Crowe

In collaboration with:

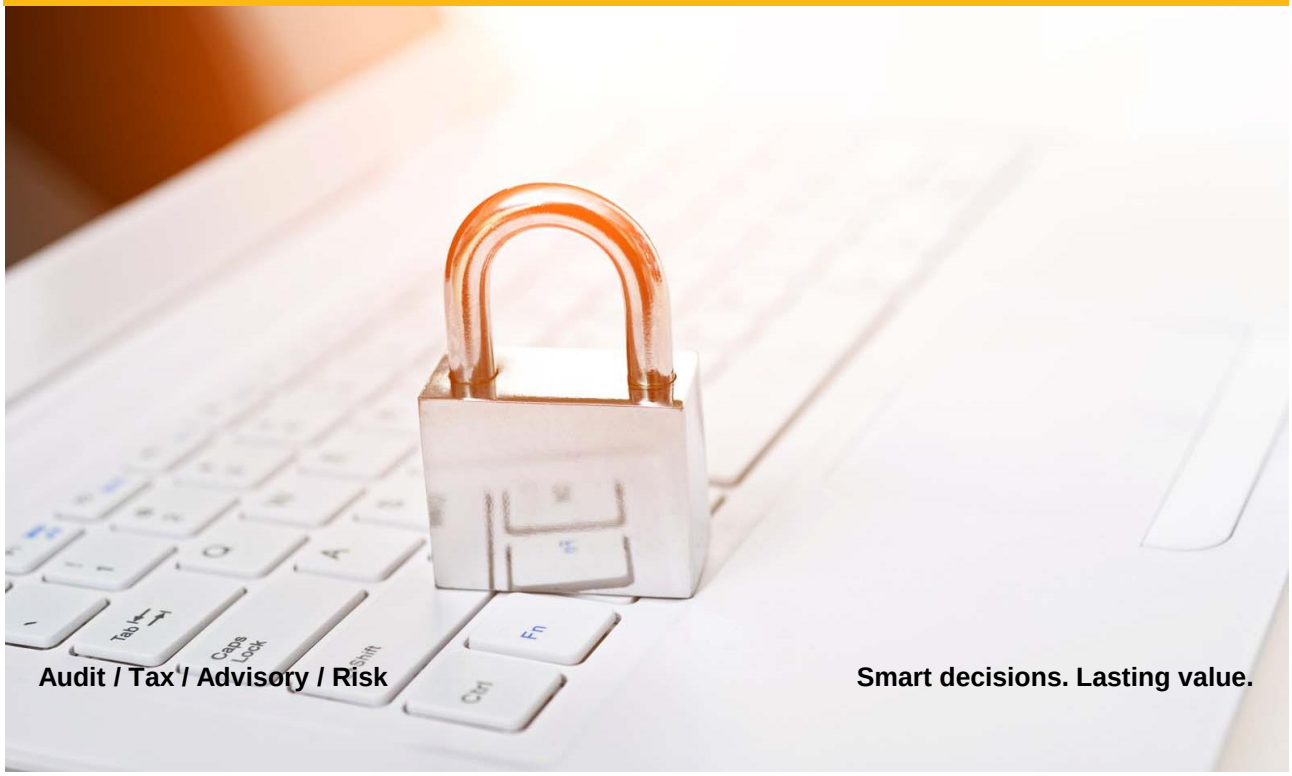
EVERSHEDS SUTHERLAND

LawDebenture

Cybercrime Governance and Data Law in the Pensions Sector

Our most frequently asked questions

July 2022



Did you miss our recent webinar where specialists from **Crowe**, **Eversheds Sutherland**, **Law Debenture** and the **Pensions Regulator** came together to discuss the big cybercrime issues and data law responsibilities impacting the pensions sector?

Not to worry, we have compiled responses to a number of frequently asked questions which we received during and after the webinar. The responses will be equally useful to those who did, or didn't, attend the webinar.

Q. How does the risk to pension schemes posed from a cyber attack differ to more traditional business risks?

A. Cyber is an ever evolving and mutating threat which impacts all organisations across all sectors. Unfortunately, no organisation can ever be 100% secure as cybercriminals are constantly finding new vulnerabilities to exploit. It therefore requires a proportionate response to manage it as an ever-developing risk. Unlike most traditional business risks, such as workforce or supply chain challenges, cyber risk can arise anywhere in the world and infiltrate and compromise systems. In comparison to a normal business, pension schemes do not exist as a single entity; multiple systems, service providers, and even individuals in the form of Trustees make up the scheme's operations. Trustees must have the on-going ability to assess, manage and mitigate any potential threat which could arise across all these fronts, therefore keeping their schemes as resilient as possible.

Q. Are pension schemes being targeted with cyber attacks regularly? I've heard ransomware is often used against them…

A. Cybercrime and fraud now equates to 54% of all reported crime in the UK. The ICO reported a rise from an average of 2 pension scheme data breaches per month pre-COVID, to an average of 5 reported breaches from schemes a month post-COVID. Pension schemes are attractive targets to cybercriminals, because of the rich personal data they control and process and the crucial importance of continuing to pay pensions uninterrupted. This makes them particularly vulnerable to ransomware attacks, which remain the biggest cyber threat to the UK, closely followed by phishing and other online attacks.

Q. What should the trustee being doing to make sure our scheme is resilient to a cyber attack?

A. Firstly, you need to be aware that a cyber attack could happen anywhere in the scheme's eco-system, with the end result being just as damaging. The National Cyber Security Centre's (NCSC) Cyber Assessment Framework provides best of practice standards for a scheme to assess and build its cyber resilience against (cyber resilience involves strengthening defences to prevent a breach from occurring). The scheme should begin by assessing its own resilience (including the trustee and any sponsoring employer) and the resilience of its third-party suppliers. It should then assess the resilience around the data which is shared with those suppliers. External assurance should, wherever possible, be sought to review the real cyber resilience of the scheme's eco-system and satisfy the trustees' obligations.

From there the scheme will be in a position to remediate any issues and then develop a cyber resilience policy which provides expected outcomes and actions, as well as metrics to review over time. Lastly, a cyber incident response policy should be developed which the trustee can follow in the event of an attack or breach. This policy shouldn't include any technical jargon - it exists for the trustee to make governance decisions, so must be in plain English, dictating the roles and responsibilities for those involved when an incident occurs.

Q. I am a trustee of a pension scheme with limited knowledge of cyber security. How can I prepare myself for what to do in the event of a cyber attack?

A. As mentioned in the previous answer, a cyber incident response policy is crucial to know who is responsible and what roles they will carry out in the event of an attack or breach. It is particularly useful to carry out a role play exercise, where a fictional cyber-attack takes place from which the trustees can familiarise themselves with the cyber incident policy at a rapid pace, relative to a real attack.

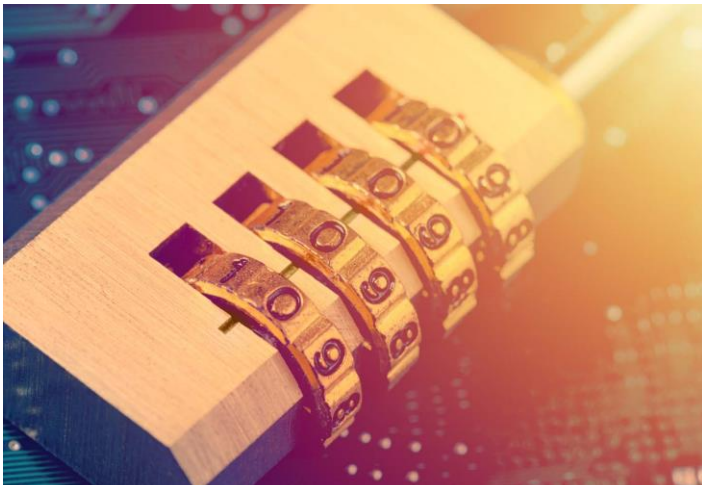
Q. If personal data is breached, what responsibility does the trustee have to report it? And to whom?

A. TPR needs to be told if the breach is of material significance to the regulator. It can impact on governance.

The ICO needs to be told without undue delay and in any event within 72 hours of when the controller (the Trustee/ees) is/are aware. Don't wait for absolute certainty – if there's a reasonable degree of certainty that a personal data breach has occurred guidance says that's when the clock starts to tick. There's no need to tell the ICO if the breach is unlikely to pose any risk for data subjects (members etc) – e.g. where data is encrypted to industry standard.

Data subjects need to be told if there is high risk to them. A much higher bar. Easily passed if there's NINO, DOB, address, health data, or indeed any combination causing risk of e.g. financial loss, ID theft, distress. Likewise, if a member's log in to a portal is compromised criminals could see their data. Notification fatigue from over-reporting (when there is not high risk) does not help individuals to help themselves, says the ICO.

Reporting to Action Fraud/the police and to the NCSC can also be relevant.



Q. Why is paying a ransom to cyber criminals a bad idea?

A. There are many reasons. We won't get into the morality of this. From a legal perspective, this is a potential corporate crime issue, which could involve breaching sanctions, money laundering and counter terrorist financing laws.

The ICO and National Cyber Security Centre have said that paying ransoms does not reduce the risk to individuals or safeguard data. It's not a mitigating factor for the ICO's enforcement investigation either.

Schemes should have offline back-up files to protect themselves from being held to ransom for release of data.

Q. What is the latest on 'the legals' for ransomware?

A. Take account of industry guidance from:

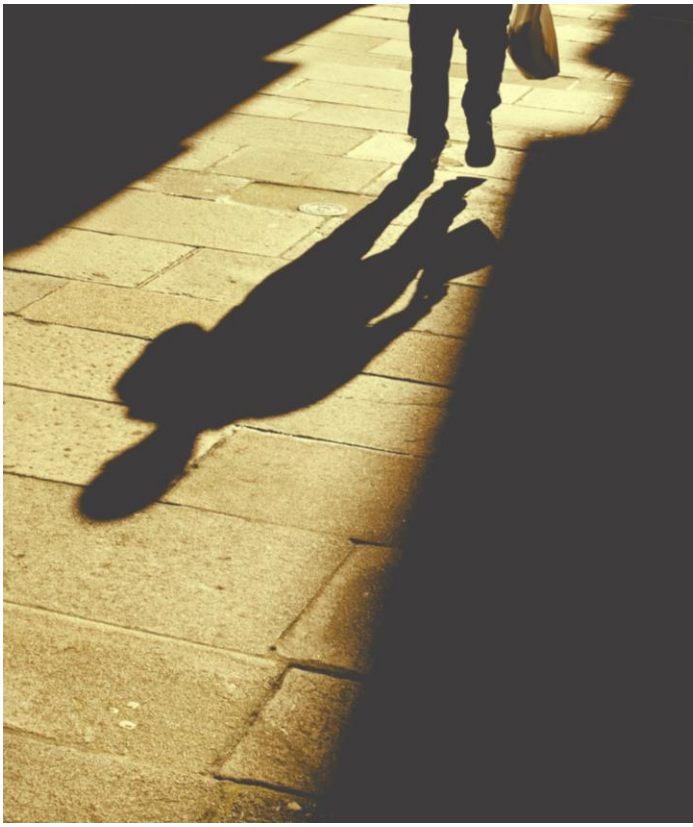
- the NCSC
- the ICO

The ICO issued its first fine against a victim in March 2022. Three key learning points arise for schemes from the enforcement decision.

- The controller processed personal data on a remote archive server which should have been encrypted and on an infrastructure containing known critical vulnerabilities which should have been patched.
- The ICO raised concerns about too much data being held; not following data protection by design (this means 'baking in' data protection from the start). This made things worse.
- The controller did not comply with the security measures described in its own data protection policy. If you don't live out what's in your policy – address this.

Q. Is a fine from the ICO linked to turnover relevant to a Trustee?

A. The ICO's maximum fine under UK GDPR for a trustee board is usually £17.5m. The employer's turnover (or that a professional trustee firm) is unlikely to be relevant to a fine for the Trustee.



Webinar: Cybercrime Governance and Data Law in the Pensions Sector

Don't forget, you can also watch the recording of the webinar if you missed it.

Watch on-demand

Start the conversation

Tim Robinson
Senior Manager, Forensic Services
Crowe
tim.robinson@crowe.co.uk

Lorna Doggett
Legal Director
Eversheds Sutherland
lornadoggett@eversheds-sutherland.com

Elizabeth Hartree
Director
Law Debenture
elizabeth.hartree@lawdeb.com

About us

Crowe UK is a leading audit, tax, advisory and risk firm with a national presence to complement our international reach. We are an independent member of Crowe Global, one of the top 10 accounting networks in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to businesses of all sizes, professional practices, social purpose and non profit organisations, pension funds and private clients.

We work with our clients to build something valuable, substantial and enduring. Our aim is to become trusted advisors to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

www.crowe.co.uk

@CroweUK

@Crowe_UK