BIY BUSINESS INSTITUTE YANGON

othm® qualifications

OPTIMUM INSTITUTE

OTHM Level-4 Diploma

Diploma in Information and Technology

Cyber Security

Lesson One

U Tin Naing Htwe
Senior Lecturer(ICT)
Optimum Institute

Today’s Lesson

Cyber Security

OTHM Level 3 Syllabus

1.	Coding and Website Development
2.	Social Media for Business
3.	Computer Systems
4.	Networks
5.	Mobile Communications
6.	Cyber Security

OTHM Level 4 Syllabus

1.	Systems Analysis and Design
2.	Managing Digital Information
3.	Principles of Computer Programming
4.	Web and Mobile Applications
5.	Computer and Network Technology
6.	Cyber Security

Cyber Security

1. Understand the fundamentals of cyber security.
2. Understand cyber security protection methods.
3. Understand how to manage a cyber security attack.

1. “ Understand the fundamentals of cyber security ”

1.1 Define the term ‘cyber security’.

1.2 Explain how cyber security risks are managed in an organisation.

1.3 Describe the laws and regulations associated with cyber security

1.4 Summarise the historical development of cyber security.

1.5 Explain the impact cyber security has on individuals and organisations.

1.6 Explain how to keep up to date with the latest cyber security information.

OTHM Academic Global Assignment Framework

Part 1 : The submission is in the form of a 10-minute presentation equivalent to 700 words and must be in a recognized PowerPoint presentation format.

2. “ Understand cyber security protection methods ”

2.1 Describe network security protection methods.

2.2 Evaluate the impact of penetration and vulnerability testing has to an organisation.

2.3 Describe end user device protection methods.

2.4 Describe the importance of implementing and reviewing access controls in an organisation.

2.5 Explain how end users can be educated and aware of cyber security.

OTHM Academic Global Assignment Framework

The submission is in the form of a report written in Microsoft Word format for both Part 2

Part 2 - the recommended word limit is 800 words.

The word limit is excluding diagrams, references, and appendices.

3. “ Understand how to manage a cyber security attack ”

3.1 Evaluate the impact a cyber-attack has to an organisation.

3.2 Describe the content of an organizational incident management plan.

3.3 Explain the importance of internal and external communication when managing a cyber-attack.

3.4 Describe the roles and responsibilities for incident management.

3.5 Analyse the actions to take when responding to an incident.

3.6 Explain the importance of post cyber-attack reviews.

OTHM Academic Global Assignment Framework

The submission is in the form of a report written in Microsoft Word format for both Part 3

Part 3 - the recommended word limit is 800 words.

The word limit is excluding diagrams, references, and appendices.

OTHM Academic Global Assignment Framework

Cyber Security Intelligence Presentation (Microsoft PowerPoint Format File)

□ **Part 1 - Understand the fundamentals of cyber security**

□ **Word Count 700**

Cyber Security Training Handbook Documentation (Microsoft Word Format File)

□ **Part 2 - Understand cyber security protection methods**

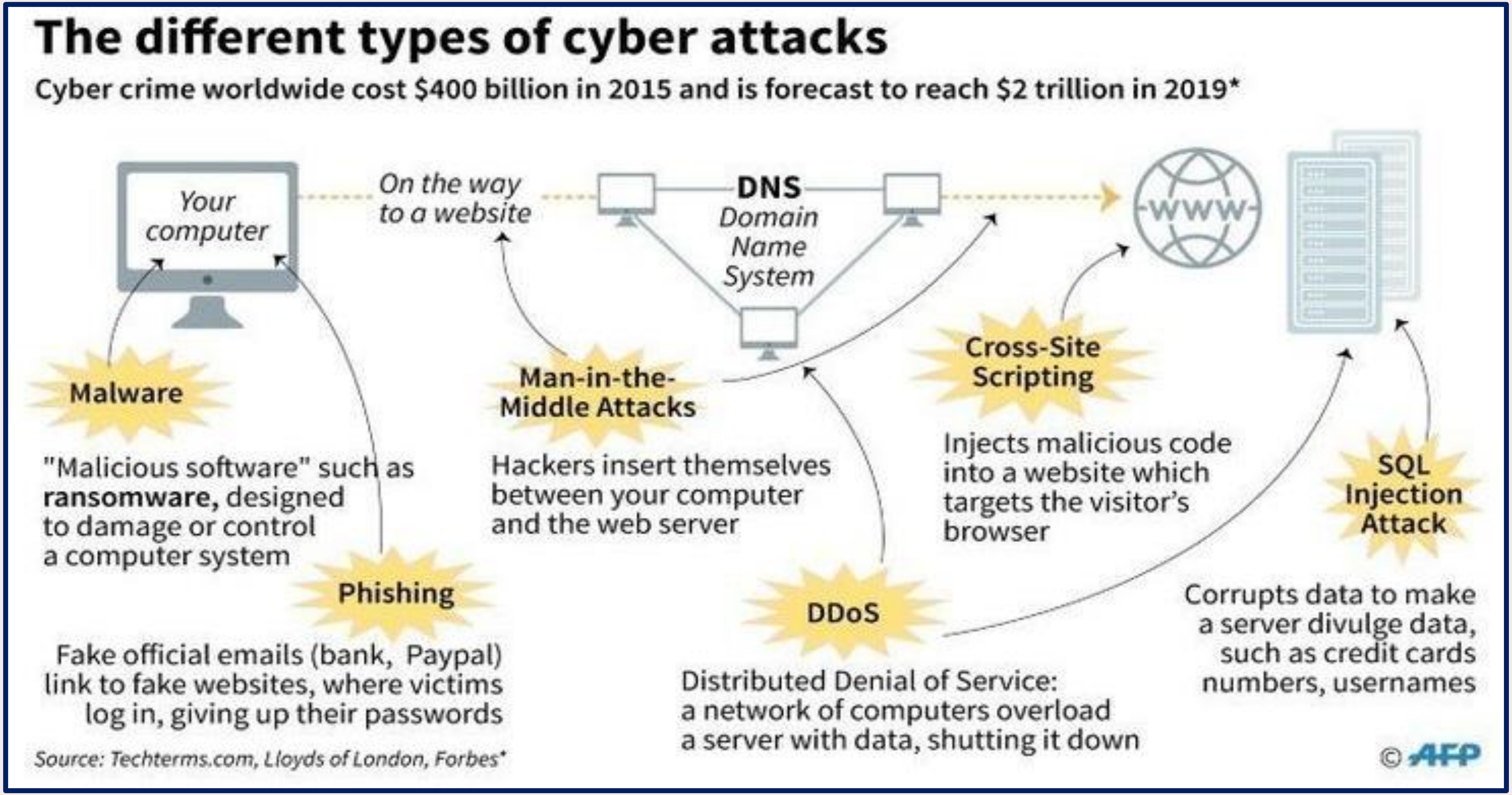
□ **Part 3 - Understand how to manage a cyber security attack**

□ **Word Count 1,600**

Part 1

1.1 Define the term ‘cyber security’.

Networks
ATTACKS
DATA
HARDWARE
Protect
Computer
SPYWARE
CYBERATTACKS
DATA
SYSTEM
Computer
Internet
SAFE
Systems
DANGER
PROTECT
SOFTWARE
OPERATING
SECURE
CYBERSECURITY
Vulnerability
Bootkits
SPYWARE
Trojans
PHISHING
PROTECT
Payloads
Web shells
BACKDOORS
DIGITAL
PROTECTION
Information Technology
RANSOMWARE
VIRUS



The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*

Malware

"Malicious software" such as **ransomware,** designed to damage or control a computer system

Phishing

Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Man-in-the-Middle Attacks

Hackers insert themselves between your computer and the web server

DDoS

Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Cross-Site Scripting

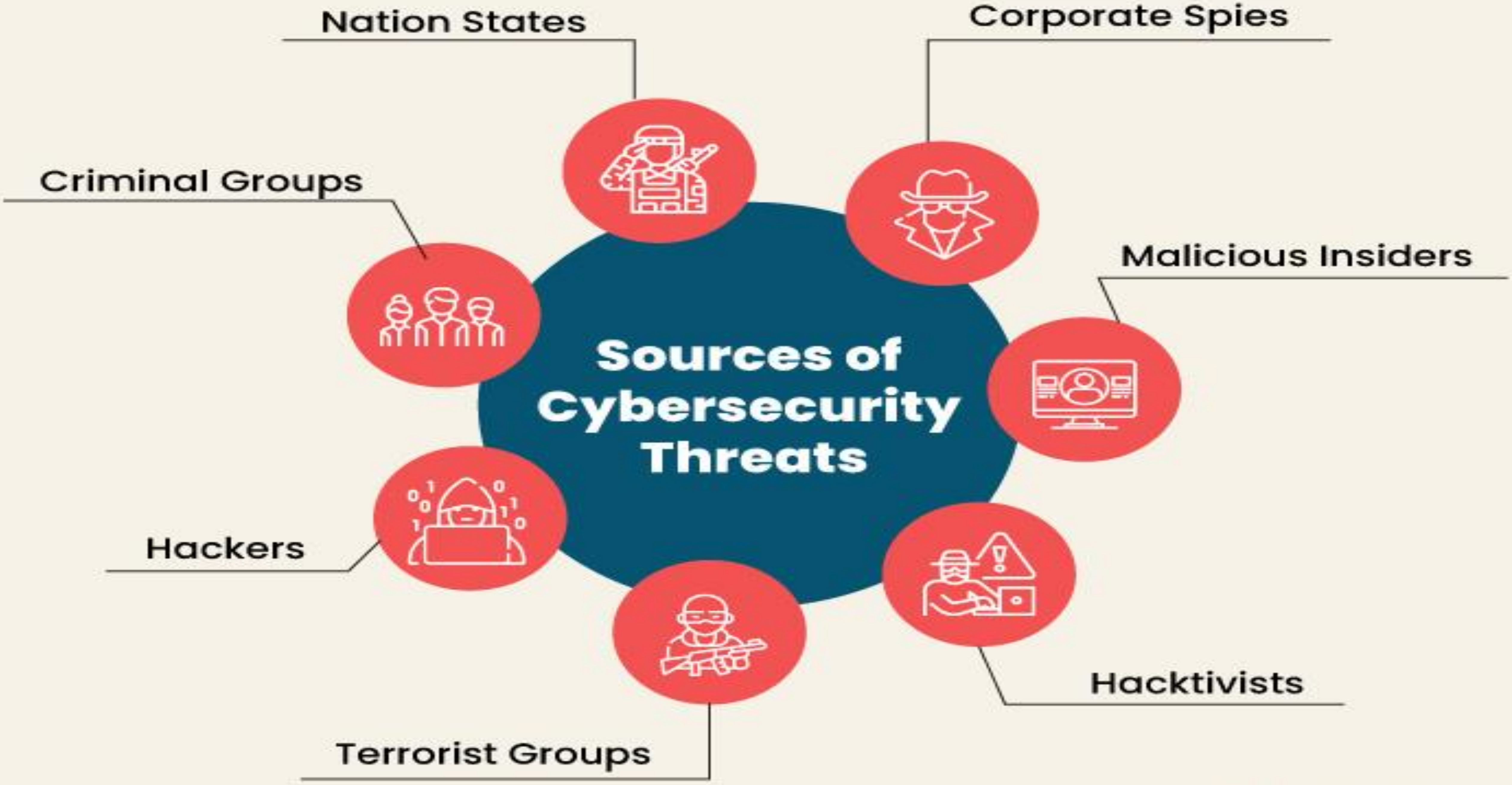
Injects malicious code into a website which targets the visitor's browser

SQL Injection Attack

Corrupts data to make a server divulge data, such as credit cards numbers, usernames

Source: Techterms.com, Lloyds of London, Forbes*

© AFP



Sources of Cybersecurity Threats

- Nation States
- Corporate Spies
- Malicious Insiders
- Hacktivists
- Terrorist Groups
- Hackers
- Criminal Groups

Types of Computer Security

1. **Cyber security** is defending all technological devices from online threats. Many categories like mobile computing and business use this term frequently.
2. **Network security** is securing a computer network from any type of cyber attack.
3. **Application security** is protecting software and programs and is usually inbuilt in the applications.
4. **Information security** is responsible for protecting the integrity and privacy of data everywhere.
5. **Operational security** involves protecting the data assets by deciding their storage and accessing procedures.
6. **Disaster recovery and business continuity** is the response of the cybersecurity accident leading to loss of data. The recovery policies define the procedure to continue operations in the organization. Business is the plan by which this operation takes place.
7. **End-user education** refers to the measures that the user takes on a personal level to protect themselves from these threats.

Computer Security Terminology

1. **Unauthorized access** – Gaining access to data, server, etc. without having the permission of the administrator.
2. **Hacker** – A person who exploits people by breaking into their device.
3. **Threat** – An action that may lead to a breach in cyber security.
4. **Vulnerability** – A problem or an error that leads to undesirable events in cyber security.
5. **Attack** – An assault by someone on cyber security.
6. **Antivirus or Antimalware** – program to protect devices from malicious software.
7. **Social Engineering** – A technique to steal data using psychological manipulation and social scenes.
8. **Virus** – A malicious software that downloads on its own on the computer for unethical purposes.
9. **Firewall** – A filter to manage network traffic rules

CYBER SECURITY DEFINITION

- 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.
- The application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks.
- **Aims : reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.**

Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

How does cyber security work?

Cybersecurity uses people, processes and technology to protect businesses from cyber threats.

People with highly specialized skills provide round-the-clock eyes on the business digital environment to safe guard them from potential cyber threats and attacks.

- ✓ These heroes are know by the following names; Managed Security Services, Cyber Security Analysts, Threat Hunter, Blue Team, Red Team, Purple teams, Ethical Hackers/Penetration Testers and more.

Processes include Security Operation Centers (SOC), security compliance to industry standards, and security audits. A SOC runs 24x7x365 on digital assets in a business using many processes for monitoring, detecting and neutralizing cyber threats and attacks.

- ✓ A business may choose to comply with guidelines from security frameworks such as NIST and ISO27000. Regular security audits can be performed by businesses to insure that their security policy is being followed. All of these put together constitute the processes needed by a business to secure itself.

Technology is the brawn of the cyber security world and do the heavy lifting of examining millions of threats from various threat vectors.

- ✓ They use state of the art technologies such as Artificial Intelligence, Machine Learning, synchronized security, next-gen security for endpoints, wifi, network, mobile devices and SOAR (Security Orchestration, Automation and Response) platforms.

What the benefits of having cyber security?

Having cybersecurity service or solution for an individual or business enhances the businesses in four key ways;

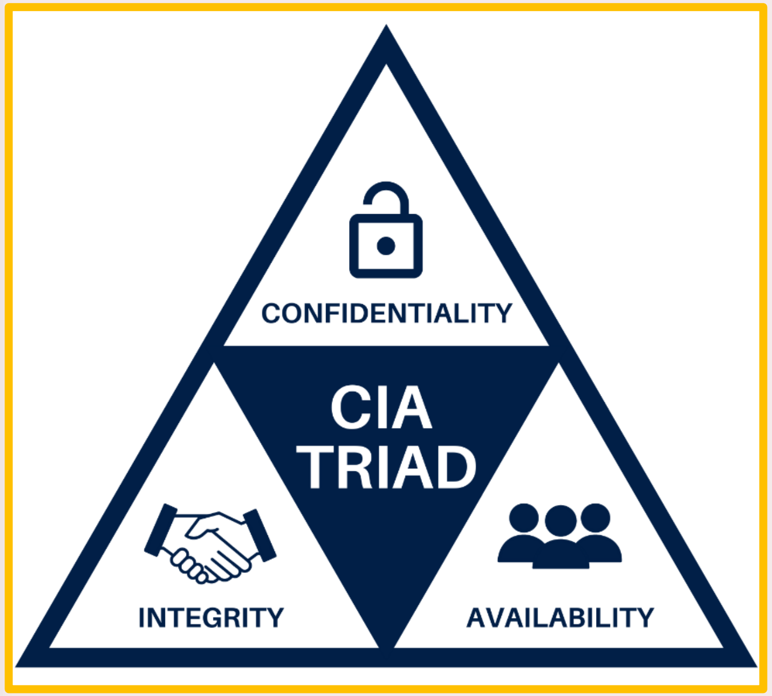
1. Reducing business risk

2. Protecting Reputation

3. Preventing Revenue Loss

4. Differentiating business from others

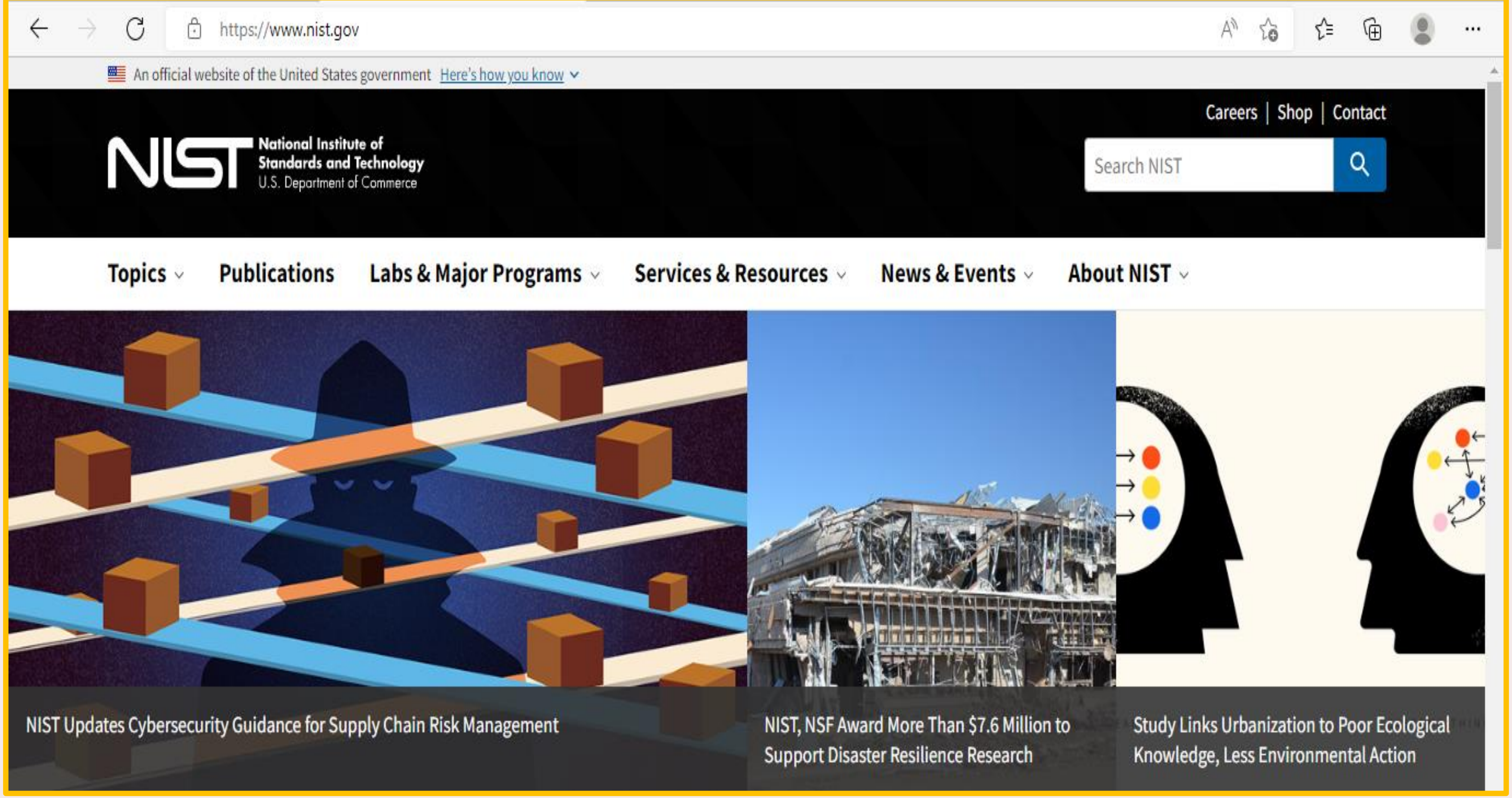
Principles of Cyber Security



- ❑ A large contributor to the notion of cyber security is Information Security, widely regarded as comprised of three main elements:
- ❑ **Information security :** Preservation of *condentiality*, *integrity* and *availability* of information.
- ❑ In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
- ❑ The security community commonly refers to a triangle of three related principles that ensure data is secure, known as the CIA triad:
- ❑ The primary objective of cyber security is to protect data.

Principles of Cyber Security

- These three concepts form what is often referred to as the **CIA triad**. The three concepts embody the fundamental security objectives for both data and for information and computing services.
- For example, the NIST(US National Institute of Standards and Technology) standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.
- FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Availability



https://www.nist.gov
An official website of the United States government Here's how you know
Careers | Shop | Contact
NIST National Institute of Standards and Technology U.S. Department of Commerce
Search NIST
Topics
Publications
Labs & Major Programs
Services & Resources
News & Events
About NIST

NIST Updates Cybersecurity Guidance for Supply Chain Risk Management

NIST, NSF Award More Than $7.6 Million to Support Disaster Resilience Research

Study Links Urbanization to Poor Ecological Knowledge, Less Environmental Action

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

This definition introduces three key objectives that are at the heart of computer security:

1. **Confidentiality:** This term covers two related concepts:
   - ✓ **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
   - ✓ **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2. **Integrity:** This term covers two related concepts:
   - ✓ **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
   - ✓ **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
3. **Availability:** Assures that systems work promptly and service is not denied to authorized users.

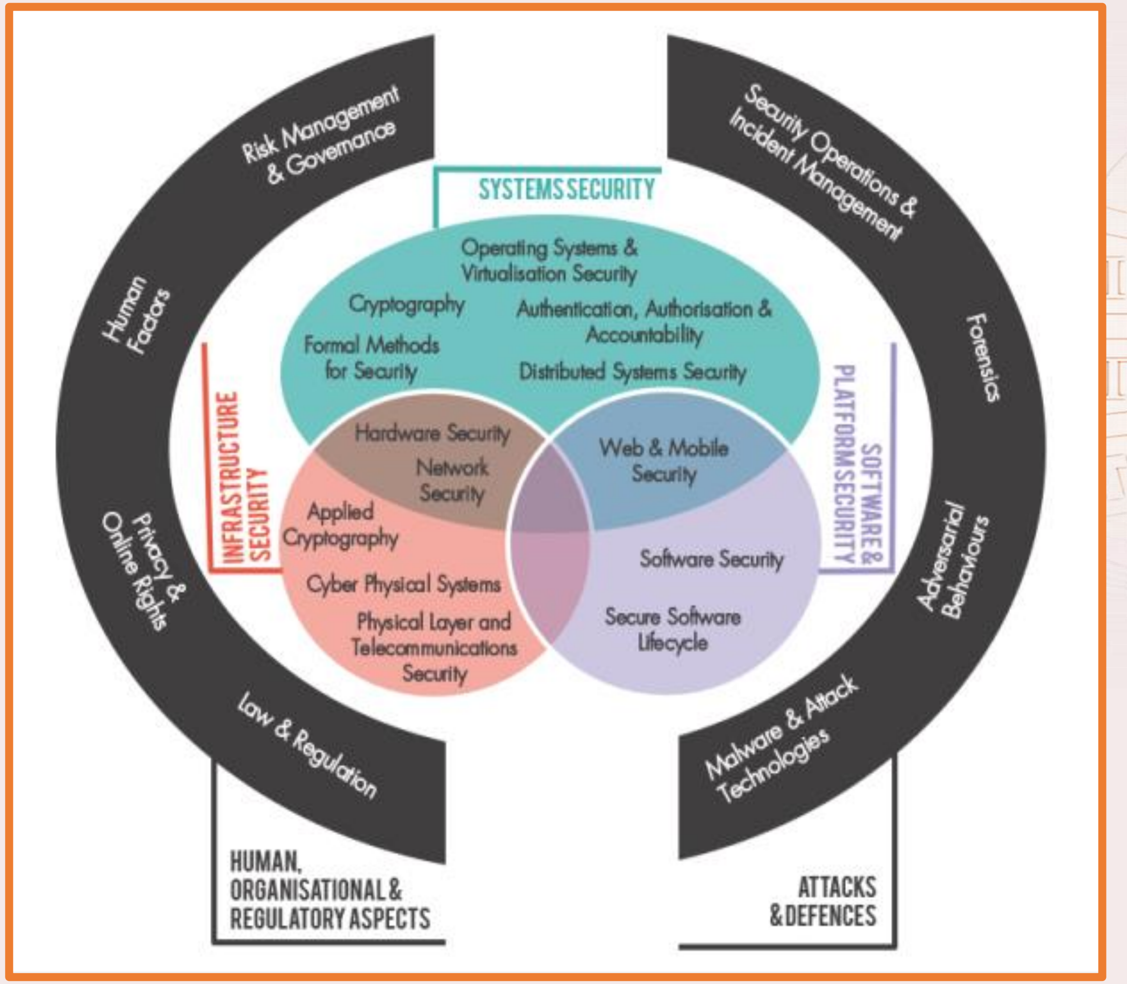
Two of the most commonly mentioned are as follows:

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

The 21 Knowledge Areas (KAs) in the CyBOK Scope

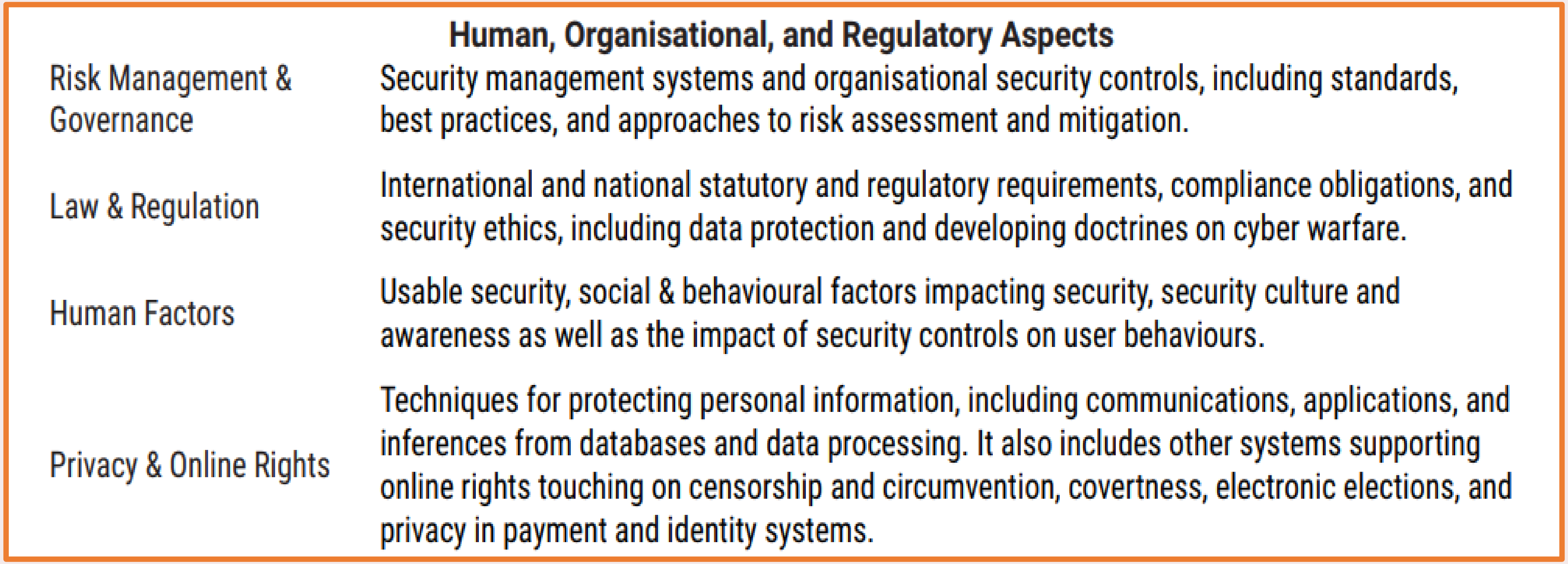
Cyber Security Body Of Knowledge (CyBOK)


Risk Management & Governance
Security Operations & Incident Management
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
Human Factors
Forensics
INFRASTRUCTURE SECURITY
SOFTWARE & PLATFORM SECURITY
Hardware Security
Network Security
Web & Mobile Security
Applied Cryptography
Software Security
Cyber Physical Systems
Physical Layer and Telecommunications Security
Secure Software Lifecycle
Privacy & Online Rights
Adversarial Behaviours
Law & Regulation
Malware & Attack Technologies
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
ATTACKS & DEFENCES

1. Human Organisational and Regulatory Aspects
2. Attacks and Defences
3. System Security
4. Software Platform Security
5. Infrastructure Security

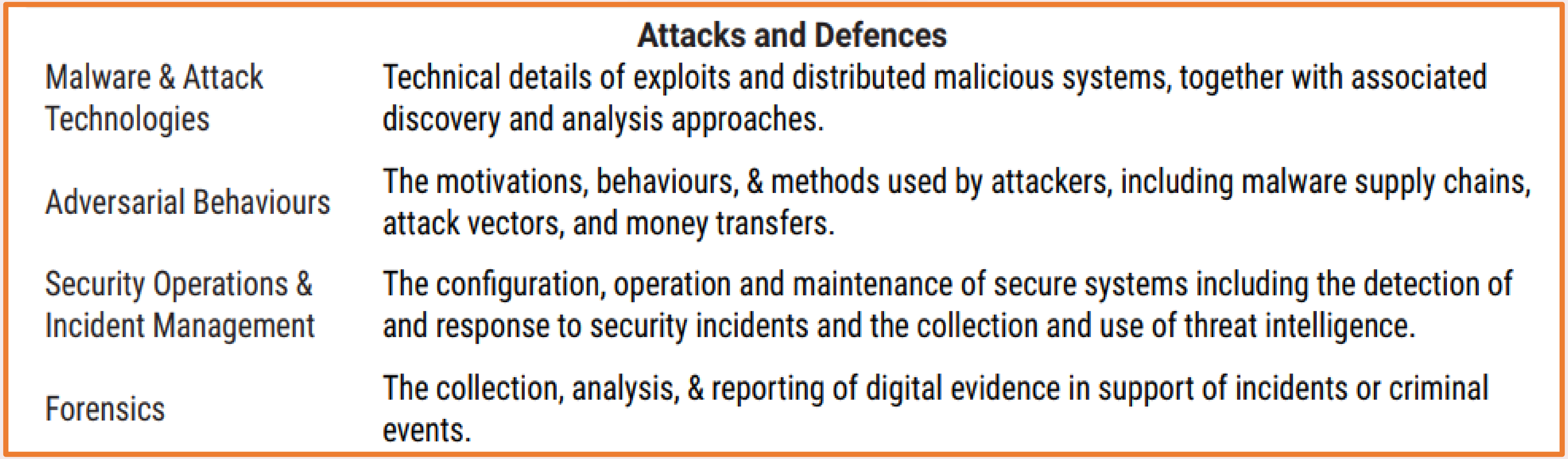
4 + 4 + 5 + 3 + 5 = 21 Knowledge (CyBOK)

1. Human, Organisational and Regulatory Aspects



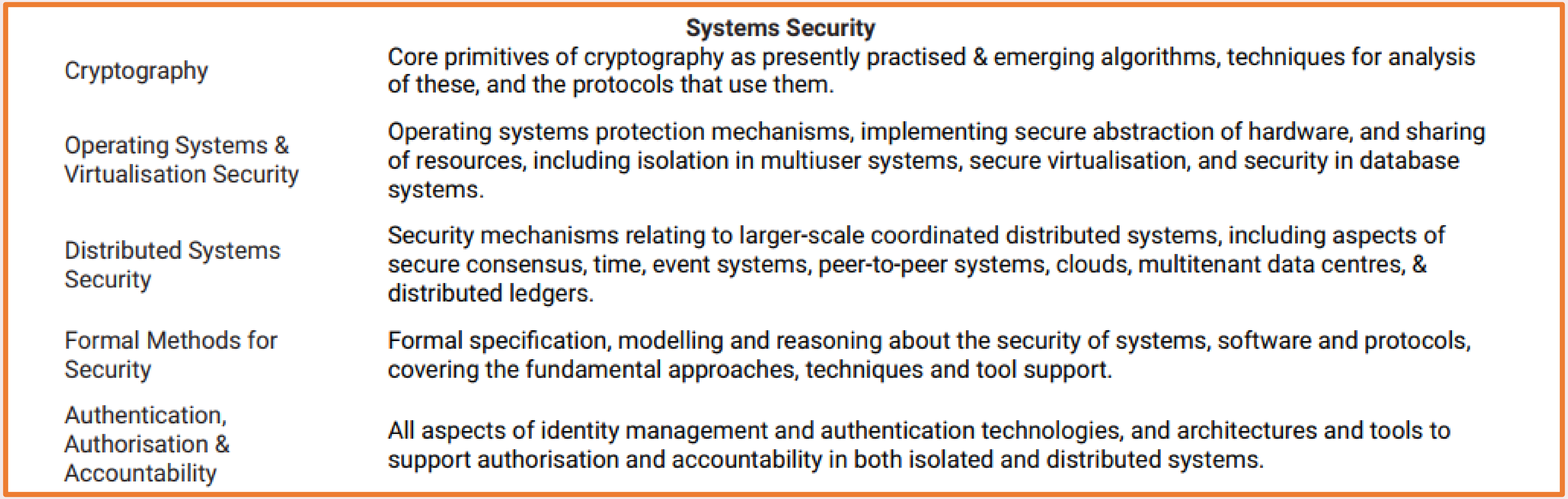
	Human, Organisational, and Regulatory Aspects
Risk Management & Governance	Security management systems and organisational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law & Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social & behavioural factors impacting security, security culture and awareness as well as the impact of security controls on user behaviours.
Privacy & Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.

2. Attacks and Defences



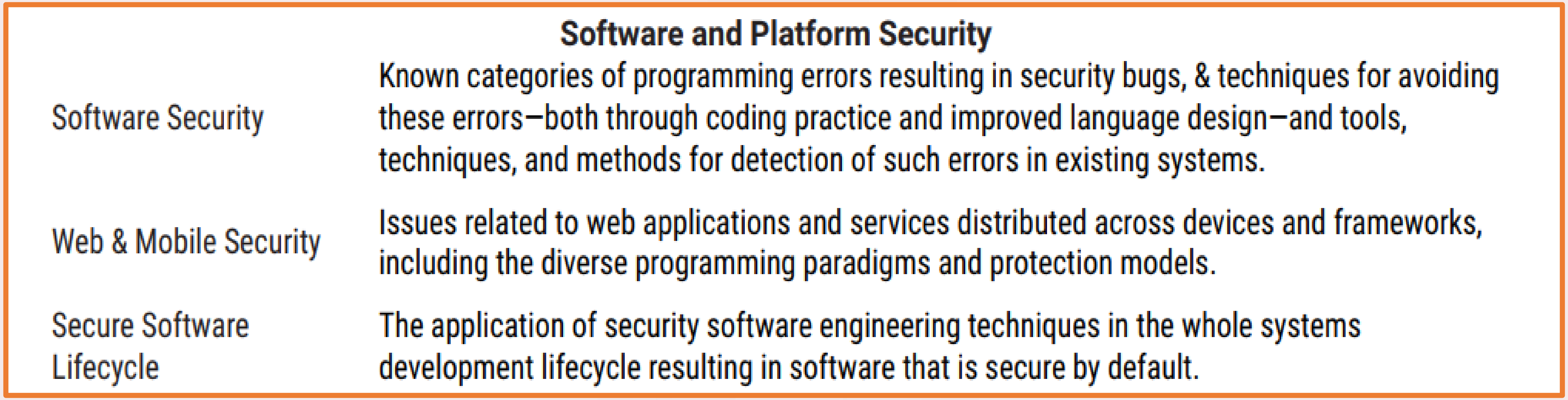
Attacks and Defences	
Malware & Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviours	The motivations, behaviours, & methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations & Incident Management	The configuration, operation and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, & reporting of digital evidence in support of incidents or criminal events.

3. Systems Security



	Systems Security
Cryptography	Core primitives of cryptography as presently practised & emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems & Virtualisation Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualisation, and security in database systems.
Distributed Systems Security	Security mechanisms relating to larger-scale coordinated distributed systems, including aspects of secure consensus, time, event systems, peer-to-peer systems, clouds, multitenant data centres, & distributed ledgers.
Formal Methods for Security	Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support.
Authentication, Authorisation & Accountability	All aspects of identity management and authentication technologies, and architectures and tools to support authorisation and accountability in both isolated and distributed systems.

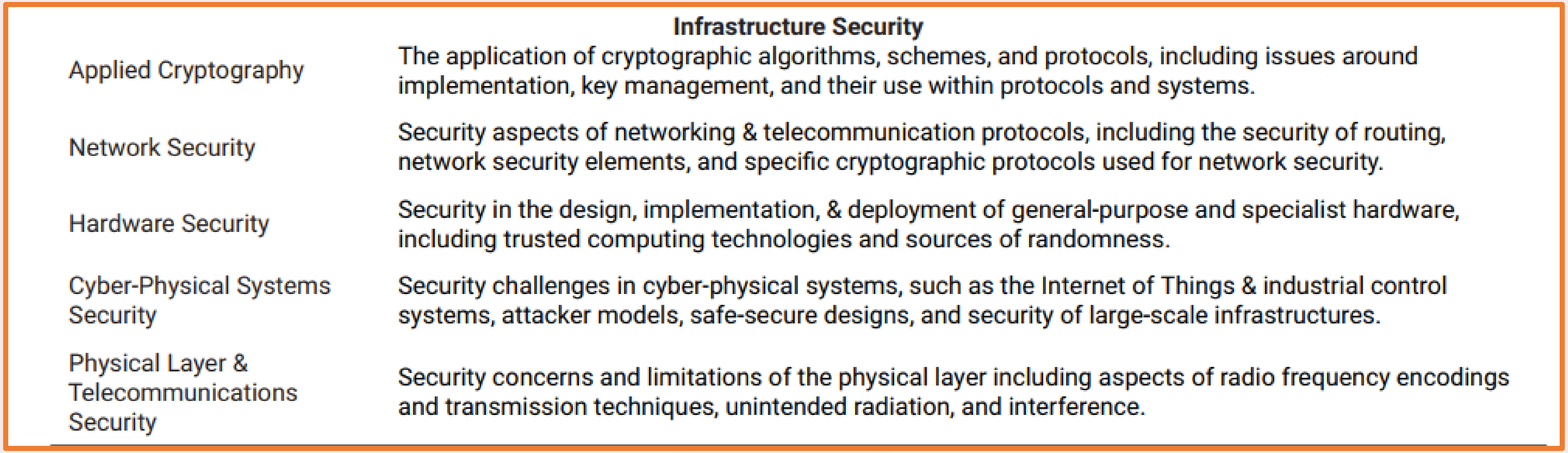
4. Software and Platform Security



Software and Platform Security

Software Security	Known categories of programming errors resulting in security bugs, & techniques for avoiding these errors—both through coding practice and improved language design—and tools, techniques, and methods for detection of such errors in existing systems.
Web & Mobile Security	Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models.
Secure Software Lifecycle	The application of security software engineering techniques in the whole systems development lifecycle resulting in software that is secure by default.

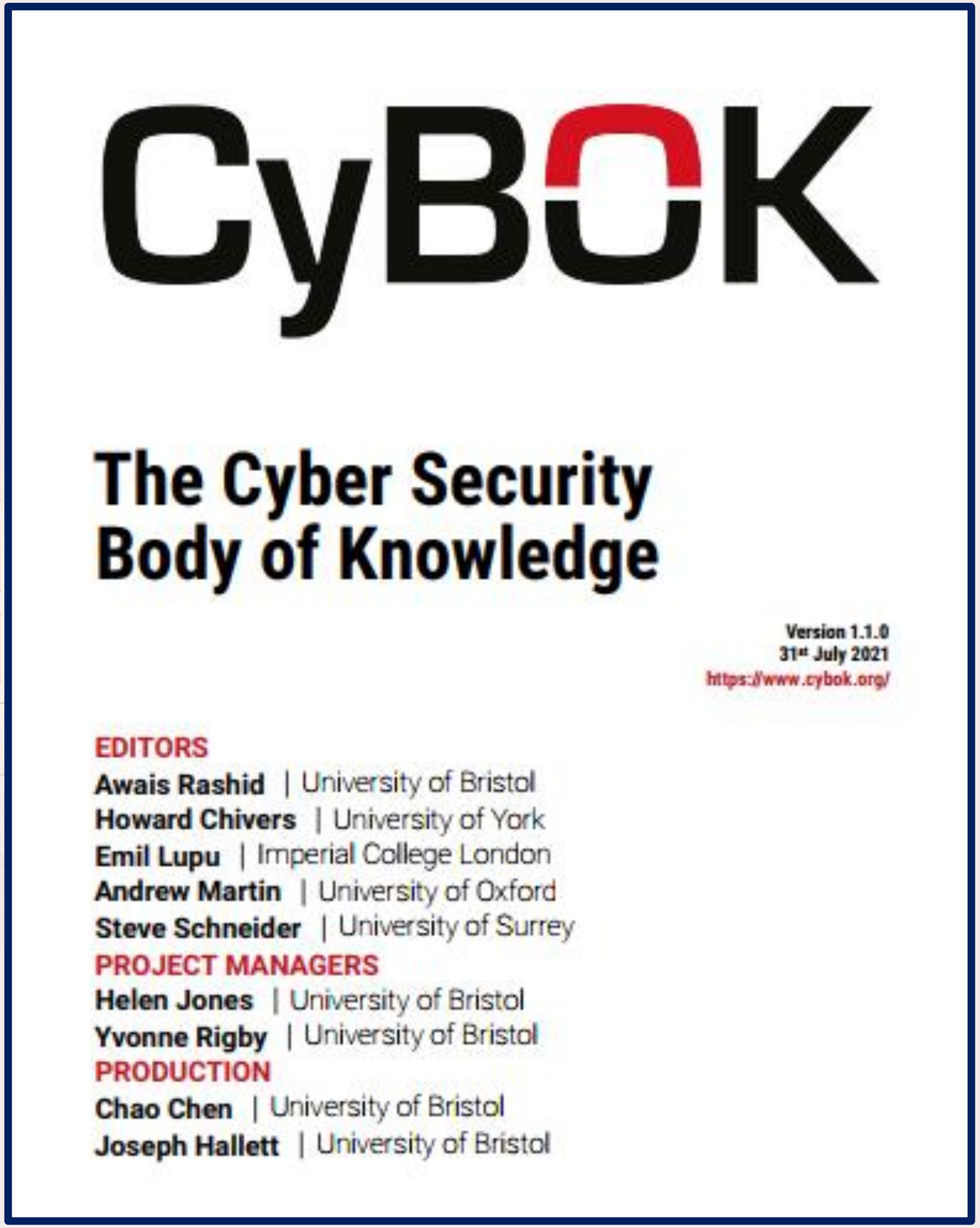
5. Infrastructure Security



Infrastructure Security

Applied Cryptography	The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems.
Network Security	Security aspects of networking & telecommunication protocols, including the security of routing, network security elements, and specific cryptographic protocols used for network security.
Hardware Security	Security in the design, implementation, & deployment of general-purpose and specialist hardware, including trusted computing technologies and sources of randomness.
Cyber-Physical Systems Security	Security challenges in cyber-physical systems, such as the Internet of Things & industrial control systems, attacker models, safe-secure designs, and security of large-scale infrastructures.
Physical Layer & Telecommunications Security	Security concerns and limitations of the physical layer including aspects of radio frequency encodings and transmission techniques, unintended radiation, and interference.

Reference Book



CyBOK

The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey

PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol

PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol

Thank You!

Lesson One Completed!

U Tin Naing Htwe
Senior Lecturer(ICT)
Optimum Institute