Institute and Faculty of Actuaries

Garon Anthony: Squire Patton Boggs (UK) LLP
Data breach, cyber attacks and managing the risk: a rough guide

31 October 2017

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

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.

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

Questions

Comments

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries

Contact

Garon Anthony

Partner

+44 121 222 3507

Garon.anthony@squirepb.com

SQUIRE PATTON BOGGS

Institute and Faculty of Actuaries