Post event report

Principal Sponsor

CROWDSTRIKE

Strategic Sponsors

Gigamon®

LogRhythm

Menlo Security

okta

proofpoint.

SentinelOne

Education Seminar Sponsors

cybereason

digital shadows_

edgescan™

egress

illumio

INTSIGHTS
Defend Forward™

kaspersky

Networking Sponsors

ThreatConnect™

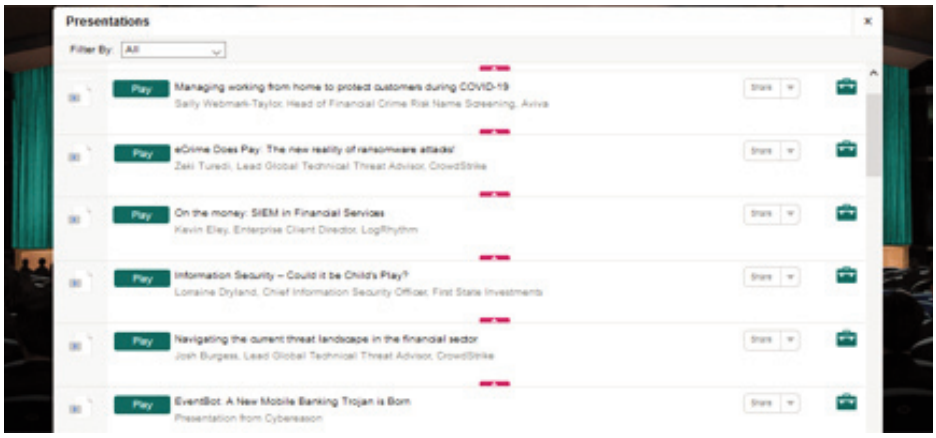
VERACODE

"I enjoyed the conference very much. I thought the platform and the format was exceptional. Liked the idea that I could do my day to day and still catch up on the presentations I wanted to attend. Well done."
Senior IT & Cybersecurity Risk Manager, Scotiabank Europe

"Very interesting speakers/ catch up with contacts etc. Also fantastic virtual experience – well thought out and added lots of value – actually preferred it on one level to the normal (always good) previous events."
Senior Technology Risk Manager, Credit Suisse

"The level of engagement yesterday was outstanding and we have already managed to book 2 meetings as a result, live on the day."
Regional Marketing Manager EMEA/APAC, Veracode

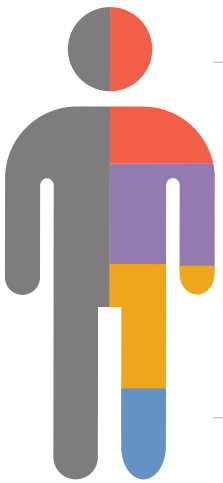
Inside this report:



Key themes

- Protecting the customer, securing e-/mobile channels
- Securing and protecting remote employees
- Blurring the boundaries in financial crime
- Securing FinTech
- Cybersecurity by remote control
- Control, supervision, audit
- Best practice in the cloud
- Protection versus business needs

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

Fahim Afghan, Senior Product Marketing Manager, Egress Software Technologies

Liz Banbury, Head of Information and Cyber Policy, Standard Chartered Bank

Rob Bolton, Senior Director, Insider Threat Management, Proofpoint

Simon Brady, Managing Editor, AKJ Associates

Matt Bryant, CISO, Monese

Josh Burgess, Lead Global Technical Threat Advisor, CrowdStrike

Kacey Clark, Team Leader Cyber Intelligence Analyst, Digital Shadows

Maxim Denizhenko, Business Development Lead Enterprise Blockchain Security, Kaspersky

Lorraine Dryland, Chief Information Security Officer, First State Investments

James Easton, Senior Solutions Architect, Gigamon

Kevin Eley, Enterprise Client Director, LogRhythm

Martin Farrelly, Information Security Architecture and Strategy, Allied Irish Bank

Max Faun, EMEA Head of Business Consulting, Okta

Andrew Fleming, Global Compliance MI Senior Risk Reporting Manager, HSBC

Alex Guirakhoo, Team Lead, Threat Researcher, Digital Shadows

Denis Heneghan, Cyber Security Outreach Manager, Allied Irish Bank

Eoin Keary, CEO & Founder, Edgescan

Jonathan Lee, Sr. Product Manager, Menlo Security

Andrew Mason, Head of Financial Crime, Bó

Pavel Mucha, Systems Engineer, Cybereason

Raghu Nandakumara, Field CTO EMEA, Illumio

Michael Owen, Head of Systems Engineering UK&I, IntSights Cyber Intelligence BV

Jan Tietze, Director Security Strategy EMEA, SentinelOne

Zeki Turedi, Lead Global Technical Threat Advisor, CrowdStrike

Sally Webmark-Taylor, Head of Financial Crime Risk Name Screening, Aviva

Agenda

08:00 Login and registration

09:05 Chairman's welcome

09:10 **Managing working from home to protect customers during COVID-19**

Sally Webmark-Taylor, Head of Financial Crime Risk Name Screening, Aviva
- Keeping 'Business as Usual' going: helping customers during the health crisis
- Coping with working from home and managing financial crime risks
- Financial crime, fraud and security – Covid threats and challenges to Aviva and its customers

09:30 **e-Crime does pay: the new reality of ransomware attacks!**

Zeki Turedi, Lead Global Technical Threat Advisor, CrowdStrike
- What does ransomware mean to you? An annoyance that can easily be fixed, an automated attack, or a tool used by a human actor to take your business to ransom?
- Learn about the tactics, techniques and procedures e-Crime actors have been using to benefit
- How can finance organisations better arm themselves against these evolving attacks

09:50 **On the money: SIEM in financial services**

Kevin Eley, Enterprise Client Director, LogRhythm
- According to the Verizon Data Breach Investigations Report 2020, organised criminal gangs are the top threat actor for the financial services, and financial gain is the main motivation
- How a SIEM can be leveraged to detect and respond to such attacks and provide defence for financial service organisations
- The importance of continual alignment between SIEM and the threat landscape
- The criticality of teaming with the business for success

10:10 **Information security – could it be child's play?**

Lorraine Dryland, Chief Information Security Officer, First State Investments
- ADAPTING: Morphing policy and standards
- COMMUNICATION & COLLABORATION: Using goals to talk to the business
- SECURITY CONSCIOUS CULTURE: Speak the language of employees and make learning interactive
- DEFENCE for GLOBAL BUSINESS: Don't get trapped in complexity

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

CrowdStrike	Cybereason	Kaspersky
Navigating the current threat landscape in the financial sector	**EventBot: a new mobile banking trojan is born**	**Cybersecurity in enterprise blockchain. Best practice, experience, tips**
Josh Burgess, Lead Global Technical Threat Advisor, CrowdStrike	**Pavel Mucha,** Systems Engineer, Cybereason	**Maxim Denizhenko,** Business Development Lead Enterprise Blockchain Security, Kaspersky

11:00 Networking break

11:30 **Protecting the digital customer**

Martin Farrelly, Information Security Architecture and Strategy, Allied Irish Bank, and
Denis Heneghan, Cyber Security Outreach Manager, Allied Irish Bank
- The community of branch-based customers have now gone digital
- The rise in phishing, smishing and multi-channel fraud
- Methods of educating customers on security best-practice
- The increase in reliance on remote banking services: tackling the security challenges

11:50 **The threat hunting challenge: detect, prevent, respond and hunt – every second, every day**

Jan Tietze, Director Security Strategy EMEA, SentinelOne
- Learn how Endpoint Detection & Response (EDR) technologies pick up where antivirus technologies leave off
- Understand why EDR should be an essential part in every Endpoint Security Strategy
- Learn how EDR auto-immunises the endpoints against newly discovered threats and provides rich forensic data, mitigate threats and performs network isolation
- Demo

12:10 **Securing financial services in the age of digital transformation**

James Easton, Senior Solutions Architect, Gigamon
- The old cliché "you can't protect against what you can't see" holds as true for cybersecurity as for physical security
- Financial services organisations have been at the forefront of digital transformation and have realised that, without the right planning and tools, security can become a casualty in this process
- Gigamon discusses these issues and highlights ways you can protect yourselves and your customers in the digital transformation process

Agenda

12:30 — Zero trust internet – moving beyond 'almost safe'

Jonathan Lee, Sr. Product Manager, Menlo Security

- Enterprise spending on cybersecurity continues to go up, yet they keep getting infected again and again and again
- Digital transformation is accelerating the adoption of cloud-based apps and services, rendering legacy security architectures obsolete
- How we need to invert our thinking from being app/data centric to a cloud-based, user centric approach
- Can we move beyond good vs. bad and 'almost safe' to zero trust?

12:50 — Education Seminars | Session 2

Digital Shadows	Edgescan	IntSights
Dark web digest: gaining valuable threat intelligence from cybercriminal forums	**Enemy at the gates…why traditional vulnerability management has failed. AKA 'Why hackers don't give a damn'**	**Protecting the business with intelligence from outside the wire**
Alex Guirakhoo, Team Lead, Threat Researcher, Digital Shadows, and **Kacey Clark,** Team Leader Cyber Intelligence Analyst, Digital Shadows	**Eoin Keary,** CEO & Founder, Edgescan	**Michael Owen,** Head of Systems Engineering UK&I, IntSights Cyber Intelligence BV

13:20 — Lunch and networking break

14:10 — Who secures the financial services?

Simon Brady, Managing Editor, AKJ Associates

- A broad and comprehensive overview of cybersecurity trends within the financial services informed by AKJ Associates' original research
- From the trading floor to the employee home; how a crisis has transformed our understanding of operational resilience throughout the organisation and the supply chain
- Accelerated digitisation and an expanded attack surface. Where are the major vulnerabilities in the financial services?

14:30 — You're only supposed to blow the bloody doors off! Defending against the next generation of bank jobs

Max Faun, EMEA Head of Business Consulting, Okta

- The finance sector finds itself at the centre of persistent, sophisticated hacks and attacks just as customers are demanding the same frictionless experience they have with the world's largest online retailers
- This session re-examines traditional security approaches and to these challenges and explores how Identity and Access Management must now take centre stage to defend against future security attacks
- Topics include: Credential theft and compromise; Gaps in the security landscape; The missing ingredient, Identity; Adaptive multi-factor authentication; Strategic direction for identity-driven security

14:50 — A people-centric approach to managing the risk of insider threats

Rob Bolton, Senior Director, Insider Threat Management, Proofpoint

Insider threats are on the rise. According to a new research study from Ponemon, the financial services sector experienced the highest total average annual cost to contain insider threat incidents, at $14.50 million a 20.3% increase since 2018. In this session learn:

- Why insider threats are unique, and require context around both user and data activity
- How to gain visibility into the different types of insider threats your organisation faces
- How a modern people-centric approach can help you manage the risk of insider-led data breaches
- The types of insider threat profiles and how to address them
- How to reduce response time by accelerating investigations

15:10 — Education Seminars | Session 3

CrowdStrike	Egress Software Technologies	Illumio
Navigating the current threat landscape in the financial sector	**Solving your #1 security risk**	**Why you should implement micro-segmentation for regulatory compliance**
Josh Burgess, Lead Global Technical Threat Advisor, CrowdStrike	**Fahim Afghan,** Senior Product Marketing Manager, Egress Software Technologies	**Raghu Nandakumara,** Field CTO EMEA, Illumio

15:40 — Networking break

16:00 — Using standardised digital identification and electronic signatures in data governance

Andrew Fleming, Global Compliance MI Senior Risk Reporting Manager, HSBC

- Reducing financial crime risk to the business through bio metrics
- Enhance the customer experience across different internal divisions
- Overlay the personalised data across transaction monitoring to reduce false positives and improve alert generation

16:20 — Data management in the financial sector Q&A

Liz Banbury, Head of Information and Cyber Policy, Standard Chartered Bank

- What are your critical assets, and how is your data managed?
- What has the WFH period taught you about your data governance methodology?
- How strong cyber risk policy can become core to operational resilience strategy
- Securing a global financial institution

16:40 — EXECUTIVE PANEL DISCUSSION — Fintechs in 2020: Security and financial crime under lockdown

Like any organisation, fintechs and digital banks have had to transform their operations to adapt to C19 and WFH. Having often been portrayed as being more naturally suited to security and financial crime prevention due to their digital nativeness, smaller size, and lack of silos and legacy systems, has security flourished in the new environment? And as larger financial institutions witness migration from branch banking to virtual customer interaction, are fintechs leading the way?

Matt Bryant, CISO, Monese

Andrew Mason, Head of Financial Crime, Bó

17:00	Closing remarks	**17:10**	Networking	**17:30**	Conference close

Education Seminars

CrowdStrike

Navigating the current threat landscape in the financial sector

Josh Burgess, Technology Strategist, EMEA, CrowdStrike

At CrowdStrike, we put a lot of time and effort into understanding intelligence trends and profiling the attackers behind attacks. We even name our attackers individually to give them identity – since we spend so long trying to learn all about them! One thing we have learnt is that nation-state and criminal threat actor groups can have a particular threat to the financial sector. In this session, we will review associated threat actor capabilities and infrastructures as well as their tactics, techniques and procedures.

- Discuss specific implications to the financial sector
- How current events (such as the Covid-19 pandemic) are influencing cybersecurity threats to the financial sector and what the latest attack types are
- Understand mitigation strategies to stop these attacks
- Truly 'know' the adversary in order to properly build the best defences to stop the actor and not just the malware

Cybereason

EventBot: A new mobile banking trojan is born

Pavel Mucha, Systems Engineer, Cybereason

The Cybereason Nocturnus team has been investigating a new type of Android malware dubbed EventBot, which was first identified in March 2020. This malware appears to be newly developed with code that differs significantly from previously known Android malware. EventBot is under active development and is evolving rapidly; new versions are released every few days with improvements and new capabilities.

In this session you will learn:

- How Cybereason classifies EventBot as a mobile banking trojan and infostealer based on the stealing features discussed in this research. It leverages webinjects and SMS reading capabilities to bypass two-factor authentication, and is clearly targeting financial applications
- How EventBot targets users of over 200 different financial applications, including banking, money transfer services, and crypto-currency wallets
- Introducing a new offering, Cybereason Mobile, that strengthens the Cybereason Defense Platform by bringing prevention, detection, and response capabilities to mobile devices. With Cybereason Mobile, our customers can protect against modern threats across traditional and mobile endpoints, all within a single console

Digital Shadows

Dark web digest: gaining valuable threat intelligence from cybercriminal forums

Alex Guirakhoo, Team Lead, Threat Researcher, Digital Shadows, and **Kacey Clark,** Team Leader Cyber Intelligence Analyst, Digital Shadows

In our team's latest dark web findings, we have observed notable changes in criminal forum activity and trends. Dark web forums harbour a dynamic environment for criminals looking to buy or sell compromised data, zero-day exploits, and system accesses. This environment and the findings associated with it can uncover how criminals may use your individual or organisational information on the dark web, leading to further compromise, profit loss, data loss, or reputational damage. During this session, we will cover the risk impact of dark web findings, explore the evolution of dark web forums, and trends observed across platforms.

Key takeaways:

- Insights into current dark web trends
- Tactics and techniques attackers use to collect or share your data
- How to gain visibility into your organisation's dark web risk
- Strategies for fortifying your defences and mitigating dark web risks

Edgescan

Enemy at the gates…why traditional vulnerability management has failed. AKA 'Why hackers don't give a damn'

Eoin Keary CISSP CISA, CEO & Founder, Edgescan

- Why traditional vulnerability management has failed in keeping us secure
- What it takes to deliver vulnerability management at scale and how can we keep pace with the speed of development
- What is the trade-off between speed and accuracy and why is this acceptable?
- We shall also cover off highlights of the Edgescan Vulnerability Stats report 2020 focusing on the most common vulnerabilities and what it means to deliver a robust cybersecurity programme for any enterprise

Education Seminars

Egress Software Technologies

Solving your #1 security risk

Fahim Afghan, Senior Product Marketing Manager, Egress Software Technologies

Employees sending emails in error is the top cause of security incidents reported to Information Commissioner's Office. And large-scale remote working isn't helping: the COVID-19 pandemic has resulted in more information being shared by email than ever before – significantly increasing the risk of a security incident. For financial services firms, this risk is aggravated by high-pressure and fast-paced environments. So, how can CISOs and their security teams ensure employees send the right email to the right recipients, with the right level of security, while maintaining efficiency during remote working?

Join Egress Senior Product Marketing Manager, Fahim Afghan as he explains why human-activated email data breaches are your most significant security risk, examines the most common causes of these incidents, and looks at how contextual machine learning can eliminate this threat.

Key learning points:

- Understand the changing risk from human-activated email data breaches and identify the common causes of these incidents in your firm
- See how contextual machine learning can understand individual employee's email usage to prevent these incidents and protect data
- Learn how intelligent email security can increase effective TLS usage for enhanced data protection and usability
- Identify the areas where human layer security and contextual machine learning can improve data security in your firm

Illumio

Why you should implement micro-segmentation for regulatory compliance

Raghu Nandakumara, Field CTO EMEA, Illumio

Whether a sophisticated adversary or a fast-spreading ransomware attack, a common element across all high-profile breaches is lateral movement – the ability for malicious actors or malware to traverse a network.

This session will:

- Explain Illumio's approach to micro-segmentation focuses on blocking any network communications that are not explicitly authorised, stopping an adversary or malware in its tracks
- Prove the value of micro-segmentation in how it stops an adversary or malware in its tracks
- Discuss how a host-based approach can be used to help achieve compliance with industry standards

IntSights

Protecting the business with intelligence from outside the wire

Michael Owen, Head of Systems Engineering UK&I, IntSights Cyber Intelligence BV

Threats exist well before the targets are aware of them. In this fast moving environment, time is your most valuable asset. Understanding that a threat exists, or has growing potential before the attack has been weaponised, can be a major element of defence in your arsenal against the attackers.

This presentation will cover how intelligence gathered from outside your business can help you better protect it. In this 25 minute presentation elements such as what the problem is, how we can use this intelligence and what it can be used to protect against as well as where and how we find it in the first place, will be discussed and examples given.

What the attendees will learn:

- Where the problem exists and how it manifests itself
- The type of intelligence that can prove useful to providing an early warning of attacks
- How that intelligence can be used to mitigate the threat

Kaspersky

Cybersecurity in enterprise blockchain. Best practice, experience, tips

Maxim Denizhenko, Lead Business Development, Enterprise Blockchain Security, Kaspersky

At the session you will get a recap about blockchain technology in enterprises, overview of the threat landscape and corresponding cybersecurity measures. We will talk about best practices from real life use cases based on our experience.

In this presentation we will discuss:

- Enterprise vs Crypto
- Main attacks in corporate blockchains
- Enterprise blockchain case studies
- How to secure trust?