CYBER SECURITY STRATEGY 2025 - 2028

UNIVERSITY COLLEGE BIRMINGHAM

CONTENTS

FOREWORD

This strategy emphasises the University's dedication to both technical excellence and a broader ethical perspective in the ever-evolving field of cybersecurity.

In today's digital world the education sector has an ever-increasing reliance on technology which has presented opportunities and challenges to institutions across the globe.

This Strategy demonstrates that the University recognises the security challenges of cyber space and the threat to data, systems, students and staff, it stresses the importance of a coherent approach, and it will put in place the structures that the institution needs to navigate together new and existing work and drive forward a programme to meet our strategic objectives. The Strategy highlights the need for the University and its partner network to work together to meet our strategic objectives of reducing risk and exploiting opportunities by improving knowledge, capabilities and decision-making in order to secure the Universities future in the cyber security space.

Regards

Pooran Kumar

Director of IT & Digital Infrastructure

Executive Summary

The evolving threat landscape in cybersecurity necessitates a robust and adaptive strategy to safeguard the University's digital assets, personal data, and intellectual property. This strategy outlines the vision, goals, and actionable steps for enhancing our cyber defence mechanisms from 2025 to 2028.

The University will continue to secure its digital transformation by innovating and collaborating in Cyber Security, to create a dynamic learning environment and safeguarding for its students and staff.

This strategy will continue to safeguard assets, data, and students across campus, and to ensure security is at the forefront of all operations throughout campus.

Vision

The purpose of this strategy is to establish a resilient, secure, and compliant cyber environment that supports academic excellence and operational efficiency. This strategy will involve a systematic approach to tracking, identifying, assessing, and mitigating risks while establishing guidelines for incident response and adherence to compliance National standards.

Strategic Objectives

Strengthen & Enhance Cyber Defences
Strengthen perimeter defences and internal network security Implement advanced threat detection and response systems. Regularly update and patch all systems to mitigate vulnerabilities.

Ensure Compliance and Data Protection
Align with regulatory requirements such as GDPR, Implement robust data encryption practices Conduct regular data privacy impact assessments.

Foster a Culture of Cyber security Research & Innovation
Support projects focused on cyber security advancements. Collaborate with industry partners for cutting-edge solutions and third-party vendors for the latest trends on Cyber initiatives.

Promote Cyber Security Awareness & Training
Develop a comprehensive cybersecurity training awareness program for students, faculties, and staff. Conduct Regular phishing simulation exercises.

Strengthen Incident Response and Recovery
Develop and test incident response plans. Enhance the cyber incident response team (CIRT) Ensure business continuity through regular disaster recovery testing.

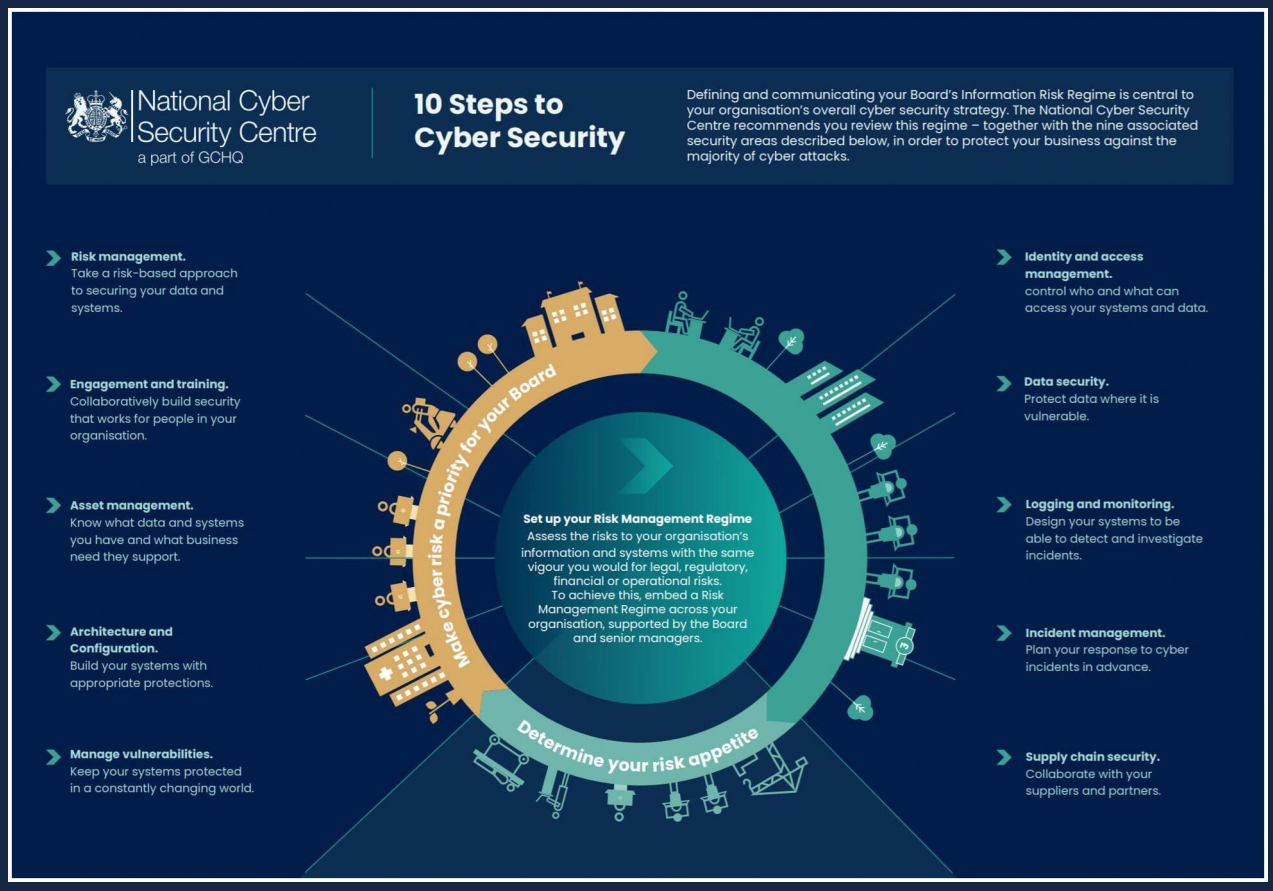
Implement Zero Trust Architecture
Adopt a zero-trust security model, verifying all users and devices. Segment networks to minimize potential breach impacts. Use multi-factor authentication (MFA) and continuous monitoring

Risk Assessment and Management

With the increasing sophistication of cyber-attacks, institutions face challenges to mitigate these current and emerging threats;

Risk mitigation plans will prioritise actions based on the potential impact and likelihood of risks. This will include implementing advanced threat detection technologies and enhancing staff training.

The National Cyber Security Centre 10 steps to Cyber security will be the cornerstone of the strategy;



The multiplication of digital uses, devices and users is generating an increasingly complex landscape and is also creating more potential entry points for potential cyber-attacks. Emerging technologies such as Artificial Intelligence computing and 5G will also create both opportunities and risks. Cyber security has become paramount to protect our students, staff, systems, data and institutional reputation.

Cyber security will continue to evolve in both threat and response to those threats. Cyber criminals now have more innovative ways to perform more devastating and diversified attacks.

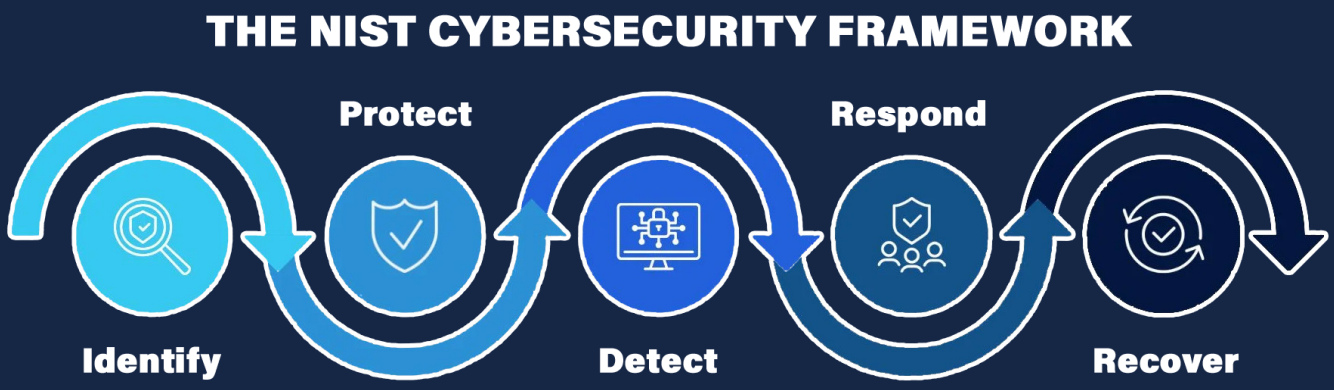
The rapid acceleration to digital operations, and an increasing amount of data is shared and stored digitally, Cyber risks extend well beyond the cyber ecosystem.

Cyber Governance

The University Digital Transformation Group comprising members from various departments will oversee and guide cyber security initiatives across campus.
Regularly review and update cyber security policies to address emerging threats and regulatory changes. Policies will cover areas like data protection, acceptable use, incident response plans and disaster recovery.

Incident Response and Recovery

The NIST Cybersecurity framework will be adopted to respond to threats



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

Continuous Cyber Improvement and Success Measures

Conduct regular audits and assessments, both internal and external, and engage third-party contractors to conduct independent assessments of the cyber security program. Testing and reviewing the disaster recovery plans to ensure it is current and robust.

It is important to remember the Cyber space landscape does not stay static, it is a fluid environment and external threats will come and go. The level of risk will also change, it is therefore essential cyber resilience is monitored and tested regularly.

To effectively measure the success of our Cyber security program, focus will be on a combination of quantitative and qualitative metrics;

- Risk Reduction – vulnerability management, threat intelligence and incident response
- Compliance – adherence to regulatory standards and audit outcomes
- Incident and Breach Metrics – measure frequency of incidents over time
- Security Awareness Training – Phishing click rates and training completion
- Independent network penetration test

Budgetary Impact of Strategy

Budgetary impact of the strategy is listed in the table below. This breaks down into the following components;

Next Generation firewall maintenance and updates	50,000 p/a
Threat hunting & MDR software maintenance and renewals	20,000 p/a
Automated Detection & Protection	3,000
Cyber training materials for staff	5,000 p/a

Year 3 of the strategy will trigger a review of all systems and cyber software in place and plan refresh accordingly, to ensure maximum protection from external threats across the institution.

Collaboration and Partnerships

Cross-departmental collaboration will be encouraged on cyber security initiatives to ensure comprehensive coverage of security across campus with all stakeholders.

Jisc

We will actively engage with our partners JISC to ensure compliance of cyber space and continuity of our SOC (security operations centre).

Knowledge and cyber initiatives will be shared with other educational institutions and engage in partnerships which foster collaboration and sharing of cyber technological trends.

CONCLUSION

The University is continually facing unprecedented change at all levels and with an aspiration for growth this is only going to continue. With this change comes challenges in all areas of the University but not least its digital and technological footprint in what it delivers to enhance and change learning and teaching. These challenges mean an ever-increasing cyber risk is posed to the University. Through the delivery of this Cyber Security Strategy to formalise and harmonise the approach to cyber risks of the institution, this will put the University in a richer position for whatever uncertain cyber challenges we face in the future. This will allow the instituition to deliver innovation into the University business and teaching and learning.