V-INSURANCE GROUP

EMERGING CYBER RISKS

PAYMENT REDIRECTION SCAMS

INTRODUCTION

As Australia largest specialist sports and leisure Insurance Broker we are seeing a significant increase in incidents relating to "payment redirection" scams. This type of computer / cyber scam is also known as Social Engineering, Account Impersonation and Account Takeover. This is now recognised globally as one of the largest types of fraud.

WHAT IS PAYMENT REDIRECTION SCAMS AND SOCIAL ENGINEERING FRAUD?

Payment redirection and billing scams are an example of Social Engineering Fraud which is a broad term that refers to the scams used by Cyber criminals to track, deceive and manipulate their victim into divulging confidential information and making payments.

In the last 12 months we have seen a lot of incidents for sporting bodies where they are paying fake invoices. This can occur when the sports server or computer has been hacked by a cyber criminal or a suppliers server/computer system has been hacked.

Losses have also occurred when emails impersonating a known source (i.e the CEO or President) are received by the Treasurer or Accounts department and they are requiring urgent payment. The payment is then made, and it is found to be a fake email and bank account due to a cyber hack.

A REAL LIFE EXAMPLE

Each year a sports club purchases a significant amount of sports equipment and uniforms for the new season from a regular supplier. The costs of the goods are just under $100,000. An invoice is sent to the sports club, and it highlights that the providers bank account details have changed. The invoice came from the normal Account's Department email address and looks exactly the same as the invoices that have been provided in the past.

The invoice is approved by the club treasurer and paid as normal. The club did not verify the changed bank account details or send an email verifying the invoice had been paid. After two weeks the club contacted the supplier to ask when they would receive their equipment and uniforms. The supplier advised that as per normal procedure they would be sent when the funds had been received. The club said the funds were sent 2 weeks ago. The supplier checked their bank account and advised they has not received the money.

The club contacted their own bank and the police became involved. Unfortunately, the money was diverted to an overseas account and was not recovered. The club's Australian bank did not refund the lost funds.

After investigation it was found the computer belonging to the club secretary had been hacked into and the original invoice from the equipment supplier had been deleted and replaced with a fraudulent invoice and bank account details.

HOW DOES PAYMENT DIRECTION / CYBER SOCIAL ENGINEERING FRAUD OCCUR?

There are many causes associated with social engineering and payment diversion fraud losses.
An adequate controls framework, including verification controls is vital in mitigating and reducing the likelihood and impact of these types of loss, as well as ensuring that processes and procedures are actually followed.

Security breaches, of both the insured and third-party provider are also a cause of social engineering losses where hackers have managed to infiltrate systems and takeover client accounts or send fraudulent payment instructions.

Hackers will exploit any weakness – One of the key elements identified through our analysis is that in most cases clients' emails were compromised. Hackers generally monitor e-mail traffic for months to familiarise themselves with the style and tone of communications.

Warning signals - Written communications requesting urgent or confidential payments should throw up red flags, as should any requests for payments where there are changes in bank details. Hackers will often target firms that process a high number of payments, so that one fraudulent request can slip through.

Verification is key - So called "spoofing" is a very common means for hackers to deceive you into believing that they are communicating with your club and vice versa. Software is available to ensure that e-mails received are from the domain that they purport to have been sent from. However, if e-mails have been compromised and the hackers are able to send e-mails from genuine domains, these software solutions will offer no protection. Verbal verification with your client, vendor or internally seems to offer the best security. However, always ensure that the contact details used for verification are not sourced from the e-mail as that might be fraudulent as well.

HOW CAN YOU REDUCE PAYMENT REDIRECTION / CYBER SOCIAL ENGINEERING INCIDENTS?

- Ensure that where possible duties are segregated so that the same person at a club 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 request to change supplier or customer bank details (including account number, email address, contact information or bank routing number) implement call back procedures (other then responding via email) to the contact phone number in place prior to receipt of the change request.
- If you receive an urgent payment request either from new or familiar contact, look into the request. Call the person that sent you the request to verify its authenticity.

However always ensure that the contact details used for verification are not sourced from the email as they might be fraudulent as well.

ENQUIRIES

Sports have unique exposures that require expert advice an experience. V-Insurance Group have been looking after the sports fraternity in Australia for decades and are always available to help you with qualified independent advice. This includes Risk Management advice and procedures. With all the sporting and leisure organisations V-Insurance looks after, we are directly involved in arranging insurance for more than 4 million people.

September 2021

V-Insurance Group Pty Ltd
Level 25, Angel Place, 123 Pitt Street Sydney NSW 2000 Australia
Call 1300 945 547 **Telephone** +61 2 8599 8660 **Fax** +61 2 8599 8661
Email sports@vinsurancegroup.com **www.vinsurancegroup.com**

V-INSURANCE GROUP