an executive introduction to

managing digital risk

Oxford Cyber Academy

CYBER SECURITY COURSE

An online, self-paced learning programme of 5 hours per week over six weeks. This course will give you an essential insight into cyber security and how it impacts your organisation. From the threat landscape through to cyber regulations and industry standards, and from the roles of security departments to future challenges in cyber security risk management, this modular course is a must for anyone facing the intricacies and uncertainties of today's technology led environment.

innovate inspire inform

an executive introduction to

managing digital risk

who is this course for?

Non-technology executives at any level who want to support their organisation to reap the full benefits of digital transformation, while minimising the security risks;

Technology and security specialists who need a broader view of cyber risk management as part of their progression to leadership roles;

Managers and analysts who need to communicate the implications of cyber threats to stakeholders.

course content

You will learn how to accurately assess an organisation's cyber risk profile, in terms both of potential threats and also of governance structures, systems and process.

You will understand the range of implications for an organisation that come with legal requirements for compliance with standards and regulation.

You will appreciate how the introduction of new digital technologies brings new challenges in cyber security.

At the end of the course, you will be prepared to support senior management decisions about the governance and mitigation of cyber risk.

duration

6 weeks with 5 hours per week of self-paced learning, entirely on-line.

an executive introduction to
managing digital risk

module 1
why cyber security matters - the threat landscape

Explore how all previous industrial revolutions differ radically from 'Industry 4.0'.

Through a series of case-studies, investigate the main cyber security threat actors, their motivations and methods, and the different sectors or types of organisation they often attack.

Understand how they threaten an organisation's integrity by attacking its critical business systems and data.

Begin work on aligning this knowledge with how your own organisation thinks about cyber threats. This is the start of an on-going project in which you will assess the vulnerabilities of your own organization and how they can be mitigated.

module 2
understand your organisation's 'crownjewels'

Discover who hackers are likely to choose as their targets and the likely impacts of successful cyber-attacks

Through a series of case-studies, understand which data systems, networks and processes are critical and important to an organisation's operations.

Learn to prioritise investment in resources and technology to appropriately mitigate cyber risks.

Apply this knowledge to your own organisation, and assess how different cyber-attack scenarios might compromise its normal working functions.

module 3
enterprise risk management

Understand the importance of a strategic and holistic approach to managing cyber risk. Identify the key stakeholders inside and outside the organisation (for example in the supply chain), and their roles in ensuring the effective governance of cyber risk.

Understand that leadership from the top is crucial; it must engage every part of the organisation and its employees to demonstrate the importance of a strong security culture.

Explore the resource implications of an effective risk management approach, including the allocation of financial resources, and developing an accurate metrics system to keep track of the security systems that need to be put in place.

As part of your continuing project, suggest how your organisation could improve its management processes to mitigate cyber threats.

an executive introduction to
managing digital risk

module 4
the role of the security department

Identify the different roles of security in an organisation, and the tools that security departments can apply to mitigate cyber risk.

Understand the main types of technology available to defend an organisation's data, systems, processes and networks, and the value of cyber threat intelligence. - Appreciate that the 'human factor' is also crucial; an holistic approach demands a proper consideration of physical and personal security, as well as fraud management and forensic investigations.

Assess the role of your own organisation's security departments in managing cyber threats.

module 5
legislation, regulation and standards

Understand the roles of states in managing cyber risk through legislation and regulation across different sectors, particularly in the critical national infrastructure.

Consider the implications for business of differing national and international compliance standards in different jurisdictions.

Understand the implications of failing to meet legal and compliance requirements. Consider the utility of private-public partnerships in promoting cyber security.

Identify the compliance requirements of your own organisation's sector and the implications of non-compliance.

Consider the utility of private-public partnerships in promoting cyber security.

module 6
future challenges in cyber security

Examine the future direction of cyber security as new use cases in Industry 4.0 and beyond become available: super-fast mobile, artificial intelligence, big data, the 'internet of things' and industrial control systems, quantum computing and so on.

Consider what increased security risks could accompany these advances.

Assess the increased security risks that could accompany these advances, and their potential effect on your own organisation.

Oxford Cyber Academy
www.oxfordcyberacademy.com