MERCER | MARSH

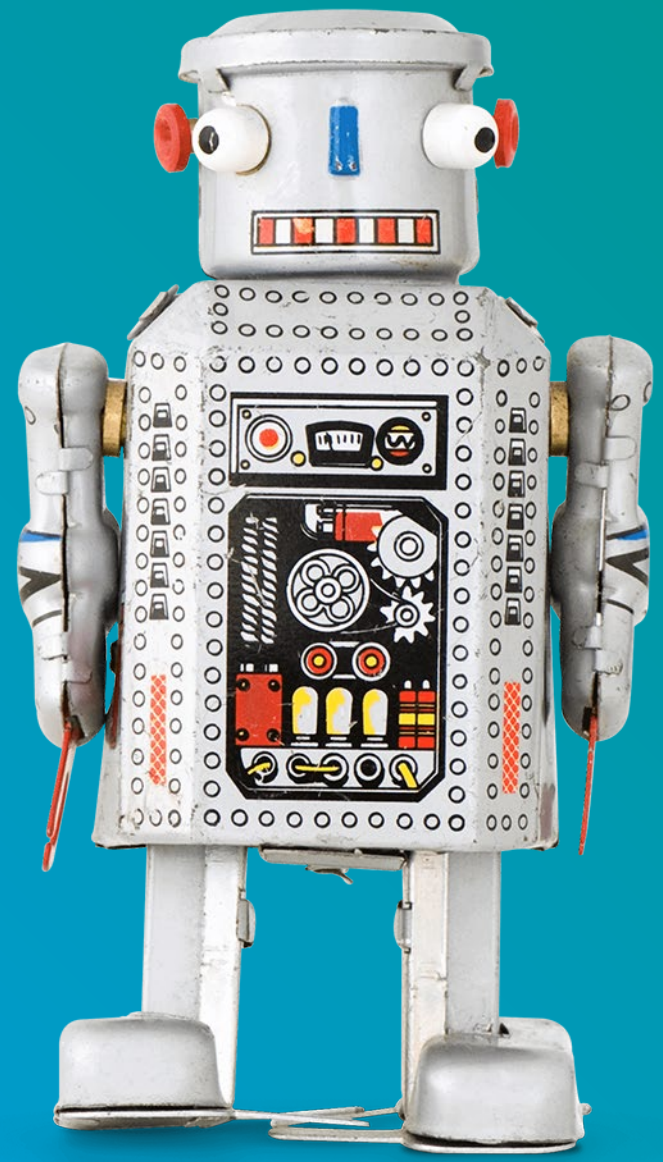
Webinar

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

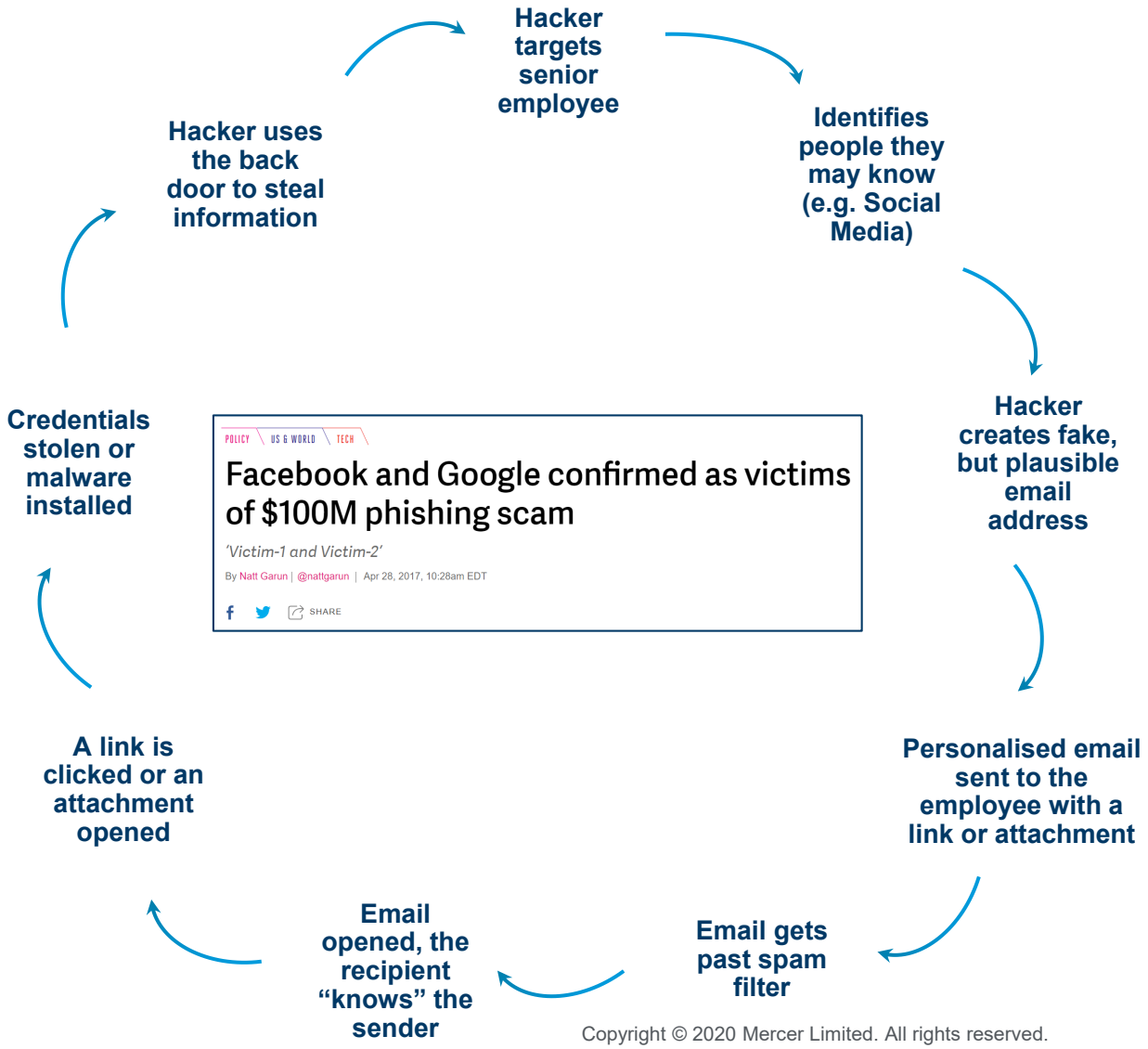
Leading to claims for:

Consequence

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

MERCER

Cyber risk in action: Phishing attack



MERCER

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

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

Technology

Coronavirus: Russian spies target Covid-19 vaccine research

By Chris Fox & Leo Kelion
Technology reporters, BBC News

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.

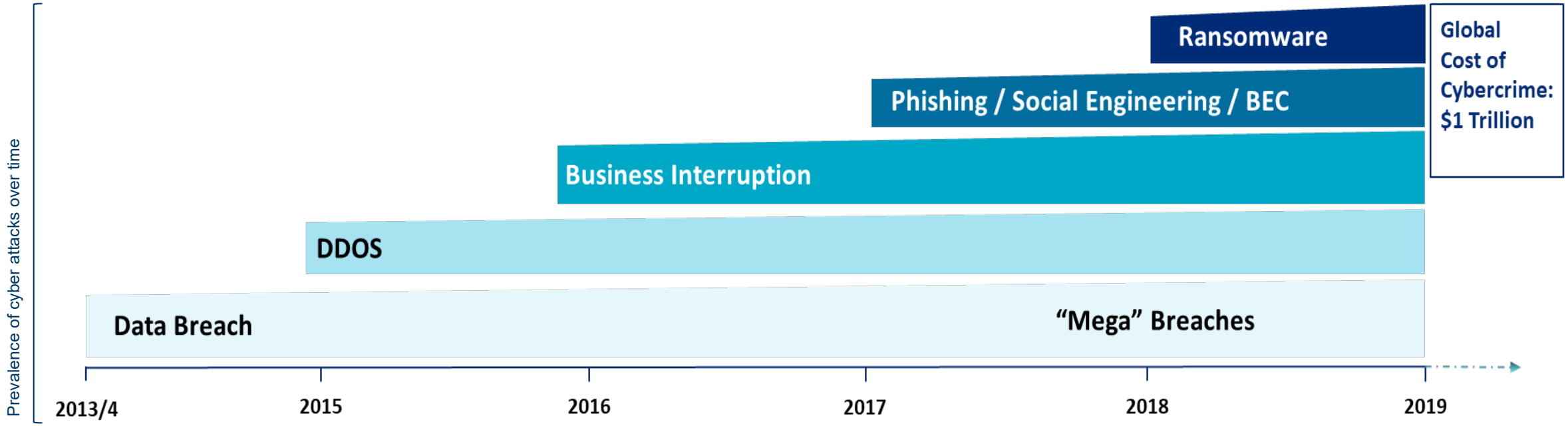
Saudi spies tracked phones using flaws the FCC failed to fix for years

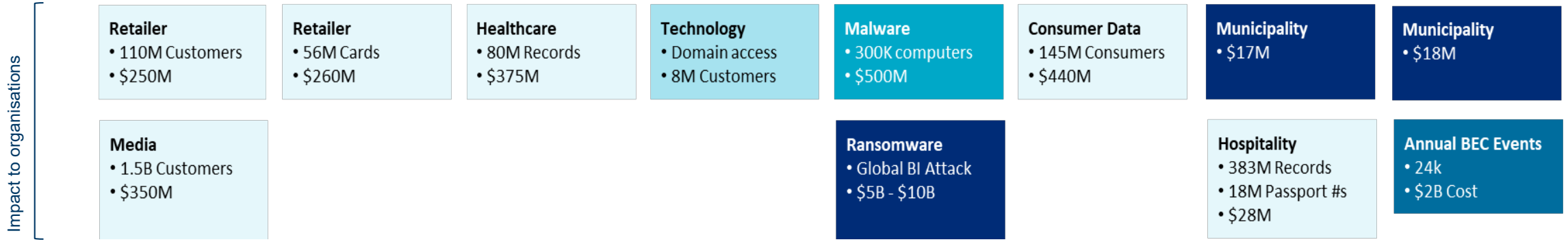
Zack Whittaker @zackwhittaker / 11:38 pm BST • March 29, 2020 Comment

MERCER

Cyber threat landscape is dynamic and evolving

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





MERCER

Why is Cyber Risk important for pensions?

Pension schemes are particularly exposed to cyber risk

Volume of data

Pension schemes process and manage large volumes of personal and financial data, making them a tempting target for hackers and increasing data breach and fraud risk

Sensitivity of data

Pension schemes have access to personal and financial data of a sensitive nature, which if compromised carries increased penalties

3rd party exposure

Large number of suppliers increases the potential for cyber risk to be introduced

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

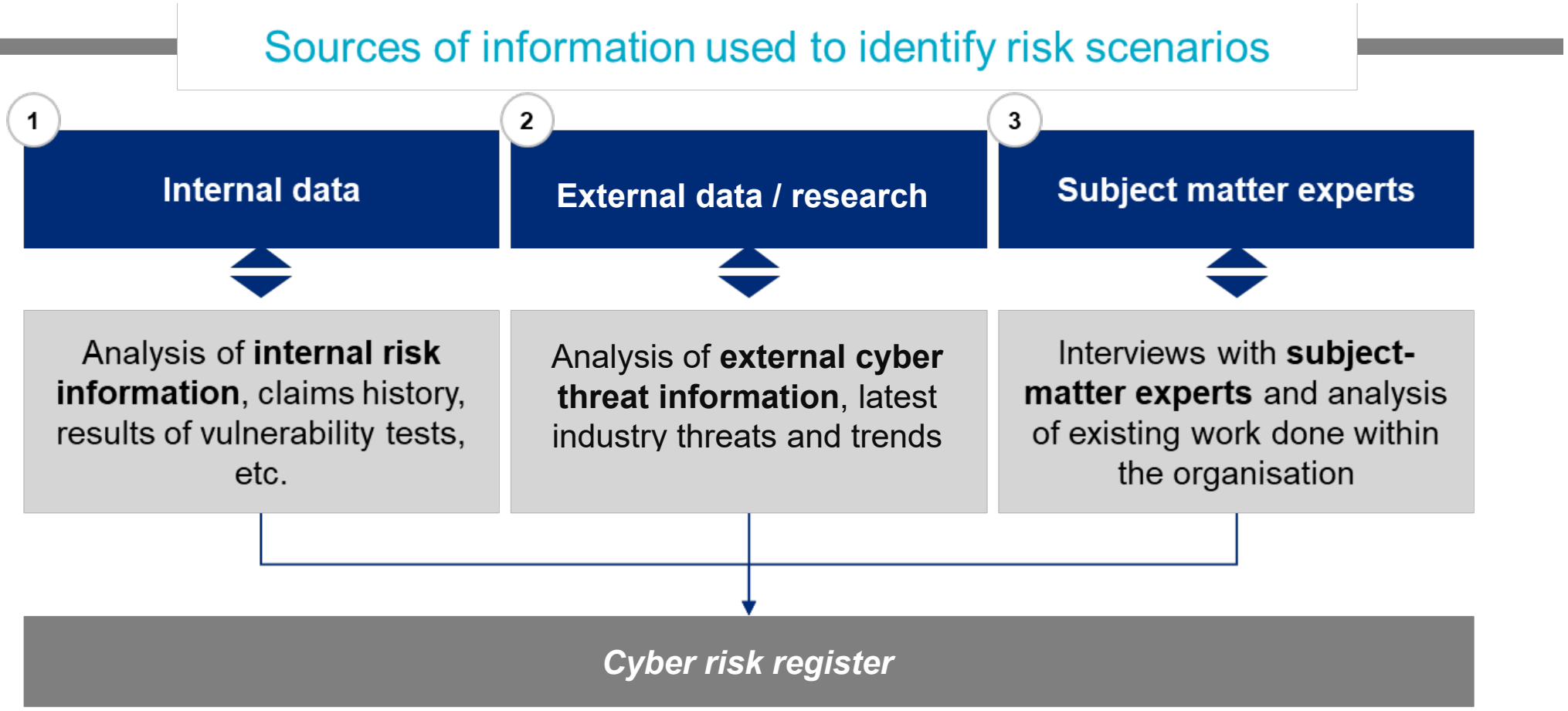
The Information Commissioner has power to apply penalties where GDPR is breached (up to 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher)

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?

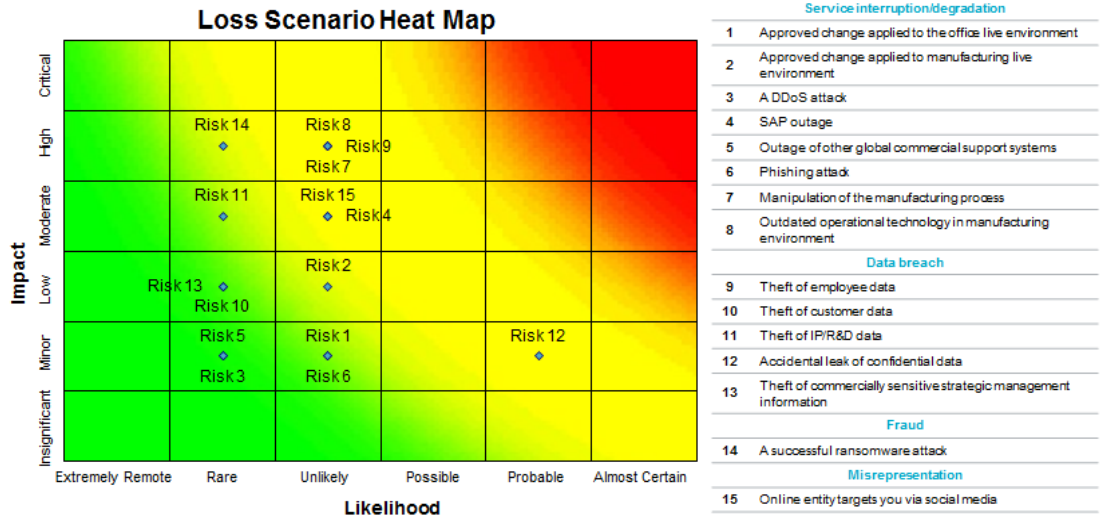
Practical steps
Identify cyber risks



Practical steps
Identify cyber risks

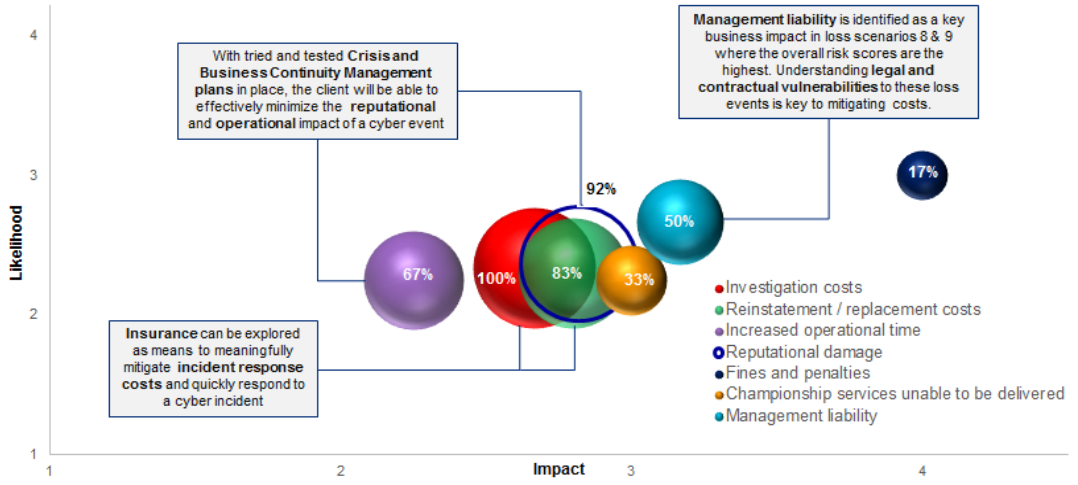
Cyber risk register

- 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

1. **Investigation costs**
2. **Reputational damage**
3. **Reinstatement/replacement costs**
4. **Management liability**
5. **Increased operational time**

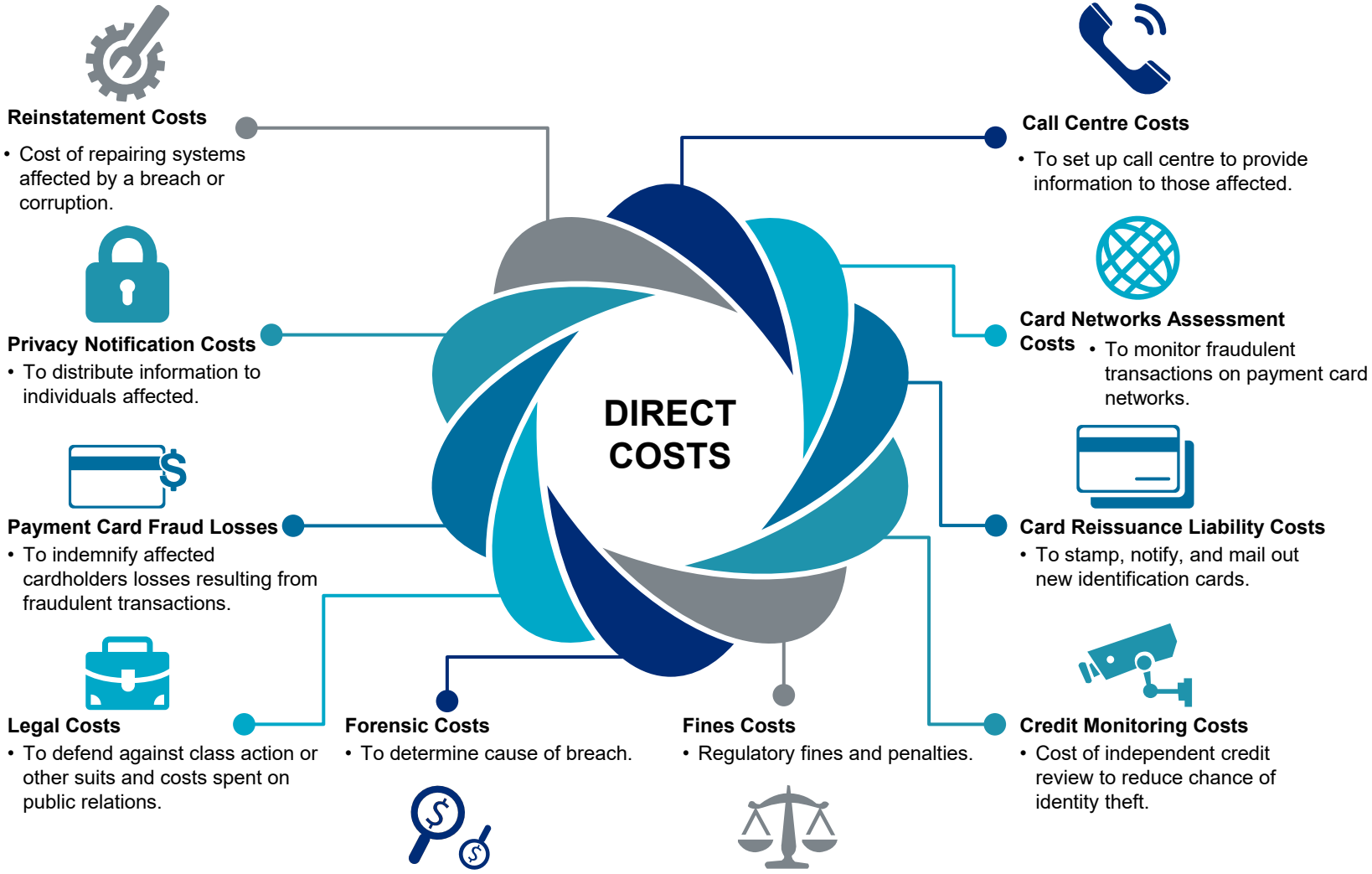


Practical steps
The Cyber Risk Register

Assess and understand the risk | Put controls in place | Monitor and report

		Impact types			
Event categories	**Potential risk scenarios**	**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

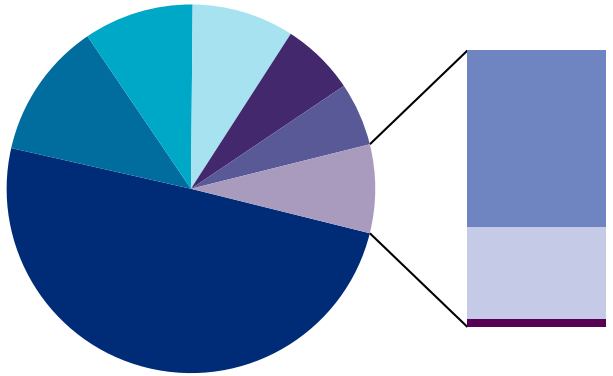
Assess and understand the risk | Put controls in place | Monitor and report

No. of records:

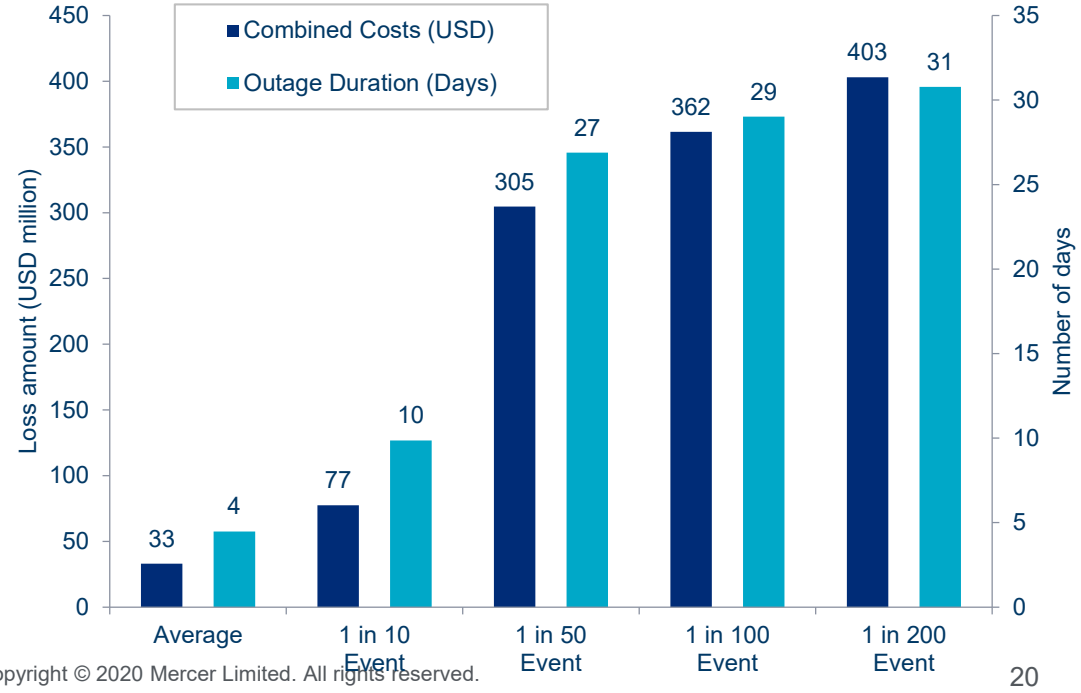
Personally Identifiable Information (PII)	80,000,000
Protected Health Information (PHI)	157,000,000

	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



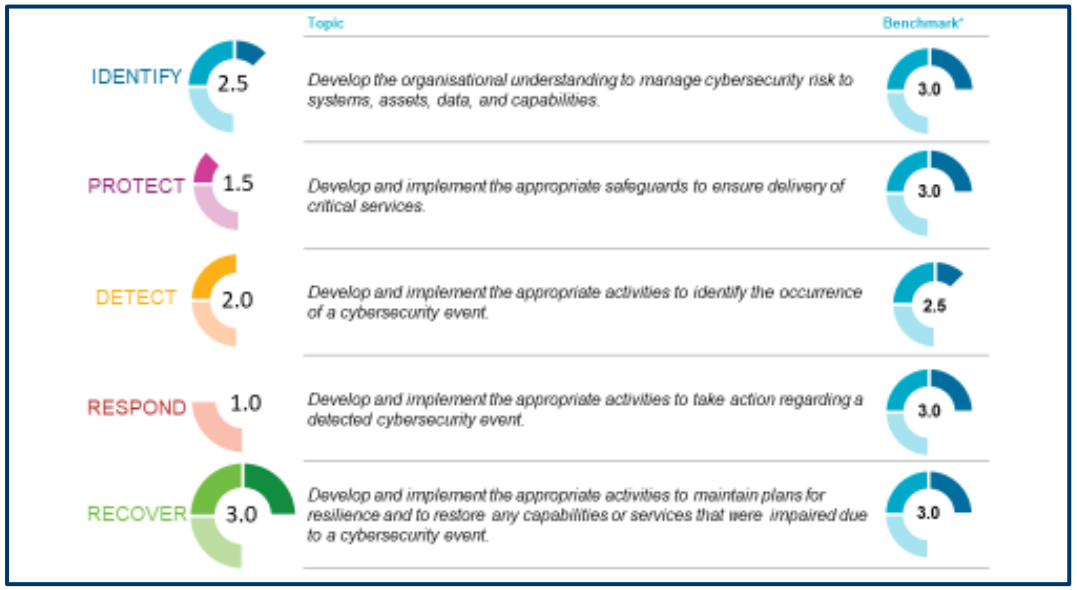
- Credit Monitoring Costs (49.6%)
- Privacy Notification Costs (12.0%)
- Forensic Costs (9.6%)
- Fines Costs (9.0%)
- Reinstatement Costs (6.5%)
- Legal Costs (5.5%)
- Ransom Costs (5.0%)
- Revenue Loss (2.6%)
- Call Centre Costs (0.2%)



MERCER

Practical steps
Controls assessment and improvement

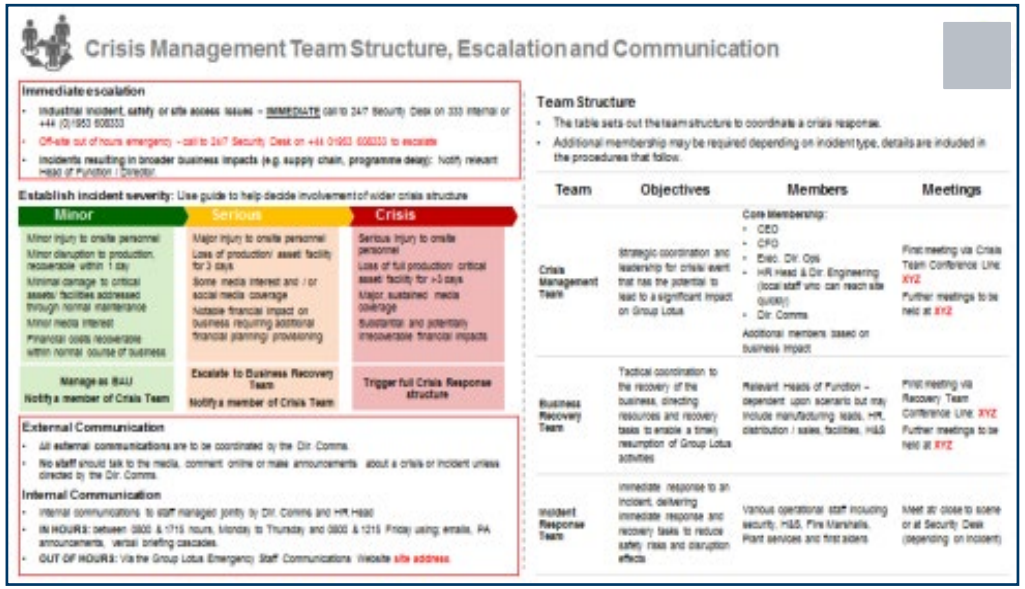
Assess the current maturity of your controls against your cyber risks



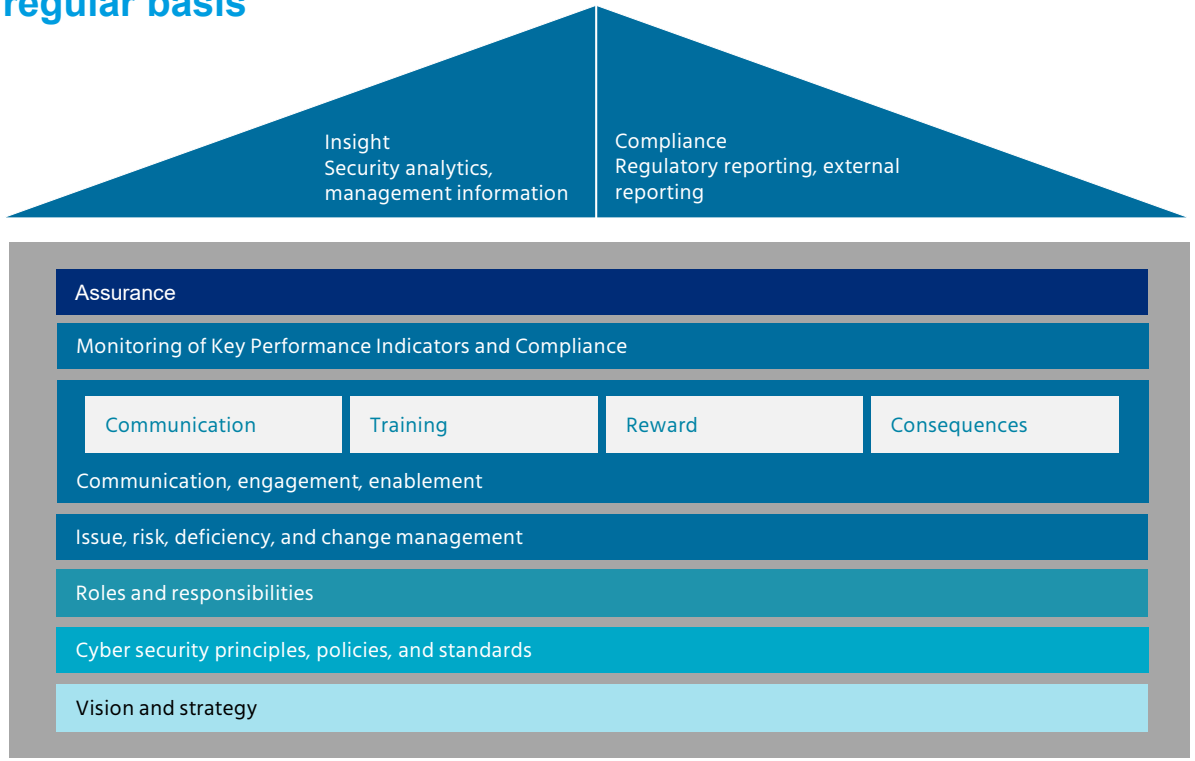
Create a forward looking improvement plan to enhance controls linked to cyber risks

Practical steps
Continuous review and improvement

Incident response plans and simulations



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.

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