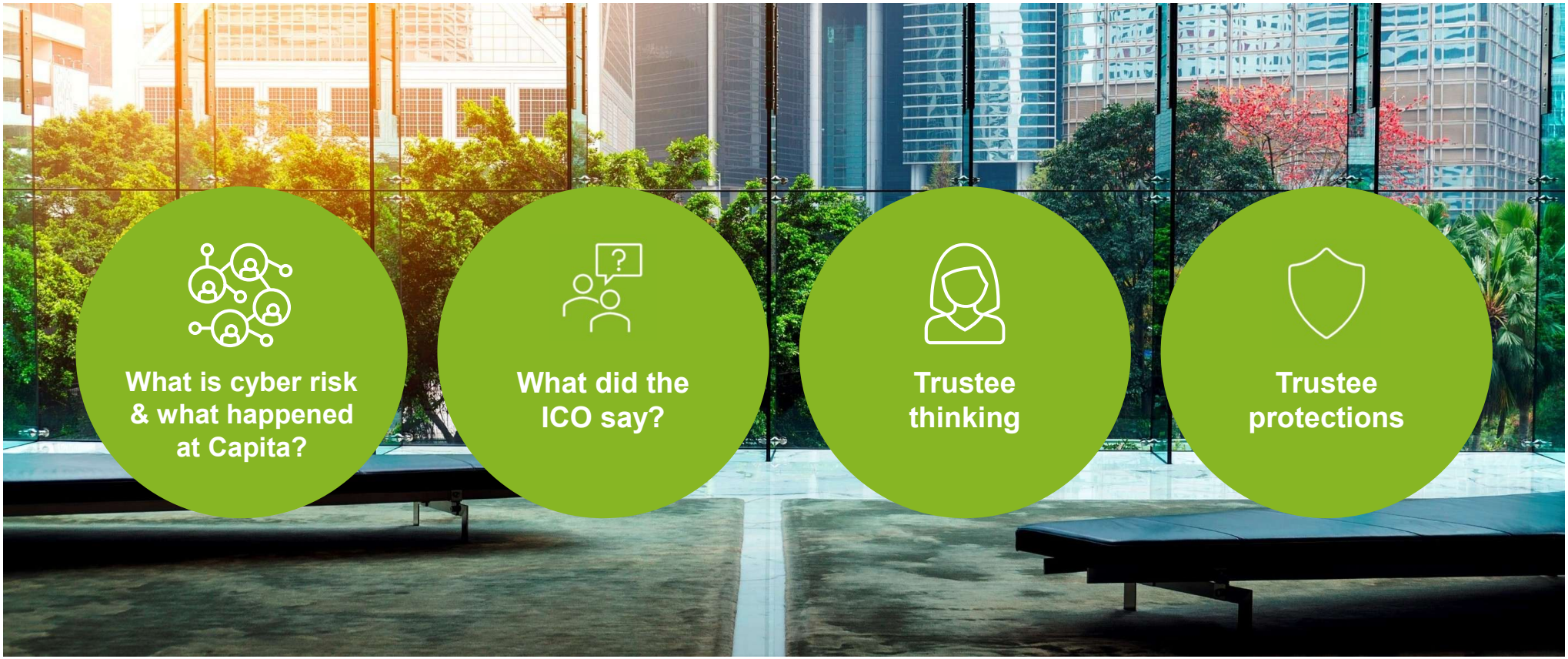
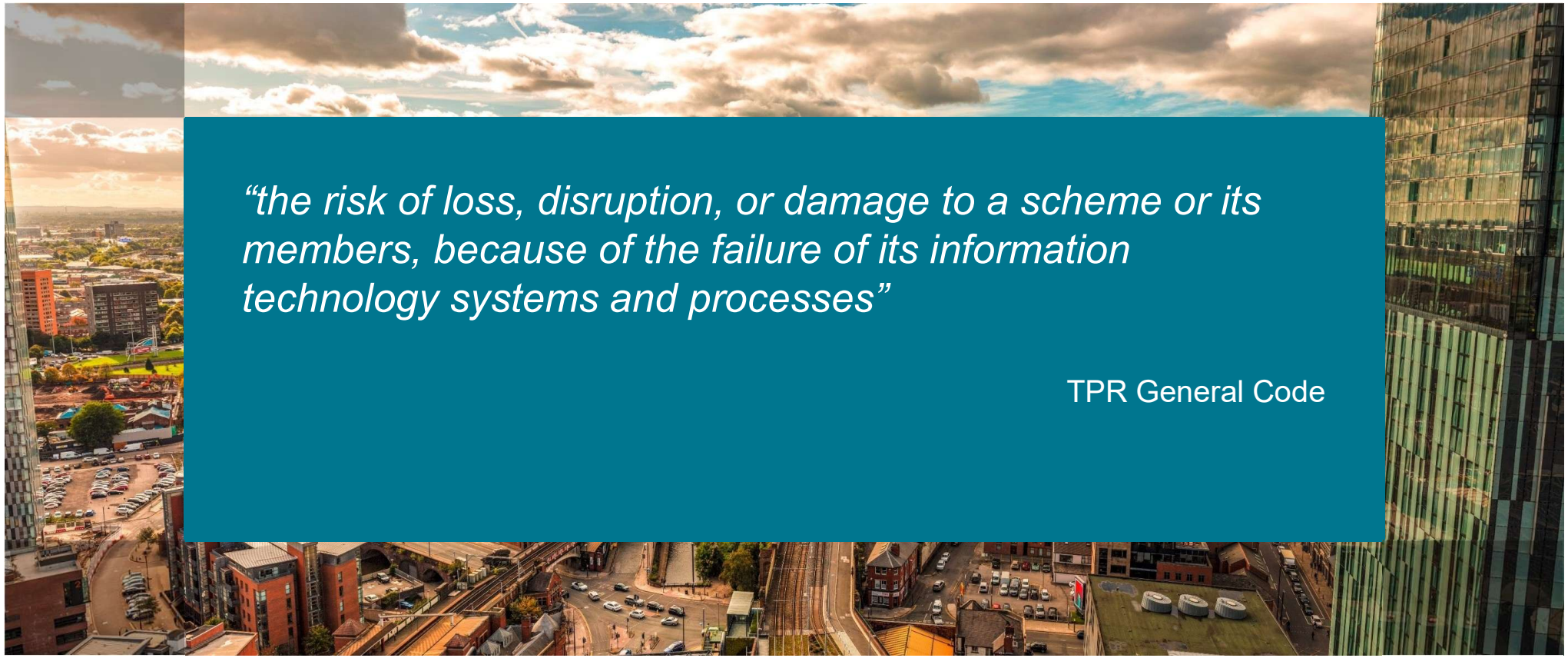
Alexandra Tomlinson

Introduction



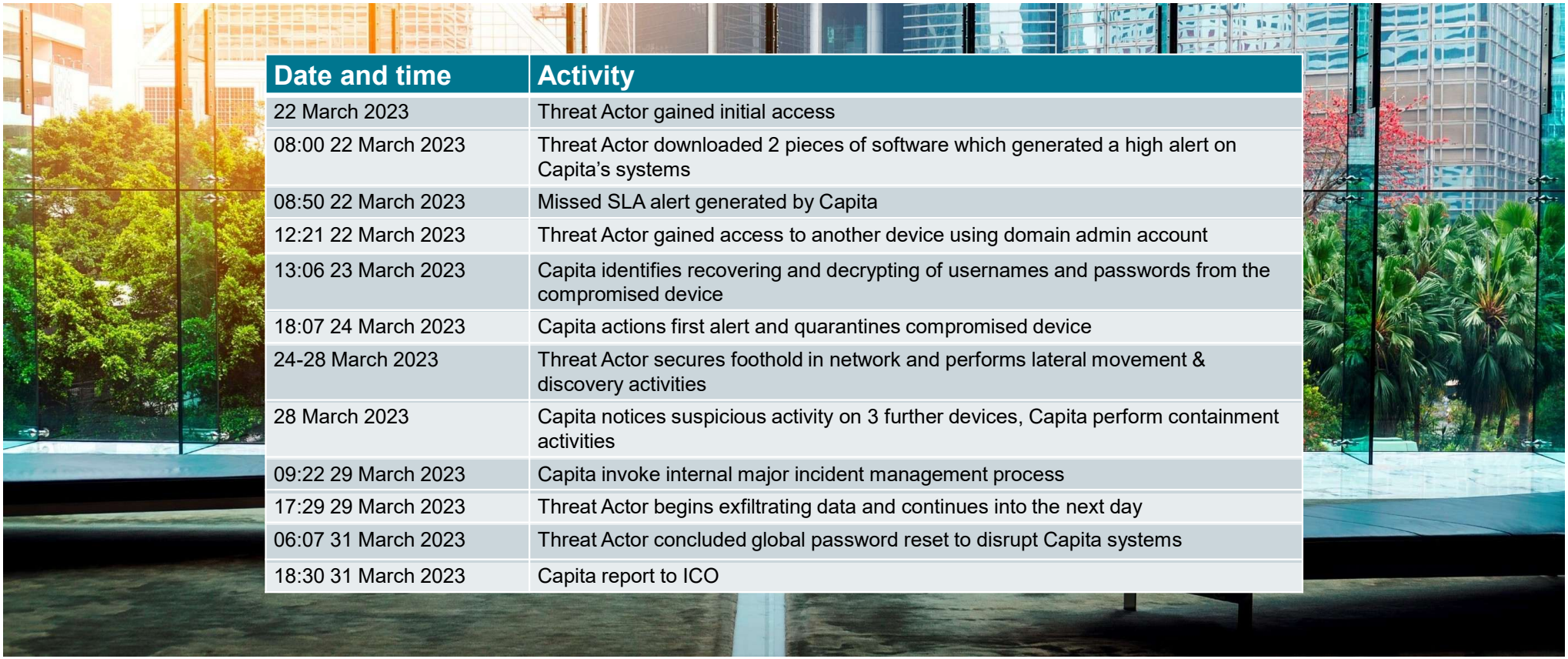
What is cyber risk?



“the risk of loss, disruption, or damage to a scheme or its members, because of the failure of its information technology systems and processes”

TPR General Code

Timeline



Date and time	Activity
22 March 2023	Threat Actor gained initial access
08:00 22 March 2023	Threat Actor downloaded 2 pieces of software which generated a high alert on Capita's systems
08:50 22 March 2023	Missed SLA alert generated by Capita
12:21 22 March 2023	Threat Actor gained access to another device using domain admin account
13:06 23 March 2023	Capita identifies recovering and decrypting of usernames and passwords from the compromised device
18:07 24 March 2023	Capita actions first alert and quarantines compromised device
24-28 March 2023	Threat Actor secures foothold in network and performs lateral movement & discovery activities
28 March 2023	Capita notices suspicious activity on 3 further devices, Capita perform containment activities
09:22 29 March 2023	Capita invoke internal major incident management process
17:29 29 March 2023	Threat Actor begins exfiltrating data and continues into the next day
06:07 31 March 2023	Threat Actor concluded global password reset to disrupt Capita systems
18:30 31 March 2023	Capita report to ICO

What happened with Capita?

- 6,656,037 individuals had data exfiltrated
- Password reset affecting 59,359 accounts
- 57 hour delay from time when human intervention may have helped
- Confusion and difficulty knowing what to communicate to members
- Capita liaised with ICO and TPR: no direct TPR instructions to schemes
- 99% of systems restored by 17 May 2023, 100% by mid-June

What did the ICO say?

£14m fine *"effective, proportionate and dissuasive sanction"*

Reduced in recognition of Capita's settlement and agreement not to appeal

Capita accepted it had failed to apply appropriate technical and organisational security measures required under GDPR and sample contracts

Previous penetration testing had shown weaknesses which Capita failed to address

Capita either aware or ought to have been aware of "high risk" issue in systems

Internal SLAs missed repeatedly

ICO accepted Capita had controls in place but *"for those controls to be effective there also needs to be appropriate measures in place to ensure that those alerts are responded to in a reasonable time to prevent unnecessary and avoidable harm"*

How did this impact Trustee thinking?

Before

- 2004 Pensions Act
  - S247 TKU
  - s249A *"establish and operate an effective system of governance including internal controls"*
- 2016 GDPR
- 2018 Data Protection Act
- 2018 TPR Cyber Security Principles

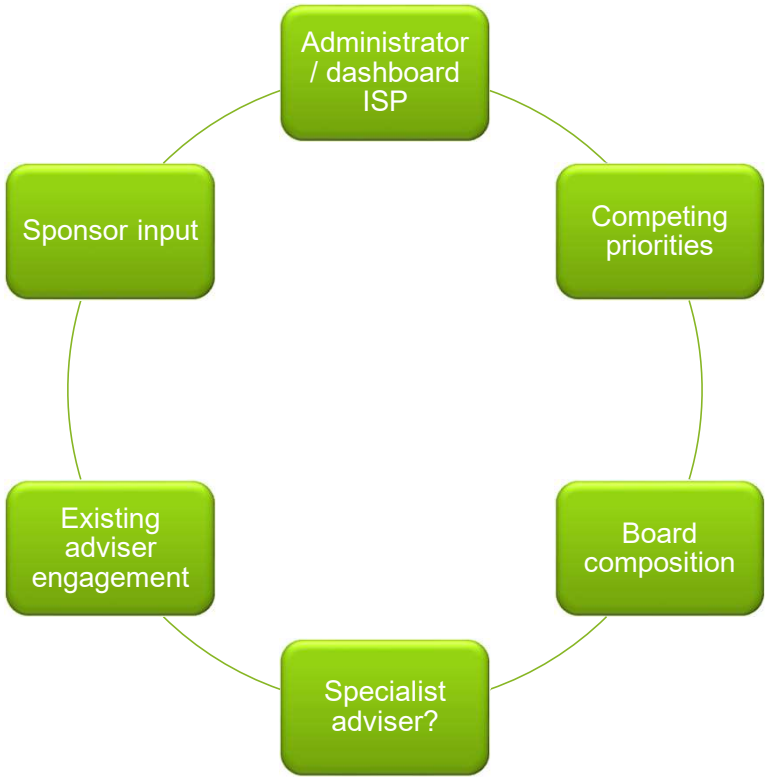
During

- Spotlight
- First test of a scheme's data protection plans / policies?
- Confusion
- Past service providers / retention of data
- Member complaints

After

- Member complaints
- Class Action
- Claims against Capita?
- 2024 TPR General Code
- 2025 TPR Admin Guidance
- 2025/6 DWP Consultation on Trust Based Pension Schemes
- What to do about this?

How do Trustees approach data / cyber issues? Where are the risks?



GMP equalisation and dashboard requirements have driven trustees to focus on some administration services, but the focus is very much requirement driven. TPR engagement with schemes indicates that trustees' focus on data remains very much driven by specific 'projects' such as implementing dashboards, rectification (GMP equalisation / McCloud) or derisking (e.g. a DB scheme preparing for buy out).

DWP consultation on Trust Based Pension Schemes

What would best in class look like?

- Detailed understanding of data/cyber risk with specialist advice & regular reviews
- Appropriate contractual terms & liability caps commensurate with risks
- Insurance coverage
- Indemnity protections

Key messages

Data breach rather than the fine itself impacted Trustee thinking

Trustees should be focussing on this now

Changes to Admin?
Further regulatory involvement?