Post event report

Strategic Sponsors

Integrity360 – your security in mind

RISK LEDGER

rubrik

SolutionLab

THREATLOCKER

Education Seminar Sponsors

Abnormal

KnowBe4

HOXHUNT

Recorded Future®

> “ Thank you again for inviting me to the conference. I found it really valuable, and I hope I will have the chance to join the next one. ”
> **Information Security Analyst, Euroclear Sweden**

> “ I had such a great time. Well organised, great speakers, tips, insight and networking. 10 out 10. Knocked it out of the park! ”
> **SIT Security, Kronans Apotek**

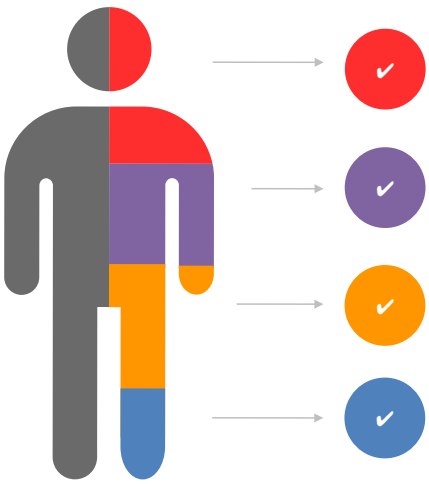
> “ Attending the congress was an incredibly rewarding experience. I gained valuable insights from industry peers, expanded my professional network, and left feeling inspired and energised. It was a great opportunity for learning and growth. ”
> **Cyber Security Risk Advisor, Nordea**

Inside this report:

Key themes

- Building a next gen security architecture
- What do regulators really want?
- Cybersecurity as a service: the pros and cons
- Making the most of AI and ML
- Developing the next generation of security leaders
- Cybersecurity for SaaS/IaaS/PaaS

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Jonathan Armstrong, Partner
Punter Southall Law

Måns Blacker,
Senior Incident Response Analyst
Integrity360

Haydn Brooks, CEO
Risk Ledger

Maxime Cartier, Head of Human Risk
Hoxhunt

Rune Espensen,
Head of Information Security Office
Nordea

Sofia Frederiksen, CISO
Apoteket

Fredrik Hertz,
Regional Lead Cybersecurity Consulting
EY

Andrés Jato, Ambassador for
International Cyber and Digital Affairs
Swedish Ministry of Foreign Affairs

Björn Johrén, CISO
Max Matthiessen

Edvinas Kerza, Managing Partner
ScaleWolf on behalf of SolutionLab

Sami Laurila, Account Executive
Rubrik

Sachin Loothra,
Lead Solutions Architect
Telia

Julius Nicklasson,
Manager, Intelligence Services
Recorded Future

Simon Rosén,
Regional Account Executive |
Human Risk Management Advocate
KnowBe4

Elin Ryrfeldt, CISO
Axfood

Manit Sahib,
Ethical Hacker & Former Head of
Penetration Testing & Red Teaming
Bank of England

Amanda Spångberg, Account Director
Integrity360

Eric Stenberg,
Information Security Officer
Swedbank

Elnaz Tadayon,
Cybersecurity Area Manager
H&M

Jake Wardell, Senior Engineer
Abnormal Security

Agenda

08:30 Breakfast networking and registration

09:20 Chair's welcome

09:30 **DDoS – A Nordic bank's perspective**

Rune Espensen, Head of Information Security Office, Nordea

- Overview of the DDoS attack on Nordea in the fall: scale and impact
- How Nordea detected, mitigated, and responded to the attack in real-time
- Lessons learned and future strategies to enhance resilience against DDoS threats

09:50 **Defending data in the age of AI, how to securely accelerate enterprise AI adoption**

Sami Laurila, Account Executive, Rubrik

- Join us for a dynamic session as we unveil how Rubrik is transforming data protection in the era of artificial intelligence
- AI can be a key business enabler, but with that opportunity come significant potential risks
- As custodians of customer data, Rubrik's solutions are uniquely designed to safeguard sensitive data, ensuring robust security and compliance as businesses harness the power of AI
- Learn more about Data Security Posture Management (DSPM), and the recently announced Rubrik Annapurna for Amazon Bedrock, and how it helps customers better leverage all their data – regardless of where it resides – to drive customised, secure generative AI applications

10:10 **The heart of IT security – blood, sweat and tears… of joy?**

Björn Johrén, CISO, Max Matthiessen

- Security first culture and how will we cope with the change?
- With all AI in the tech around us, do we still need humans? [or will AI prove humans are surplus to requirements?]
- The strongest line of defence and the most vulnerable link – the human paradox

10:30 **Education Seminars | Session 1**

Hoxhunt	Recorded Future
From metrics to meaning: Proving the true impact of your phishing training	**The geopolitics of cybercrime**
Maxime Cartier, Head of Human Risk, Hoxhunt	**Julius Nicklasson,** Manager, Intelligence Services, Recorded Future

11:10 Networking break

11:40 **Securing critical infrastructure with IAM in an elevated threat landscape**

Sachin Loothra, Lead Solutions Architect, Telia

- Evolving threat landscape and its impacts on critical infrastructure
- Regulations on critical infrastructure and demands towards IAM
- How IAM solutions can be setup to meet the demands

12:00 **Fake it till you break it: combating deepfakes & AI trickery**

Amanda Spångberg, Account Director, Integrity360 & **Måns Blacker,** Senior Incident Response Analyst, Integrity360

- How do you defend against what you can't trust your eyes or ears to detect?
- We'll dive into the growing challenge of deepfake technology
- Exploring how it can bypass traditional security controls, erode trust, and be weaponised for social engineering and disinformation
- We'll also look at the solutions that can combat this new and growing challenge

12:20 **Education Seminars | Session 2**

Abnormal Security	KnowBe4
The AI threat: Protecting your email from AI-generated attacks	**Effectively managing human risk in cybersecurity**
Jake Wardell, Senior Engineer, Abnormal Security	**Simon Rosén,** Regional Account Executive | Human Risk Management Advocate, KnowBe4

Agenda	
13:00	Lunch & networking break
14:00	**Mitigating personal liability: The changing climate for security professionals** **Jonathan Armstrong,** Partner, Punter Southall Law • The changing politics of security • Current cases • Social media scrutiny • Insurance options for CISOs • Golden parachutes and legal support
14:30	**Cybersecurity in changing the geopolitical environment: Lessons learned in the Baltic States** **Edvinas Kerza,** Managing Partner, ScaleWolf on behalf of SolutionLab • The geopolitical situation causes challenges to transform • State-funded actors found new ways to hack us • Secure by design does not exist • There are ways to counter and fight today's challenges
14:50	**Untangling the supply chain problem: Managing concentration risk** **Haydn Brooks,** CEO, Risk Ledger • Explore different types of supply chain risk and how they impact companies ability to deliver against its business goals • How to move past risk management into operational cyber-capabilities within the supply chain • How to talk to your board in a way that makes this problem not only digestible but also interesting • Leave with actionable insights and key questions to consider when strengthening their organisation's resilience against these critical threats
15:10	**Leveraging DORA TLPT (Threat-Led Penetration Testing) to enhance cyber-resilience** **Manit Sahib,** Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England • How DORA TLPT aligns seamlessly with TIBER-EU, CBEST & DORA to enhance cyber-risk management • Discover the benefits of an EU-standard approach to threat-led testing • See how DORA TLPT boosts readiness for live system testing • Learn how to start using DORA TLPT for ongoing cyber-resilience and regulatory compliance
15:30	Networking break
15:50	**EXECUTIVE PANEL DISCUSSION** **Critical functions: What really matters?** **Fredrik Hertz,** Regional Lead Cybersecurity Consulting, EY (Moderator); **Eric Stenberg,** Information Security Officer, Swedbank; **Elnaz Tadayon,** Cybersecurity Area Manager, H&M; **Sofia Frederiksen,** CISO, Apoteket; **Elin Ryrfeldt,** CISO, Axfood • Prioritisation: Are you and your stakeholders truly aligned on what's mission-critical? • Third-party dependence: Trust is good – but how much control do you actually have over critical processes? • Incident reporting: With rising regulatory demands for transparency, what does effective cyber-incident reporting really involve – and what value does that data bring?
16:30	**Sweden's foreign and security policy strategy for cyber and digital issues** **Andrés Jato,** Ambassador for International Cyber and Digital Affairs, Swedish Ministry of Foreign Affairs • Sweden's strategic vision: Aligning cyber-policy with national security, EU frameworks, and international stability • Geopolitical challenges: Addressing state-sponsored threats, cyber-warfare, and global tensions • Public-private collaboration: Strengthening partnerships to enhance cyber-resilience and critical infrastructure security • Global cyber-norms: Advancing cyber-diplomacy, regulatory frameworks, and responsible state behaviour
16:50	Conference close

Education Seminars	
Abnormal Security **The AI threat: Protecting your email from AI-generated attacks** **Jake Wardell,** Senior Engineer, Abnormal Security	Email security is at a turning point. The rise of generative AI is transforming the threat landscape, enabling attackers to craft hyper-personalised, convincing phishing emails at scale. Traditional defences – built to detect outdated attack patterns – are struggling to keep up. Attendees will learn: • The evolution of email-based attacks – How cyber-threats have advanced and why AI is accelerating their effectiveness • The new cybersecurity reality – With 91% of security professionals reporting AI-enabled attacks in the last six months and 97% acknowledging that traditional defences are ineffective, how can we adapt? • Good AI vs Bad AI – How attackers leverage AI to bypass defences, and why security teams need AI-driven solutions to fight back • Taking an Abnormal approach to cybersecurity – Real-world examples of AI-generated threats stopped by Abnormal Security, showcasing how behavioural AI can detect and block even the most sophisticated attacks
Hoxhunt **From metrics to meaning: Proving the true impact of your phishing training** **Maxime Cartier,** Head of Human Risk, Hoxhunt	Phishing simulations are a key component of security programmes, but traditional metrics like click rates often fail to reflect their true effectiveness. Instead of focusing solely on failures, how can security teams measure real behaviour change and risk reduction? Join Maxime Cartier, Head of Human Risk at Hoxhunt, as he explores advanced phishing training metrics – including report rates, dwell times, and real-world threat detection – that provide a clearer picture of security resilience. Learn how these insights can help identify high-risk groups, refine training strategies, and strengthen overall defence. Backed by success stories from companies like Qualcomm, this session will equip you with actionable strategies to demonstrate measurable impact, gain leadership buy-in, and align phishing training with broader security goals. Whether you are a CISO, security specialist, or analyst, you will walk away with practical ways to turn phishing training data into meaningful risk insights – and prove its value beyond just the click rate. Attendees will learn: • How metrics influence the way an organisation thinks about security and its culture • Proven interventions that transform high-risk employees into proactive defenders • How companies like Qualcomm overcame their repeat-clicker challenge • How to communicate the impact of human risk resilience efforts to leadership and secure buy-in for long-term security culture improvements
KnowBe4 **Effectively managing human risk in cybersecurity** **Simon Rosén,** Regional Account Executive | Human Risk Management Advocate, KnowBe4	Despite strong defences, organisations often fall victim to cyber-attacks due to misaligned focus. This presentation explores effective cyber-risk management, emphasising human behaviour as a critical factor. We will explore why traditional security measures may fall short and how a single vulnerability can lead to a breach. Attendees will learn: • Identifying and prioritising actual cyber-threats • Aligning defensive measures with real risks • Addressing human behaviour as a key vulnerability

Education Seminars

Recorded Future

The geopolitics of cybercrime

Julius Nicklasson, Manager, Intelligence Services, Recorded Future

This presentation explores how geopolitics shapes cybercrime, especially how state relationships with cybercriminals influence the types of attacks we see. Data shows that ransomware and extortion disproportionately target NATO countries, often serving both strategic disruption and financial gain. In contrast, 'free market' cybercrime ecosystems focus more on cyber-fraud and crypto theft and carry a much wider spread of geographic targeting.

Attendees will learn:

- A spectrum of state responsibility helps explain these patterns – covering examples from state-prohibited environments through to examples of state-integrated models, where cybercrime is used for geopolitical objectives and economic support to finance government initiatives
- Industries like healthcare, manufacturing, and transportation are frequent targets due to their high disruption impact. Meanwhile, state and criminal groups are evolving in parallel, often adopting techniques inspired by one another – criminals adopt espionage techniques such as abusing legitimate services, while states begin to use GenAI and deepfakes
- Find out which cybercriminal groups are also growing, often operating across Southeast Asia, driven by economic pressures and weak oversight, with some relying on human trafficking and coerced labour in large-scale fraud schemes