Cyber MAR

Mitigation and Remediation

UNIVERSITY OF PLYMOUTH

Rory Hopcraft, University of Plymouth

9th May 2022

MITIGATION | Introduction

Structure

- The Basics

Understanding the risks

- Threat Modelling
- Vulnerability Testing
- Penetration Testing

Security Cultures in Action

- Developing a Security Culture
- Social Engineering
- Data Theft

BE CYBER AWARE AT SEA
KEEP YOUR P@55WORD5 LONG & STRONG
PASSW...
Simple passwords can be unlocked easily, keep yours long and strong. Change your passwords regularly.

MITIGATION | The Basics

Remediation:

means addressing a breach and limiting the amount of damage that breach can potentially cause to your business. If you fail to notice and act upon a breach in time, it can grow so big that it becomes almost impossible to contain it ….

Mitigation:

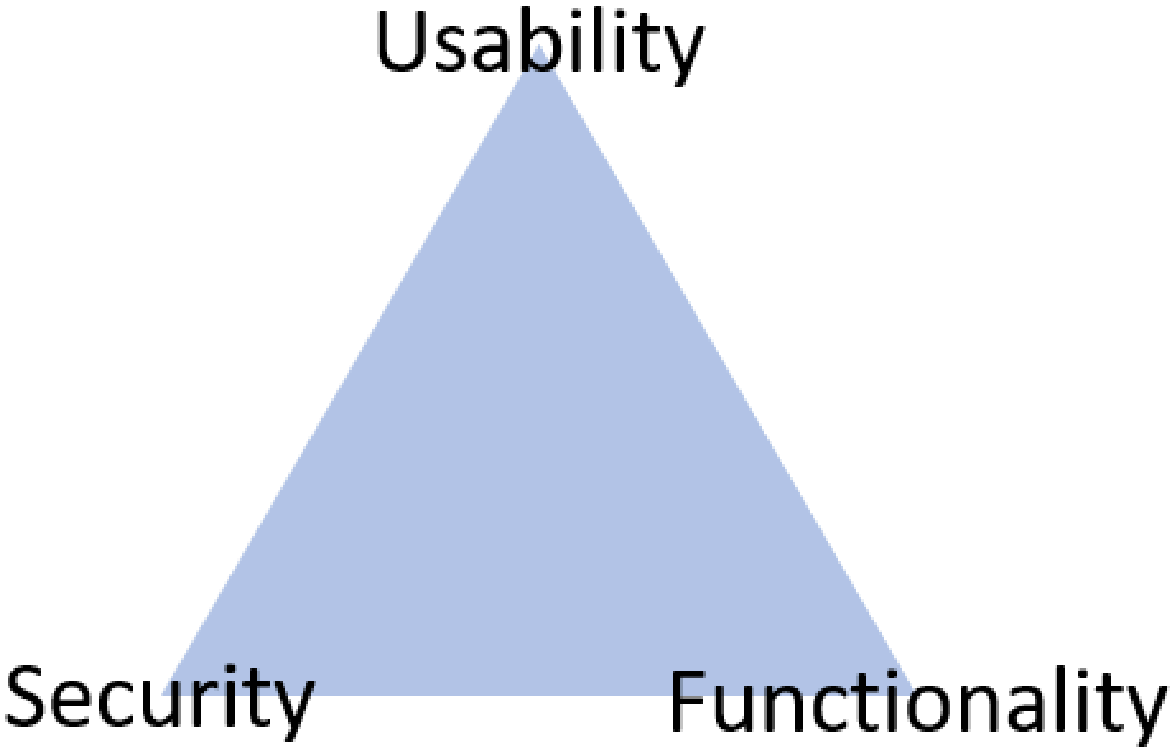
Refers to policies and processes put into place to help precent security incidents and data breaches.

- Threat prevention
- Threat Identification
- Threat Remedy

MITIGATION | The Basics

Countermeasures

- Security policy
- Physical
- Firmware management
- Patch management
- Software
- Personnel



MITIGATION | The Basics

Cyber Security Risk Management

Must have 3 key characteristics:

Being SECURE means having risk prioritized controls to defend critical assets against known and emerging threats.

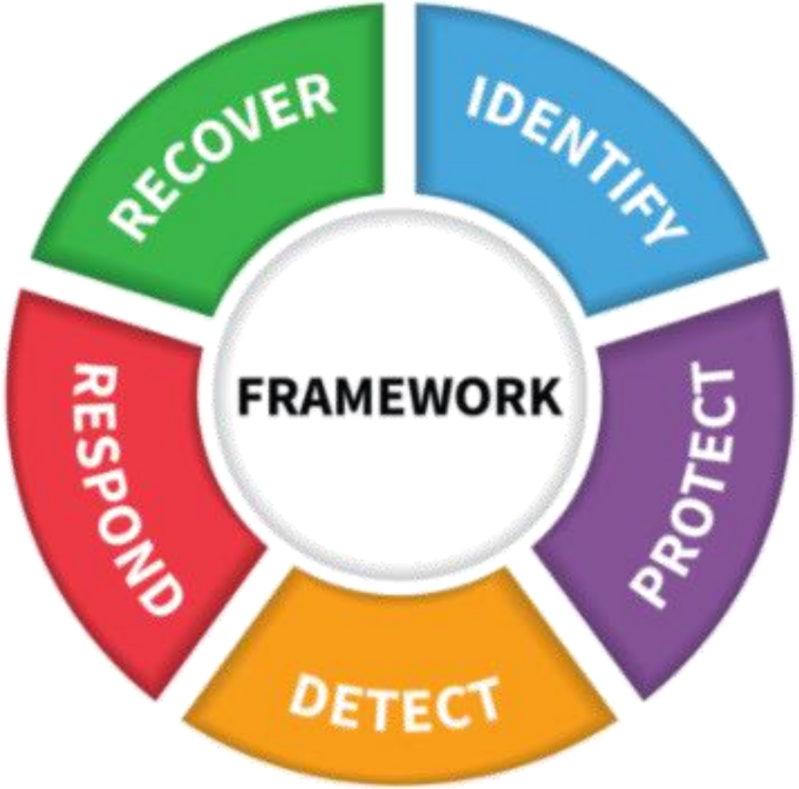
Being VIGILANT means having threat intelligence and situational awareness to anticipate and identify harmful behavior.

Being RESILIENT means being prepared and having the ability to recover from cyber incidents and minimize their impact.

MITIGATION | The Basics

NIST Cybersecurity Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



Source: https://www.nist.gov/cyberframework/framework

Threat Modelling

MITIGATION | Threat Modelling 01

What is Threat Modelling?

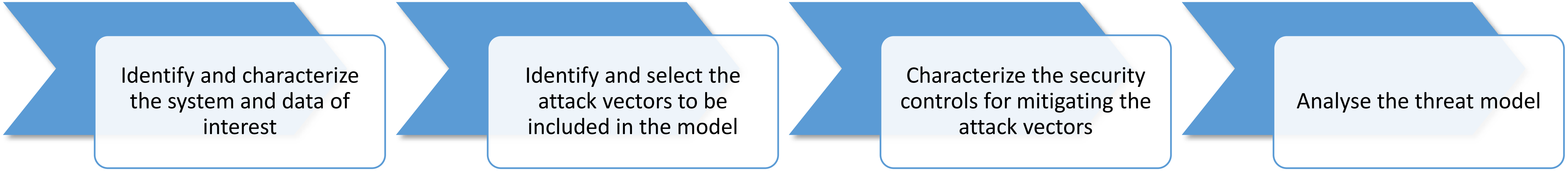
Is the structured process through which a company identifies potential security threats and vulnerabilities, quantify the seriousness of each, and prioritize techniques to mitigate attack and protect IT resources.

Best Practice

- Do it at the start of a project
- Do not view systems in isolation
- Don’t focus on the headlines
- Don’t forget the users
- Should be a living document

MITIGATION | Threat Modelling 02

NIST Threat Modeling



Identify and characterize the system and data of interest

Identify and select the attack vectors to be included in the model

Characterize the security controls for mitigating the attack vectors

Analyse the threat model

MITIGATION | Vulnerability Assessment

Vulnerability Assessment

MITIGATION | Vulnerability Assessment 01

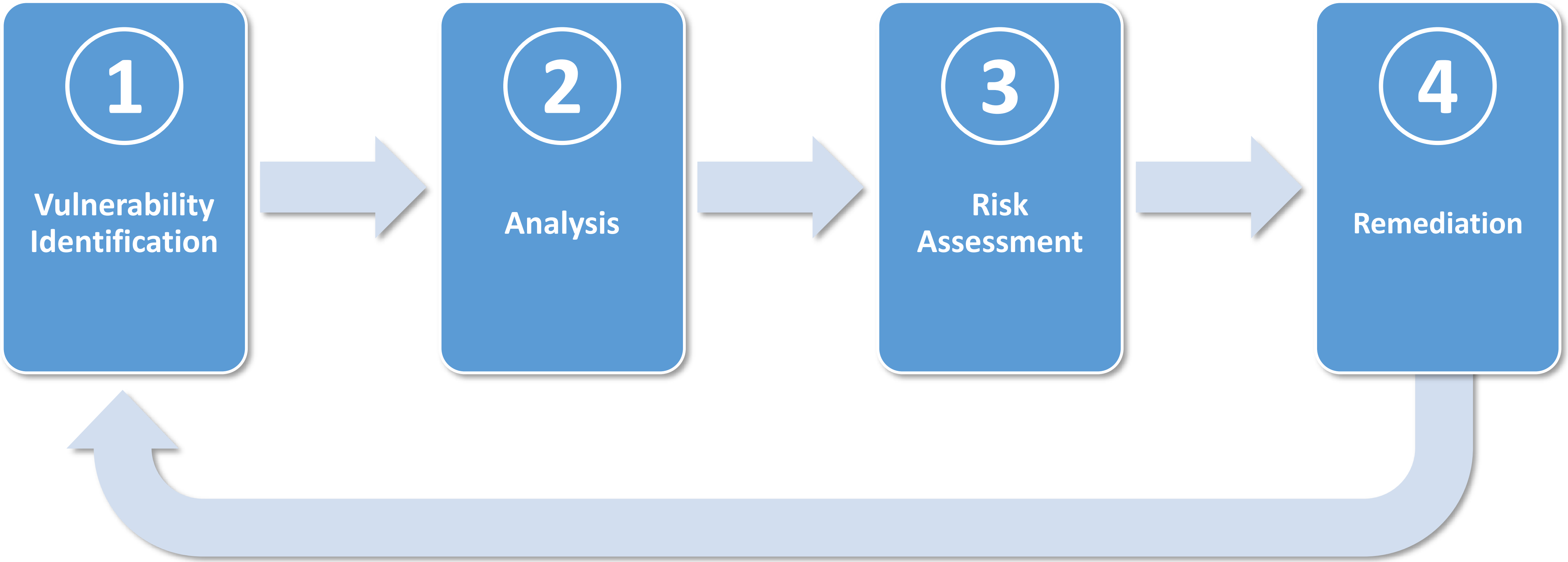
Vulnerability Assessment

Is a systematic review of security weakness in an information system. It evaluates if the system is susceptible to known vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Types

1. Host assessment
2. Network and wireless assessment
3. Database assessment
4. Application scans

MITIGATION | Vulnerability Assessment 02



1

Vulnerability Identification

2

Analysis

3

Risk Assessment

4

Remediation

MITIGATION | Penetration Testing

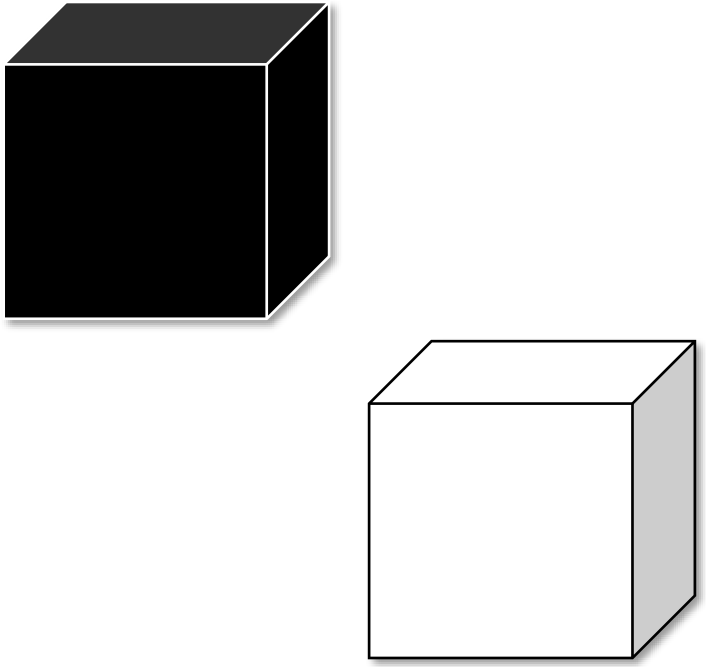
Penetration Testing

MITIGATION | Penetration Testing 01

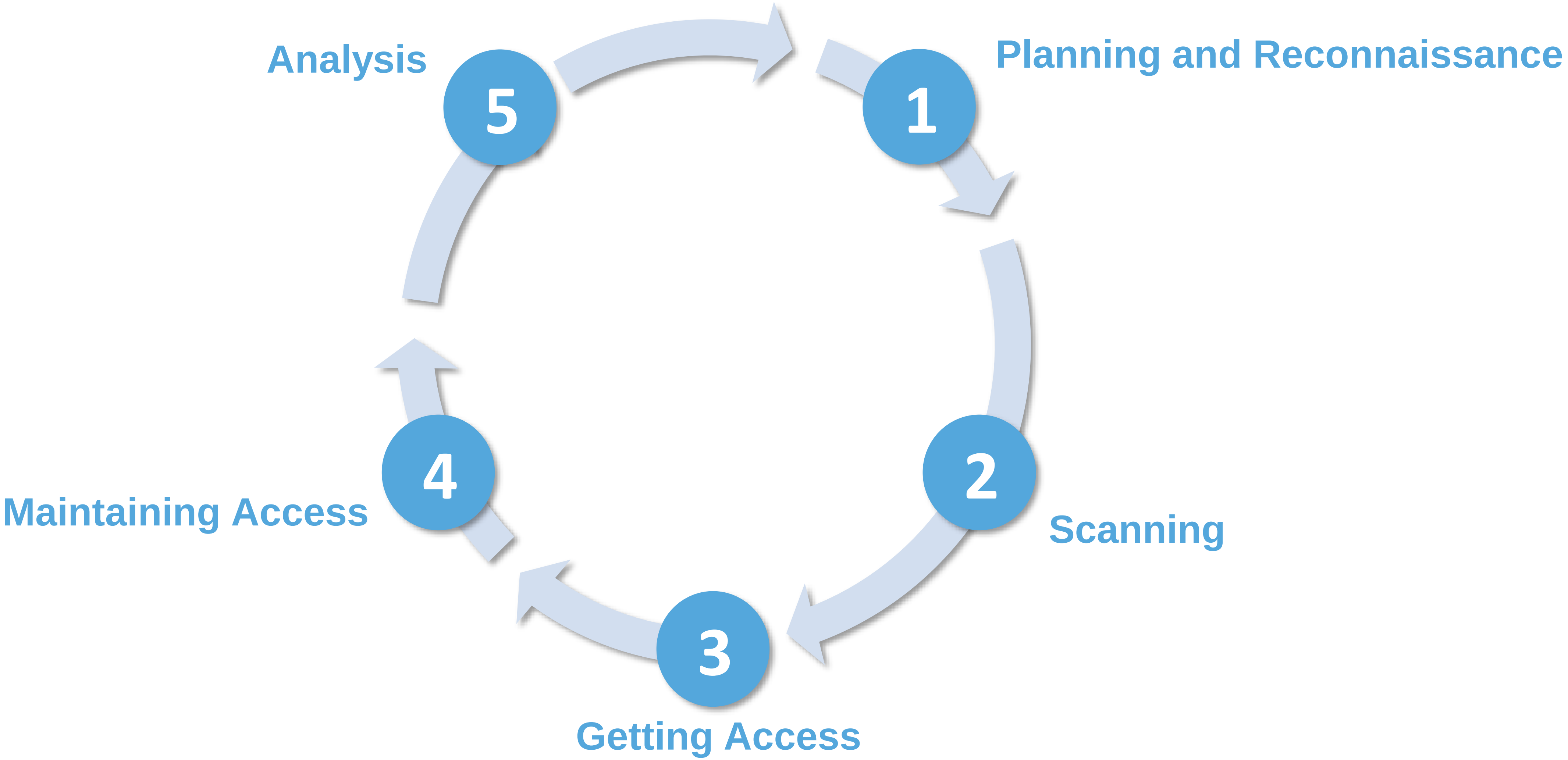
Penetration Testing

A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.

Should be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities.



MITIGATION | Penetration Testing 02



Security Culture

MITIGATION | Security Culture 01

Why develop a security culture?

It ensures personnel have the knowledge and expertise to do the right thing at the right time in both routine, and emergency situations

All individuals should achieve the following:

1. Know the cyber risks and threats
2. Know how to handle, control, transfer and dispose of information
3. Know how to us operational technology systems safely
4. Use the organisation’s cyber security procedures in accordance with the goals

MITIGATION | Security Culture 02

A Security Culture is based on 3 things:

Mutual Trust

Provide a blame-free reporting mechanism to encourage reporting of all issues without fear of retribution.

Being open, honest and direct about cyber safety risks and measures

Being supportive of personnel's ideas and concerns

Be willing to explain the actions and decisions taken

Shared Understanding of Cyber Security

Requires the collection, analysis and dissemination of cyber risk information.

Sharing relevant information encourages people to engage with risk management, and raises awareness of those risks.

Companies should be seen to priorities safety and security through awareness campaigns and training.

Confidence in Preventative Measures

There is a trade-off between safety, usability and functionality.

Measures should be decided with the input of personnel as this develops trust, and understanding in preventative measures.

This will allow personnel to make better informed decisions – even determine if the correct procedure might not be the safest course of action in an emergency.

Security Culture in Action

MITIGATION | Social Engineering

How can I stop a Social Engineering attack?

1. Build a Positive Security Culture
2. Learn the Psychological Triggers
3. Train Your Staff
4. Test the Effectiveness of Your Mitigation
5. Implement Appropriate Technical Measures

MITIGATION | Data Theft

Minimise the risk of a Data Breach

- **R**eputation evaluation
- **E**valuate plans, policies and procedures of 3rd parties
- **F**inancial assessment – insurance etc
- **E**stablish clear expectation and contractual terms
- **R**eview performance

Strengthen against a Data Breach

- **Policies and Procedures**
  - Password protection
  - Physical security
  - Access riles
  - BYOD
  - Suspicious Emails and Links
- **Awareness**
  - Communicate risk and explanations
  - Share Phishing examples
  - Table top scenarios

MITIGATION | Conclusion

Conclusion

MITIGATION | Conclusions

If you forget everything else, remember this...

- Mitigation and remidiation should be a constant process
- Assess and prorities risks appropriately
- Remember the balance between *Usability, Functionality and Security*

- It is not only attacks that you need to protect against!
  - Humans make mistakes too

- Develop a good security culture and posture

Cyber MAR

www.Cyber-MAR.eu

Cyber_MAR

Cyber-MAR EU Project

Cyber-MAR

info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

UNIVERSITY OF PLYMOUTH

Rory Hopcraft, University of Plymouth

✉ Rory.Hopcraft@plymouth.ac.uk

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement No. 833389