pib insurance brokers

Trustees Indemnity and Cyber Risks

Stewart Archdale
Charity and Not for Profit Director

With you all the way

www.pib-insurance.com

PART OF pib Group

Topics to be covered:

- **Trustees Indemnity:**
  - **Who is covered?**
  - **What protection is provided?**
  - **Claims examples**
  - **Potential pitfalls**
- **Cyber Risks:**
  - **Exposures in the Hospice/Charity sector**
  - **Proactive risk management measures**
  - **Cyber insurance as risk transfer**
  - **Claims example**

Trustees Indemnity - Who is Covered?:

- **Trustees/Directors**
- **Employees with Management Responsibility**
- **All Other Employees**
- **Volunteers**
- **The Organisation**

Trustees Indemnity – What protection is provided?

- **Civil Claims**
  - **Mismanagement**
  - **Bullying/Harassment**
  - **Defamation**

- **Regulatory Claims**
  - **CQC, HSE, Charity Commission**
  - **Investigation Costs and Defence Costs**

- **Employment Practices (Optional)**
  - **Most common claim within management liability portfolio**

- **Employee Theft**

Trustees Indemnity – Claims Examples

- **Civil Claims**
  - Allegation of Breach of Contract in relation to care provided in Hospice, successfully defended at cost of £16k

- **Regulatory Claims**
  - Legal Representation expenses in relation statutory investigation of historical abuse. Overall cost £700k

- **Employment Practices**
  - Alleged unfair dismissal, successfully defended at Tribunal. Defence costs of £20k incurred

- **Employee Theft**
  - Fraudulent transactions made using company funds. Claim paid £21k

Trustees Indemnity – Potential Pitfalls

- **Late Notification**
  - Failure to disclose potential claim at appropriate time

- **Misrepresentation**
  - Incorrect information provided to insurers as part of inception/renewal process.

- **Inappropriate Exclusions**
  - Exclusions that remove significant elements of policy coverage that are particularly relevant to hospice/healthcare activity – e.g. absolute bodily injury exclusions, absolute abuse exclusions, absolute medical malpractice exclusions.

Trustees Indemnity – Q&A

Cybercrime Landscape:

- **Cybercrime is now the fastest growing crime in the world**
- **86% of breaches were financially motivated and 10% were motivated by espionage** (Verizon)
- **Ransomware and Business Email Compromise make up the majority of attacks**

Cyber Risks in the Hospice/Charity Sector

- **Ransomware**
- **Phishing**
- **Malware**
- **Third Party Providers**
- **Regulator Action**
- **Loss of Reputation**

Proactive Cyber Risk Management

- **Good Practice**
  - **Do employees receive regular training with practical testing?**
- **Data Minimisation**
  - **Can data be disposed of or archived off network?**
- **Access Control**
  - **Is access segregated depending on duties, are these separate networks?**
- **External Advice**
  - **Have you engaged an expert to conduct threat/vulnerability testing?**
- **Detection**
  - **Are systems in place to detect unusual activity either within network or at network perimeter?**

Cyber Insurance as risk transfer

- **First Party Losses - where the Organisation suffers direct financial loss**
  - **IT Security and Forensic Costs**
  - **System Damage and Rectification Costs**
  - **Privacy Breach Management Costs**
  - **Loss of Profit or Increased Costs of Working**
  - **Hardware Replacement Costs**
  - **Legal and Regulatory Costs**
  - **Funds Transfer Fraud**
  - **Extortion**
  - **Telephone Hacking**
  - **Regulatory Fines**

Cyber Insurance as risk transfer

- **Third Party Losses - where the Organisation is alleged to have caused financial loss to a Third Party**
  - **Privacy Liability**
  - **Network Security Liability**
  - **Media Liability**
  - **Infringement of Intellectual Property Rights**

Ransomware

Ransomware is one of the main drivers of cyber losses and has wreaked havoc on countless organisations in recent years, and those operating in the third sector are no exception to this.

A type of malicious software or encryption program which

- Encrypts data on a network
- Leads to a demand for a ransom to be paid in exchange for decryption key to regain access to the data

> “ …those operating in the third sector are no exception to this. ”

The attack begins

The incident began with a phishing email. In this case an employee received an email from what they assumed was a trusted contact.

The email:

- Part of a pre-existing email chain
- Word document attached
- Latest email in the chain stated “Please see attached”
- Employee clicked on the attachment
- To view the document, the “enable content” button had to be clicked
- Wanting to see what the document contained, the employee clicked the “enable content” button

The attack begins

By clicking the “enable content” button, the employee enabled macros to run.

Macros:

- A function of the Microsoft Office suite of products
- Used to automate common tasks
- Can help productivity
- Pose a security risk because cyber criminals can create malicious macros to automate commands and execute malicious code onto the end user’s computer

The attack progresses

Unfortunately for this organisation, the document that the employee had clicked on contained malicious macros.

By enabling macros:

- Word document automatically executed a series of commands
- Resulting in malicious software being downloaded onto the employee's computer
- Allowing the hacker to gain remote access to the device
- Signalled basic network information back to the threat actor e.g. domain name, helping the criminals decide whether to pursue the attack

The ransom note

Having established that the organisation made a suitably lucrative target, the threat actor then downloaded a password scraping software from the internet.

Password scraping:

- Hacker gains access to every password ever used on the employee's computer, including the original domain administrator account and password
- Gains higher access privileges across the network
- Launches encryption software across multiple servers
- ...Ransom note for £195,000 in bitcoin, in exchange for decryption key

Organisation engages cyber insurer

After discovering the ransom note and realising that their computer systems were no longer accessible, the organisation notified the insurer's incident response team to determine next steps.

Incident response team

- Establish the status of the organisation's back-ups
- Fortunately offline back-ups stored on a USB flash drive to recover from
- Organisation largely regained access to its computer systems within a 72-hour period without paying the ransom

Incident response team's work not over yet

Cyber insurer's incident response team were alert to the fact that the ransomware variant used in the attack had been associated with data exfiltration in previous attacks.

Incident response team's focus shifts

- To establish whether data had been accessed and stolen from the organisation's systems
- Digital forensics firm appointed to carry out this task

Stolen data

After the organisation had recovered from back-up, those responsible for the attack made contact, explaining that they had stolen data during the attack and threatened to publish it on a public file sharing website.

Organisation opts not to pay the ransom

- Questions over the threat actor's reliability
- Depending on the type of data stolen the organisation would have to notify any private individuals at risk of harm, and commercial partners would be notified out of courtesy
- Initial findings from forensic investigation suggested that the data that had been exfiltrated was largely benign

Stolen data is published

With the organisation deciding not to make the ransom payment the cyber criminals responded by making good on their threat and publishing the stolen data on a file sharing website.

Incident response team helps again

- Contacts the file sharing website requesting that the data be removed
- Explains that the data had been stolen and this breached the file sharing service's own terms
- File sharing website receptive and promptly removed the data
- The website also noted that the file had only been downloaded a few times, all traceable to the organisation itself

A costly experience

Although the organisation managed to recover from back-ups and avoided paying the ransom demand, the incident was not without its costs.

Costs of £61,155 incurred, consisting of

- Forensic investigation of the organisation's computer systems to establish the root cause of the loss and extent of the data breach = **£27,450**
- Third party legal assistance to help the organisation determine the correct course of action = **£33,705**
- All recoverable under the organisation's cyber insurance policy

What if the attack had been more severe?/ Other Insurances?

Exposure	Cost	Covered by Traditional Insurance?	Covered by Cyber Insurance?
Incident Response - Root cause analysis - Network security assessment - Forensic investigation	£27,450	✗	✓ Incident Response costs covered
Legal Costs	£33,705	✗	✓ Legal Costs covered
Further costs - Crisis communication costs - Breach notification to individuals & credit monitoring - Civil claims - ICO investigation	Dependent on no. of data records affected	✗ (D&O policy may provide some coverage, although more exclusions being introduced)	✓ Breach Notification / Credit Monitoring / Civil claims covered
Business interruption - Direct loss of income / effect on reputation? - Increased costs of working	How does achieved income compare to anticipated income?	✗	✓ Direct loss of income and increased costs of working covered

Typical cyber insurance policy – Additional risk management benefits

Online Training Modules e.g.

- Ransomware prevention
- Mobile and Wi-Fi Security
- Preventing Phishing

Cyber risk rating reports based on features of your organisation's internet presence/digital footprint

Cyber incident response planning templates and tools

Breach Alerts

Continuous searches of the dark web for information specific to your organisation, followed up with
real-time alerts to possible breaches of your data

pib insurance brokers

Q&A

With you all the way

www.pib-insurance.com