Post event report

Strategic Sponsors

CROWDSTRIKE

e2e assure

KnowBe4
Human error. Conquered.

S-RM

tenable®

> “ The sessions were relevant and up to date regarding the challenges we currently face in cybersecurity within the higher education sector. I found it was worthwhile attending and will be registering for future events. ”
> **Deputy CISO, University of Edinburgh**

Inside this report:

Key themes

- Getting better at 'basic' cyber hygiene
- The importance of awareness
- Defending against the latest ransomware variants
- Upgrading Incident Response
- The role of threat intelligence in security
- Identity is essential

Who attended?

Cyber-security
We have a 20-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

Majid Ali, UK Public Sector CTO, CrowdStrike

Professor Eerke Boiten, Professor in Cybersecurity, Head of School of Computer Science and Informatics, De Montfort University

Olly Burnand, Senior Associate, Cybersecurity, S-RM

Dominic Carroll, Director of Portfolio, e2e-assure

Dr Chris Fullwood, Chartered Cyberpsychologist and Founding member, British Psychological Society's Cyberpsychology Section

Mike Groves, Director, Cybersecurity, S-RM

Gary Henderson, Director of IT, Millfield

Javvad Malik, Lead Security Awareness Advocate, KnowBe4

Bernard Montel, EMEA Technical Director and Security Strategist, Tenable

Garry Scobie, Deputy CISO, The University of Edinburgh

Hayden Taylor, Enterprise Regional Account Manager, KnowBe4

Claire Walden, Cybercrime Education and Partnership Coordinator, South East Regional Organised Crime Unit

Agenda	
09:25	Chairman's welcome
09:30	**Dark academia: Shining a light on cyber-attacks** **Garry Scobie,** Deputy CISO, The University of Edinburgh • Why is the education sector a prime target for cyber-attacks? • What are the main cyber-threats faced by academia? • How do we address the main challenges in achieving cyber-resilience? • What are the top three things we need to do right now to improve our security posture?
09:50	**Exploring the cyber-challenges facing the education sector** **Majid Ali,** UK Public Sector CTO, CrowdStrike • In an increasingly interconnected and digitalised world, the education sector continues to face an increased number of cyber-threats • From identity-based attacks through to data extortion, the risks to education institutes have never been greater • Join us to explore some of the key risks identified by JISC facing the education sector in the UK and as we shed light on what those who have been tasked with defending the education institutes can do to help mitigate the threat
10:05	**Cyber in schools: Doing the basics and preparing for the worst** **Gary Henderson,** Director of IT, Millfield • The context of cyber and schools, and increasing risks and limited budgets and resources • Doing the basics to reduce risk • Preparing for the worst • Taking a risk-based approach
10:25	**Cybersecurity and incident response** **Mike Groves,** Director, Cybersecurity, S-RM, and **Olly Burnand,** Senior Associate, Cybersecurity, S-RM S-RM specialists will share their experience helping universities across the UK and globally to prepare for, respond to, and recover from cyber-incidents. Our session will cover: • Stories from the front line – major cyber-incidents affecting universities that S-RM has responded to, and the lessons we have learned • Common pitfalls – why universities are particularly exposed to cyber-threats, and what they should be doing to address them • Simulation exercising – how to examine, test, and rehearse your responses to major cyber-attacks, and why exercising is so essential • Crisis communications – principles for protecting reputation in a worst-case scenario incident or data breach, with learnings from recent case studies
10:40	**Strengthening the weakest link: Psychological factors in cybersecurity behaviour in the educational context** **Dr Chris Fullwood,** Chartered Cyberpsychologist and Founding member, British Psychological Society's Cyberpsychology Section • Highlight various human factors (e.g., mood, attention, fatigue) which are known to impact on an individual's ability to carry out safe cybersecurity practices • Consider the role that enduring individual difference variables (e.g., personality, self-esteem) may play in increasing one's vulnerability to different types of cyber-threats • Evaluate the use of psychological principles as a toolkit to support managers with cybersecurity education

Agenda

11:00	**Tough lessons for education – How academic institutions can prevent rising cyber-attacks**
	Bernard Montel, EMEA Technical Director and Security Strategist, Tenable • 2023 Global Threat Landscape • What are the consequences when the education sector is under attack? • How can we reduce the exposure risk of the attack surface?
11.20	**A holistic cybersecurity maturity assessment framework for higher education institutions**
	Professor Eerke Boiten, Professor in Cybersecurity, Head of School of Computer Science and Informatics, De Montfort University • A capability maturity model for the specific context of cybersecurity in HEI • Security regulation, privacy regulation, and best practices • Self-assessment and auditing
11.40	**Proactive cyber-defence strategies for protecting student data and intellectual property**
	Dominic Carroll, Director of Portfolio, e2e-assure • The cyber-threat landscape in education • The limitations of traditional Security Operations Centres (SOCs) • The power of proactive attack disruption • Quick wins for enhancing cybersecurity in education
12:00	**Cyber Choices: Safeguarding against cybercrime**
	Claire Walden, Cybercrime Education and Partnership Coordinator, South East Regional Organised Crime Unit • Why do schools and school IT providers need to know about cybercrime? • What are the risks to young people? • Indicators of risk • The referral process • What the Cyber Choices team does
12:20	**Networking with the enemy: Understanding the psychology of social engineering**
	Javvad Malik, Lead Security Awareness Advocate, KnowBe4, and **Hayden Taylor,** Enterprise Regional Account Manager, KnowBe4 Social engineering is a growing threat in today's digital world, where attackers use psychological manipulation to gain access to sensitive information. This talk will explore the psychology behind social engineering, and discuss how attackers use deceptive tactics to gain trust and access. We will examine the various motives behind these attacks and the ways in which attackers use psychological techniques to gain access. We will also look at how to recognise and protect yourself from social engineering attacks, as well as how to create a culture of awareness and prevention in your organisation. By understanding the psychological elements of social engineering, we can better protect ourselves and our organisations from these threats. • Understanding the psychology behind social engineering and the tactics attackers use to gain trust and access • Knowing how to recognise and protect yourself and your organisation from social engineering attacks • Creating a culture of awareness and prevention in your organisation to protect against social engineering
12:40	Chairman's closing remarks