Post event report

Strategic Sponsors

ARCTIC WOLF

BeyondTrust

CROWDSTRIKE

KnowBe4
Human error. Conquered.

rubrik

securonix

SentinelOne

SOCRadar

Education Seminar Sponsors

Abnormal

COFENSE

illumio

VECTRA

Networking Sponsor

Silobreaker

Branding Sponsor

HUNTERS

“ Even though I am not a super expert in either of the topics on the agenda, I participated with curiosity and an open mind and was not let down. It gave me some good insights of how the future could look in the fraud landscape and also gave me some insights on to whom we can turn to when we are looking for solutions or tools to prevent future threats. ”

Product Owner in Fraud management, Nordea

“ The conference was thought-provoking. Life in the cyber-world is, as evidenced daily and underlined by insightful speakers at the event, complex. How to be on top of a constantly moving target? There were some good thoughts and tips but no universal panacea. Clearly various non-financial risk disciplines that fall under operational risk category, including cybersecurity, would benefit from a more holistic appoach and better collaboration with internal and external stakeholders, including regulators. Hopfully the code of how to solve this challenge will be cracked by the speakers next year. Looking forward to this. ”

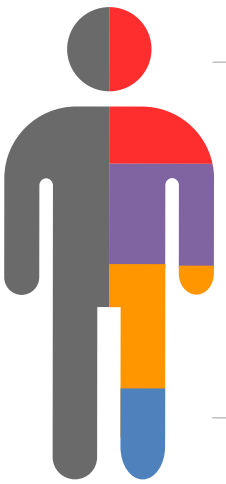
Operational Risk Director, Intrum

Inside this report:

Key themes

- Are AI/ML solutions the answer?
- Closing the cybersecurity skills gap
- Here comes real cybersecurity regulation
- Cloud native next
- Can zero trust be done?
- Embracing digital risk management
- From smart machines to smart cities – securing the IoT
- Developing the next generation of security leaders
- Securing digital currencies
- Ransomware – dealing with the new normal
- Securing the citizen
- Building better Cloud security

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

Christian Borst, EMEA CTO, Vectra AI

Simon Brady, Managing Editor, AKJ Associates

Geir Arild Engh-Hellesvik, Director, Defence against Advanced Digital Threats, Norwegian National Security Authority

Tom Engly, Former CISO Tryg, Senior Cybersecurity & Crisis Management Advisor, Tryg

Predrag Gaikj, Chief Information Security Officer, Qliro

Stephen Gailey, Sr. Director of Solution Architecture, Securonix

Petter Glenstrup, Senior Systems Engineer – Nordics, Arctic Wolf

James Hickey, Director, Sales Engineering, Cofense

David Lomax, Systems Engineer, Abnormal Security

Henrik Løth Thiesen, Global Director Information Security & Risk Management, Vestas

Raghu Nandakumara, Head of Industry Solutions, Illumio

David Palmer, Business Lead for Blockchain Technology, Vodafone

Mikkel Planck, Senior Cybersecurity Specialist, CrowdStrike

Patrick Reischl, Strategic Solutions Engineer, SentinelOne

Ensar Seker, VP of Research, Advisory Information Security Officer (CISO), SOCRadar

Matt Sturman, Solutions Engineer, BeyondTrust

Mads Syska Hasling, CISO, Saxo Bank

Gøran Tømte, Field Security Responsible Germany and NEUR, Rubrik X

Bjørn R. Watne, Senior Vice President and Chief Security Officer, Telenor Group

Jelle Wieringa, Security Awareness Advocate, KnowBe4

Thomas B. Zuliani, Director, Information Security & Data Privacy, Pandora

Agenda

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **Emerging technologies and advanced threats – a perfect storm**

Geir Arild Engh-Hellesvik, Director, Defence against Advanced Digital Threats, Norwegian National Security Authority

- Geopoliticial tensions are increasing, we are seeing an increase in advanced threat actor activity
- We need to understand our adversaries, their tools and techniques
- Emerging technologies (5G, AI/ML, quantum computing) are adding complexity
- Is our toolbox up to the task? How can we evolve our protective measures collectively?

09:20 **Cybersecurity has an effectiveness problem**

Petter Glenstrup, Senior Systems Engineer – Nordics, Arctic Wolf

- Cyber-risk is a business risk. Unfortunately, the cybersecurity industry has proven ineffective in reducing organisational cyber-risk
- To solve the effectiveness problem in cybersecurity, organisations have realised they need a solution that combines technology with human expertise and delivers it in a way that addresses day-to-day security needs while also ensuring that their overall security posture gets stronger over time.
- This realisation has led to the emergence of Security Operations as its own discipline, reducing the likelihood and the impact of a breach and end cyber-risk

09:40 **Lessons learned from multibillion-dollar ransomware empires**

Ensar Şeker, VP of Research, Advisory Information Security Officer (CISO), SOCRadar

- How ransomware groups evolved and built multi-billion-dollar crime 'business' ecosystems
- What percentage of the million-dollar ransom request is paid after negotiations (w/ real-life examples)
- TTPs of most active ransomware groups
- How to mitigate ransomware risk with early-warning cyber-threat intelligence methodologies

10:00 **We need to talk…**

Henrik Løth Thiesen, Global Director Information Security & Risk Management, Vestas

- How security risk should be measured via financial impacts
- How strategic threat intention is a part of how to quantify the likelihood
- How to communicate with executives continuously

10:20 **Education Seminars | Session 1**

Abnormal Security
Key considerations for choosing the right cloud email security platform
David Lomax, Systems Engineer, Abnormal Security

Illumio
From digital laggard to cyber-leader
Raghu Nandakumara, Head of Industry Solutions, Illumio

11:00 Networking break

11:30 **EXECUTIVE PANEL DISCUSSION** **CISOs and security technology**

Predrag Gaikj, Chief Information Security Officer, Qliro; **Bjørn R. Watne,** Senior Vice President and Chief Security Officer, Telenor Group; **Henrik Løth Thiesen,** Global Director Information Security & Risk Management, Vestas

This panel will look at:

- Different approaches to selecting and consolidating security technologies
- Budget and investment questions as more vendors broaden their capabilities
- Replacing legacy cybersecurity technology
- One-stop shop versus security stack
- Building a continuous control environment for cybersecurity

11:50 **Debunking common myths about XDR**

Patrick Reischl, Strategic Solutions Engineer, SentinelOne

- What is XDR and why should I consider the technology in my enterprise security stack?
- What should I expect from vendors who claim to have built the perfect mousetrap?
- What is reality, and what is just hype?
- What common myths around XDR continue to muddy the water for security teams?

12:10 **Psychology of a social engineering attack**

Jelle Wieringa, Security Awareness Advocate, KnowBe4

In this talk, you will better understand how cybercriminals leverage the power of your own mind to make you do their bidding. And how a better understanding of yourself can help to better protect against this. Get actionable insights on:

- The tricks cybercriminals use to manipulate you
- How psychology plays a vital role in social engineering
- How to better protect yourself

Agenda

12:30 **The path to Zero Trust by securing privileged identities**

Matt Sturman, Solutions Engineer, BeyondTrust

Zero Trust is built on foundations that are essential across your cybersecurity strategy, delivering greater value from existing cyber-investments. In this session, Chris will outline:

- Why protecting identities is fundamental to achieving Zero Trust
- Practical steps you can take NOW to secure your privileged identities
- The pivotal role Privileged Access Management plays in achieving Zero Trust

12:50 **Education Seminars | Session 2**

Cofense	Vectra AI
Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence	**Erasing surface, identity, complexity and unknowns**
James Hickey, Director, Sales Engineering, Cofense	**Christian Borst,** EMEA CTO, Vectra AI

13:30 Lunch break

14:20 **The metaverse opportunity**

David Palmer, Business Lead for Blockchain Technology, Vodafone

- What are the key enablers for virtual and real worlds to co-exist?
- The key challenges
- Security, identity, jurisdiction, copyright and ownership

14:40 **The challenge with modern cybercrime against businesses**

Gøran Tømte, Field Security Responsible Germany and NEUR, Rubrik X

- Ingress: Evolution is running as always. This is relevant and good for business, digitalisation, and technology
- Criminals adopt and evolve with all the changes, revealing new vulnerabilities and all the new capabilities in new technology. It's important to stay up to date to be best prepared
- Let's look at the business consequences before, during and after an incident

15:00 **How to address the skills shortages in a proactive manner to respond to adversaries**

Mikkel Planck, Senior Cybersecurity Specialist, CrowdStrike

- Tooling and techniques to address skills shortages
- Automation and services to keep you ahead of attackers
- How technology can help you become proactive and stop breaches

15:20 **Rules, Alerts, Context and Anomalies (RACA) – modern detection techniques for modern e-crime**

Stephen Gailey, Sr. Director of Solution Architecture, Securonix

- Early detection is of paramount importance in the fight against e-crime yet the average time to identify a breach or fraud still runs into the hundreds of days
- This presentation will explore how modern techniques can significantly improve early detection
- Looking at why do we fail to detect e-crime, what is the current best practice, how modern techniques work and why deployment is such a pain

15:40 **Fireside chat: A CISO's perspective on....**

Simon Brady, Managing Editor, AKJ Associates and **Mads Syska Hasling,** CISO, Saxo Bank

- How the macroeconomic downturn will affect CISOs, budgets and security
- Dealing with the risks of state-sponsored cyber-attacks and spillovers
- Practical tips for implementing a risk-based approach to cybersecurity

16:00 Networking break

16:20 **Developing the next generation of security leaders**

Predrag Gaikj, Chief Information Security Officer, Qliro

- The role of the information security – different interpretations in different companies
- How is the role changing?
- What does a next-gen CISO look like and are you one of them?

16:40 **EXECUTIVE PANEL DISCUSSION CISO future challenges**

Thomas B. Zuliani, Director, Information Security & Data Privacy, Pandora; **Bjørn R. Watne,** Senior Vice President and Chief Security Officer, Telenor Group; **Tom Engly,** Former CISO Tryg, Senior Cybersecurity & Crisis Management Advisor, Tryg

This panel will look at the challenges posed by:

- Asset inventories (devices, applications, identity, network, data)
- Overall technology landscape complexity,
- 'Digital' transformations of the business/products
- Testing and measuring the effectiveness of the cybersecurity control environment
- Incident response and problem management
- Ensuring the same coverage/visibility over cloud environments as on-prem
- Managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid)
- Web 3.0 and the next generation of the internet: securing new technologies and services which are inherently decentralised?

17:00 Conference close

Education Seminars

Abnormal Security

Key considerations for choosing the right cloud email security platform

David Lomax, Systems Engineer, Abnormal Security

Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars.

Unfortunately, email threats are only growing in number. Business email compromise accounts for 35% of all losses to cybercrime, and the Verizon Data Breach Investigations Report holds that phishing remains the top entry point for breaches – a position it has held for years.

Does that mean email is doomed, and we should give up? Quite the opposite. But the shift to cloud email requires one major thing: a shift to cloud email security.

Attend the Abnormal Security session for answers to your most pressing questions, including:

- What are modern email threats, and how are they different from legacy attacks?
- Which email threats are most concerning, and how can we defend against them in the cloud environment?
- Which technical capabilities are required when protecting cloud email?
- How can cloud email security platforms detect the most dangerous attacks?

Cofense

Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence

James Hickey, Director, Sales Engineering, Cofense

What is an adaptive security architecture and what are the objectives? With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation.

In this session, we'll:

- Walk you through the benefits and objectives of implementing an adaptive security architecture and risk framework
- The current situation in email and phishing security. We'll share some of the latest insights from the industry and what we're seeing through our unique combination of artificial, human, and high-fidelity intelligence
- Implementing adaptive security architecture and risk framework with Cofense. We'll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity

Illumio

From digital laggard to cyber-leader

Raghu Nandakumara, Head of Industry Solutions, Illumio

The need for business to transform was driven by the pandemic with the adoption of new applications and automation. The challenge is delivering cyber-resilience as the criminal gangs have transformed the way they operate, improving their evasion techniques for detection products and targeting critical infrastructure. Adopting Zero Trust is a simple way to deliver a structured approach to security.

In this session, we will look at:

- Some of the issues and lay out an effective approach to identifying risk and deploying preventive measures to contain an attack
- Limiting the spread of ransomware and breaches

Vectra AI

Erasing surface, identity, complexity and unknowns

Christian Borst, EMEA CTO, Vectra AI

Threat intelligence has been a critical component to knowing threat types, methods, and profiles. As enterprises shift to cloud, security and risk leaders are facing an onslaught of unknowns. Unknown compromises, attack progressions and prioritisation challenges require more reliable, accurate, and timely insights into advanced attacks.
In this session learn how security operations need to shift their focus to be more proactive in identifying and stopping sophisticated ATPs.

During our presentation, we will cover:

- What is threat intelligence and how it benefits your organisation and SOC team
- How to analyse the data to understand the threat landscape, anticipate attackers' next moves and take prompt action to stop attacks
- The importance of ongoing intelligence to prevent emerging risks and threats