BUSINESS OWNERS' PERSPECTIVE: PAYMENT REDIRECTION SCAMS

All businesses are vulnerable to Cyber scams and with Cyber criminals becoming ever more sophisticated, their methods are evolving faster than traditional insurance policies may cater for. With over $5.5 million lost in Australia through billing scams in 2018, we want to ensure you aren't one of their victims. Payment redirection scams are just one of many tactics cyber criminals employ to steal data and money. Remember cyber criminals only need to fool one employee in order to gain access to your business' data and money!

WHEN IS A CYBER CRIME NOT COVERED BY A CYBER OR OTHER INSURANCE POLICY?

With almost 11,000 reported billing scams reported in 2018 alone, along with the investment criminals are making in this area and its continual sophistication, don't be one of the statistics.

Billing scams are an example of "social engineering fraud", which is a broad term that refers to the scams used by cyber criminals to trick, deceive and manipulate their victims into divulging confidential information and making payments.

Even though these scams can potentially be traced back to a cyber hack or incident, many cyber insurance policies exclude direct financial loss and therefore will not respond to pay these claims. Furthermore, other insurance policies that specifically cover losses as a result of third party crime are either outdated and hence do not contemplate this type of fraud, or specifically exclude social engineering fraud claims.

A REAL LIFE EXAMPLE

The Accounts Payable (AP) of an organisation receives a phone call from one of their suppliers advising the supplier's bank account details have changed. This person even quotes the Invoice Number which is due for payment. The AP asks for a written request from the supplier to amend their bank account details as per normal procedure of their organisation. The written request is received signed by the Managing Director of the supplier on the supplier's letterhead. The bank account details are amended, and the weekly payments are processed.

A couple of days later the AP receives a call from the supplier following up the payment of the outstanding invoice. On investigation it is discovered that the amended bank account did not belong to the supplier.

Even though the AP's bank, the bank receiving the funds and the police are immediately notified, the money has already disappeared to another country with very little chance of getting it back.

WHAT YOU CAN DO TO PROTECT YOUR BUSINESS

- Ensure you have the crime and social engineering controls in place in order to procure insurance cover. We can help you to ensure you have the right controls in place. For example:
  - Ensure that where possible duties are segregated so that the same person does not both authorise and make payments, and that dual signatories are required on all payments;
  - Implement call-back procedures with customers or suppliers to authenticate any significant fund transfer instructions prior to transfer;
  - Upon receipt of any email requests to change supplier or customer bank account details (including account number, email address, contact information, bank routing number) implement call-back procedures (i.e. other than responding via email) to the contact phone number in place prior to receipt of the change request.
- You need expert advice from your Broker on emerging risks and the insurance and risk management options available to protect you and your business. Talk to your Edgewise Account Manager today who can explain your options.

PROTECT THE FUTURE OF YOUR BUSINESS BY CONTACTING US

edgewise insurance brokers

+61394251333 email@edgewise.com.au +61394251399 edgewise.com.au