UNIVERSITY
COLLEGE
BIRMINGHAM

University College Birmingham

Cyber Security Strategy

2021 – 2024

Contents

Forword

Organisations and businesses are increasingly dependent on technological systems, digital transformations and innovation to carry out operations. The advancement of Digital Communications carries significant Cyber threats on organisations and such attacks are leading to large scale damage and disruption to corporations' operations.

The education sector is not immune to the threat of Cyber-attacks, such incidents have affected the industry, both Further Education and Higher Education, across the country. It has been reported that one Cyber-attack per week is compromising the education sector within the UK. *Source; JISC*

This strategic document sets out the university's application of Cyber Security and Information standards to protect systems, data, student cohort and the services we provide from unauthorised access, harm or miscue. Embracing the need for a robust Cyber Security Strategy and being prepared for such attacks represents significant challenges for the University.

It is the University College Birmingham's Cyber Security commitment to our staff and students and emphasise the importance of Cyber Security across the whole of the University.

What is Cyber Security

Cyber security is how individuals and organisations reduce the risk of Cyber-attacks. It is also the practice of ensuring the confidentiality, integrity and availability (CIA) of data and information.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access - both online and at work - from theft or damage. One core feature of Cyber security is to prevent unauthorised access to the vast amounts of personal information and data we store across the Universities network and computer systems.

The University, in order to deliver to its core business of teaching and learning, stores large amounts of personal data, including personal and financial data which unauthorised access or exposure will have serious consequences.

An effective Cyber Security Strategy is critical in ensuring our services are operational at all times and functioning effectively. It is also imperative that our customers trust the University with their information. A Cyber attack could have serious consequences, both in terms of disrupting services, and through damage to the Universities' reputation.

Strategic Context

UCB mission statement

To promote and provide the opportunity for participation in the learning process by those with the ambition and commitment to succeed and to maintain a learning community that meets the diverse needs of our students, the economy and society at large

University Corporation

This strategy will support the corporation's mission by providing a framework to harness the benefits of the digital transformation for all stakeholders. This strategy will sit alongside the IT strategy and will be supported by UCB operational policies.

Purpose

The Cyber Security Strategy has been introduced in response to the growing Cyber-attacks and threats on public and private organisations. The purpose of this strategy is to give assurance to the university student cohort, staff and stakeholders of the commitment in delivering robust information security measures to protect data from misuse and threats, and to safeguard privacy through increasing secure and modern information governance and data sharing arrangement.

Scope of the Strategy

This strategy will cover all UCB information systems, the data held on the systems, and the services the systems provide. The strategy will increase Cyber security posture and awareness across the university, students and Its stakeholders.

The university is digitalising its core information systems, deploying devices and gadgets to its core customers. Much of this is on-line and brings threats that need mitigating. The digitisation will accelerate, making Cyber security ever more crucial in protecting against new types of threats, risks and vulnerabilities.

With this change will come extra pressures and challenges in all areas of the organisation, especially its technological and digital footprint in what it delivers to enhance and innovatively change teaching and learning. These challenges mean an ever-increasing Cyber risk is posed to the University. Through the delivery of the Cyber Security Strategy to formalise and harmonise the approach to Cyber risks of the institution, this will put the University in a strong position for whatever uncertain Cyber challenges that will be faced in the future.

- **Cybercrime global cost $6 trillion in 2021**
- **Projected to rise to $10 trillion by 2025**

Source; Cybersecurityventures.com

Cyber Security Threats and Vulnerabilities

A Cyber or Cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital operations in general. Cyber-attacks include threats for example computer viruses, malware, data breaches, and Denial of Service (DoS) attacks.

Types of Threats

- Ransomware – a serious attack which encrypts data and systems with the potential to shut down entire organisation operations
- Malware – software program that performs a malicious task on a target device or network, corrupting data or taking over a system
- Email Phishing – victim receives a spoofed malicious email, impersonating as a trusted entity into opening an email. The victim is tricked into clicking the malicious

link which results in system being infected with malware

- Denial-of-service attack (DoS) – Cyber-attack where a perpetrator seeks to make a system unavailable to its customers. DoS attacks accomplish disabling services by flooding network traffic or submitting information that triggers system crashes
- DNS (Domain Name System) attack – exploits vulnerabilities in the DNS by flooding the system making the DNS service inoperable
- Advanced persistent threat – stealth infiltration attack gaining access to systems which are undetected for an extended period

Common Sources of Cyber Security Threats

Cyber attackers come in various forms and identities. Attackers can be grouped by their set of goals, motivation and capabilities. As Digital Transformations gather apace globally, this presents attackers with opportunities and motivation to hack corporate systems for personal and financial gain.

- Cyber Criminals – attackers who commit cybercrime by stealing sensitive data
- Hacktivists – carry out malicious activity to promote beliefs and ideology
- State-Sponsored attackers – highly skilled operatives objectives aligned with their nation state
- Insider threats – internal attacks from employees present and past and third parties

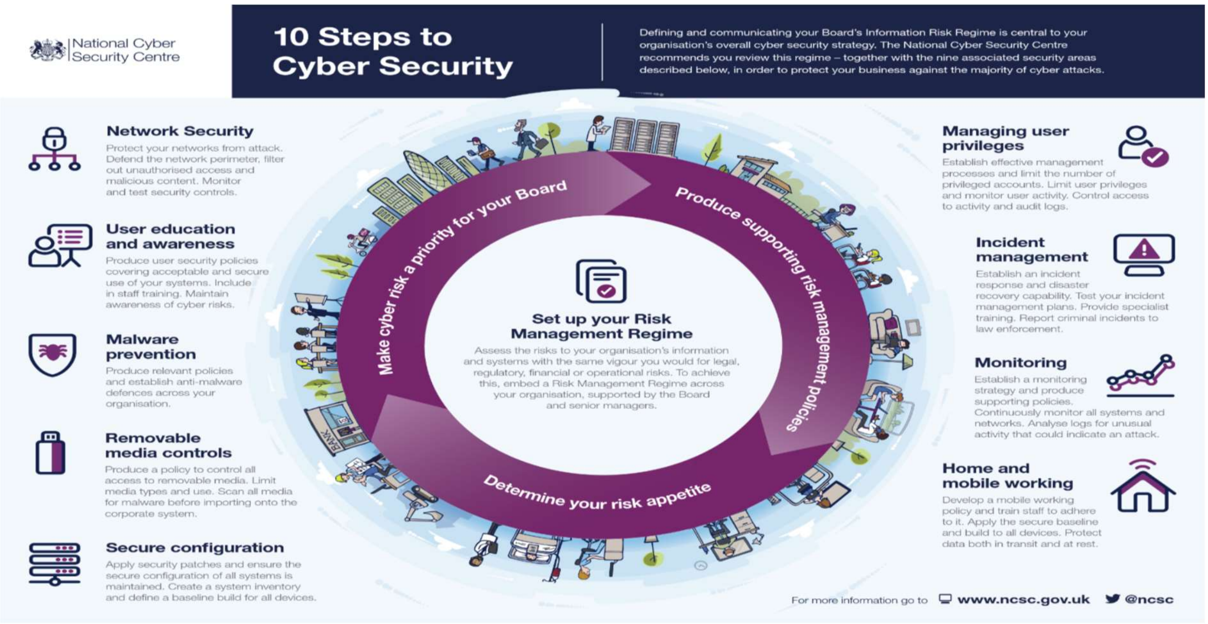
Strategic Actions

To achieve a robust Cyber Security Strategy, UCB will proactively enhance measures to protect and strengthen the corporation’s security systems and protocols by;

- Implementing Next Generation Cyber Security Services,
    - Firewall
    - Anti-Virus
    - Endpoint Detection & Response (EDR)
    - Managed Detection & Response (MDR)
    - Multi-Factor Authentication (MFA)
    - Security Information Event Management 24/7 monitoring (SIEM)
- Certification of Cyber Essentials and/or ISO 27001 accreditations
- Effective Data Backup strategy segmented from core network
- Systems updated with critical security software patches
- Network Access Control policy
- Robust password policy

- Raise Cyber Security awareness; training, bulletins and seminars
- Network Penetration and Phishing simulation tests
- Build and test Cyber Incident Response Plan
- Train and up-skill IT staff in Cyber Security awareness and emerging solutions

To complement the strategic actions and ensuring UCB have a robust and resilient IT Infrastructure, the National Cyber Security Centre, 10 Steps to Cyber Security framework will be adopted to increase the overall security posture;



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

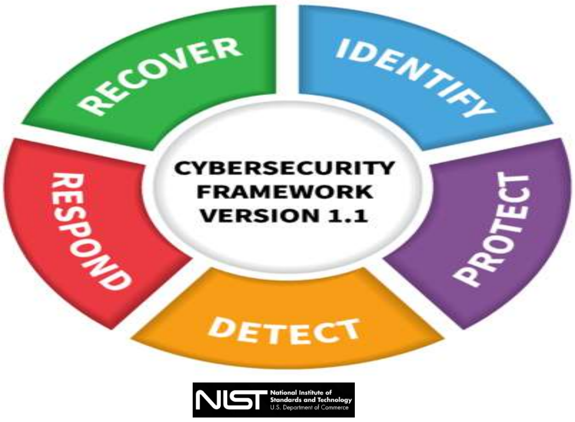
For more information go to www.ncsc.gov.uk @ncsc

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

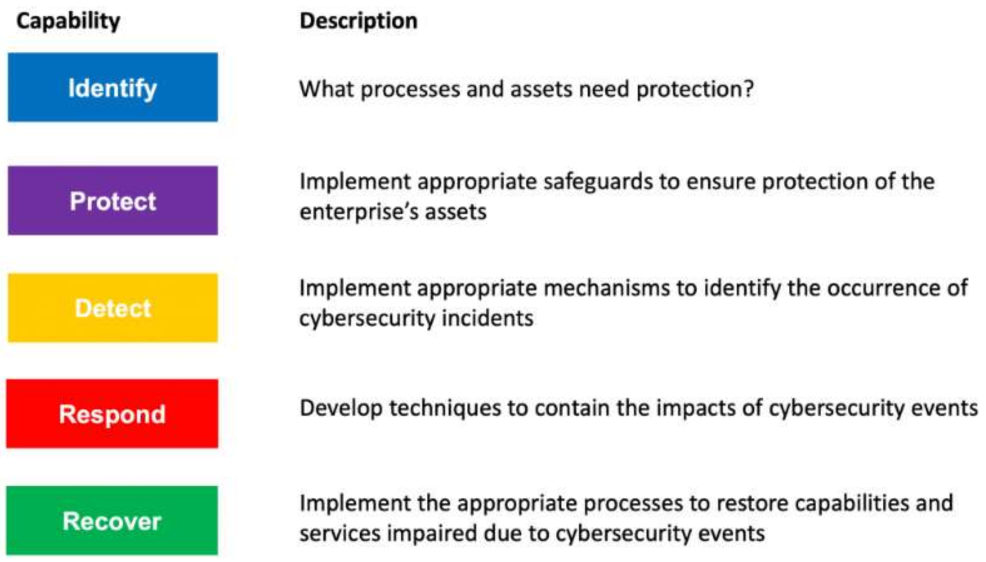
- **Network Security**; Protect the infrastructure against external and internal threats. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls
- **User Education & Awareness**; Produce user security policies covering the acceptable and secure use of organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks
- **Malware Prevention**; Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation
- **Removable Media Controls**; Control all access of removable media. Limit media types and use. Scan all media for malware before importing into the corporate system
- **Secure Configuration**; Apply security patches and ensure that the secure configuration of all IT systems is maintained. Create a system inventory and define a baseline build for all IT devices
- **Managing User Privileges**; Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs

- **Incident Management**; Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to the authorities
- **Monitoring**; Establish a monitoring strategy and develop supporting policies. Continuously monitor all IT systems and networks. Analyse logs for unusual activity that could indicate a cyber attack
- **Home and Mobile Working**; Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest
- **Data Breach Notifiers**; Protect your network against internal and external data breach attempts. Install the devices that would alert immediately if someone has infiltrated your systems

To complement the NCSC model, UCB will also be adopting and implementing the National Institute of Standards and Technology (NIST) framework to further strengthen its Cyber Security posture;


RECOVER
IDENTIFY
CYBERSECURITY FRAMEWORK VERSION 1.1
RESPOND
PROTECT
DETECT
NIST National Institute of Standards and Technology U.S. Department of Commerce

The framework provides a common understanding, managing, and expressing Cybersecurity risk both internally and externally. It is a set of guidelines and best practices on improving Cybersecurity posture. The framework sets out a set of recommendations and standards to assist organisations in identifying and detecting Cyber-attacks. The framework also provides on how to respond, prevent and recover from such attacks.



Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

NIST Cybersecurity Framework

This approach will enable the continuous improvement of the security maturity of the University, as well as maintaining and updating ongoing BAU activities and project strategic support (security advice, security incident management, project assurance, monitoring activities, vulnerability scanning, penetration testing) to ensure they remain fit for purpose.

Success Measures

To provide assurances to the corporation on the effectiveness and robustness of UCB security systems, the following measures will be developed in line with the strategic actions set out;

- Define Cyber Security governance process
- Develop Cyber Risk Management Framework which feeds into the IT Strategies
- Review policies and procedures on systems access regularly
- Create Incident response Plan and tested periodically
- Create standard test plans with security testing reporting to the EMT
- Apply government guidance and best practise to operational processes
- KPI reporting to EMT on security breaches

Summary

This Cyber Security Strategy will ensure the University has in operation adequate controls and measures of protection against external Cyber-attacks. These protocols will ensure safe and secure systems are in place to deliver services our customers expect. The implementation of this strategy is our commitment to take active steps towards delivering the Cyber security vision, to assess and improve organisational maturity in delivering against industry standards.