# Welcome to the
# Cyber Security Module

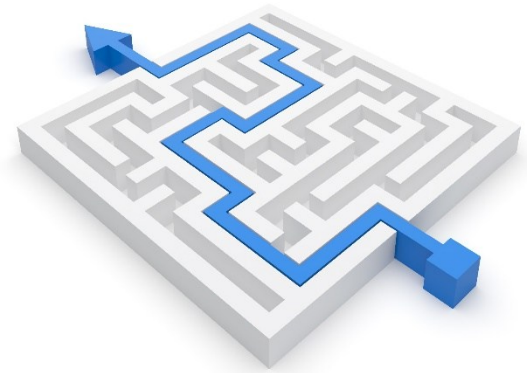
# Today’s Insights…

**Module Overview**

- About this module
- Content Agenda
- Assessments and LOs
- Your Responsibilities
- Tools to support your learning
- An Introduction to Cyber Security
- Release of Portfolio 01

# Learning Style on this Module?

- Studio work like culture
- Problem and Project Centred
- Experiential
- Collaborative and Altruistic
- Discover & Share



# Aims

- High Expectations
- It is a very testing module. Can be very frustrating.
- The goal is to help you to become emerging technology professionals that can do real things in a real context.

# Your Responsibilities

You must comply with the university's **Academic Integrity Requirements** and sign up to the **Student Cyber Security Code of Conduct and Ethics**…

# Your Responsibilities

**Attend** and complete the labs….

and **you will pass**!

# Your Responsibilities

**Engage** with the content and activities…and you will learn some really  useful skills!!

# Your Responsibilities

**Backup your work!!!!**

This is a fundamental of cyber security.

Use **the cloud** (e.g. OneDrive, Google Drive, Dropbox etc.) **&&** your own **USB drive**.

# Your Responsibilities

## Attention to detail.

## Take and maintain detailed notes!!!!

Use an outliner tool like Dynalist, a note taking app like Obsidian, or capture notes as documents on your own private **GitHub repo**.

# Your Responsibilities

**Ask Questions, but do investigate, read error messages carefully, check syntax.**

As a problem-centred module, you are expected to try and resolve  problems both individually and collaboratively, in order to enhance initiative and independence.

# Resources, Tools and Technologies

- Moodle
  - Knowledge Share (may lead to Wow Factor marks)
- O’Reilly: https://www.oreilly.com/
- Internet
- Generative AI (be sure to cite & paraphrase accordingly)

# Resources, Tools and Technologies

- Hypervisor
  - VirtualBox (Windows, Linux and Intel-based Macs)
  - Not all VirtualBox VMs will run on Mac so UTM may be an option
- Virtual Machines
  - Kali Linux
  - Ubuntu Server Linux
  - WordPress
  - OWASP Juice Shop
  - Zabbix
- Networking

# Assessments & Learning Outcomes

**Coursework** (2 x Portfolios) **60%**

**By the end of this module, you should have acquired degrees of competence in the following...**

- **LO1:** Investigate and apply measures that can be taken to prevent or mitigate the undesirable effects of cyber-crime.
- **LO2:** Understand, analyse and practically apply the security properties of confidentiality, integrity, and availability through the use of cryptographic primitives and related techniques.
- **LO3:** Evaluate risks to privacy and anonymity in commonly used applications.

# Assessments & Learning Outcomes

**In-class Practical Exam** (multiple choice, multiple answer) **40%**

**By the end of this module, you should have acquired degrees of competence in the following under time constrained conditions...**

- **LO1:** Investigate and apply measures that can be taken to prevent or mitigate the undesirable effects of cyber-crime.
- **LO2:** Understand, analyse and practically apply the security properties of confidentiality, integrity, and availability through the use of cryptographic primitives and related techniques.
- **LO3:** Evaluate risks to privacy and anonymity in commonly used applications.

# The Concept of “**Wow Factor**”

**Portfolio marks are structured as follows:**

- **65%** task completion mark.
- **35%** discretionary “Wow Factor” mark.

**Wow Factor** typically evidences additional learning beyond the coursework brief that is:

- Appropriate & Relevant
- Aims to be unique and different to work submitted by others.

**NOTE:** If others complete the same or similar Wow Factor submissions, it is no longer Wow Factor.

# The Concept of “Wow Factor”

**The aim of the Wow Factor concept is to encourage:**

- Increasingly higher standards
- Individual creativity
- Inquisitiveness
- Independence
- Ownership
- Deep engagement in learning

**It is optional.**

# An Introduction to Cyber Security

Through 5 Questions!

# 1) What is Cyber Security?

Cyber security refers to the **protection** of **information** systems (**hardware, software and associated infrastructure**), the **data** on them, and the **services** they provide, from **unauthorised access**, **harm** or **misuse**. This includes harm caused **intentionally** by the operator of the system, or **accidentally**, as a result of failing to follow security procedures.

SOURCE: https://www.cybok.org/media/downloads/Introduction_v1.1.0.pdf

# 2) What is the context of Cyber Security?

Cyber Security is a **multidimensional** field that comprises the following assets:

- People
- Technology
- Data
- Infrastructure
- digital systems
- Processes
- Societal factors

Without these, there is no cyber security.

# 2) What is the context of Cyber Security?

**The digital age,** we are **Interconnected 24/7 – 365**

- https://www.youtube.com/watch?v=qxOshY-KjDM

Digital **Transformation** and **Societal Changes**

- https://www.youtube.com/watch?v=6k_G_h41ZaQ

Cyberthreat Minute: The **scale and scope of worldwide cybercrime** in 60 seconds

- https://www.microsoft.com/en-us/security/business/security-insider/anatomy-of-an-external-attack-surface/cyberthreat-minute/

# 2) What is the context of Cyber Security?

**SECTORS IMPACTED**

- Financial Services
- Healthcare
- Retail and E-Commerce
- Information Technology and Telecommunications
- Government and Public Sector
- Energy and Utilities
- Manufacturing

**SECTORS IMPACTED**

- Transportation and Logistics
- Education
- Hospitality and Entertainment
- Legal and Professional Services
- Real Estate
- Agriculture and Food Industry
- Automotive

# 2) What is the context of Cyber Security?

**JOB ROLES IMPACTED**

- CEO and Other C-Level Executives
- Human Resources Professionals
- Marketing Professionals
- Legal Professionals
- Financial Officers and Accountants
- Customer Service Representatives
- Project Managers

**JOB ROLES IMPACTED**

- Sales Professionals
- Supply Chain and Logistics Managers
- Product Managers
- Administrative and Office Staff
- Healthcare Professionals
- Educators and Academic Administrators
- Facility Managers

# 2) What is the context of Cyber Security?

**TECH JOB ROLES IMPACTED**

- Software Developer/Engineer
- Network Administrator
- Database Administrator
- Systems Engineer
- IT Support Specialist
- Cloud Engineer/Architect
- Data Analyst/Scientist

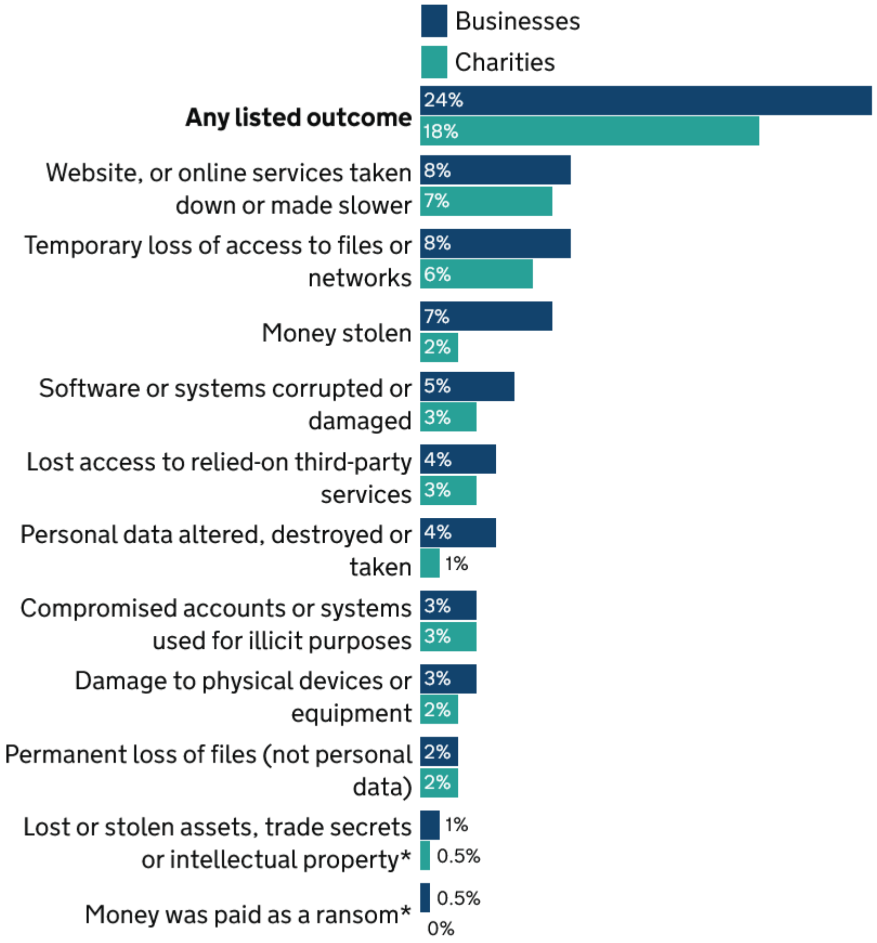
**TECH JOB ROLES IMPACTED**

- DevOps Engineer
- IT Project Manager
- Quality Assurance (QA) Tester
- Mobile Application Developer
- Web Developer
- Business Intelligence Analyst
- IoT Developer
- AI/Machine Learning Engineer

# 3) What are the consequences and impact of cyber incidents?

- Financial Loss
- Data Loss or Compromise
- Operational Disruption
- Reputational Damage
- Legal and Regulatory Consequences
- Compromise of Personal Information
- National Security Threats
- Psychological Impacts
- Resource Drain
- Impact on Shareholder Value
- Escalation into Larger Conflicts
- Innovation Disruption

# 3) What are the consequences and impact of cyber incidents?



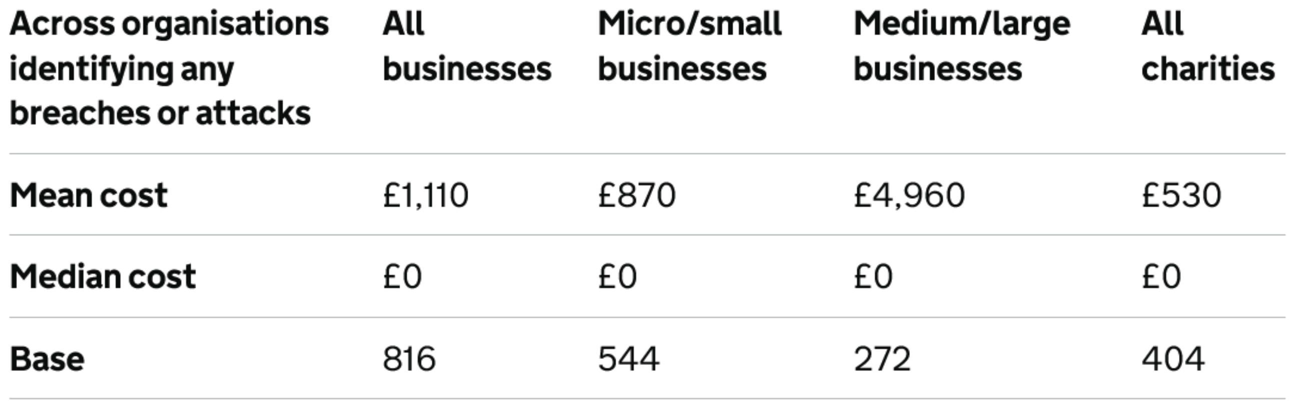
From the:
**Cyber Security Breaches Survey 2023**

Random probability telephone and online survey of **2,263 UK businesses**, **1,174 UK registered charities** and **554 education institutions** from 27 September 2022 to 18 January 2023.

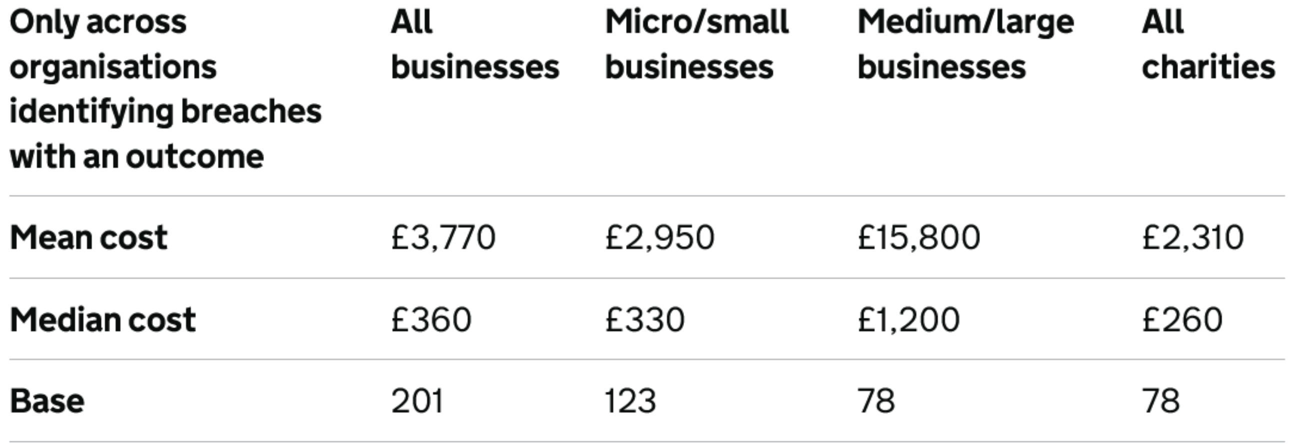
Figure 4.7: Percentage that had any of the following outcomes, among the organisations that have identified breaches or attacks in the last 12 months

Source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

# 3) What are the consequences and impact of cyber incidents?



| Across organisations identifying any breaches or attacks | All businesses | Micro/small businesses | Medium/large businesses | All charities |
|---|---|---|---|---|
| **Mean cost** | £1,110 | £870 | £4,960 | £530 |
| **Median cost** | £0 | £0 | £0 | £0 |
| **Base** | 816 | 544 | 272 | 404 |



| Only across organisations identifying breaches with an outcome | All businesses | Micro/small businesses | Medium/large businesses | All charities |
|---|---|---|---|---|
| **Mean cost** | £3,770 | £2,950 | £15,800 | £2,310 |
| **Median cost** | £360 | £330 | £1,200 | £260 |
| **Base** | 201 | 123 | 78 | 78 |

From the:
**Cyber Security Breaches Survey 2023**

Random probability telephone and online survey of **2,263 UK businesses**, **1,174 UK registered charities** and **554 education institutions** from 27 September 2022 to 18 January 2023.

Table 4.5: Average total cost of the most disruptive breach or attack from the last 12 months

Source: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

# 4) What are the goals of Cyber Security?

- Protect Assets (where assets are ppeople, technology, data, infrastructure, digital systems, processes, society ) using **CIA**
  - **Confidentiality** (Private and sensitive assets are only available to those intended – Encryption, ACL
  - **Integrity** (Assets remain in the state intended) – Hash functions, transactions in a database are unaltered.
  - **Availability** (Assets accessible where and when required) – DDoS, website offline.
- Identify, evaluate & mitigate risks
- Minimise societal disruption
- Maintain business and societal continuity

# 5) Where can we find cyber security guidance?

NCSC: 10 Steps to Cyber Security

- https://www.ncsc.gov.uk/collection/10-steps

NCSC: Cyber Essentials

- https://www.ncsc.gov.uk/cyberessentials/overview

NCSC: Small Business Guide: Cyber Security

- https://www.ncsc.gov.uk/collection/small-business-guide

The Cyber Security Body of Knowledge (CyBOK)

- https://www.cybok.org/

NIST Cybersecurity Framework

- https://www.nist.gov/cyberframework

# Become familiar with Cyber Security Terminology

**Become familiar with Cyber Security Terminology**

- UK Cyber Security Council Glossary of Cyber Security Terms
- SANS Glossary of Cyber Security Terms
- NICCS Explore Terms: A Glossary of Common Cybersecurity Words and Phrases
- NIST Glossary

# Coursework Portfolio 01

Moodle