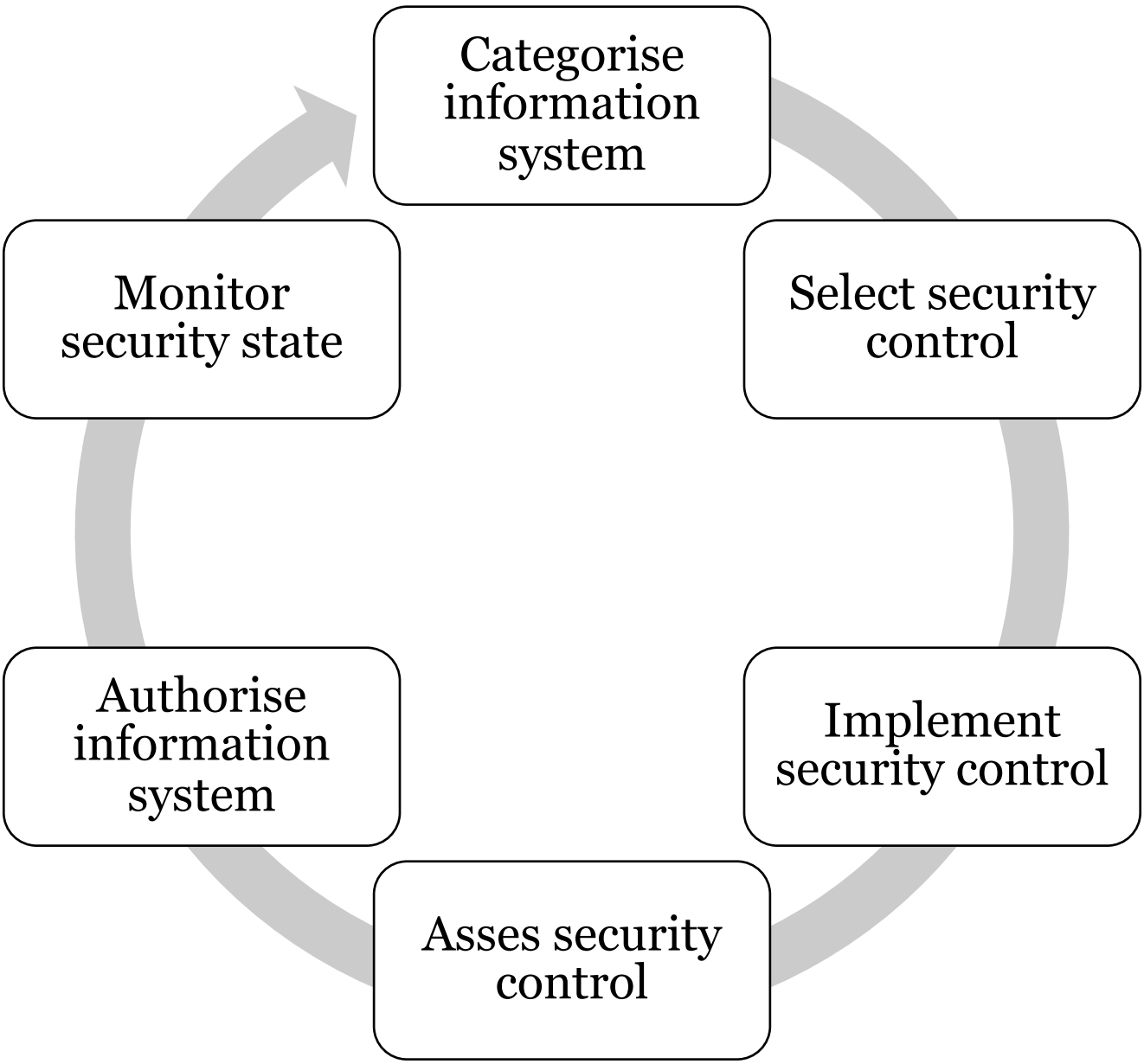
Dr Federica Paci

GCHQ Academic Centre of Excellence EPSRC

Question

What is security lifestyle? … is there such a thing?

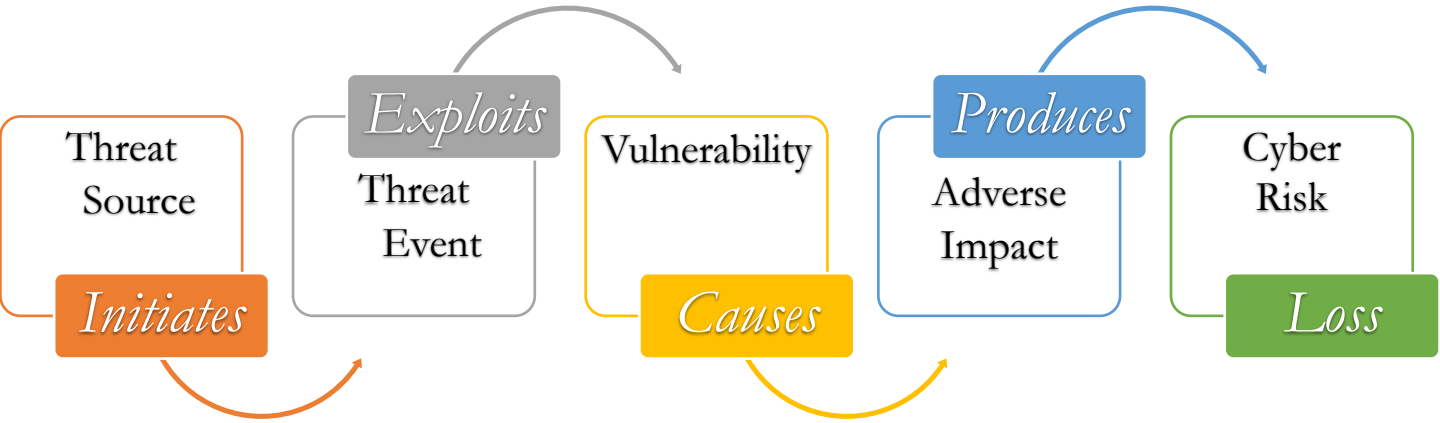
Compliance Security life cycle



Question

What is Risk?

What is Risk?


Threat Source
Initiates
Exploits
Threat Event
Vulnerability
Causes
Produces
Adverse Impact
Cyber Risk
Loss

Insurance

Organisations must decide how much time and money to spend protecting their technology and services.

But mainly how much its going to cost.

Why Risk Management?

One of the main goals of risk management is to *inform* and *improve* organisation decisions.

Also, It is an explicit requirement of the most important standards and regulations:

- ISO 27001 (ISMS)
- GDPR
- PCI DSS
- 10 Steps to Cyber Security

Risk Management Methods and Standards

I. ISO/IEC 27005:2018
II. Information Security Forum (ISF) IRAM 2
III. US National Institute of Standards and Technology (NIST) SP 800-30
IV. Octave Allegro
V. ISACA COBIT 5 for Risk

NIST 800-30

Step 1 - Prepare for Assessment

- Identify the **purpose** of the assessment
- Identify the **scope** of the assessment
- Identify the **assumptions** and **constraints** associated with the assessment
- Identify the **risk model, assessment approach**
- Identify **analysis approach** to be used in the risk assessment

Step 2 - Conduct Assessment

- Identify **Threat sources**
- Identify **Threat events**
- Identify **Vulnerabilities**
- Determine **Likelihood**
- Determine **Impact**
- Determine **Risks**

Step 3 - Communicate Results

- Communicate the results to organisation decision makers to support risk responses
- Share risk-related information produced during the risk assessment with appropriate organisational personnal

Step 4 - Maintain Assessment

- Determine the effectiveness of risk responses
- Identify risk-impacting changes to organisational assets
- Verify compliance

NIST 800-30

Step 1 -Prepare for Assessment

- Identify the **purpose** of the assessment
- Identify the **scope** of the assessment
- Identify the **assumptions** and **constraints** associated with the assessment
- Identify the **risk model, assessment approach**
- Identify **analysis approach** to be used in the risk assessment

Risk Models

I. **STRIDE**
II. **PASTA**
III. **LINDDUN**
IV. **CVSS**
V. **Attack Trees**
VI. **Persona non Grata**
VII. **Security Cards**
VIII. **hTMM**
IX. **Quantitative Threat Modeling Method**
X. **Trike**
XI. **VAST Modeling**
XII. **OCTAVE**

NIST 800-30

Step 2 - Conduct Assessment

- Identify **Threat sources**
- Identify **Threat events**
- Identify **Vulnerabilities**
- Determine **Likelihood**
- Determine **Impact**
- Determine **Risks**

NIST 800-30 - Step 2 – Conduct Risk Assessment - Produce a list of risks

Identify

- **Threat sources**
- **Threat events**
- **Vulnerabilities**

Determine

- **Likelihood**
- **Impact**
- **Risks**

Step 2-1 Identify Threat Sources

Objective: Identify threat sources of concern

TYPE OF THREAT SOURCE	DESCRIPTIONS	CHARACTERISTICS
ADVERSARIAL Outsider Insider Competitor Supplier Nation State	Individuals, groups, organizations, or states that seek to exploit the organisation' dependence on cyber resources	Capability, Intent, Targeting
ACCIDENTAL User Privileged User	Erroneous actions taken by individuals	Range of effects
STRUCTURAL IT Equipment Environmental Controls Software	Failure of equipment, environmental controls, or software	Range of effects
ENVIRONMENTAL Natural or Man-Made Disaster Infrastructure Failure	Natural disasters and failures of critical infrastructures on which the organization depends	Range of effects

Step 2-2 Identify Threat Events

Start with worse case scenario. If you have nothing.

Start with actual threat events if they were disclosed.

Step 2-3 Identify Vulnerabilities

Assess the vulnerabilities that a threat event can exploit and their severity

What can make the threat event “Craft Phishing Email possible?

NIST 800-30 - Step 2 – Conduct Risk Assessment - Produce a list of risks

Identify

- **Threat sources**
- **Threat events**
- **Vulnerabilities**

Determine

- **Likelihood**
- **Impact**
- **Risks**

Step 2-4 Determine The Likelihood

For adversarial threat events consider the

I. Skills
II. Motive
III. Objective

For non adversarial threat events use

I. statistical data

Step 2-4 Determine Likelihood

Determine the likelihood of threat event

What is the likelihood of “Craft Phishing Email”?

Likelihood of Threat Event Occurrence	Likelihood of Threat Event Result in Adverse Impact				
	Very Low	Low	Moderate	High	Very High
Very High	*Low*	*Moderate*	*High*	*Very High*	*Very High*
High	*Low*	*Moderate*	*Moderate*	*High*	*Very High*
Moderate	*Low*	*Low*	*Moderate*	*Moderate*	*High*
Low	*Very Low*	*Low*	*Low*	*Moderate*	*Moderate*
Very Low	*Very Low*	*Very Low*	*Low*	*Low*	*Low*

Step 2-5 Determine Impact

Identify the potential harm caused to organisational assets

The likelihood the threat event result in adverse impact is assessed based on the safeguards/security controls that are deployed by the organisation

Type of Impact	Impact
Harm to Operations	• Inability to perform current business functions • Non compliance • Direct Financial Costs • Damage to image of reputation
Harm to Assets	• Damage to or loss of physical facilities • Damage to or loss of information systems or networks • Damage to or loss of equipment • Damage to or loss of information assets • Loss of intellectual properties
Harm to Individuals	• Loss of life • Identity Theft • Loss of PII • Damage to the reputation
Harm to Other Organizations	• Non compliance • Direct Financial Costs • Damage to image of reputation
Harm to the Nation	• Damage to a critical infrastructure

Step 2-5 Determine Impact

What is the impact of “Craft Phishing Email”?

Impact	Description
Very High	Threat event could have multiple severe or catastrophic adverse effects on organisational operations, assets, individuals, other organisations or the Nation
High	Threat event could have severe or catastrophic adverse effects on organisational operations, assets, individuals, other organisations or the Nation
Moderate	Threat event could have serious effects on organisational operations, assets, individuals, other organisations or the Nation
Low	Threat event could have limited effects on organisational operations, assets, individuals, other organisations or the Nation
Very Low	Threat event could have negligible on organisational operations, assets, individuals, other organisations or the Nation

Step 2-5 Determine Risk

Determine the level of risk as a combination of likelihood and impact

What is the risk level of “Craft Phishing Email”?

Likelihood of Threat Event Occurrence	Likelihood of Threat Event Result in Adverse Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

NIST 800-30

Step 3 - Communicate Results

Communicate the results to organisation decision makers to support risk responses

Share risk-related information produced during the risk assessment with appropriate organisational personnal

NIST 800-30

Step 4 - Maintain Assessment

Determine the effectiveness of risk responses

Identify risk-impacting changes to organisational assets

Verify compliance

Summary

Risk Management is the process of prioritizing the identified risks in terms of likelihood of occurrence, then making coordinated efforts to minimise, monitor and control the impact of those risks.

Risk Assessment is the process of Identifying and assessing the level of risk faced by an organisation

That's all folks!

Recommended Readings

- Introduction to the risk management for cyber security guidance. Available at: https://www.ncsc.gov.uk/guidance/introduction-risk-management-cyber-security-guidance
- NIST. Guide for conducting risk assessment. Avaialble at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf