Module	**CYBERSECURITY**
Jurisdictions	**UK**
Legal Expert	**BEN SYMONS** Barrister https://www.taxchambers.com/barristers/ben-symons/ https://www.linkedin.com/in/ben-symons-31090818/

Module Application

Does your organisation have systems in place to protect its network and information systems against both failure and attack?

Have your organisation's systems and processes been designed to meet its risk exposure and ensure resilience?

Do those within your organisation understand their individual obligations to mitigate and/or manage the risks?

Module Scope

The UK does not have a dedicated cybersecurity law; consequently, the obligations to safeguard its network and information system from abuse, misuse (e.g., cyber-related criminality) or attack (internal or external) are contained across a number of laws.

An organisation is nevertheless required to have a resilient network and information system to withstand potential cyber (and non-cyber) attack to prevent a breach. Additionally, if an organisation holds or processes personal data, it has a legal duty under the Data Protection Act 2018, UK GDPR and, in appropriate cases, the EU GDPR to protect the data.

The CYBERSECURITY module addresses the regulatory frameworks through a set of 20 core obligations and sub-obligations that an organisation must take into account when building its cybersecurity strategy, along with required actions and the consequences for failure in each.

The core legal and regulatory obligations are based on the following considerations:

- Decision making;
- Accountability;
- Stewardship;
- Direction; and
- Control.

An organisation is required to ensure that its staff, contractors and agents are familiar with the legal obligations to which it is subject, as well as their individual responsibility. In so doing, an organisation must also take into account any sector or industry-specific guidance; for instance, for the financial sector, an organisation will be expected to be familiar with relevant FCA and NCSC guidance.

The aim of the module is to equip the subscriber with a practical and clear understanding of their obligations when operating within UK and provide an answer to the following questions:

- What are our legal obligations?
- What is the source of the legal obligations?
- How can we ensure that we are complying with our legal obligations?
- What are the consequences of non-compliance?

The CYBERSECURITY module recognises that one of the most serious breaches for an organisation is that relating to accidental or unlawful loss, destruction or alteration of personal data. A cyber-incident (deliberate or otherwise) may potentially result in hefty financial penalties, reputational damage, temporary loss of key operations and even legal proceedings. With that in mind, the module has incorporated the legal obligations, as well as guidance and recommendations, issued by the UK National Cyber Security Centre (NCSC) to provide an organisation with practical assistance in the implementation and maintenance of best practice processes throughout the organisation. The module also covers the role of the regulator and any exemptions, if applicable.

The module is divided into 20 core obligations and sub-obligations which examine:

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management
- Identity Management, Authentication and Access Control
- Awareness and Training
- Data Security to protect the confidentiality and integrity of data, digital services and information systems
- Information Protection Processes
- Maintenance
- Protective Technologies
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
- Response Planning and Communication
- Mitigation
- Improvements and Recovery Planning
- Communications (internal and external)

As highlighted above, if an organisation processes personal data, its loss, destruction or alteration is ranked as one of the most serious breaches under the UK GDPR and Data Protection Act 2018 (as amended), leading to financial and/or non-financial penalties.

A failure to put in place adequate systems and processes to prevent a potential cyber (and noncyber) attack may also lead to other enforcement measures. The consequences vary considerably, depending on the nature and extent of the breach or failure. It is, therefore, vital that all staff are fully trained and equipped to discharge their duties, which includes having an understanding of their individual and the organisation's legal risk and exposure. At LexisNexis we appreciate the importance of helping non-legal staff understand such

obligations. The CYBERSECURITY module provides this in an easy-to-understand format that can be readily referred to and used by all staff.

Post-Brexit, the CYBERSECURITY module now focuses primarily on UK law and does not cover EU regulations or directives (unless applicable). The module does not, however, address the rights or entitlements of individuals who have suffered damages or losses due to breaches of cybersecurity obligations by UK organisations, nor does it cover the process that an entity or an individual would follow to report or seek compensation for the breach and any loss.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.