Director Development

Cyber Security – Practical Relevance for Directors

Course Details

Price
£215.00

Length
Half day (09:00-12:30)

Course Overview

Cyber security attacks exploit technology and the users of technology, but the impacts effect business operations and the data used by the organisation. In the end the big decisions to be made over how much or how little security to invest in, or how to manage a business that has suffered a cyber attack, will fall on the Directors and Executives. This course will explore the practical relevance of cyber security for the Directors who do not specifically manage technology but oversee the overall risks and successes of their business/organisation. It will help you in your decision making and knowing what questions to ask technical staff, suppliers and team members.

Course Content

The course will follow a set of topics to ensure that we cover the important themes but will also be interactive with anonymous voting on ideas and also open discussions.

The key topics are:

Why is cyber security such a big issue? - How different waves of technology bring value but also cyber security risk, including Internet/cloud, mobiles, AI etc. What attacks happen, to whom and why? A dip inside some relevant and recent incidents.

Who does what in cyber security? – Where do the responsibilities lie in managing cyber risk? – Technical staff, suppliers, business/organisation management, staff, Executives and Directors. What tools and ways of presenting and measuring cyber risk and security can help understanding?

The Guernsey Context – actual attacks and what is proportionate for smaller organisations (including input from Black Arrow Consulting)?

Strategy, investment and sustainability, regulatory and legal obligations – how to decide how much security/investment is enough and what is over the top? The role of insurance. What do laws and regulations generally expect? Practical experiences of an expert witness.

Assurance and Compliance – trust but verify – how to measure how well security is working and how services are being delivered. Practical examples, including working in partnership with suppliers and third parties.

Response and resilience – dealing with an incident. What we would be wise to prepare for. Living through an incident as a Director, when can you help or hinder? How a business can recover from an attack.

Q&A – The course tutor will be happy to answer questions based on his experience as a Chief Information Security Officer, strategy advisor and expert witness in civil and regulatory cyber cases.

Benefits

The course will help Directors understand how cyber security decisions and implications can affect their organisations and what they are able to do without needing a background in technology. It will provide a view across the breadth of cyber security so that you can understand how well and appropriately cyber security risks are being managed on your behalf by others in your organisation and your suppliers/ business partners. It will help you in your decision making on cyber security.

Next Steps

If you would like to book a place on this course please click on the 'Book Course' button to the right of this page and login or register for a user account to complete your booking(s). Any queries please do not hesitate to contact us via admin@gta.gg or call us on 01481 224570.

Flexible learning that works for you
E: admin@gta.gg | T: 224570 | W: gta.gg

Proudly part of
THE
GUERNSEY
INSTITUTE

If no date is scheduled for this course at the present time please click on the 'Register Interest' button and login or register for a user account so that we can add you to our course interest register. This register allows us to contact our tutors and finalise dates for a course as soon as we have a few people who have expressed their interest, so the more delegates who register their interest, the sooner we can schedule a particular course.

Course Tutor

Paul Dorey

Professor Paul Dorey CISM, FCIIS is a Guernseyman and Visiting Professor/Lecturer in Cyber Security at Royal Holloway College, University of London. In his career he has been Group Chief Information Security Officer (CISO) at Barclays, London Head of Information Security at Deutsche Bank Morgan Grenfell, Global CISO at both BP and GSK. He is active supporting businesses and governments in Cyber Security Strategy development and acts as an expert witness in civil and regulatory cases following cyber security breach.