Munich RE

Cyber attack

Loss bulletin

Risk Solutions

The Boiler Inspection and Insurance Company of Canada

390 Bay Street
Suite 2000
Toronto, ON, M5H 2Y2
Tel: (416) 363-5491
munichre.com/hsbbii

Connect with us

HSB BI&I

Disgruntled ex-employee hacks transportation firm's system

A transportation contractor failed to change passwords after a disgruntled employee left. Shortly afterwards, the system began to act erratically: crucial software programs were unavailable and large amounts of data appeared to have been deleted.

The firm's I.T. contractor spent 30 hours recovering electronic data from damaged storage devices. Not all of the data could be recovered, however, so the firm paid to have some of its historical records, still maintained in paper form, inputted manually.

The contractor spent 45 hours reinstalling software, re-configuring the firm's servers and repairing other damage to the firm's computer system. In addition, the firm replaced various pieces of cargo tracking software that had been damaged or destroyed.

Business income was lost over the course of several days while systems issues were being addressed.

A public relations firm was hired to help it communicate with its customers about the incident.

Insured losses: $43,850

Equipment dealer's virus infected external customer computers

The customers of an equipment dealer received strange emails appearing to have come from the firm. Worried, the firm's owner called an outside I.T. consultant who investigated and fixed the problem. The dealer's computer had been infected by a virus, but it had been easy to remove. The consultant left a bill for $200.

Several weeks later, the dealer received a lawyer's letter alleging a customer had been infected by a virus received in the email message sent by the dealer. According to the letter, the former customer had suffered a variety of different kinds of harm related to the virus and had incurred significant cost to have the virus removed.

The equipment dealer engaged an attorney of its own and, by the time the matter had been resolved, the dealer had written a $30,000 cheque to settle the dispute with the customer, while its own attorney had left a bill for $18,000.

Insured losses:
- First party: $200
- Third party: $48,000

Property management firm's virus infects client

A property management firm learned its systems were infected by a virus when a client reported receiving a strange email from the firm.

I.T. consultants spent two hours investigating and fixing the problem.

A month later a former client alleged it had suffered damage by a virus received in an email attachment sent by the firm.

After stress-filled weeks of negotiation, the firm settled the dispute for $30,000. The property manager's attorney billed the firm $7,000.

Insured losses: $37,000

Small law firm becomes victim of mass-injection attack

Hackers gained access to the servers running databases behind the website of a small law firm.

The firm learned of the attack when Google notified that the site had been infected and had blocked access to it.

An outside I.T. firm was hired to find and delete the malicious code—three times. The first two fixes lasted only a week before the infection recurred.

Insured losses:
I.T. work and lost business: $16,000

Sales training firm website attacked

A firm providing on-line and in-person sales and marketing training discovered its website had been hacked.

The website had been rendered unusable, displaying a threatening message demanding an unspecified amount of money.

The attack forced the company to shut down its site for six weeks to overhaul its computer system.

Insured loss:
$75,000

NOT IF, BUT HOW