Post event report

Strategic sponsors

Attivo NETWORKS

BITSIGHT
The Standard in SECURITY RATINGS

CROWDSTRIKE

KENNA Security

OneTrust
Privacy
PRIVACY MANAGEMENT SOFTWARE

SECUREDATA
PART OF ORANGE CYBERDEFENSE

VECTRA
Security that thinks.

ZIMPERIUM
MOBILE THREAT DEFENSE

Networking sponsor

Integrity Scotland
IT Solution Experts

“ Exposure to the latest features of security services and applications is invaluable; condensed into a few hours with knowledge shared from those working in security and e-crime every day. Superb! ”

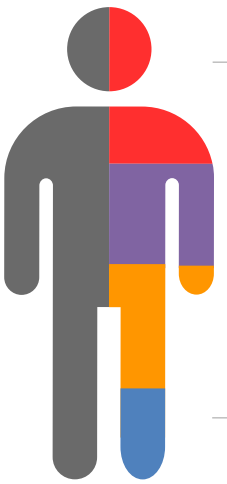
Policy Specialist, Morgan Stanley

Inside this report:

Key themes

- Getting the basics right
- Securing digital transformation
- A different approach to the issue of us
- Breaking down the barriers
- Managing the privileged few
- Slow train coming: the wait for intelligent cybersecurity

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

Arunava Banerjee,
Cybersecurity Manager
NHS Greater Glasgow and Clyde

Damien Behan, IT Director
Brodies

Nick Brownrigg, Security Consultant
SecureData

Paul Chapman, Head of Public Sector Cyber Resilience
Scottish Government

Dino Constantinou, UK & Northern Europe Channel Director
Zimperium

David Creighton-Offord,
Senior Information Security Consultant
The University of Edinburgh

Andrew Dillin,
Threat Intelligence Lead, Cyber
RBS

Mark Gale,
Head of Global Fraud Risk Management
Citi

Mark Howell, VP UK & Ireland
Attivo Networks

Fiona Kelly, Information Security & Resilience Risk Manager
TSB

Keith McDevitt, Cybersecurity-Integrator
Scottish Government

Chris Paterson,
Privacy Engineer, CIPP/E
OneTrust

Craig Potter, Detective Constable,
Specialist Crime Division
Police Scotland

Tony Povoas, CISO
Aegon UK

Stephen Roostan, VP EMEA
Kenna Security

Andrew Smith, CTO
Nucleus Financial

David Stevenson,
Head of Cyber Analytics Technology
Morgan Stanley

Chris Ulliott, CISO
RBS

Matt Walmsley, EMEA Director
Vectra

Mark Ward, Senior Solutions Architect
CrowdStrike

James Warriner,
EMEA Channel Sales Manager
BitSight Technologies

Agenda

08:00	Registration and breakfast networking
08:50	Chairman's welcome
09:00	**Why CISOs hate the word 'cyber': challenging the current cybersecurity paradigm, and aligning it with business goals** **Chris Ulliott,** CISO, RBS • The word cyber has become overloaded and there is little agreement on what it actually means – rather than talking about a vague cyber thing, we need to discuss the impact of insecure technology on our business objectives. Which leads to: • Challenging the current cybersecurity paradigm. What are the business demands on today's information security leader and how can they align their priorities with overall business objectives and continue to be seen as a business enabler? • Recent regulation has focussed the board's mind, but from a cybersecurity perspective, there is little that is new for those of us in the highly regulated financial sector. The senior manager regime has consequences for me as a CISO, but that's unusual – as experts we should be held to account for our decisions
09:20	**Defending against adversaries – what tactics can sport and warfare teach us to actively defend our networks from threat actors** **Mark Howell,** VP UK & Ireland, Attivo Networks • Tactics lessons from sport and warfare – what works when defending • Honeypots – from science project to modern day deception • Deception – attackers use it, defenders must • How can we apply these tactics in the cyber-realm?
09:40	**The time for change is now: the Scottish Government is upping the standards of cyber-resilience** **Paul Chapman,** Head of Public Sector Cyber Resilience, Scottish Government, and **Keith McDevitt,** Cybersecurity-Integrator, Scottish Government • First-hand exclusive case study covering the first two years of the Scottish Government's Public Sector Action plan – where we were, where we are now and where we're going • The Cyber Resilience Framework: why the need to up the standards of cyber-resilience is now • Ramifications for the private sector, and how to achieve greater public-private collaboration
10:00	Refreshments and networking
10:30	**5 a day: promoting good cyber-hygiene in healthcare** **Arunava Banerjee,** Cybersecurity Manager, NHS Greater Glasgow and Clyde • Meaningful cyber-awareness to develop a culture of good cyber-hygiene among healthcare professionals • Handling insider threats and other major risks with cyber-awareness • How to overcome challenges – product cost, staff time, organisational diversity, hours and location of working
10:50	**HACKING EXPOSED: Lessons in dealing with e-crime from the front line** **Mark Ward,** Senior Solutions Architect, CrowdStrike • How nation-state threats are crafted and how their Tactics, Techniques, and Procedures (TTPs) are infiltrating the corporate world in the form of advanced attacks • Who are the most notable adversaries in 2019 and the key European security themes based on the latest threat intel report published by CrowdStrike's global intelligence operation • What are the indicators of attack and how you can apply them to defeat the adversary?
11:10	**Why understanding your attack surface matters?** **Nick Brownrigg,** Security Consultant, SecureData • What does it mean to obtain and use 'cyber-intelligence' in a manner that effectively prioritises scarce resource across the full spectrum of 'Assess, Protect, Detect & Respond' cybersecurity disciplines? • Threats in cyber-space arise for two main reasons: weakness in IT infrastructure and an interest taken by an attacker. Most businesses know they must mitigate cyber-threats for their own good but also because regulators require them to • But the threat landscape is ever changing as technology evolves and attackers innovate. Ensuring an organisation has the skills, agility and underlying platforms and processes to understand, detect and manage cyber-threats is one of the most compelling challenges faced by any 21st century business. Regulatory changes have pushed to issue up to board level • What should the priority be for an organisation that wants to improve its cybersecurity posture, finding and removing vulnerabilities in its infrastructure or assessing the external threats it faces?
11:30	Refreshments and networking
12:00	**Agility ability: case study on managing cyber-risk alongside agile methodologies** **Andrew Smith,** CTO, Nucleus Financial • Case study: the relationship between the technology and the financial disciplines within Nucleus Financial • How to build effective risk modelling structures for cyber? The contrasts and similarities of cyber-risk and other forms of risk • The move to agile, and how digitalisation and automation impacts information security. Incorporating information security into agile methodologies
12:20	**Third-party risk management: overcoming today's most common security & privacy challenges** **Chris Paterson,** Privacy Engineer, CIPP/E, OneTrust • Review the drivers and challenges organizations face when managing third-party vendor risk • Identify priorities before, during and after vendor procurement • Takeaway a six-step approach for automating the third-party vendor risk lifecycle • Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk

Agenda

12:40 — Cybersecurity ratings adoption: security performance management and third-party risk

James Warriner, EMEA Channel Sales Manager, BitSight Technologies

- What is driving the adoption of cybersecurity ratings?
- What is the latest information they are providing and how does this differ from other cybersecurity data?
- What are the advantages and challenges in using cybersecurity ratings?
- Use cases: How are cybersecurity ratings being deployed 'in the wild'?

13:00 Lunch and networking

14:00 — AI and machine learning: a cybersecurity silver-bullet?

David Stevenson, Head of Cyber Analytics Technology, Morgan Stanley

- How AI and ML can address today's cyber-challenges, including:
  - the cyber-skills gap
  - dealing with the information deluge
  - protecting the enterprise from cyber-threats
- Where and how ML can help, with examples
- Is AI and ML a cybersecurity silver bullet?
  - Challenging the perceptions of machine learning and cybersecurity
  - What are the inconvenient truths?

14:20 — AI in security operations: what we have learnt so far

Matt Walmsley, EMEA Director, Vectra

Time and talent are key factors in preventing a data breach. Learn from peers how AI enabled them to:

- Detect hidden threats in cloud and enterprise networks
- Perform conclusive incident investigations
- Respond at previously unattainable speed and efficacy

14:40 — Time-based vulnerability mitigation

Stephen Roostan, VP EMEA, Kenna Security

- IT risk and security risk are not the same! How do you get both sides engaged?
- How should success be measured? Number of vulnerabilities? Risk? Time?
- Can you drastically improve both effectiveness & efficiency?

15:00 — Cyber under arrest. The conflict between law enforcement and business. And what needs to change

Craig Potter, Detective Constable, Specialist Crime Division, Police Scotland

- How digitalisation, and in particular, cryptocurrencies are changing the fraud, AML and financial crime landscape and introducing new risks and challenges for law enforcement. International cryptocurrency case study
- Competing objectives between law enforcement and business. Small picture Ethics vs Big picture Ethics
- Reporting. Why does reporting remain a major frustration amongst law enforcement globally? Why is transparency such an issue, and what can be done to increase effective reporting and ensure the greatest value from reporting to law enforcement? Case studies

15:20 — Mobile devices are a much bigger security problem than traditional computers

Dino Constantinou, UK & Northern Europe Channel Director, Zimperium

- Mobile devices are an unprotected endpoint with access to or containing all of the information of a traditional endpoint
- The differences between Mobile Device Management (MDM) Enterprise Mobility Management (EMM) and Mobile Threat Defense (MTD)
- The different ways hackers are attacking your mobile device – network attack, phishing attacks, device attacks and app attacks
- How to protect businesses and government agencies from these mobile threats

15:40 Refreshments and networking

16:00 — EXECUTIVE PANEL DISCUSSION — Breaking the cyber-bank: lessons from the FS in cyber and fraud risk

Andrew Dillin, Threat Intelligence Lead, Cyber, RBS
Fiona Kelly, Information Security & Resilience Risk Manager, TSB
Mark Gale, Head of Global Fraud Risk Management, Citi
Tony Povoas, CISO, Aegon UK

- Three's not a crowd: examining the three lines of defence, and their stake in cyber-risk
- Biometrics and risk metrics: how digitalisation is changing, and aiding, fraud risk
- What are the main challenges facing one of the most highly regulated industries? And what can others learn from them?

16:20 — Information security culture: a never ending story

David Creighton-Offord, Senior Information Security Consultant, The University of Edinburgh

- Knowing what you have already, for better or worse: your audience, your infrastructure, your support network
- The challenge: inertia, excess momentum, change fatigue
- What you can do about it: knowing your audience, making security easier, streamlining and diversifying your message

16:40 — Audits and questionnaires: does scrutiny deliver security?

Damien Behan, IT Director, Brodies

- As customers manage their supply chain ever more closely, organisations are required to fill out ever lengthier questionnaires and submit to audits. But these are often blunt instruments that don't allow for nuance or compensating controls
- An industry has grown up around these compliance exercises, but is ticking boxes now more important than addressing risks? Is our effort going in the right area?
- Can we use audits and questionnaires to collaboratively improve what we do? Are we just trying to pass the test or to improve?
- What, if any, competitive advantage is there in a higher degree of compliance – i.e. once the required baseline is achieved, is there business sense in going above and beyond?

17:00 Conference close