CHARITY FRAUD AND CYBERCRIME

Welcome

Charity fraud and cybercrime: Prevention and cure

SHOOSMITHS Innovation Broking

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Robert Nieri
Principal Associate

Robert.Nieri@shoosmiths.co.uk

Hannah Howard
Associate

Hannah.Howard@shoosmiths.co.uk

Matthew Howarth
Partner

Matthew.Howarth@shoosmiths.co.uk

Jonathan Taylor, Innovation Broking Director, London and Head of Charities and Care

jonathan.taylor@innovationbroking.com

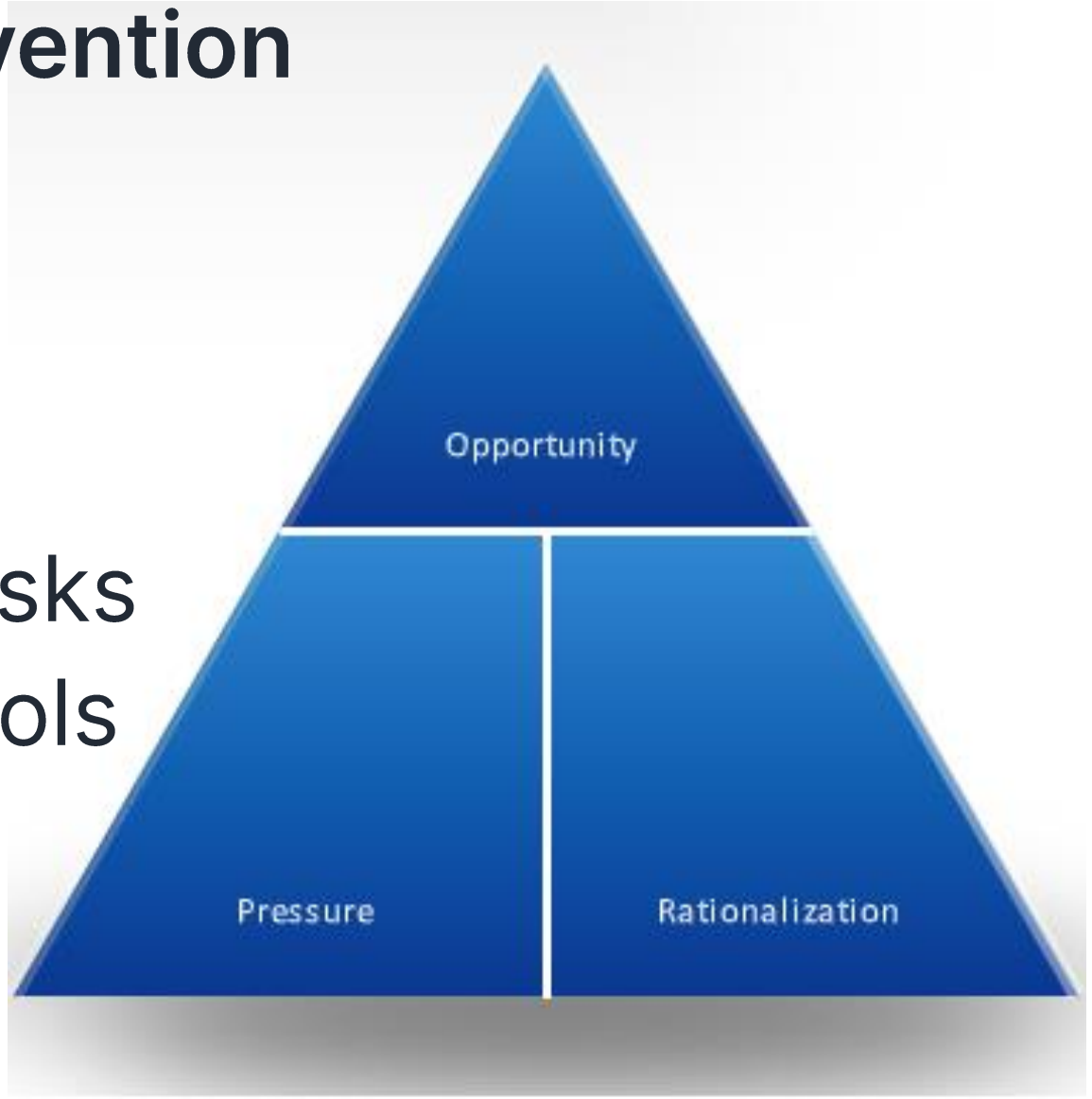
The duty of charity trustees (CC3)

Section 7: Manage your charity's resources responsibly

- You must act responsibly, reasonably and honestly. This is sometimes called the duty of prudence. You must avoid exposing the charity's assets, beneficiaries or reputation to undue risk.
- You and your co-trustees should manage risk responsibly. You have a duty to avoid exposing your charity to undue risk. This doesn't mean being risk averse. Risk management is the process of identifying and assessing risks, and deciding how to deal with them. (section 7.1)
- You and your co-trustees are responsible for your charity's money. Your charity should have effective processes for handling money, to help avoid poor decisions and accidental errors, as well as theft and fraud. Failure to do so is likely to result in a breach of your duty. You should protect the charity from financial crime such as theft or fraud. (section 7.5)

Prevention

- Better than cure
- Fraud Triangle
- Identify and Manage Risks
- Internal Financial Controls
- Culture
- Fraud Response Plan



Detection and Investigation

- Implement Fraud Response Plan
- Get Legal Advice
    - Investigation
    - Reporting
    - Liability
- Example

Hannah Howard
Associate
Hannah.Howard@shoosmiths.co.uk

Civil Recovery – Head or Heart

1. Consider what Primary Objective is – setting example, or recovery of funds
2. Recovery means investing time and funds to establishing what has happened
3. Investigatory – secure evidence, consider third party evidence, follow the money
4. Action- who and where is the target. Options include interim relief – freezing orders, search and seizure orders, asset tracing

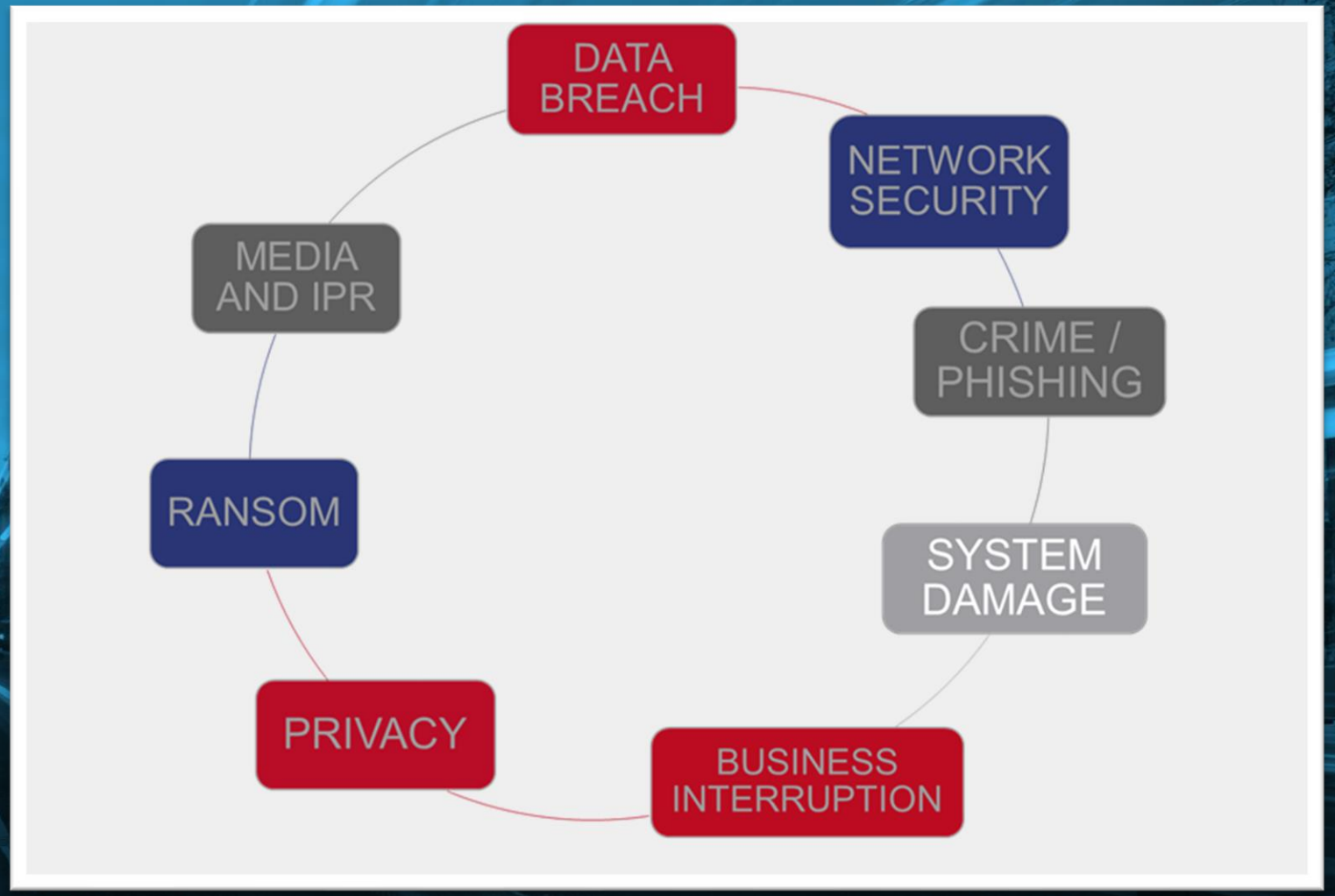
Matthew Howarth
Partner
Matthew.Howarth@shoosmiths.co.uk

Innovation Broking

Cyber Risk

Jonathan Taylor
Director, London and Head of Charities and Care
Innovation Broking

Cyber insurance



Cyber insurance

Cyber Incident Response		
	Incident Response Costs	£5,000,000 each and every claim, and overall, per sub section shown (unless shown otherwise)
	Legal & Regulatory Costs	
	Security & Forensics Costs	
	Crisis Communication Costs	
	Privacy Breach Management Costs	
	Third Party Privacy Breach Management Costs	£50,000/10% claim paid limit
	Post Breach Remediation Costs	
Cyber Crime		
	Funds Transfer Fraud	£250,000 each claim
	Theft of Funds Held in Escrow	£250,000 each claim
	Extortion	£5,000,000 each claim
	Corporate Identity Theft	£250,000 each claim
	Telephone Hacking	£250,000 each claim
	Push payment fraud	£50,000 each claim
	Unauthorized use of Computer resources	£250,000
System Damage & Business Interruption		
	System Damage & Rectification Costs	£5,000,000 each claim
	Direct Loss of Profit and increased costs of working 12 months indemnity	£5,000,000 each claim
	Additional increased cost of working	£100,000 each claim
	Dependent Business Interruption	£5,000,000 sub limited to £1,000,000 for system failure
	Consequential Reputational Harm 12 months indemnity	£5,000,000 each claim
	Claim preparation costs	£25,000 each claim
	Hardware replacement costs	£5,000,000 each claim
Network Security & Privacy		
	Network Security Limit	£5,000,000 each and every claim, and overall, per sub section shown (unless shown otherwise)
	Privacy Limit	
	Management Liability	
	Regulatory Fines	
	PCI Fines, Penalties and Assessments	
Media Liability and Technology errors and Omissions		**No cover provided as insured under another policy**
Excess applicable to Incident Response		No excess for incident response
Excess all other claims		£5,000 each claim

Control Risks

Friday 5 Mar 2021

core+ cyber

Cyber Espionage, Cyber Crime, Cyber

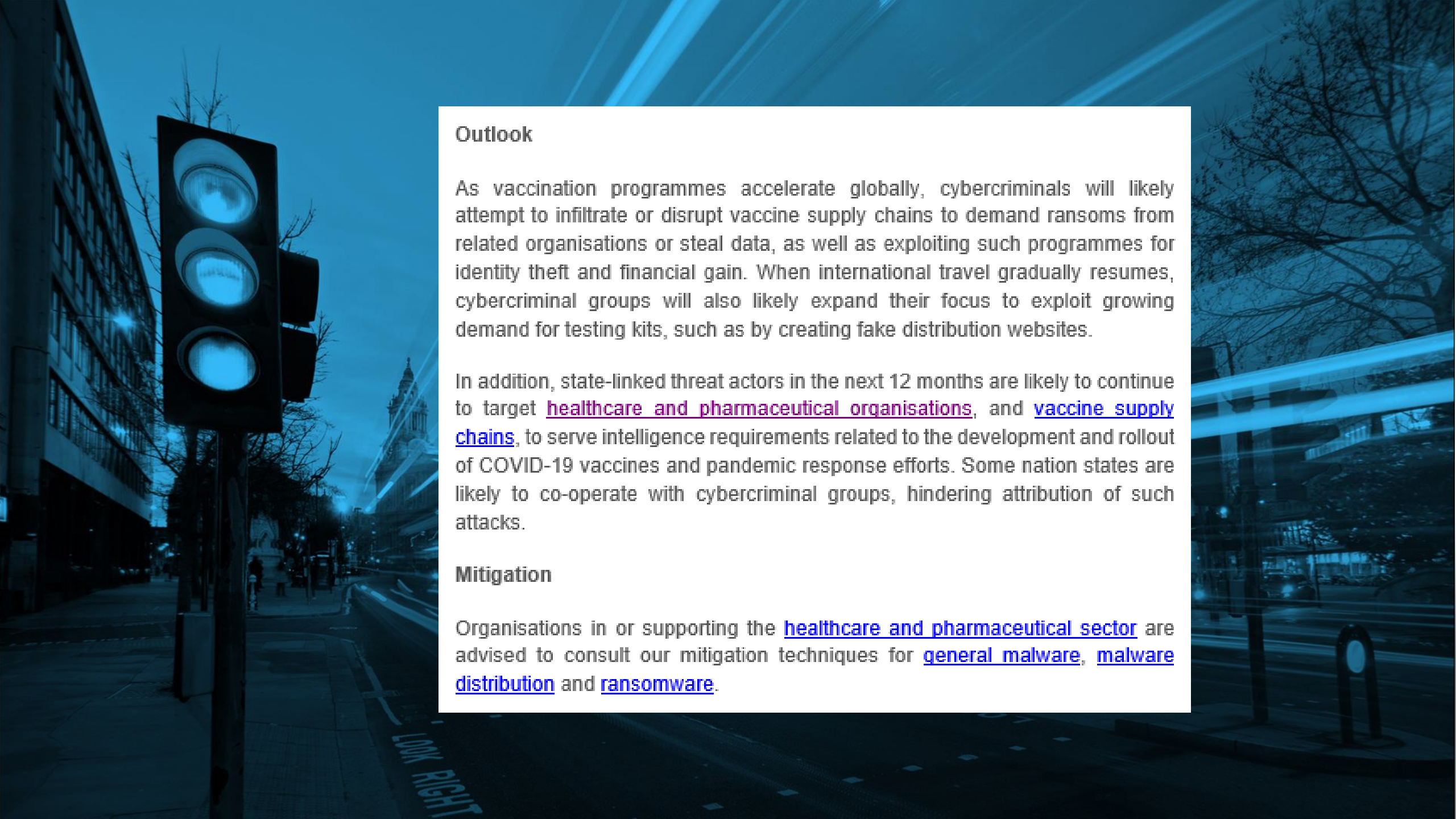
COVID-19: Attack on Oxford University lab reinforces high cyber threats to virus research

Severity: High **Sectors:** Pharmaceuticals medical supplies and health,Pharmaceuticals

Security researchers on 25 February reported that threat actors have compromised Oxford University's biomedical lab researching COVID-19.[1] According to the report, the breach took place in mid-February, when attackers left screenshots from inside the lab's network on a poorly secured server.

- An organised and capable cybercriminal group was likely behind the attack, seeking intelligence and intellectual property for financial gain. The attackers were likely seeking data to sell to, or on behalf of, a state actor.

- A range of cybercriminal groups are highly likely to continue to target organisations involved in COVID-19 research and vaccine development in the coming months. Such attacks will seek to steal data, extort ransoms or obtain intelligence to sell to third parties.



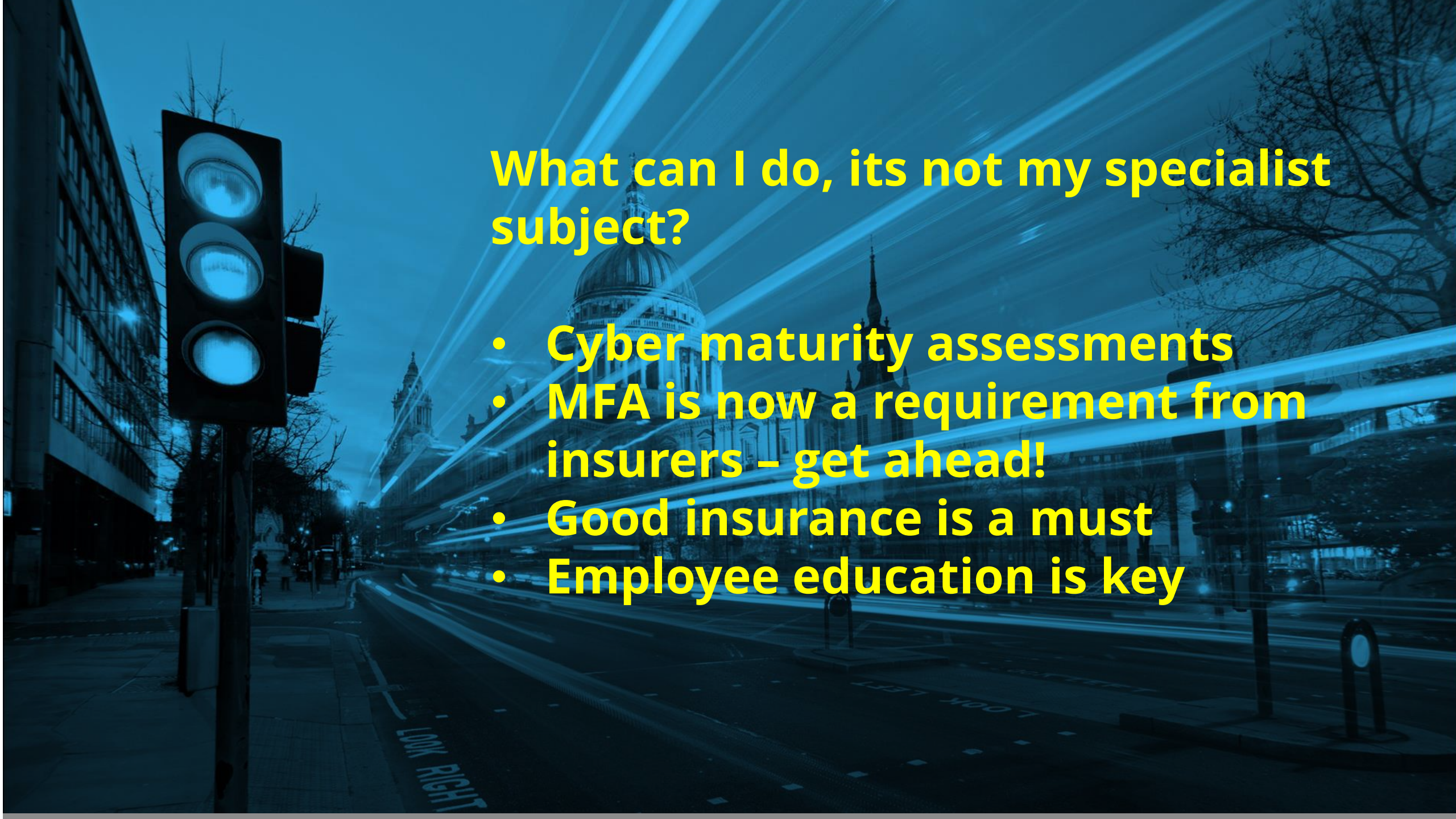
Outlook

As vaccination programmes accelerate globally, cybercriminals will likely attempt to infiltrate or disrupt vaccine supply chains to demand ransoms from related organisations or steal data, as well as exploiting such programmes for identity theft and financial gain. When international travel gradually resumes, cybercriminal groups will also likely expand their focus to exploit growing demand for testing kits, such as by creating fake distribution websites.

In addition, state-linked threat actors in the next 12 months are likely to continue to target healthcare and pharmaceutical organisations, and vaccine supply chains, to serve intelligence requirements related to the development and rollout of COVID-19 vaccines and pandemic response efforts. Some nation states are likely to co-operate with cybercriminal groups, hindering attribution of such attacks.

Mitigation

Organisations in or supporting the healthcare and pharmaceutical sector are advised to consult our mitigation techniques for general malware, malware distribution and ransomware.



What can I do, its not my specialist subject?

- Cyber maturity assessments
- MFA is now a requirement from insurers – get ahead!
- Good insurance is a must
- Employee education is key

Your hosts

Connect with your hosts on LinkedIn by scanning the QR codes below.

Robert Nieri
Principal Associate

Robert.Nieri@shoosmiths.co.uk

Hannah Howard
Associate

Hannah.Howard@shoosmiths.co.uk

Matthew Howarth
Partner

Matthew.Howarth@shoosmiths.co.uk

Jonathan Taylor, Innovation Broking Director, London and Head of Charities and Care

jonathan.taylor@innovationbroking.com