DAVID ROBERTS & PARTNERS INSURANCE BROKERS LTD

CYBER ATTACK CASE STUDY

CONSTRUCTION

Criminals swindle a construction firm out of large payment by impersonating a subcontractor.

Many construction companies have been slow to implement cyber insurance due to not holding large amounts of sensitive data or relying on computer systems, construction companies don't often believe that they are overly exposed to cyber risk. Most modern businesses will hold data on employees, use email to communicate with supplier and use bank accounts to send and receive funds.

One of the main cyber risks for construction companies is funds transfer fraud with invoices for supplies and materials frequently being paid, cyber criminals are constantly looking to intercept and divert these payments. In this case study is a small construction firm with revenues below £50 Million specialising in commercial construction projects ranging from office buildings to warehouse units – commonly using subcontractors to assist with projects.

The scam began when an employee clicked a link on a credential phishing email sent by a fraudster pretending to be from Microsoft. The link took the employee to a fake log in page where they handed over their credentials to the fraudster believing they were signing into their Microsoft account. The company didn't have 2 factor authentication enabled on employee accounts, so the hacker was able to log in to and monitor the account without any issues.

A few weeks after the account was breached, the employee was in contact with a subcontractor who they owed £93,425 for structural steel fabrication work on a recently completed project, the fraudster chose this moment to strike. Firstly, the fraudster set up a rule on the employee's inbox so that any legitimate emails from the steel fabrication company were instantly moved to the deleted folder on the employee's inbox. The fraudster then set up an email address impersonating the managing director of the steelworks company – to the untrained eye the difference was un-noticeable. The final step was to send an email to the employee from this fake email and claim to be the managing director of the steel fabrication company saying that the invoice they had previously sent had incorrect bank details and attaching a new invoice with the fraudsters bank details. The fraudster used the exact email and invoice template that the company would've used so the employee didn't have any reason to believe that it wasn't a genuine email. The finance department transferred the funds to the fraudster without using a secondary method to verify the change in bank details.

Weeks later the director of the steel fabrication firm phoned the employee about the status of the payment, it was only then that the scam was discovered. Both banks were notified but by then it was too late, the money was gone. The company had no choice but to pay the invoice again but thankfully they were able to recoup the funds through their cyber insurance policy. This case highlights the skill of cyber criminals it also shows how human error can cause a major loss for a company further showing that almost all modern businesses have some form of cyber exposure.