LOCKTON

UNCOMMONLY INDEPENDENT

Architects Cyber Case Studies

Not a Random Ransom

A European architecture practice was the victim of a recent ransomware attack. A wide selection of the firm's data was stolen and encrypted, its server having been held to ransom.

Cyber criminals blocked access to the business's data and threatened to publish it online if ransomware demands were not met. Threats were made to release private emails, bank documents, payroll records and employee details into the public domain. Furthermore, it transpired that the criminals had access to highly confidential and sensitive data regarding a high-profile commercial development, including financial records and valuable architectural intellectual property.

The company reported the incident to its cyber insurers. A breach response team was appointed and the Information Commissioner's Office was notified. Cyber specialists were appointed to assess the attack, secure the firm's computer network, restore back-ups where possible and investigate the full extent of the theft and compromise of data. Once further details were to hand, the practice's customers and stakeholders were advised and updated as matters progressed.

The architecture firm's strongly-held position was that it did not wish to pay the ransom demand but faced with the prospect of considerable commercial and reputational damage from the data breach, the business agreed to engage a specialist adviser to negotiate with the criminal. The ransom demand was reduced by 70%, and upon payment in Bitcoin, a decryption key was made available and the stolen data destroyed. The ICO took no further action.

Thankfully, lost revenue owing to network and system downtime was limited as the IT forensic team was able to restore the operational network within a fairly short period of time. The business's cyber insurance policy responded in full to first party losses and third party claims, subject to the payment of the retention.

Advanced Persistent Threat

An Advanced Persistent Threat (APT) is a prolonged and targeted cyber-attack in which the intruder gains access to the network and remains undetected for an extended period of time. APT attacks are initiated to steal data or generally obtain information, rather than cause damage to the target organisation's network. The goal of many APT attackers is to steal an organisation's most valuable intellectual property. It is part of a long-term strategy with specific goals and sophisticated methods. APT attackers may work for months or years to research targets, infect systems, explore the enterprise network, and then either steal secrets or attempt to cause maximum hack-attack damage. Whilst APTs are often levelled at high value targets such as nation states and large corporations, this is not always the case.

In February 2019, an architectural firm in the UK was the victim of an APT which took place over a series of calculated stages. In the first stage, a cyber-criminal sent a phishing email message to an employee of the firm. An infected attachment that the employee clicked on, caused the insertion of malware into the target network, providing "tunnels" for the criminal to move around the system undetected. Over three months, the hacker gained greater levels of access and moved around at will, gaining a full understanding of how the system worked and allowing the criminal to harvest the information needed. In the final stage, the criminal tricked an employee of the firm into sending an insurance premium to the hacker's bank account.

The cyber policy responded to the network security breach and covered the costs involved in dealing with the incident (subject to the retention). The cyber policy included a cyber-crime reimbursement provision which meant that the lost funds were reimbursed.

Overloaded Resources

Distributed Denial of Service attacks are cheap and easy to generate. DDoS attacks involve disruption of internet and website services caused by using more computer system resources than are available. The services become overloaded and no longer accessible to the public.

In July 2019, a global architectural firm experienced a DDoS attack. The attack on the infrastructure was well-planned and staged, with abrupt large volumes of data disrupting the service provider in two separate attacks within four hours of each other.

It is estimated that the DDoS attack generated more than 40 to 48 times the normal traffic volume, causing major connectivity issues. While no data was stolen, the attack was disruptive. All of the business's online services were rendered unavailable by the attack, including internal internet access and staff email. Building Information Modelling software (allowing the firm to access and manage vital centralised architectural, engineering and construction processes) was unavailable.

The firm engaged IT forensic specialists who agreed a solution with their internet service provider to divert the attack into a "black hole". This allowed the majority of services to be reinstated, with only one portal disabled. Two days later, the portal was reinstated, unfortunately prompting a second DDoS attack and service was again interrupted. A more permanent solution was required to allow all portals to become fully operational, prompting a cloud-based solution at significant cost.

The incident created significant financial, reputational and systemic damage to the business which was met by the cyber insurance response (less the retention and up to the indemnity limit).

For further information, please contact:

Vanessa Cathie
Vice President, Global Professional & Financial Risks
T: +44 020 7933 2478
E: vanessa.cathie@uk.lockton.com

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.

LOCKTON
UNCOMMONLY INDEPENDENT