BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Cyber Security for Public Leadership: Planning, Policy and Strategy

Module Guide

What to expect

The contents of each module will be released weekly, and we expect you to dedicate around 3–5 hours to studying each week. Tasks and content vary per week but that is the guideline.

The course is deliberately designed to be flexible around your schedule. There are no live elements to the course – videos are pre-recorded and tasks are pre-set – so it can be picked up whenever you want during the seven days each module is live. You will have the opportunity to interact with the course Facilitator via email and within the learning platform, and there are discussion forums to engage with peers.

Module 0:
Getting started

Introduce yourself to your cohort and meet the Facilitator who will support you throughout the duration of the course. Learn more about what the course offers and how to navigate through it. Tell us about yourself by answering the questions and posting to the discussion board.

Module 1:
Cyber insecurity: The harms caused by malicious cyber activity

Find out how and why malicious cyber activity causes harm and what sort of harm public sector organisations are likely to encounter.

You can expect to do the following:

- analyse a real-life case study;
- reflect on experiences of your own organisation; and
- discuss what you would change to reduce risk in the future.

Module 2:
The basics of technology and its misuse

In this module, you will build a basic understanding of how technology works and how it is misused.

You can expect to do the following:

- understand the basics of how technology functions;
- examine how malicious cyber operators misuse technology;
- complete a research activity that includes gathering information on the types of hacking tools available; and
- reflect on how the topic of this module will impact

Module 3:
Who is hacking, and why?

This module will allow you to understand how computer hackers think and work.

You can expect to do the following:

- analyse an interview with an ethical hacker;
- investigate the national risk of nation state hackers; and
- reflect on who would be likely to attack your organisation and question why they would do that.

Module 4:
Building the cyber defences of an organisation

Examine how to build an effective cyber security operational strategy for a public authority.

You can expect to do the following:

- analyse a recent public authority case;
- build the cyber security strategy of a new public authority, using a real organisation as a base; and
- reflect on the challenges facing organisations when planning to mitigate the risks of cyber harm.

Module 5:
A real-life cyber security incident response exercise

Learn to respond effectively to a cyber security incident through a simulation exercise.

You can expect to do the following:

- explore what happens when your organisation has just been hacked;
- step into the shoes of a senior executive to complete a three-part simulated cyber security incident; and
- reflect on how the activities in this module have better prepared you, should a similar event happen in your organisation.

Module 6:
Public policy and cyber security

Gain a greater awareness of the political and geopolitical environment in which cyber security and technology policy operates.

You can expect to do the following:

- explore the ways that the government is encouraging competition whilst also ensuring regulation and enforcement, using the UK as an example;
- understand the regulation of technology for security; and
- research policies that enable a chosen country to regulate and enforce against cyber security risk.

Module 7:
Cyber security in times of tension and crisis

Build on the previous module with a better understanding of how to manage cyber risks within the political and geopolitical environment.

You can expect to do the following:

- understand how tensions and risks in cyber space increase at times of geopolitical crisis, such as war;
- reflect on the key takeaways that could inform your future practice, including making strategy decisions; and
- examine a real-world case study and reflect on the decisions made.

Module 8:
Final assessment

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.

How to earn a certificate and succeed in this course

To succeed in this course, you are expected to:

- watch all videos;
- respond to all activities;
- reflect on what you're learning;
- share your ideas with your peers in the discussion forum; and
- apply what you learnt to complete the final assignment.

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:

Multiple choice quizzes = 10%

Facilitator-graded discussion forums = 15%

Recorded presentations = 25%

Final assignment [summative assessment] = 50%

Note that certificates do not indicate your score, only whether you have passed. Your certificate will be issued by the platform.

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Thank you again for choosing to study with the Blavatnik School of Government, University of Oxford.