Engineering Case Studies

May 2020

Construction Engineering Firm Falls Prey to Ransomware

In early 2019, an engineering firm in the UK was hit by ransomware which caused its data to become encrypted. The firm had been running a local back-up on a hard drive which had also become encrypted meaning access to technical drawings, design specifications and other vital data, was out of reach.

The business received a demand for £3m in exchange for the decryption key and was threatened that, in the event of the ransom not being met, some files would be destroyed and others would be released into the public domain.

The firm had access to consultants under its cyber policy which, through the 24/7 breach response services, provided advice to the business as to how best to deal with the ransomware demand, manage potential public relations issues and generally monitor the situation.

A specialist negotiator was brought in who was familiar with the particular type of ransomware, and the cyber-criminals behind it. As a result of the consultant's involvement, the demand was reduced by 75%.

Lawyers and IT forensic specialists were engaged at the earliest stages to analyse the extent of any privacy breach and whether any notifications to the ICO were necessary.

There was significant financial fallout from the incident. The specialist IT, legal and negotiating costs were met under the breach event cost provisions of the policy (subject to payment of the retention).

The firm decided to pay the reduced ransom (in Bitcoin) and as it had extortion cover within its policy, that cost was also met. The business was provided with access to most of its files 13 days after the initial incident. It has been estimated that approximately 5% of the files have not been recovered. Thankfully, it was determined that no privacy breach took place.

The incident had a considerable effect on the construction time-line at what was a critical time in the programme. Not only did the disruption create delays on the specific project but the engineering firm was unable to use the encrypted information for wider initiatives, namely marketing and bid preparation, for a period of time, creating significant lost opportunities.

The forensic accountants are working with the insurers with respect to a business interruption loss claim under the cyber policy.

Engineering Firm is Social Engineered

We are aware of an engineering firm which recently suffered a business email compromise attack. An employee received a highly-personalised email message ostensibly from a senior partner. The email attached a link to a legitimate document-sharing site but the site hosted a number of infected documents, providing tools to allow the cybercriminal to carry out keylogging, the use of a computer programme to record keystrokes made by a computer user.

Keylogging allowed the hacker access to the employee's locally stored information by enabling remote login to the employee's computer.

The cybercriminal was easily able to obtain data relating to the e-payment system of the firm including PIN codes and account numbers. The hacker was able to transfer £155,000 out of the firm's account. Discovery of the fraud took place a short time later but too late for the money to be recovered by the firm's bank.

The engineering firm's cyber insurance policy covered breach response costs including IT forensic costs which allowed consultants to identify the source and extent of the breach as well as take steps to terminate the threat.

Legal costs were also incurred as the firm needed to understand what private data had been compromised and whether any notification to the ICO or individuals, was necessary; the resulting legal costs were reimbursed by the insurer.

Finally, as the business had a cyber-crime retention, reimbursement for the theft of funds was also forthcoming (subject to payment of the retention).

Compromised Platform

Many businesses within the construction industry use programmes such as Computer Aided Design (CAD) or Building Information Modelling (BIM). While the process of allowing input from various parties on the same integrated (single network) model at the same time has clear benefits, such technology increases the risk of a cyber-attack.

A UK civil engineering firm, hosting a BIM platform for the use of various parties working on a large construction project, experienced an external cyber threat to the platform causing compromised BIM data, hefty delays and disruption to the construction project. The delay led to a number of third party claims based on the engineer's contractual liabilities to those parties. The firm's own business interruption losses over the 3 ½ week period (during which the IT consultants investigated, assessed and then ultimately terminated the threat) were considerable. Further, the reputational damage to the company necessitated the engagement of a PR consultant.

The cyber insurance policy met all first party costs and the losses involved in the third party claims (subject to payment of the retention).

For further details please contact:

Vanessa Cathie
Account Executive,
Global Professional & Financial Risks

vanessa.cathie@uk.lockton.com
+44 (0) 20 7933 2478

The Lockton Global, Cyber and Technology team works with clients to help protect their business from cyber risks, from ransomware to phishing, targeted hacks, malware, IP theft and various cyber complexities. Due to the sensitive and confidential nature of such risks, we have created fictional case studies to demonstrate examples of cyber complexities a client might experience.

The case studies are inspired by real matters, however, some facts have been amended to protect client confidentiality. These case studies do not constitute advice. Please seek appropriate advice before taking any action.