CYBER CRIME CLAIMS CASE STUDIES

Phishing scam

The financial controller of a small high street law firm received a call from someone purporting to be from the firm's bank, advising that some suspicious wire transfers had been flagged on the business account. The caller insisted that the firm may have already had funds stolen from their account and were in immediate danger of all of the remaining funds being drained unless they put a freeze on the account, for which the bank would need to be told the password and pin code.

Not wanting to be the cause of any further loss, the financial controller confirmed the pin code and password to the caller, who then confirmed that the freeze had been successfully applied and that they would be in touch again once the situation was resolved. Upon calling the bank the next day to check in, the financial controller was told that the bank had not in fact been in contact and that $89,991 had been wired to three overseas accounts in nine separate transactions. It was now too late to recall the transactions and has they had seemingly been authorised, no reimbursement was offered by the bank.

Malware theft

Hackers sent a phishing e-mail with a bogus word document attachment to a member of the accounts team within a small firm of accountants. Upon opening the attachment, a piece of key logging software was automatically installed which allowed the hackers to gather crucial access data and then log into the firm's bank portal with the credentials of one of their users.

The insured was contacted by the bank after the hackers had initiated several wire transfers and ACH batches from the insured's account to accounts located in Nigeria. After checking with the user whose credentials had been used to instruct the transactions, the firm instructed an IT forensics company to establish what had happened and to remove the malware from the system. After managing to recall some of the wire transfers, the firm were left with $164,000 lost in theft of electronic funds and costs of $15,000 for IT forensics work.

Telephone hacking

A firm of insurance brokers recently had a new VOIP (web hosted) telephone system installed in their offices to reduce call costs. Fraudsters managed to use a piece of software to crack the password to the phone network and programmed the telephone system to repeatedly make calls to a premium rate number owned by them.

One month later, the firm was contacted by their telephone network provider to confirm that they had racked up $25,000 worth of calls. Despite confirming that they had been the victims of hacking, the telephone company insisted on payment of the outstanding bill.

Ransomware

The head GP at a private doctor's surgery switched on his computer on a Monday morning to be greeted with a message stating that every single patient record on the network had been encrypted and that a sum of $30,000 was to be paid in bitcoin in exchange for the decryption key.

The insured contacted an IT forensics firm who confirmed that the level of encryption meant that it was going to be almost impossible to access the data without the encryption key and that the only other alternative was wiping the network of the ransomware which could lead to all data files being deleted. It had been a week since the last software back up, meaning critical patient data would be lost - and so the ransom was paid. Forensics were then engaged to remove any remaining malware from the network at a cost of $10,000.

CEO Fraud

A fraudulent yet almost identical looking e-mail address for the Managing Director of a medium sized building contractor was created by fraudsters who used it to instruct an individual in the accounts department to make a wire transfer payment of $50,000 to a new materials supplier. The e-mail stated that the new supplier was being used to source additional materials for a crucial job and that payment had to be made urgently to secure delivery of the goods.

The e-mail was sent whilst the MD was on holiday so that no face to face verification could be made. The account to which the funds were transferred actually belonged to the fraudsters who were able to retrieve the money before the transaction could be recalled.

CYBER CLAIMS CASE STUDIES
CANADA

CFC INSURED #1 (2016)
An Ontario healthcare clinic released paediatric medical records to the non-custodial parent of a minor. Investigative costs have totalled $10k CAD to date, and are expected to increase with notification costs.

CFC INSURED #2 (2016)
A Canadian consulting firm lost $20,000 in funds after an employee transferred over money to the "CEO", a classic phishing scam.

CFC INSURED #3 (2016)
An Ontario brokerage knowingly wired funds to an unauthorized third party; coverage was denied as a cyber crime option had not been purchased.

CFC INSURED #4 (2016)
A community living centre in Ontario had their systems locked down by a hacker trying to extract funds from the insured to avoid compromising the system – total costs TBD.

HEALTHCARE FACILITY (2014)
To date the largest healthcare cyber claim in Canada. The theft of an unencrypted laptop of one of IT vendors containing the private health information of 620,000 patients resulted in an $11M class action suit.

PROFESSIONAL ASSOCIATION (2015)
A successful phishing attack in September against a professional association in Alberta yielded members' names, emails and ID numbers. The association has 75,000 members, but has not reported how many names were exposed.

RETAILER (2015)
A Calgary liquor store paid a ransom to regain access to its computers after hackers infected its database with ransomware. The store ended up paying $500 in Bitcoins (approx. $400K CAD) to ensure they did not lose their data.

FINTECH COMPANY (2015)
A Bitcoin exchange company closed its doors after discovering an outdated database of theirs had potentially been compromised. Their decision was based on the reputational harm alone, with no actual proof of records exposed.

HEALTHCARE FACILITY (2015)
The organization lost an unencrypted USB drive with information on 9,000 employees, a third of which included SIN's.

WHY CFC?

CFC is the UK's largest independent MGA and was one of the first Lloyd's backed MGAs to underwrite cyber. Our policies benefit from an A+ security rating (Standard & Poor), and we insure over 20,000 cyber clients in more than 20 countries globally. We are proud to have the largest team of dedicated cyber underwriters in the London market, and focus on providing exceptional service to our broker partners worldwide. Our dedicated claims handling specialists manage all claims in-house, working closely with our network of local Canadian partners and global experts.

INSURANCE CONSIDERATIONS

Businesses today face a wide range of exposures and require a cover that adequately insures them against those risks. Our cyber and privacy liability policy is designed to address the many aspects of modern business operations:

- Full retroactive cover
- Entity wide coverage
- PCI fines/penalties
- Coverage for cloud computing providers
- Worldwide coverage territory
- Breach response vendors
- First party limits
- Systems business interruption
- Incident response teams
- Cover for portable media devices
- Affirmative coverage for healthcare records
- Social engineering fraud

CONTACT US

Cyber team mailbox	cyber@cfcunderwriting.com
Lindsey Nelson, Cyber Underwriter	lnelson@cfcunderwriting.com
Joe Duplock, Cyber Underwriter	jduplock@cfcunderwriting.com