



Institute
and Faculty
of Actuaries

Garon Anthony: Squire Patton Boggs (UK) LLP

Data breach, cyber attacks and managing the risk: a rough guide

What's the risk...and why?

- Pensions industry is a very attractive target for cyber attackers. Money + data = risk of theft:
 - More member online experiences/Money and data transfers.
- Is the industry worse than others when it comes to cyber risk?
 - Less regulatory focus (until recently)
 - Increasingly sophisticated attackers.
- Domestic and international experiences:
 - TalkTalk, Tesco, Ashley Madison, NHS etc, etc, etc
 - Japanese Pension Service/Ukrainian Pension Fund/Belgium.

What does the threat look like?

- Many different varieties, but all as risky and disruptive as each other:
 - Hacking against scheme, employer or third party administrator
 - Loss of laptop
 - Non-encryption of data/stolen/cracked passwords
 - Virus/malware/phishing.
- From governments, criminals, political activists, disgruntled employees, bored teenagers.

What are the consequences?

- In 2016 estimated that cyber attacks cost UK Plc £34billion, with over 50% of companies suffering an attack. Potential losses?
- Business interruption and reputational loss.
- Fines (ICO/TPR/FCA/GDPR).
- Professional costs.
- Legal claims and complaints:
 - Court
 - Ombudsman.

The Scenario

Responding to initial crisis (first 24-48 hours):

- Initiate cyber attack response plan (assuming you have one!).
- Contact and alert key players and decision-makers:
 - IT team urgent investigations
 - Legal advice (privilege)
 - Notifications decisions
 - Insurance.

Updated Scenario

Several members receive calls from banks regarding suspicious activity:

- Forensic IT investigations/assistance now needed from outside.
- ICO notification (almost certainly).
- PR issues.
- Mitigation of breach.
- Insurance.
- Prepare for regulatory investigations.
- Think about third party claims.

Lessons learnt/long-term activities

- Prevention always better than cure, so trustees must ensure:
 - Cyber at top of risk agenda
 - IT security taken very seriously
 - Cyber attack plan in place (tested/refreshed)
 - Adequate insurance
 - Third party cyber security.
- Correct IT vulnerabilities.
- Staff training/certification.
- Third party claims.

Cyber liability insurance

- Why have it and common misconceptions.
- What's the state of the market?
- Extent of coverage.
- Typical t's and c's.

Questions

Comments

The views expressed in this [publication/presentation] are those of invited contributors and not necessarily those of the IFoA. The IFoA do not endorse any of the views stated, nor any claims or representations made in this [publication/presentation] and accept no responsibility or liability to any person for loss or damage suffered as a consequence of their placing reliance upon any view, claim or representation made in this [publication/presentation].

The information and expressions of opinion contained in this publication are not intended to be a comprehensive study, nor to provide actuarial advice or advice of any nature and should not be treated as a substitute for specific advice concerning individual situations. On no account may any part of this [publication/presentation] be reproduced without the written permission of the IFoA [or authors, in the case of non-IFoA research].

Contact



Garon Anthony

Partner

+44 121 222 3507

Garon.anthony@squirepb.com

SQUIRE
PATTON BOGGS



Institute
and Faculty
of Actuaries