Cyber crime claim

Organisations are under increasing threat of cyber attacks with 32% of businesses and 22% of charities suffering a cyber attack within the last 12 months.

Charity cyber attack

While it is tempting to think it will happen to someone else, research shows that regardless of the size and complexity of your organisation, anyone can be targeted.

In July 2019, a charity in Manchester became the victim of an email/bank scam where a payment of almost £100k was transferred to the incorrect bank account.

The organisation was undergoing an extension to their centre and had been paying their invoices by BACS transfer for several months. A copy of a valid invoice and a request for change of bank details (on the building company's letterhead) was received via email.

At this point, the organisation's finance manager was on holiday and did not respond to the email straight away. Upon their return, they received a call chasing the payment and checking that the bank details had been changed.

The caller provided a legitimate excuse, explaining that the details needed to be changed due to fraudulent activity on the previous account. The finance manager replied that they had already paid the invoice for that period but confirmed they would update the bank details in preparation for the next payment.

When the next valid invoice was received the funds were transferred to the new account as requested. It wasn't until the real building contractors began chasing for payment that the scam was revealed. It was a simple mistake but it resulted in significant cost to the organisation.

Applying cyber cover

This type of spear phishing attack is not uncommon and 80% of businesses and 81% of charities reported having received fraudulent e-mails or being directed to fraudulent websites in the last 12 months.1 It is therefore important that organisations ensure they have appropriate insurance cover in place to protect them from a range of cyber-attack scenarios and the consequences.

This type of attack fell under the Cyber Crime section of the policy. This allows for traditional crimes, such as theft or fraud, which can now be implemented using computers and often referred to as cyber-enabled crime. In this instance a Funds Transfer Fraud was committed via an e-mail resulting in the fraudulent inputting of data.

[1] Department for Digital, Culture, Media & Sport Cyber Security Breaches Survey 2019

ecclesiastical

On finding out that the payment to our building contractors had been fraudulent, I felt sick to my stomach. The loss of these funds would have seriously affected the completion of our building extension. If we needed to find replacement funds this would have taken months, if not years, to secure, which would have had a detrimental effect on our ability to deliver much needed support and services to young people.

Following an extensive investigation into our systems and cyber security, having Ecclesiastical Cyber cover in place meant that we were reimbursed for our lost funds within two weeks of the fraud having taken place, allowing us to not suffer any delays in our building project.

The missing link that allowed the fraud to slip through our robust financial controls was that we did not call the supplier direct to confirm the change - we accepted their incoming call as approval. Since the event we have contacted all of our suppliers to confirm the details that we hold are correct and now contact all suppliers by phone to confirm bank details prior to us processing significant payments. I would say to all companies Stay vigilant. Check, check and check again!

Prevention is protection

Organisations need to take measures to protect their systems and prevent or limit the impact of cyber crime. As cyber crime evolves, these types of attack (and the subsequent claims) are likely to increase. Basic cyber security measures include:

- Implementing training to ensure staff and volunteers are able to recognise and respond to threats.
- Updating antivirus software and other software programmes to ensure that they include the latest patches.
- Using strong passwords and encryption to protect data.
- Backing-up data to a safe and secure location on a regular basis.

Find more detail about how to protect your data and organisation from cyber crime by downloading our cyber security guidance notes.

Cyber insurance

Cyber insurance is another way to manage cyber risks. It's important first and foremost, that organisations defend themselves by having cyber security controls in place. However, cyber insurance can provide additional protection and support.

Cyber insurance from Ecclesiastical can be bought in conjunction with your insurance or as a separate stand-alone policy.

What does cyber insurance cover mean?

Ecclesiastical's cyber insurance can cover:

- Computer, data and cyber risks, designed to meet the needs of small and medium sized organisations.
- Costs of dealing with cyber liability claims.
- Costs of dealing with data breaches excluding legal fines.
- Costs of dealing with systems and data damage and the resulting loss of business income.
- Costs of dealing with cyber crime and any financial loss.

The policy also includes access to expert advice and support such as PR and crisis management when an incident occurs to help mitigate the financial impact or reputational damage. You can read our cyber insurance policy summary for more details.

ecclesiastical

PD3410 1 03/21