ISTARI
ACADEMY

NAVIGATOR

Elevating cyber leaders into transformative business leaders.

**20TH - 24TH OCTOBER, 2025
CAMBRIDGE, UK**

NAVIGATOR
2025
2025
NAVIGATOR

Designed and delivered
in collaboration with:

**UNIVERSITY OF
CAMBRIDGE**
Judge Business School
ExecutiveEducation

Certified
Ⓑ
Corporation

Downing College, University of Cambridge

Executive education on cyber resilience for senior cyber leaders.

ISTARI was founded with the belief that knowledge is protection. Cybersecurity has become one of the most critical risks businesses face in today's digital world, making it essential for us to come together to learn from each other to meet the challenge. We believe in collective power, convening and partnering with world-renowned institutions and leading experts that can help us on our journey to cyber resilience.

That's why we created and designed this unique programme with one of the world's most prominent academic institutions, the University of Cambridge Judge Business School. CJBS Executive Education prides itself on offering an interdisciplinary, interactive learning environment that celebrates and creates real-world impact, shaping leaders who change the world.

This programme will help new and aspiring CISOs embrace the knowledge and skills needed to grow in confidence, evolve and adapt in an ever-changing cyber landscape. Learn to lead purposefully, manage effectively and innovate nimbly in an increasingly challenging — and critical — business role.

Navigator is designed to widen senior cyber leaders' knowledge, deepen their perspective and provide a unique space to share insights with their peers from across the region.

We hope to explore what it takes to forge the path to cyber resilience — now and in the future. We will provide an environment where you can contribute freely and learn directly from one another, all with the shared goal of delving into the learnings from real-life cyber scenarios and advancing toward increased resilience.

Topics covered:

Surviving a Ransomware Attack

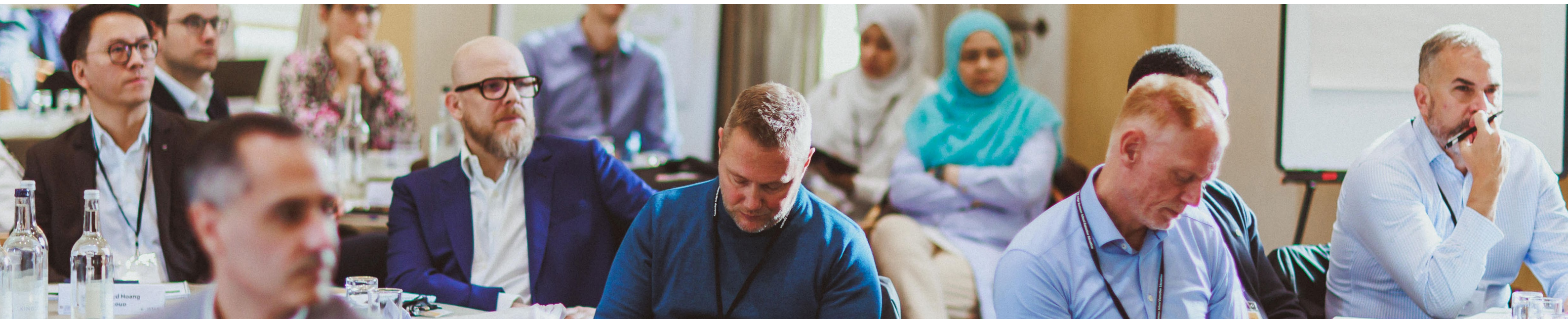How to Prevent a Crisis from Becoming a Catastrophe

Anticipating Strategic & Geopolitical Trends

Shaping Governance & Organisational Culture

Rethinking Cyber Risk Management

Crafting a Cyber Resilience Strategy

Navigating Cyber Crisis Communications

Programme overview

_____

The programme begins on Monday 20 October, with a half day of sessions and concludes early afternoon on Friday 24 October.

Converging Risks in a Fragmented World Order

Dr. Melanie Garson, ISTARI

"Technology and geopolitical expertise increasingly need to be in the boardroom. Pro-activity on this front will place boards in a strong position to steer their ships in an increasingly interconnected and rapidly changing global landscape."

Tobias Feakin, Former Ambassador for Cyber Affairs, Australia

Today's expanding technology environments expose organizations to geopolitical risk at every layer—from critical infrastructure to supply chain partners. In this session, we will map the evolving threat landscape, where opportunistic attackers, state-sponsored actors, and hacktivists increasingly target corporate vulnerabilities to create disruption. Participants will gain strategies for strengthening resilience: visualizing risk across interconnected systems, anticipating periods of heightened geopolitical tension, and protecting critical operations against emerging threats.

Surviving a Ransomware Attack

Jo De Vliegher & Jason Mallinder, ISTARI

"A cyberattack can hit all departments globally within minutes, even seconds. Not many other crises have that same immediate impact."

Jo De Vliegher, Client Partner at ISTARI and former CIO at Norsk Hydro

"It's not if, but when." In today's interconnected world, cyberattacks can cripple global operations within minutes, leaving organisations facing operational paralysis, financial loss, reputational fallout, and strategic risk.

In this session, Jo De Vliegher—Client Partner at ISTARI and former CIO of Norsk Hydro—shares firsthand lessons from one of the most significant ransomware attacks in industrial history. When Norsk Hydro's 22,000 computers across 170 sites were disabled almost instantly, Jo and his teams were forced to navigate a high-stakes recovery under extreme pressure. Through direct testimony and practical insights, participants will explore what it takes to lead through a cyber crisis, protect critical operations, and prepare their organisations for the realities of large-scale digital disruption.

Day 2
New Risk

Resilience of the Enterprise
Professor Danny Ralph

"The resilient resists shocks and stays the same; the antifragile gets better."

Nassim Nicholas Taleb, Author, Antifragile

Even well-prepared organisations and governments struggle to imagine — let alone prepare for — large-scale, systemic events. This session asks a pressing question: How can leaders navigate unpredictable crises?

Through interactive discussion, peer exchange, and scenario-based group work, participants will explore what securing organisational resilience means, how to test it, and how to strengthen it for the future.

We will examine contagion effects to identify the cascading impacts of systemic crises, apply a taxonomy of business risks to reveal organisational blind spots, and use comparative scenario analysis to assess resilience and pinpoint vulnerabilities across ecosystems. Participants will leave with practical tools to embed foresight into their risk management practices, build adaptive capacity, and position their organisations to withstand — and even thrive in — the unexpected.

Crafting a Cyber Resilience Strategy
Dr. Manuel Hepfer, University of Oxford & ISTARI

"Then, in 72 words, I laid out the strategy, which was essentially to be the conduit of capital between those who have it and those who need it. That's our job. Then we took a poll, and the result was that 98 percent understood and agreed with the strategy. Clarity of message is key."

James Gorman, CEO Of Morgan Stanley, 2019

Can you summarise your company's cyber resilience strategy in 35 words or less? If so, would your colleagues put it the same way? Very few executives can answer these simple questions in the affirmative. The companies that those executives work for are often the most successful in their industry. This session is dedicated to the art of understanding and crafting a cyber resilience strategy, then communicating it effectively.

Day 3
New Organisation

Rethinking Cyber Risk Management
David White, Axio

"We will bankrupt ourselves in the vain search for absolute security."

Dwight D. Eisenhower, 34th President of The United States, 1961

Managing cyber risk within organisations is a major, costly leadership challenge. Building and maintaining cybersecurity capability is expensive and the return on investment is often uncertain. This session focuses on expanding cyber leaders' understanding of key issues in their cybersecurity strategy, and aligning this strategy with the organisation's broader corporate governance and enterprise risk management practices and capabilities.

How to Prevent a Crisis Becoming a Catastrophe
Dr. Simon Learmount, Cambridge Judge Business School

"Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate. Something interesting is happening."

Tom Goodwin, Tech Crunch

This module is a specially designed business school case study for the Navigator programme. Focusing on Uber, it explores the strategic and disruptive forces that enabled it to become one of the world's most well-known companies. However, it also has had organisational and management challenges along the way, which has at times led towards major governance and culture issues, including its former CSO, Joe Sullivan, being prosecuted by US authorities. Accordingly, effective cyber crisis management requires the full scope of the entire company, from individuals up to the C-suite, as management of the crisis impact may last well beyond the time required to mitigate the technical incident. This session focuses on those business processes.

Day 4
New Leadership

Navigating Uncertainty and Instability in Organisational Leadership

Professor Jennifer Howard-Grenville, Cambridge Judge Business School

---

"Ultimately, being a CISO in times of crisis requires a mix of strong decision-making, clear communication, and a focus on both the technical and human elements of leadership. It's about guiding the team through challenging situations while ensuring they feel supported and confident in your direction."

Tim Brown, CIO, Solar Winds

Today's CISOs must lead at the edge of predictability—where volatility, ambiguity, and complexity converge. This session equips participants with advanced frameworks from systems thinking, culture theory, and leadership research to navigate the unknown with clarity and confidence. Through interactive exercises and peer dialogue, participants will explore how uncertainty shapes organisational behaviour, and how to respond with resilience and purpose. Drawing on the concept of liminal leadership, we will examine how to maintain agency when traditional playbooks no longer apply. Participants will leave with practical tools for sensemaking, shared leadership, and building collective direction during times of flux—embracing the CISO's evolving role as an adaptive leader in a world of continual transformation.

Case Study Workshop

When Billions Vanish: The World's Largest Documented Heist

Guy Segal, SVP Corporate Development & Yonatan Lipschitz, Director Client Leadership EMEA, Sygnia

---

"Every transaction is recorded on the blockchain forever. That makes it both the best and the worst place to commit a crime."

Michael Gronager, CEO, Chainalysis

This session is an interactive deep-dive into one of the largest crypto heists in history. Learn how attackers stole over $1.5 billion from Bybit through a highly sophisticated supply-chain attack, and how Sygnia's investigation exposed the tactics of the notorious Lazarus Group. Beyond the forensic story, this session will uncover vital lessons on navigating and communicating during a cyber crisis, offering practical insights you can apply in your own organisation. You will gain real-world knowledge to transform your cybersecurity readiness.

Workshop

AI Mastery for CISO's

Alan Bodnar, Murali Aiyer, & Dr. Melanie Garson, ISTARI

"AI is neither good nor evil. It's a tool. Just like fire. Fire kept us warm, cooked our food, and burned down our houses."

Oren Etzioni, CEO, Allen Institute for AI

This workshop is designed to equip senior cyber leaders with the knowledge and strategies needed to navigate the broader AI landscape, identify key risks and opportunities, and address capability gaps for developing an actionable AI cyber roadmap. Participants will explore the dual nature of AI as both a powerful tool and a significant security risk. We will cover how to leverage AI for enhancing security operations while simultaneously considering frameworks to mitigate the unique vulnerabilities introduced by AI systems. We will explore actionable strategies to position cybersecurity organisations for long-term success and the importance of a human approach to ensure responsible and secure AI adoption.

Through the Fog: Navigating a Cyber Crisis

Dr. Lucas Kello, University of Oxford & ISTARI

"It is easy to dismiss all communications as 'spin'. But, in a crisis, communication really matters. It must be embedded in strategy."

Alastair Campbell, Director of Communications and Strategy for Prime Minister Tony Blair

---

Get to the heart of a fast-moving cyber crisis where technical escalation meets political complexity. In this immersive tabletop exercise, participants will navigate the strategic, legal, regulatory, and ethical challenges triggered by a high-impact cyberattack of uncertain origin. Designed to mirror the realities of modern crises, this simulation tests leadership judgment, decision-making under pressure, and cross-functional coordination. Participants will rehearse how to respond when every move carries operational, reputational, and geopolitical consequences.

Putting Your Cyber Resilience Strategy into Action

Dr. Simon Learmount
Cambridge Judge Business School

"Thinking is easy, acting is difficult, and to put one's thoughts into action is the most difficult thing in the world."

Johann Wolfgang von Goethe

The final session culminates all the knowledge and skills gained throughout the programme. It provides a toolkit that can empower cyber executives to put their learning into action within their respective companies. This session serves as a platform for participants to share their strategic thinking, leadership abilities and new-found expertise and how as a cohort they can continue their journey as a community of peers.

Course Co-Directors

Dr. Melanie Garson

*Director of Research & Insights, ISTARI &
Associate Professor in International Security &
Conflict Resolution, University College London*

Dr. Simon Learmount

*Associate Professor in Corporate Governance,
Cambridge Judge Business School*

Dr. Melanie Garson is cyber and tech geopolitics policy specialist and Director of Knowledge & Insights at IS-TARI. She is also an Associate Professor in International Security in the Department of Political Science at University College London where she teaches her flagship course "From Cyberwarfare to Robots: The Future of Conflict in the Digital Age", and is a public speaker who connects the dots between new and emerging tech and its potential impact on security, foreign policy, diplomacy and the world order. Dr. Garson worked for four years as the Cyber Policy and Tech Geopolitics Lead at the Tony Blair Institute for Global Change, and is also a lawyer and mediator. Melanie regularly provides commentary in on geopolitics and tech in podcasts, webinars and at major media outlets including Bloomberg, BBC, Sky, CNBC, CNN, Fox News, France 24, and DeutscheWelle.

Previously the Director of the University of Cambridge's MBA Programme, Dr. Simon Learmount is also a lecturer in Corporate Governance, a Fellow of the Centre for Business Research (CBR) and a Fellow of Pembroke College, Cambridge. He has published extensively on the convergence of national systems of corporate governance, organisational trust and cooperation and is a world-renowned expert and lecturer on effective corporate governance of risk.

Core faculty and experts

Alan Bodnar

Principal, ISTARI

Alan is a Cloud Security expert, an area that every client expresses the need for, from set-up to remediation to secure development operations. Before ISTARI, Alan served as Director, Cybersecurity at PwC. Alan joined PwC in 2014 from Booz Allen Hamilton, where he worked as a Network and Platform Engineering Manager. He also worked at a new venture, Edgile as Senior Manager, Cloud Security. Alan holds an MBA and MSc in Information Technology from the University of San Diego.

David White

Co-Founder & President, Axio, Teaching Fellow, Carnegie Endowment for International Peace & Security

David is co-founder and Chief Knowledge Officer at Axio Global, where he helps companies evaluate and improve their cybersecurity risk management programs and deploy cyber insurance as an effective risk transfer control. He works with insurance industry leaders on improving cyber insurance products, underwriting and claims data analyses. Previously, at the CERT Program at Carnegie Mellon's Software Engineering Institute, he was responsible for a portfolio of cybersecurity and resilience maturity models, frameworks and research. He co-authored the CERT Resilience Management Model (CERT-RMM).

Dr. Manuel Hepfer

Research Affiliate, University of Oxford & Strategic Advisor, ISTARI

Dr. Manuel Hepfer is a cybersecurity researcher at Oxford University's Saïd Business School. He holds a PhD in Cybersecurity and Strategic Management from the University of Oxford. His research focuses on how organisations can build resilience to cyberattacks, and the role of CEOs and Boards in managing cybersecurity risk. He has presented at major industry conferences, including RSA and Gartner. His research has won several awards and appeared in academic and practitioner journals such as MIT Sloan Management Review and the Financial Times. Drawing on his research, he helps companies proactively strengthen their cyber resilience.

Guy Segal

SVP Corporate Development, Sygnia

Guy Segal serves as Senior Vice President of Corporate Development at Sygnia, the foremost global cyber readiness and response team dedicated to applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. Guy brings over 25 years of experience in cyber technology, analytics operations and business leadership. Before joining Sygnia, he was General Manager of Custodio-Technologies, and before that was Cyber Security Leader of IBM in Israel. Guy previously served in various professional and command roles in Unit 8200, IDF's elite cyber and intelligence unit.

Core faculty and experts

Jason Mallinder

Client Partner, ISTARI

Jo de Vliegher

Client Partner, ISTARI

Lucas Kello

Associate Professor in International Relations, University of Oxford & Strategic Advisor, ISTARI

Murali Aiyer

Principle, ISTARI

Jason is the former Global CISO and Managing Director at Credit Suisse. He was responsible for information security, including cybersecurity and technology risk management, globally. He is a certified information security manager and certified risk manager. He chaired the Investment Banking Information Security Group in the U.K. and worked closely with the Bank of England and the U.K. government on cross-sector cyber defence development, testing and exercising programs.

Jo is a client partner at ISTARI, supporting EMEA clients in managing digital risk and enhancing cyber resilience. Previously, he was Group CIO at Hydro, overseeing IS/IT, digitalization, and cybersecurity for 34,000 employees, including leading the company's acclaimed response to a major 2019 cyberattack. Before that, he held senior IT roles at solar energy firm REC in Singapore. Fluent in Dutch, English, French and Norwegian, he brings extensive global expertise in cybersecurity and IT leadership.

An accomplished academic and author, Lucas is currently an Associate Professor at Oxford University, where he directs the Academic Centre of Excellence in Cyber Security Research, with a research focus on technology and global affairs. He has authored two bestsellers on cybersecurity, "The Virtual Weapon and International Order" and "Striking Back: The End of Peace in Cyberspace and How to Restore It." Lucas advises ISTARI on thought leadership.

Murali Aiyer is a Principal at ISTARI and a seasoned Cybersecurity practitioner with cross-industry experience leading large engagements across Industrial, Lifesciences, Communication &, and Financial Services. Murali is responsible for enabling delivery of security projects and leading strategy advisory and consulting engagements. He has 28 years of advisory and implementation experience in Cybersecurity Strategy, Risk Management, Cloud Security, OT Security, Data Privacy & Protection, Threat Management & Security Transformation.

Core faculty and experts

Professor Danny Ralph

Professor of Operations Research at Cambridge Judge Business School

Professor Ralph is a member of the Operations and Technology Management group at Cambridge Judge Business School. His research focuses on systemic and emerging risk, optimisation, and decision-making in energy and equilibrium systems. He is Area Editor for Operations Research and former Editor-in-Chief of Mathematical Programming (Series B). Professor Ralph collaborates closely with industry, combining academic insight with practical impact in operations and risk management.

Professor Jennifer Howard-Grenville

Diageo Professor of Organisation Studies at the Cambridge Judge Business School

Professor Howard-Grenville is the Diageo Professor in Organisation Studies at Cambridge Judge Business School and Head of its Organisational Theory and Information Systems group. Her research explores organisational change, sustainability, and culture, with in-depth studies across industries like manufacturing and energy. A Fellow of the Academy of Social Sciences, she has published extensively and served as Deputy Editor of the Academy of Management Journal.

Yonatan Lipschitz

Director Client Leadership EMEA, Sygnia

Yonatan is a senior executive with over two decades of leadership experience in cybersecurity, information systems, and strategic program management. He has led the design and delivery of large-scale cybersecurity programs, with a proven track record of advancing organizational resilience in complex threat environments.

Navigator in numbers

4

day immersive
executive education

4.89/5

overall programme
feedback rating

150+

alumni from world
leading organisations

10

industry-leading
speakers and educators

30

global senior cybersecurity
peers for knowledge sharing

2

global cohorts
each year

Alumni

Allianz	DBS	DP WORLD
Emirates	GLENCORE	Mahindra
NIKE	randstad	REPSOL
Santander	Statkraft	TOMTOM

Course fee

The fee is £5,500 + VAT. This includes all course materials, lunches social activities and two dinners at historic University of Cambridge colleges, but excludes accommodation, travel and incidentals.

Eligibility requirements

Navigator is most suited to senior cyber or IT leaders within global organisations. We welcome applications from those looking to sharpen their understanding of governance, cyber risk and leadership competencies.

How to apply

To apply for an upcoming Navigator programme, please visit our website:
navigator.istari-global.com

For more information, please contact
istariacademy@istari-global.com

CPD
The CPD Certification Service

This programme is certified by the CPD Certification Service. It may be applicable to individuals who are members of, or are associated with, UK-based professional bodies.

Find out more about CPD

Alumni testimonials

"The Istari Navigator programme is a superb and comprehensive package for any current or aspiring CISO. I attended in October 2024 and was hugely impressed with the quality of the contents which were delivered by an array of excellent guest presenters. The sessions on strategy development and risk management were underpinned by excellent analysis, included relevant case studies and illustrated how to use a new array of tools and techniques. I would recommend the programme for anyone wanting to develop their competencies and skills to become a future CISO."

Head of Cyber and Information Security,
Rolls Royce

"Navigator was not only a highly enriching professional experience but also a deeply inspiring personal one. The course content, focusing on cyber resilience and leadership, was expertly delivered by both academic and industry leaders, offering practical strategies and insights."

Head of Security Operations – Detection & Response (DART), TomTom

"Navigator is a 'must' for organisations wishing to elevate technical leaders into transformational business leaders, and an experience I will carry with me for the rest of my life."

CISO, North Standard

"The Navigator Programme was genuinely helpful and has helped me think about cyber from new perspectives. Only problem is that now my team and I have a lot more work to do, even though I'm confident the new work will be highly valuable. Thanks to the whole group, de jure faculty members, as well as my classmate peer "instructors!"

CISO, Washington University in St. Louis