BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Cyber Security Fundamentals for Leadership Online Course

Cyber Security for Public Leadership online Course: Planning, Policy and Strategy

Background context

A major 21st century challenge

In an increasingly technology-driven world, cybersecurity concerns have become ever-more prevalent and organisations across the globe are investing heavily to safeguard their systems against cyber-attacks.

It is not just those on the front line of creating the software, programmes and protocols that keep data and technology safe who need to understand cybersecurity threats and risks.

Cybersecurity is becoming an integral part of business operations, planning and strategy and

is no longer viewed as an isolated issue to be fixed by hiring in "clever technical people".

A rapidly growing sector

The cybersecurity sector has grown exponentially in the 21st century. In the US, the Bureau of Labor Statistics estimate a 31% growth in Information Security Analysts by 2029, versus a 4% average across all sectors. Statista projects the global cybersecurity market will be worth just under $250bn by 2023 – an 80% increase from 2017.

About the Course

In today's interconnected world, understanding cyber security is of pivotal importance. This eight-week online course equips professionals with a basic understanding of cyber security, empowering them to proactively defend their organisations from potential threats respond to cyber crises in their organisations, and understand how geopolitics and technology risk shape our modern world.

As a participant on this course, you will explore the realities of cyber risks and their impact on organisations, from economic and strategic impacts to disruptive attacks, with an emphasis on real-world cases. You will learn how to protect critical data, address vulnerabilities, and create policies to maintain stability. The course also explores the infrastructure of cyberspace, focusing on how physical and geopolitical factors contribute to cyber risks. You will study cyber in wartime, and take part in a simulation on how to respond to a cyber attack.

The learning provided will teach you to effectively manage cyber security risks by considering both technical and human factors. In addition to a conceptual foundation, during the Cyber Security for Public Leadership course, you will explore:

- How and why cyber-attacks happen
- Common types of malicious practice

And you will get an understanding of:

- Who may be responsible for carrying out attacks
- The harm that can be caused by attacks
- How to manage operational risk in cybersecurity

Learning Outcomes

The course has been designed to equip you with the skills, knowledge and confidence to:

1. Make more informed decisions when procuring new technologies for public sector organisations.
2. Assess the levels of cybersecurity risk facing one's own organisation and organisations

   that are potential partners.
3. Work with technology experts to develop and implement strategies to manage the risk of cyber security harm to their organisation.
4. Effectively and efficiently respond to a cyber security incident. With a practical, case- study approach to teaching, leaders and managers will be better prepared for such events.

Who is this course for?

- Public sector officials interested in gaining the essential knowledge in safeguarding critical infrastructure and sensitive information
- Managers in public or private organisations handling significant amounts of data or operational cyber security risk
- Decision-makers and policy-makers interested in developing a holistic approach to cyber security.
- Employees in any organisation that may store personal or sensitive data will need leaders who have a clear understanding on the importance of cyber security.

Sector suitability

The course will be relevant and valuable to participants across a wide range of sectors, some examples include:

We expect participants to come from the following relevant sectors:

- Government/Civil Service departments
- Health and Social Care
- Telecommunications
- Utilities (gas, water, electricity)
- Transport
- Banking and Financial Services
- Education

This course is **not suitable** for people with a technical background looking to become technology security analysts or frontline professionals developing programmes or solutions to cyber security threats.

Reasons to enroll on the Cybersecurity for Public Leadership course

With cyber threats continually evolving, this course offers essential knowledge to stay ahead of risks and gain the insights and tools needed to protect your organisation's data and maintain operational security in an increasingly digital world. This non-technical online course will teach you how to consider cyber security strategy and threat intelligence as an integral part of your operations, policies and planning. There will be various opportunities to **put your learning into practice,** through case study approaches, a project relating the learning from the course to your current role and a simulation of a cybersecurity incident.

By the end of this course, you will be equipped to:

- Understanding the sort of cyber security threats you, your organisation and your country might face, and those that are less likely to apply to your situation
- Identify cyber security risks relevant to your organisation
- Make informed decisions on technology procurement
- Assess and mitigate potential vulnerabilities
- Respond efficiently to cyber security incidents
- Develop a sustainable cyber security strategy aligned with organisational goals.

Academic expertise – learn from the best

- Ciaran Martin, the academic teaching on the course is well-known in the industry. He was the founding Chief Executive of the National Cyber Security Centre (NCSC).

Join a community of learners who share your passion

- You will have the opportunity to connect with your peers through the virtual learning environment which allow you to discuss your career aspirations and make connections that could help you in your progression.

Assessment details

Summative assessments will be spread evenly, with typically no more than one assessment task per week. We aim to avoid significant or challenging pieces of assessment in week 1 to allow sufficient time for you to adapt to the learning environment.

Assignment tasks and weightings

In order to pass the course and qualify for a certificate of completion, you must receive an overall grade of 75% or higher. Your grade will be calculated as follows:

- 10% for completing two summative multiple-choice quizzes in Weeks 2 and 7
- 15% for completing three Facilitator graded discussion forums in Weeks 1, 3 and 6;
- 25% for submitting a recorded presentation, and a written scenario response in Weeks 4 and 5
- 50% for successfully completing the final project/assignment.

Grading will be based on the rubric in the final assignment section.

Final project

Upon completion of the course, you will produce a cyber strategy allowing you to demonstrate achievement, of course, learning objectives and application of knowledge.

Module Information

Module Title	Description and Content
Cyber insecurity: the harms caused by malicious cyber activity	This module will teach you how and why malicious cyber activity causes harm, and the types of harm public sector organisations are likely to encounter.
The basics of technology and its misuse	This module will describe the basics of how technology works. You will be instructed on how technology becomes misused and how security breaches are achieved.
Who is hacking and why?	This module will provide perspective on the ways in which hackers think and work.
Building the cyber defences of an organisation	In this module you will examine how to build an effective cyber operational strategy for a public authority.
A real-life cyber security incident response exercise	This module will involve a simulation and will see you respond effectively to cyber security incident.
Public Policy and Cyber Security	This module aims to develop your awareness of the political and geopolitical environment in which cyber security and technology policy operates. This involves: • Great power competition • The impact on law enforcement • Moves towards greater international cooperation • The regulation of technology for security
Cyber Security in times of tension and crisis	This module will build your understanding of the wider political and geopolitical factors that affect cyber security risks and threats, and your ability to manage them. You will explore cyber realism in the time of war context derived around an article written by faculty.
Preparation and Final Assignment	In the final module, you will prepare a critical incident review. You can expect to do the following:
	· identify the risks and harms of cyber security; · capture the lessons learned throughout the other modules; and · make recommendations for the future national policy framework.