

Webinar

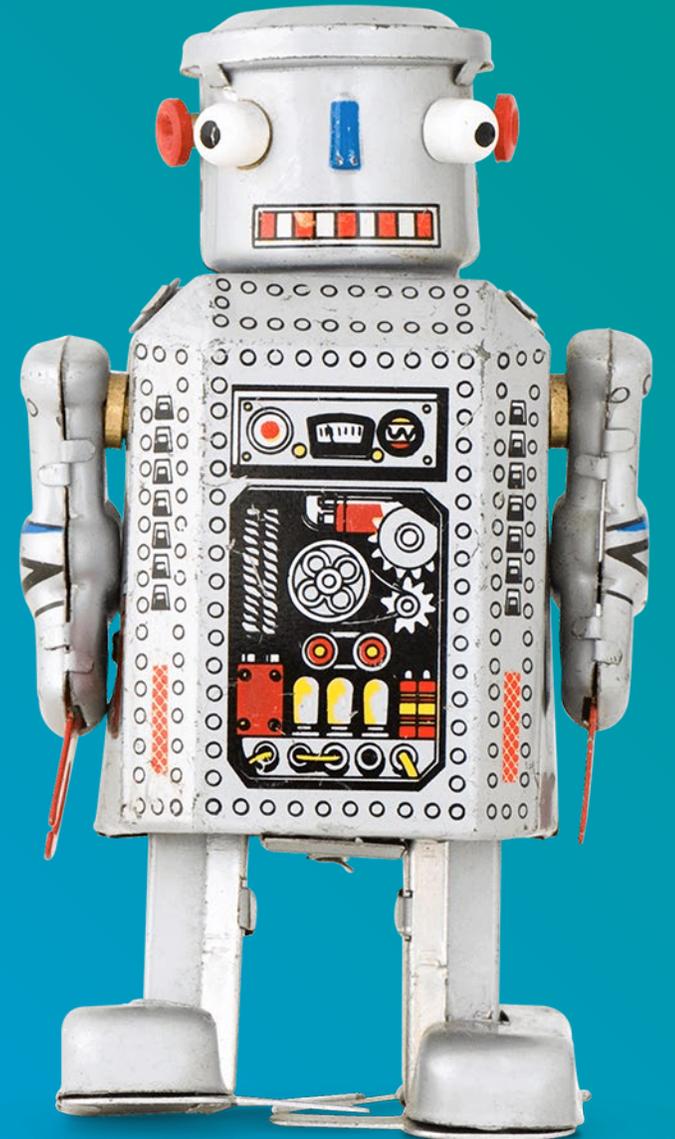
Managing Cyber Risk for pension Schemes

Marion de Voy – UK DB Governance Leader, Mercer

Cal McGuire – Vice President, Consulting Solutions, Marsh Advisory

30 September 2020

welcome to brighter



Agenda

1. Introductions
2. What is cyber risk?
3. Why is cyber risk important for pensions?
4. What should you do now?
5. Q&A

Introductions

Marion de Voy – UK DB Governance Leader, Mercer

Cal McGuire – Vice President, Consulting Solutions, Marsh Advisory

What is Cyber Risk?

What is cyber risk?



Cyber Event

Malicious attacks or accidental events impacting data, or resulting in a partial or total unavailability, or failure of computer networks, or technology.

Leading to:

Impact



Encrypted Data Security Breach Privacy Violations Regulatory Investigations Phishing /Fraud Bricked Computers Property Damage Property Damage Property Damage Bodily Injury

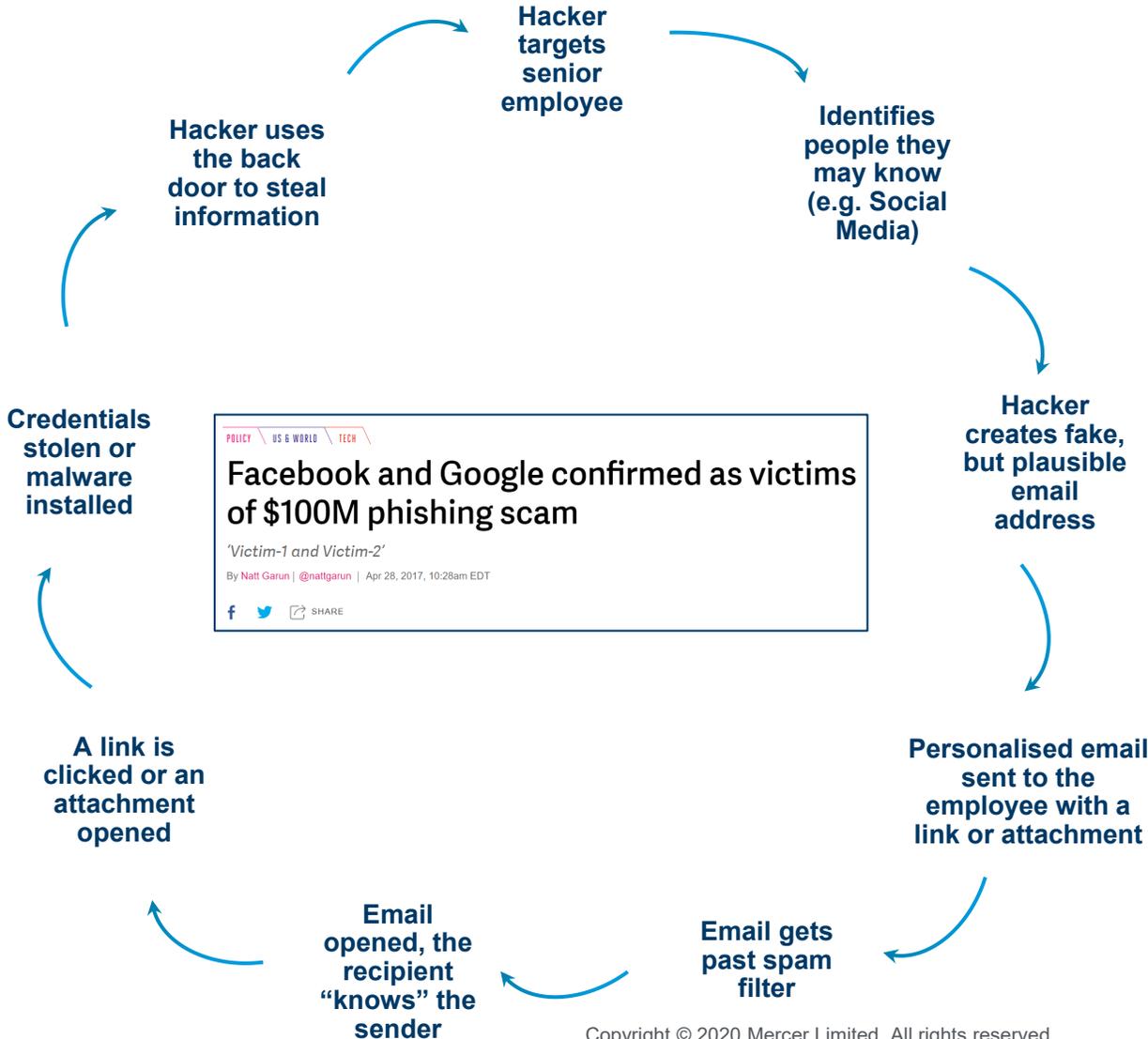
Leading to claims for:

Consequence



First-Party Costs Loss of Income Third-Party Liability Fines and Penalties Extortion Demands Negligence in Services Shareholder Litigation

Cyber risk in action: Phishing attack



Cyber risk in the last 12 months

Some examples



CYBER RISK MAY 19, 2020 / 12:21 PM / UPDATED 4 MONTHS AGO

Chinese hackers suspected of stealing details of 9 million easyJet customers

Hackers conned Norwegian investment fund out of \$10m through email scam

MAY 19, 2020

Technology

Coronavirus: Russian spies target Covid-19 vaccine research

By Chris Fox & Leo Kelion
Technology reporters, BBC News

Twitter hack: US and UK teens arrested over breach of celebrity accounts

Three men charged in hack that saw accounts of Barack Obama, Joe Biden and Elon Musk compromised in bitcoin scam

Microsoft: Russian state hackers are using IoT devices to breach enterprise networks

Microsoft said it detected Strontium (APT28) targeting VoIP phones, printers, and video decoders.

Saudi spies tracked phones using flaws the FCC failed to fix for years

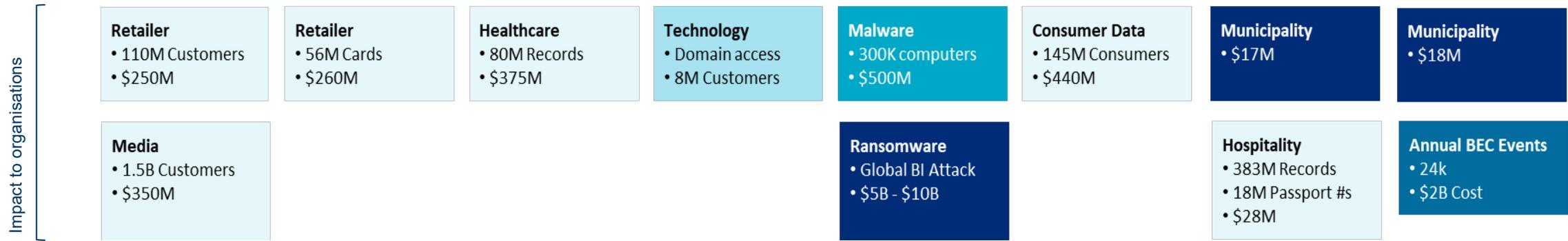
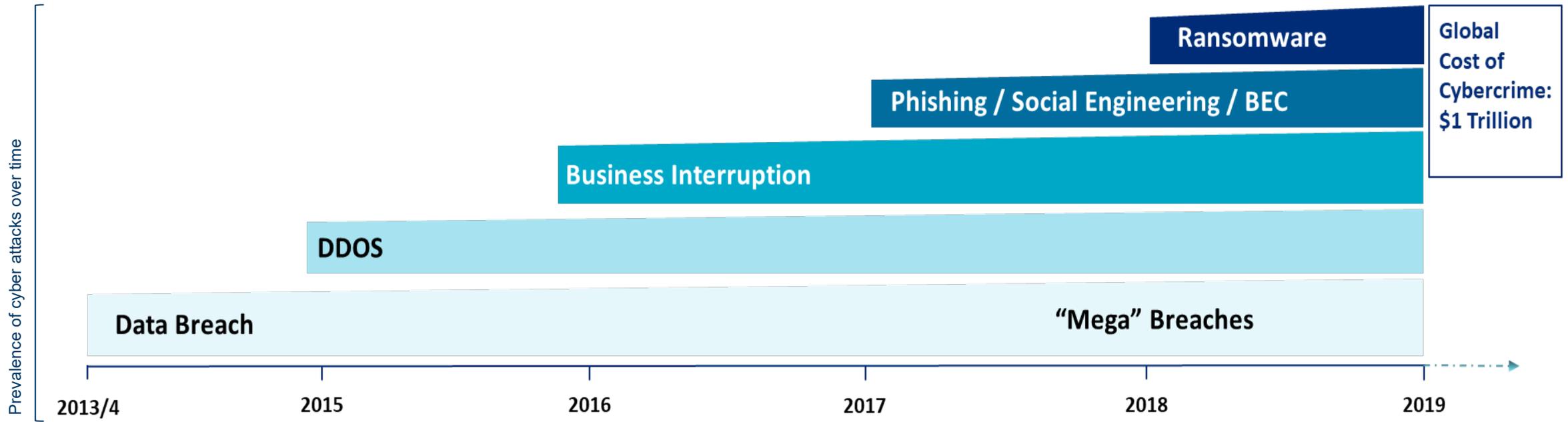
Zack Whittaker @zackwhittaker / 11:38 pm BST • March 29, 2020

Comment



Cyber threat landscape is dynamic and evolving

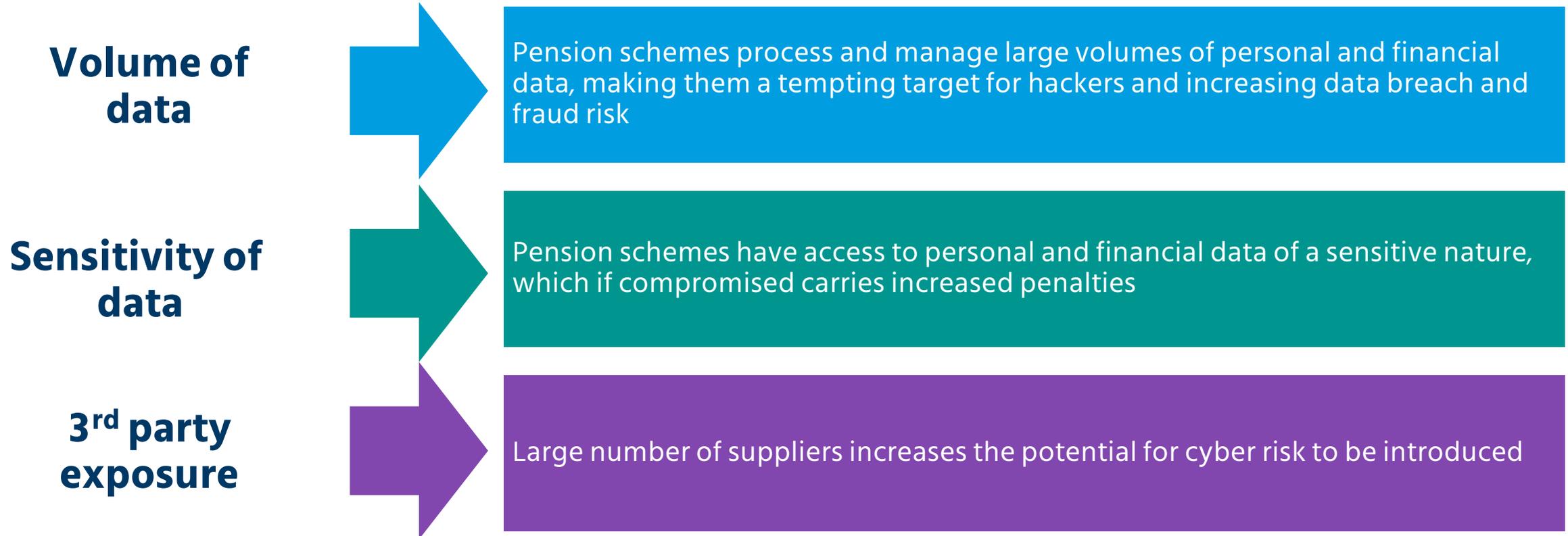
Over a 5 year period the impact and number of cyber attacks has increased



**Why is Cyber Risk important
for pensions?**



Pension schemes are particularly exposed to cyber risk



What is The Pensions Regulator's view?



The primary obligation of trustees is to act on behalf of scheme members and beneficiaries



A key element of this duty is to ensure that members, their benefits and scheme assets are not put at risk as a result of poor controls.



TPR expects trustees have a robust system of assessing, measuring and mitigating risk; cyber security is one element of the overall risk framework



Trustees are expected to take steps to build cyber resilience

- assess and minimise the risk of a cyber incident occurring, and
- Be able to recover when an incident takes place.

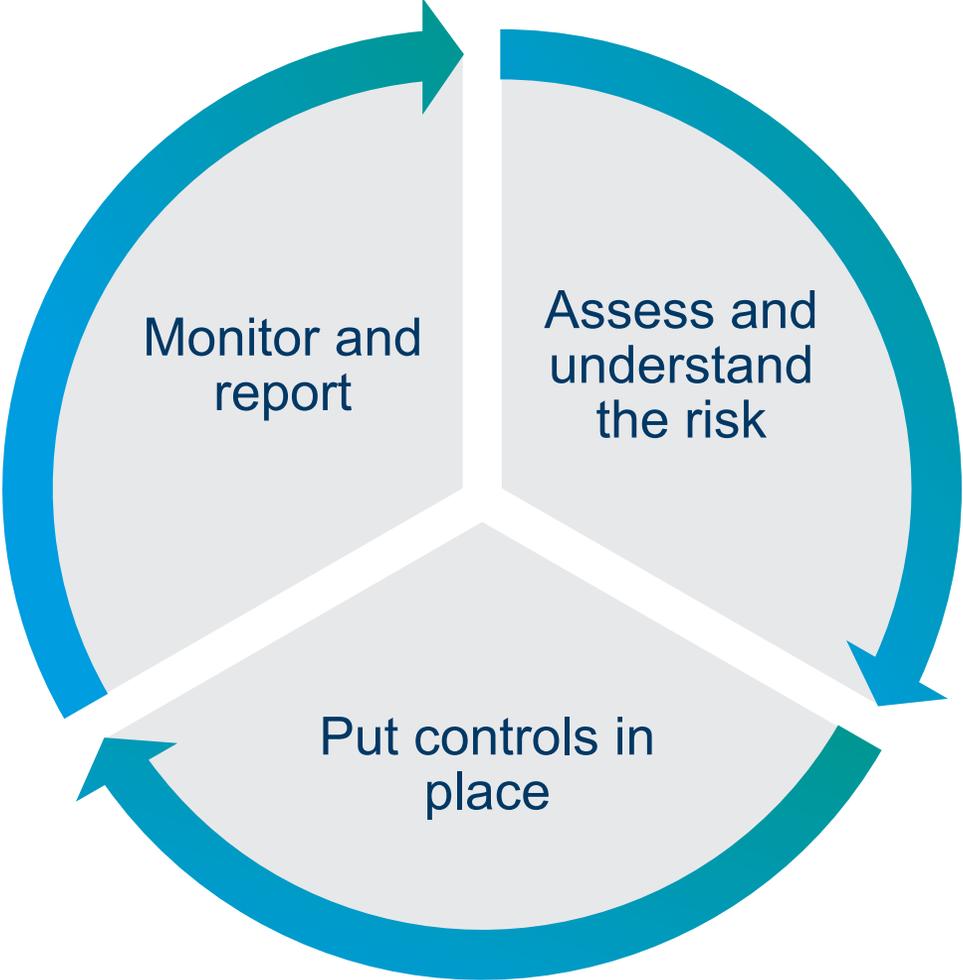


TPR's "Cyber Security Principles for Pension Schemes" (published April 2018) sets out the main principles

The Pensions Regulator advice – basic principles



The Pensions Regulator advice – basic principles



The role of the Information Commissioner and General Data Protection Regulation (GDPR)



Scheme trustees are data controllers for data protection purposes



TPR's "Cyber Security Principles" directs trustees to the Information Commissioner's guidance on IT security



The Information Commissioner has power to apply penalties where GDPR is breached (up to 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher)



After 31 December 2020 (the end of the transition period) –

- the Government has stated its intention to bring GDPR into UK law after the end of the transition period
- there may be further developments and trustees should ensure they are aware of changes that may affect their scheme

What should you do now?

Practical steps

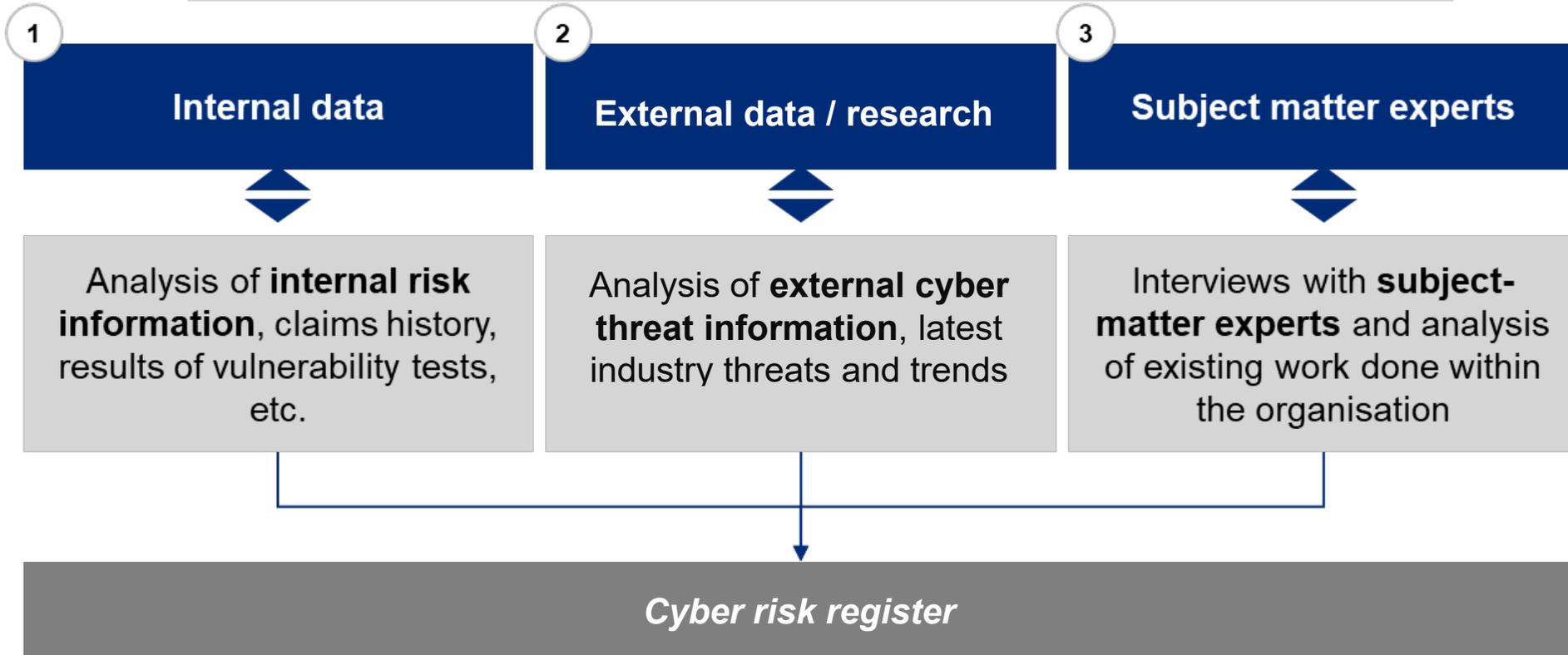
Identify cyber risks

Assess and understand the risk

Put controls in place

Monitor and report

Sources of information used to identify risk scenarios



Practical steps

Identify cyber risks

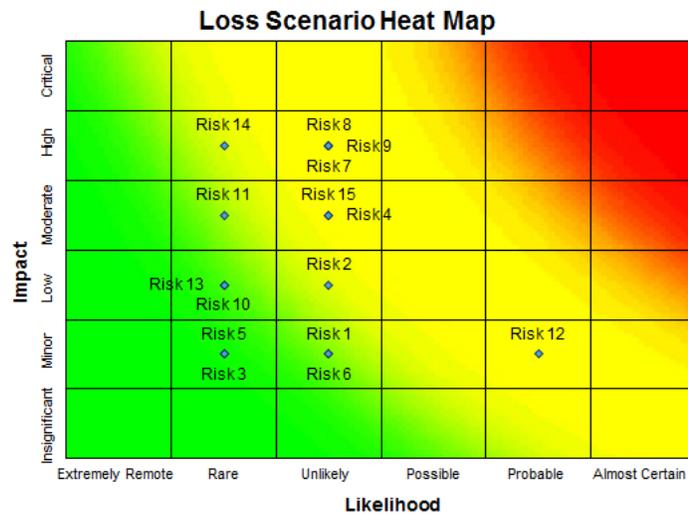
Assess and understand the risk

Put controls in place

Monitor and report

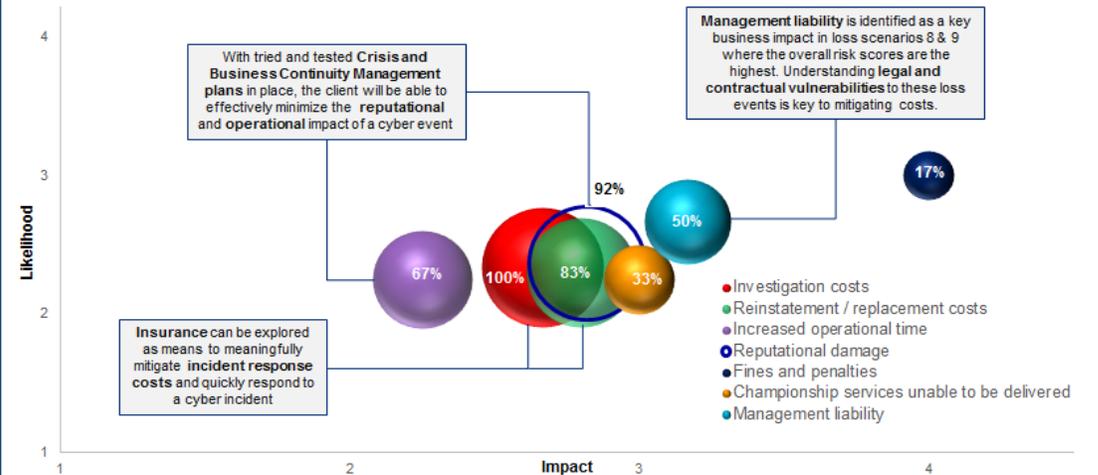
Cyber risk register

- The heat map below displays your loss scenarios plotted by **risk score** (impact x likelihood)
- Risks which are closest to the **top right hand corner** of the chart have the highest risk score



Service interruption/degradation	
1	Approved change applied to the office live environment
2	Approved change applied to manufacturing live environment
3	A DDoS attack
4	SAP outage
5	Outage of other global commercial support systems
6	Phishing attack
7	Manipulation of the manufacturing process
8	Outdated operational technology in manufacturing environment
Data breach	
9	Theft of employee data
10	Theft of customer data
11	Theft of IP/R&D data
12	Accidental leak of confidential data
13	Theft of commercially sensitive strategic management information
Fraud	
14	A successful ransomware attack
Misrepresentation	
15	Online entity targets you via social media

- Investigation costs
- Reputational damage
- Reinstatement/replacement costs
- Management liability
- Increased operational time



Practical steps

The Cyber Risk Register

Assess and understand the risk

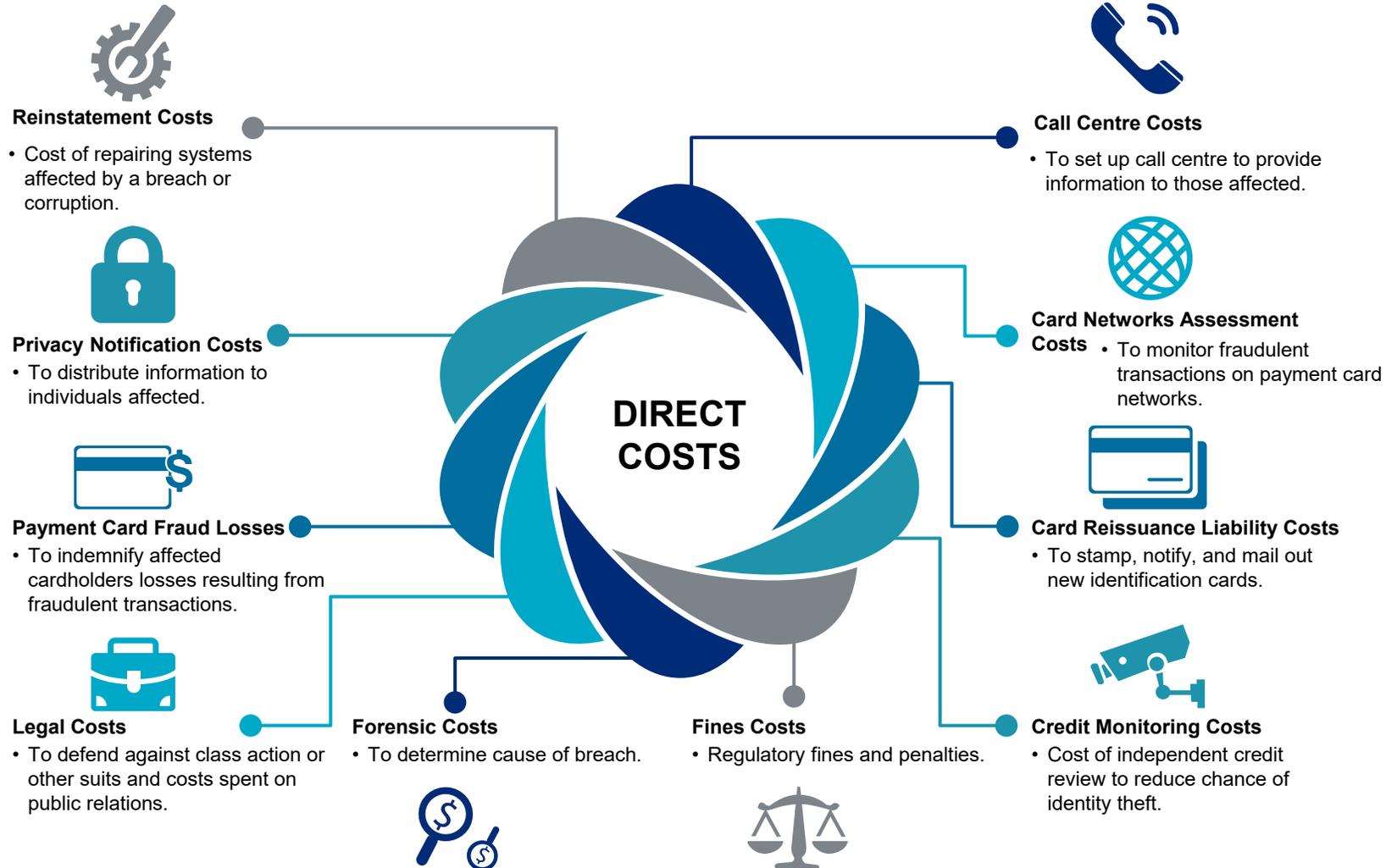
Put controls in place

Monitor and report

Event categories	Potential risk scenarios	Impact types			
		Financial	Operational	Reputational	Regulatory
Data breach	Breach of member personal data, leading to phishing attacks against members, identity theft or selling data on dark web	✓	✓	✓	✓
Service Interruption/ Degradation	Interruption of key systems / services compromising payment of benefits	✓	✓	✓	
	Ransomware attack leading to a cyber extortion to release key systems and data	✓	✓	✓	
Fraud	Compromise of trustee banking information, leading to diverted funds	✓	✓	✓	✓
	Fraudulent instructions given to investment managers, leading to diverted funds	✓	✓	✓	
	Fraudulent transfer of member benefits to alternate arrangement / scam	✓	✓	✓	✓

Practical steps

Quantifying Financial Impact



Practical steps

Quantifying Financial Impact

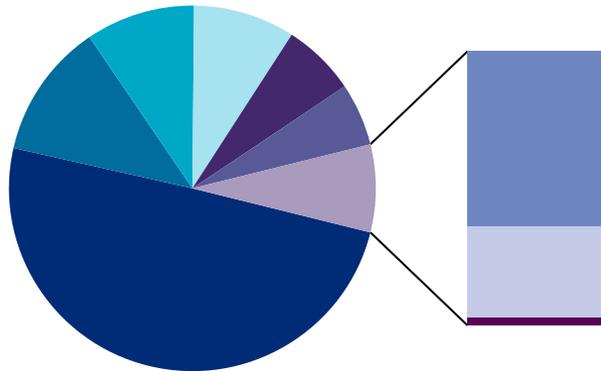


No. of records:

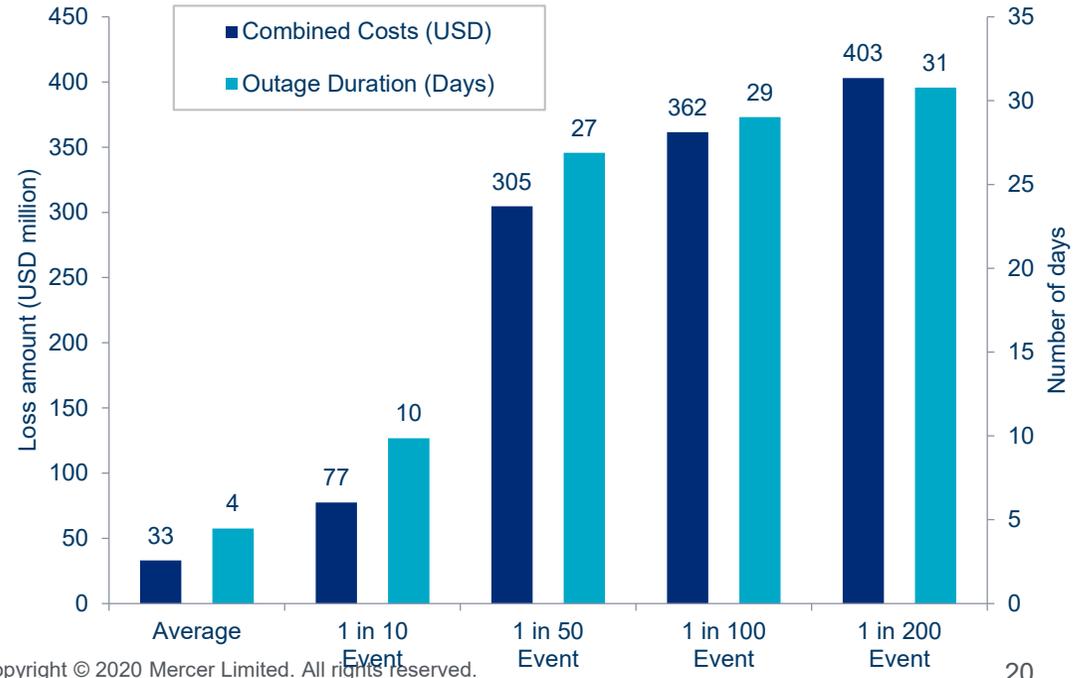
Personally Identifiable Information (PII)	80,000,000
Protected Health Information (PHI)	157,000,000

	Revenue Loss (USD)				
	Average	1 in 10 Event (10% Chance)	1 in 50 Event (2% Chance)	1 in 100 Event (1% Chance)	1 in 200 Event (0.5% Chance)
Duration (Days)	4	10	27	29	31
10% Revenue Network-Reliant	856,000	2,217,000	6,011,000	6,469,000	13,784,000
50% Revenue Network-Reliant	3,175,000	8,446,000	22,447,000	24,214,000	63,763,000
90% Revenue Network-Reliant	5,713,000	14,483,000	37,581,000	40,532,000	120,944,000

Cost Breakdown



- Credit Monitoring Costs (49.6%)
- Privacy Notification Costs (12.0%)
- Forensic Costs (9.6%)
- Fines Costs (9.0%)
- Reinstatement Costs (6.5%)
- Legal Costs (5.5%)
- Ransom Costs (5.0%)
- Revenue Loss (2.6%)
- Call Centre Costs (0.2%)

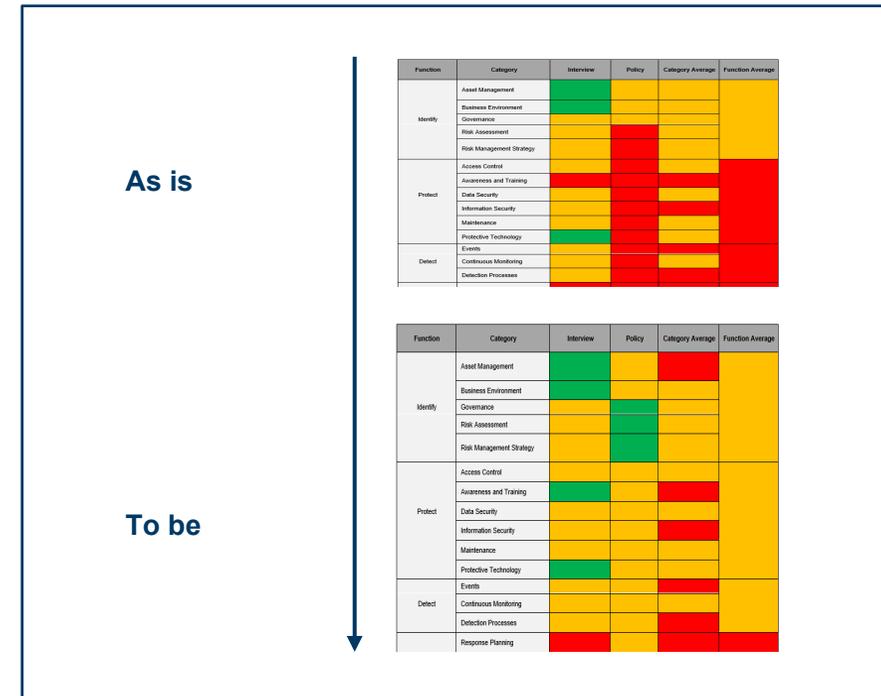
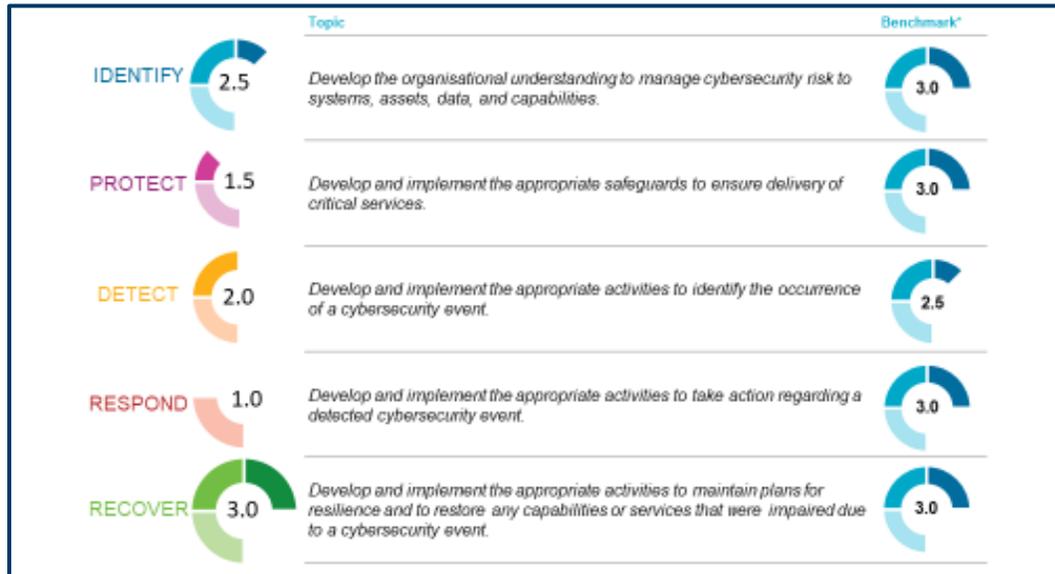


Practical steps

Controls assessment and improvement

Assess the current maturity of your controls against your cyber risks

Create a forward looking improvement plan to enhance controls linked to cyber risks



Practical steps

Continuous review and improvement

Incident response plans and simulations

Crisis Management Team Structure, Escalation and Communication

Immediate escalation

- Industrial incident, safety or site access issues - **IMMEDIATE** call to 24/7 Security Desk on 333 Internal or 444 (0)1933 808333
- Off-site out of hours emergency - call to 24/7 Security Desk on +44 01933 808333 to escalate
- Incidents resulting in broader business impacts (e.g. supply chain, programme delay): notify relevant HEAD of Function / Director

Establish incident severity: Use guide to help decide involvement of wider crisis structure

Minor	Serious	Crisis
Minor injury to onsite personnel Minor disruption to production, recoverable within 1 day Minimal damage to critical assets/facilities addressed through normal maintenance Minor media interest Financial costs recoverable within normal course of business	Major injury to onsite personnel Loss of production/ asset/ facility for 3 days Some media interest and / or social media coverage Notable financial impact on business requiring additional financial planning/provisioning	Serious injury to onsite personnel Loss of full production/ critical asset/ facility for >3 days Major sustained media coverage Substantial and potentially irrecoverable financial impacts
Manage as BAU Notify a member of Crisis Team	Escalate to Business Recovery Team Notify a member of Crisis Team	Trigger full Crisis Response structure

External Communication

- All external communications are to be coordinated by the Dr. Comms
- No staff should talk to the media, comment online or make announcements about a crisis or incident unless directed by the Dr. Comms

Internal Communication

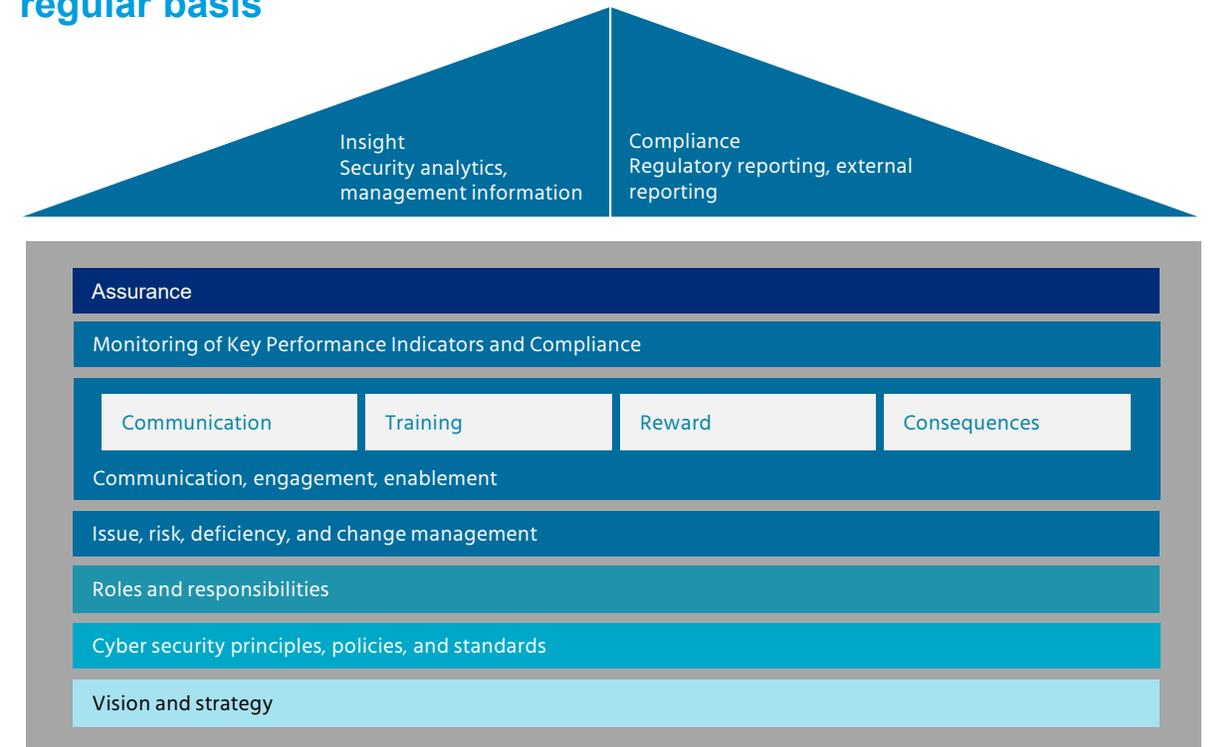
- Internal communications to staff managed jointly by Dr. Comms and HR Head
- IN HOURS:** between 0800 & 1715 hours, Monday to Thursday and 0800 & 1215 Friday using email, PA announcements, verbal briefing cascades
- OUT OF HOURS:** Via the Group Lotus Emergency Staff Communications Website **site address**

Team Structure

- The table sets out the team structure to coordinate a crisis response.
- Additional membership may be required depending on incident type, details are included in the procedures that follow.

Team	Objectives	Members	Meetings
Crisis Management Team	Strategic coordination and leadership for crisis event that has the potential to lead to a significant impact on Group Lotus	Core membership: - CEO - CFO - CEO, Dir. Ops - HR Head & Dir. Engineering (local staff who can react via quick) - Dr. Comms Additional members based on business impact	First meeting via Crisis Team Conference Line XYZ Further meetings to be held at XYZ
Business Recovery Team	Tactical coordination to the recovery of the business, directing resources and recovery tasks to enable a timely resumption of Group Lotus activities	Relevant Heads of Function - dependent upon scenario but may include manufacturing leads, HR, distribution / sales facilities, H&S	First meeting via Recovery Team Conference Line XYZ Further meetings to be held at XYZ
Incident Response Team	Immediate response to an incident, delivering immediate response and recovery tasks to reduce safety risks and disruption effects	Various operational staff including security, H&S, Fire Marshalls, Plant services and first aiders	Meet at/ close to scene or at Security Desk (depending on incident)

Trustee level Governance, KPIs and reporting, reviewed on a regular basis



Next steps

Next Steps

- Understand TPR principles and how they apply to you
- Review risk register
- Establish/review/implement appropriate controls
- Trustee training
- External review as a good option

Q&A

Important Notices

References to Mercer shall be construed to include Mercer LLC and/or its associated companies.

© 2020 Mercer LLC. All rights reserved.

This document contains confidential and proprietary information of Mercer and is intended for the exclusive use of the parties to whom it was provided by Mercer. Its content may not be modified, sold or otherwise provided, in whole or in part, to any other person or entity, without Mercer's prior written permission.

The findings, and/or opinions expressed herein are the intellectual property of Mercer and are subject to change without notice.

Information contained herein has been obtained from a range of third party sources. While the information is believed to be reliable, Mercer has not sought to verify it independently. As such, Mercer makes no representations or warranties as to the accuracy of the information presented and takes no responsibility or liability (including for indirect, consequential or incidental damages), for any error, omission or inaccuracy in the data supplied by any third party.

This document is provided for information purposes only and does not contain regulated investment advice or legal advice in respect of actions you should take. No decisions should be made based on this document without obtaining prior specific, professional advice relating to your own circumstances.

For Mercer's conflict of interest disclosures, contact your Mercer representative or see www.mercer.com/conflictsofinterest.

Issued in the United Kingdom by Mercer Limited which is authorised and regulated by the Financial Conduct Authority. Registered in England No. 984275. Registered Office: 1 Tower Place West, London, EC3R 5BU

welcome to

brighter

