ISTARI
ACADEMY

NAVIGATOR

Elevating cyber leaders into
transformative business leaders.

12TH – 16TH OCTOBER, 2026
CAMBRIDGE, UK

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

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.

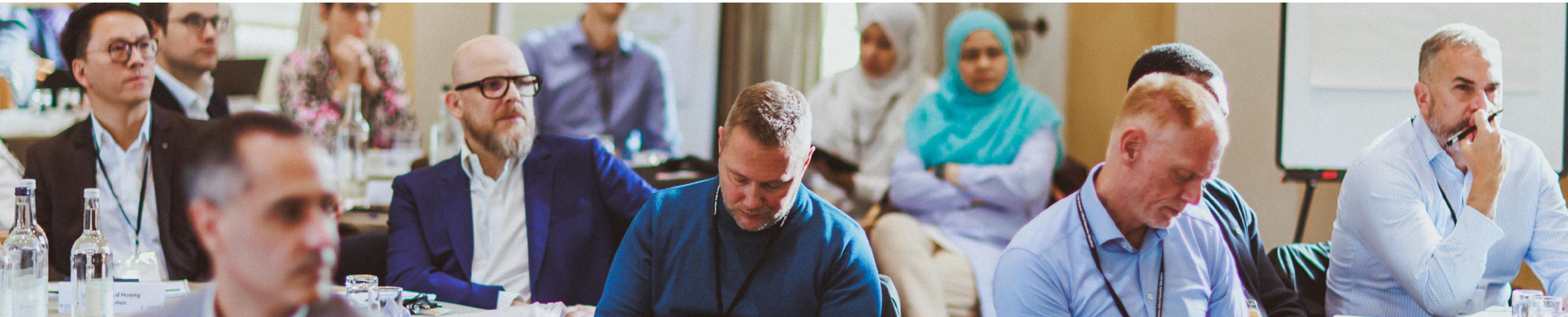
This programme will help new and aspiring CISOs embrace the knowledge and skills needed to grow in confidence, evolve and adapt in an ever-changing cyber landscape. Learn to lead purposefully, manage effectively and innovate nimbly in an increasingly challenging — and critical — business role.

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
- Navigating Unpredictable Crises
- 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 is four full days beginning on Monday, 12 October with a half day of sessions and concludes early afternoon on Friday, 16 October.

Day 1: New World

Resilience in an Era of Unpeace: Geopolitical Risk in Cyberspace

Dr. Lucas Kello,
University of Oxford & ISTARI

"We are now operating in a space between peace and war... Our world is being actively remade, with profound implications for national and international security."

Blaise Metreweli,
Chief of MI6

This session will examine how the geopolitics of cyberspace is reshaping corporate risk. It situates contemporary cyber contests in historical perspective, mapping the evolution of cyber risk across distinct stages – from the criminal nuisance of the 1980s to today's highimpact interstate operations with economic and political effects. It reviews the concept of "unpeace": a persistent condition of strategic contest below the threshold of war in which economic disruption and political subversion become common tools of statecraft. It will discuss the growing instability in cyberspace arising from the converging forces of geopolitical fragmentation and technological uncertainty associated with AI and other technological trends. Participants will leave with a sharper lens on where cyber risk intersects with great-power rivalry and what this means for enterprise resilience strategy.

The Anatomy of a Crisis

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

"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 largescale digital disruption.

Day 2: New Risk

Systemic Shocks and Resilience of the Enterprise

Dr. Mark Bloomfield

"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.

NorthRiver Health Trust: Incident Response in Critical Healthcare Infrastructure

Dr. Simon Learmount,
Cambridge Judge Business School

"Adversity does not build character, it reveals it."

James Lane Allen, 19th–20th century American author

The simulation places participants in the role ofboard members (executive and nonexecutive directors) as a cyber incident unfolds, starting from weak signals about supplier risk, through acute disruption of digital systems, ransomware and data exfiltration threats, mounting government and media pressure, internal culture fractures, and finally full system outage requiring analogue operations.

Emerging Technology and Cyber Risk: What Does AI Teach Us for the Future?

Dr. Lucas Kello,
University of Oxford & ISTARI

"We can only see a short distance ahead, but we can see plenty there that needs to be done."

Alan Turing, Mathematician

This session will examine what the recent evolution of AI can teach leaders about resilience under accelerating technological change. It traces the evolution of machine intelligence from Alan Turing's 1950 conception through rules-based systems in the 1960s to today's neural-network foundation models, with a focus on the strategic implications of agentic AI as systems shift from tools to autonomous actors. It will then structures the risk landscape around three pathways: offensive acceleration, model manipulation and compromise, and supply-chain targeting. The session also reviews the origins of quantum computing and the probabilistic timeline for universal quantum processors, translating those projections into concrete preparedness measures and decision thresholds. The central aim is preparedness: understanding why LLMs caught many organisations off guard and applying that lesson to build quantum readiness early enough to avoid strategic surprise in technology management.

Day 3: New Organisation

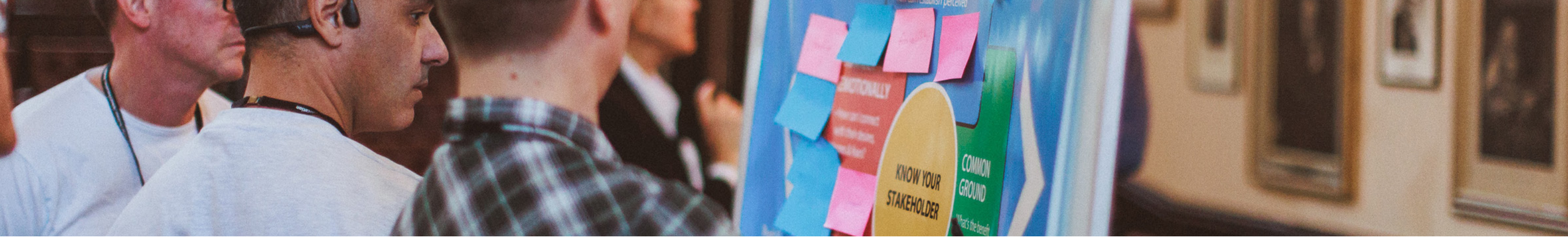
Resilience by Routine

Dr. Manuel Hepfer,
University of Oxford

"In the middle of difficulty lies opportunity."

Albert Einstein, Theoretical Physicist & Researcher

Disruption is inevitable. Yet organisations respond to it very differently. Some falter in the face of adversity, while others adapt and even thrive. Executives often describe this difference using the word resilience, yet few define it clearly. What creates resilience? What undermines it?
This session explores the core activities that enable organisations to navigate disruption and emerge stronger. Drawing on insights from strategy, risk management and research, we examine what distinguishes resilient organisations from those that struggle in times of crisis.
By the end of this session, participants will be able to articulate what resilience means in their own organisational context and identify the foundations required to build it.



Day 4: New Leadership

Cyber Risk Management

Jason Mallinder
Global Head of Academy & Client Partner, ISTARI

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

Dwight D. Eisenhower, 34th President of The United

Security budgets are rising, yet most organisations struggle to demonstrate whether investments reduce the biggest risks or just check compliance boxes. Many operate fragmented security governance where reporting, governance, and operational security work in silos. Most decisions are driven without full understanding, reacting to incidents rather than proactively preparing for the future threat. Data-driven governance measures threat exposure, control effectiveness, and incident patterns to make defensible decisions about where to invest and what risks to accept. This session examines how to build measurement frameworks that inform strategy, communicate risk at the boards in business terms, and optimise spending based on actual cyber postures. Participants will gain practical approaches to quantifying cyber risk and using real time data to drive security decisions.

Crafting a Cyber Resilience Strategy

Dr. Manuel Hepfer
University of Oxford

"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

This module is a specially designed Cambridge Judge Business School case study. Focusing on Uber and Jaguar Land Rover (JLR), the session explores the how cyber crises play out across an entire organisation, from the security operations and supply chain to the C-suite and boardroom. Both cases reveal how organisational culture, stakeholder management, governance and leadership shape the handling of cyber crises, from data breach disclosure issues and the prosecution of Uber's former CSO, Joe Sullivan, to JLR's business continuity and stakeholder impact. The session critically analyses how different types of incidents demand different crisis leadership approaches, while still relying on common foundations: clear governance, stakeholder management, well-rehearsed incident response, effective internal and external communications, and a culture that supports transparency and learning.

Systems Thinking and New Leadership in a Changing World

Dr. 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

In today's rapidly evolving organisational environment, CISOs must navigate uncertainty and instability, both internally and externally. This session equips participants with frameworks from systems thinking, culture theory, and leadership studies to strengthen their ability to lead with confidence in unpredictable conditions. Through interactive exercises, structured reflection, and practical discussions, participants will gain insights into how uncertainty and instability manifest in complex systems—and, importantly, how they can take meaningful action.

Shaping Governance & Leadership

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 Cambridge Judge Business School case study. Focusing on Uber and Jaguar Land Rover (JLR), the session explores the how cyber crises play out across an entire organisation, from the security operations and supply chain to the C-suite and boardroom. Both cases reveal how organisational culture, stakeholder management, governance and leadership shape the handling of cyber crises, from data breach disclosure issues and the prosecution of Uber's former CSO, Joe Sullivan, to JLR's business continuity and stakeholder impact. The session critically analyses how different types of incidents demand different crisis leadership approaches, while still relying on common foundations: clear governance, stakeholder management, well-rehearsed incident response, effective internal and external communications, and a culture that supports transparency and learning.

Day 5: New You

Split Second Choices - Outsmarting AI-Driven Threats: A Cyber Wargame Exercise

Chris Crummey, Director Executive & Board Cyber Services, Sygnia

"Winning is not about being the fastest, it's about making the fewest mistakes."

Alain Prost, British Formula One driver

In today's rapidly evolving organisational environment, CISOs must navigate uncertainty and instability, both internally and externally. This session equips participants with frameworks from systems thinking, culture theory, and leadership studies to strengthen their ability to lead with confidence in unpredictable conditions. Through interactive exercises, structured reflection, and practical discussions, participants will gain insights into how uncertainty and instability manifest in complex systems—and, importantly, how they can take meaningful action.

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, German Enlightenment

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 directors

Dr. Lucas Kello

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

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.

Dr. Simon Learmount

Associate Professor in Corporate Governance, Cambridge Judge Business School

Previously the Director of the University of Cambridge’s MBA Programme, Simon Learmount is a Fellow of Pembroke College, University of Cambridge and Associate Professor of Corporate Governance at Cambridge Judge Business School. He has served as Director of both the MBA and Executive MBA Programmes at Cambridge, and is recipient of the Pilkington Prize, awarded by the University of Cambridge to honour outstanding teaching across the university. His focus is on international corporate governance, sustainable business practice and ethics (especially in the US, UK, Japan and China) and digital governance (including cyber-security and AI). He serves as co-chair of the World Economic Forum Climate Governance Expert Committee, is a member of the Global Futures Council on Climate and Nature, advises multiple organisations on climate and digital governance, sustainability and green transition, risk management and director development. Before joining Cambridge Simon was a successful entrepreneur.

Core faculty and experts

Jo De Vliegher

Client Partner,
ISTARI

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.

Jason Mallinder

Global Head of Academy & Client Partner, ISTARI

Jason is a Client Partner at ISTARI and is Global Head of its Academy. He fosters long-term trusted client relationships by integrating advisory, education, and ecosystem capabilities into cohesive, high-impact outcomes that build true cyber resilience for clients. Jason brings deep practitioner expertise to his role, having served as Global CISO and Managing Director at Credit Suisse. His experience extends into the publicprivate sector, where he has worked alongside the Bank of England and the UK government to develop national cyber defence frameworks. Jason is a certified manager in both information security and risk, with a proven track record of leading large-scale technology risk operations on a global stage.

Dr. Manuel Hepfer

Research Affiliate,
University of Oxford

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.

Dr. Mark Bloomfield

Fellow, Cambridge Judge Business School
Former Director of Commercial Transformation at Global Media & Entertainment

Dr. Mark Bloomfield is a Fellow at Cambridge Judge Business School, where he teaches AI strategy, innovation, and business transformation. He advises boards and leadership teams on AI and future readiness across multiple sectors, with 15+ years of experience spanning aerospace, travel, and media. He holds a PhD in AI-based optimisation with Airbus.

Core faculty and experts

Dr. Jennifer Howard-Grenville

Diageo Professor of Organisation Studies, 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.

Chris Crummey

Director Executive & Board Cyber Services, Sygnia

Chris Crummey is a global Director for Executive and Board Cyber Services, with extensive experience advising organisations on cyber security strategy and crisis readiness. He has guided executives and boards through complex cyber incidents, focusing on risk-based decision-making, crisis communication and leadership under pressure. He also contributes to board-level education and has led global cyber simulation and response programmes.

Navigator in numbers

4

day immersive
executive education

9+

industry-leading
speakers and educators

4.89/5

overall programme
feedback rating

30

global senior cybersecurity
peers for knowledge sharing

175

alumni from world
leading organisations

1

global cohort
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.

Preferred rates at local hotels will be shared upon registration.

Eligibility requirements

Navigator is most suited CISOs and 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

ISTARI
ACADEMY

navigator.istari-global.com

UNIVERSITY OF CAMBRIDGE
Judge Business School

ExecutiveEducation

Certified B Corporation

Apply here: