Blackstone

CISO Academy 2026

Elevating cyber executives into strategic business leaders

11- 12 May, 2026
Cambridge, UK

Designed and delivered by:

ISTARI
ACADEMY

Business leadership programme for senior cyber executives

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.

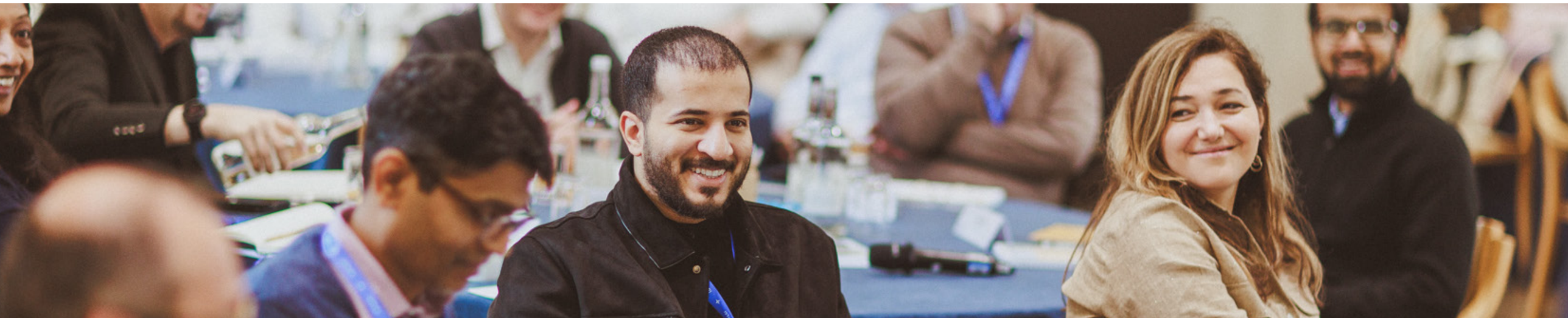
That's why we created and designed this unique programme to help cyber leaders within the Blackstone ecosystem to strengthen their strategic influence and business impact. Designed for mature CISOs and senior security executives, it explores the intersection of cyber resilience and enterprise leadership—enabling participants to drive organisational transformation from the boardroom to operations.

This interactive two-day learning experience has been developed to widen senior cyber leaders' knowledge, deepen their perspective and provide a unique space to share insights with their peers from across the region.

Together, we'll explore what it takes to forge the path to cyber resilience across the Blackstone portfolio — now and in the future. We will provide an environment where you can contribute freely and learn directly from portfolio peers, all with the shared goal of delving into the learnings from real-life cyber scenarios and advancing toward increased resilience across the ecosystem.

Topics covered:

- Geopolitical Risk
- Systems Thinking
- Executive Leadership Skills
- Crisis Management
- Supply Chain Resilience
- AI & Data-Driven Risk Management
- Board Engagement



Programme agenda

Day 1

Resilience in an Era of Unpeace: Geopolitical Risk in Cyberspace

"Boards need to understand and anticipate macro-level disruptions, including shifting trade alliances, regional conflicts, and social unrest. The speed and scope of global disruption render reactive governance models unviable — resilience planning and geopolitical risk assessments should be regular agenda items, not emergency topics."

Odgers Berndtson, Geopolitical Risks

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 high-impact 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.

Systems Thinking and New Leadership in a Changing World

"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.

The Anatomy of a Crisis

"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 largescale digital disruption.

Closing the Gap on OT-IT

"I'm in this business for 20 years, and what we saw in the lab when analyzing Stuxnet was far beyond everything we had ever imagined."

Ralph Langner

Operational technology has moved from isolated networks to IT connectivity, fundamentally changing the threat landscape. The challenge isn't simply technical—it's organizational, cultural, and operational. IT teams prioritize rapid patching and updates; OT teams prioritize uptime because stopping a production line has real-world consequences.

This session examines why traditional IT security fails in OT environments and explores practical strategies for securing converged systems without compromising operations. Participants will address vendor management in OT contexts, risk assessment that accounts for physical consequences, and governance structures that bridge IT and OT engineering teams.

Supply Chain Resilience

"Managing supply chain risk is still one of the, if not the biggest, problem for organisations. It's the greatest area of unmanaged or hard-to-manage risk."

Philip Reitinger, President and CEO, Global Cyber Alliance; Former SVP and CISO, Sony

Every vendor relationship creates a trust dependency. When that trust is exploited—as with SolarWinds, MOVEit, JLR and countless others—organizations face incidents they didn't cause but must contain. Supply chain attacks now account for in excess of 30% of all breaches.

This session moves beyond questionnaires to examine how supply chain risk actually manifests. Participants will explore risk-based vendor segmentation, management strategies for early detection and contractural controls during incidents. Through case analysis, participants will develop approaches to managing third-party risk that align with organizational reality when perfect visibility isn't achievable.

Day 2

Harnessing AI & Next-Gen Cyber Defense

“AI disproportionately helps the people defending because you’re getting a tool which can impact it at scale. If you can run a little bit faster than your adversary, you’re going to do better. That’s what AI is really giving us defensively.”

Sundar Pichai, CEO, Google

The tools we use to defend our organisations are evolving as fast as the threats we face. In this session, we will explore how to harness emerging technologies to strengthen cyber defences while maintaining robust governance and oversight. Participants will examine the balance between automation and human judgment in threat detection, and gain practical insights into enabling new capabilities securely — ensuring innovation doesn’t outpace control.

Cyber Risk Management & Data Driven Governance

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

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

Security budgets are rising, yet most organizations 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 optimize spending based on actual cyber postures. Participants will gain practical approaches to quantifying cyber risk and using real time data to drive security decisions.

Case Study Workshop: Learning from Managing a Real Crisis

"Time is the most valuable currency in a cyber crisis. Every hour of downtime translates into lost revenue, operational disruption, and reputational damage that compounds long after systems are restored."

Sygnia

This interactive workshop examines a real-world cyber crisis through the lens of those who responded to it. Rather than theoretical frameworks, participants will work through the actual decisions, trade-offs, and pressures faced during a major incident. The session explores what worked, what failed, and why. How do you maintain business operations while containing an active threat? When do you notify stakeholders? How do you coordinate across technical, legal, and executive teams when everyone wants different things?

This is not a lecture about incident response plans. It’s a chance to learn from people who have lived through the chaos and can share what actually matters when the crisis is real.

Engaging with Boards in a NIS2 World: Cyber Strategy & Board Engagement

"CISOs need to frame cybersecurity as a business enabler, not just a cost centre. Show how security investments drive customer trust and long-term resilience."

Myrna Soto, Founder & CEO, Apogee Executive Advisors; Board Director and Former CISO, Comcast

Effective cyber resilience requires more than technical excellence — it demands strategic alignment at the highest levels of the organisation. In this session, we will examine how security leaders can communicate cyber risks and resilience strategies to board members in ways that cut through complexity and drive action. Participants will explore practical techniques for building a joined-up approach to cyber resilience, ensuring boards are not just informed but actively engaged as partners in navigating today’s threat landscape and evolving regulatory environment.

Faculty & experts

Dr. 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.

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.

Jason Mallinder

Global Head of Academy & Client Partner, ISTARI

Jason leads the Academy and is a client partner at ISTARI. He 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 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.

Faculty subject to change.

Faculty & experts

Nicolas Castellon

Director Cybersecurity Services Europe, Sygnia

Nicolas is a cybersecurity executive with over 15 years of experience leading complex security transformations across the EMEA region. Director of Cybersecurity Services at Sygnia, responsible for aligning cyber resilience, technology, and business strategy to mitigate high-impact risk and enable resilient business growth. Trusted advisor to executive leadership across financial services, manufacturing, and pharmaceuticals, with deep expertise in strategic advisory, offensive and defensive security, and large-scale IT/ OT security transformation. Recognized for combining strong technical depth with clear executive communication in fast-moving, high-stakes environments.

Rachel Laursen

Partner, ISTARI

Rachel is a Partner at ISTARI with extensive experience as a senior executive leader and advisor across technology, digital, cybersecurity, and enterprise risk. Her background includes serving as CISO at Marks & Spencer and JD Sports, as well as senior leadership roles within the Office of the COO, where she supported executive teams on digital resilience, cyber risk, and critical decision-making in complex, global, and regulated environments. She has served as a National Cyber Advisory Board member for the UK Cabinet Office, contributing independent insight on cybersecurity and national resilience. At ISTARI, Rachel works with leaders to strengthen digital trust and resilience as strategic capabilities.

Programme details

Alumni of our executive education training programmes come from 175+ global organisations.

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

Course fee

The fee is £1,050 + VAT. This includes all course materials, lunches and an evening function, but excludes accommodation, travel and incidentals.

Eligibility requirements

This programme is designed for senior cyber and IT leaders across Blackstone's portfolio companies who are advancing cyber resilience as a strategic business capability.

How to apply

To register for the CISO Academy 2026, please visit our website:

https://istari-global.com/insights/events/ciso-academy-2026/

Alumni testimonials

Here's some feedback on other executive education programmes from past participants.

"A superb and comprehensive package for any current or aspiring CISO. I attended a programme 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

"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

"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 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

Blackstone

ISTARI
ACADEMY

Apply here: