TRAVELERS

CYBER

Cyber risks for small business

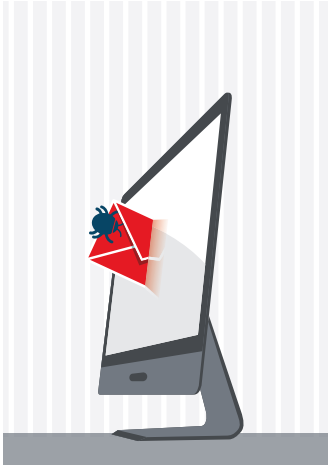
SELECT ACCOUNTS

Data breaches have become a common risk for just about every type of business, large or small. What might have once seemed like a high-tech caper targeting high-profile establishments has become an everyday crime thanks to the proliferation of electronic records, mobile devices, e-commerce and a thriving black market for personal information. Consider how these common scenarios can quickly became a cyber event for just about any type of small business.

A DANGEROUS ATTACHMENT

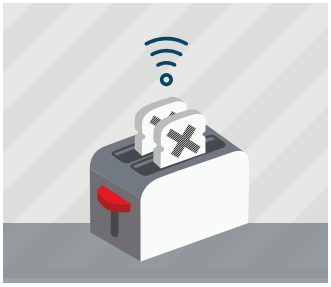
An employee of a company that manages payroll and personnel data for other businesses unknowingly opens an email attachment containing a virus. Malicious code infiltrates the computer network and provides unauthorized access to the system. Concerned about the impact to its data, the firm hires a computer forensic investigator, a specially trained professional who works with law enforcement agencies and private firms to retrieve information from computers and other types of data storage devices. The investigation confirms that personal data of the firm's own employees and that of its clients have been compromised – including names, addresses, Social Security numbers, dates of birth and bank account information.

Between the costs associated with investigating the breach, notifying affected individuals and hiring a PR firm to help with damage control, this malicious email could cost the business tens of thousands of dollars, if not more.



THE BURNT TOAST OF THE TOWN

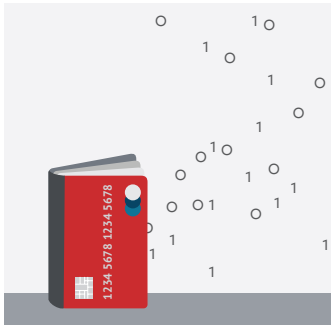
An IT company that manages network and security software saw its fame turn to infamy when a hacker breaks through the company's security software. As news of the breach spreads and the credibility of the company is called into question, the business quickly finds itself in full crisis mode. Fortunately, the IT firm carries cyber insurance. The coverage provides reimbursement for the cost of hiring a PR firm and crisis management consultants to help restore the company's reputation and keep the business running smoothly.



A SIMPLE TRANSACTION JUST GOT COMPLICATED

A bookstore owner receives a phone call from a credit card company and learns that hundreds of credit cards used legitimately at her store have been compromised. It is suspected that hackers successfully penetrated the bookstore's point-of-sale system.

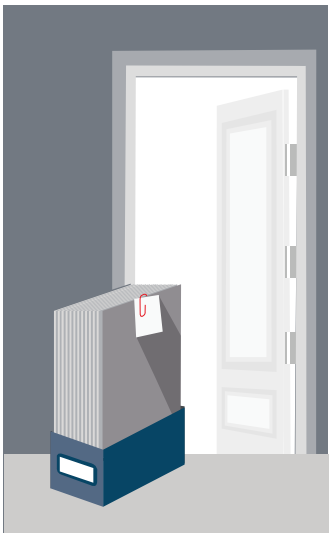
To understand what happened, the bookstore hires a certified forensic consultant to examine the point-of-sale system and related infrastructure. Additional costs pile up as the business notifies a long list of impacted customers. To make matters worse, an angry patron initiates legal action, requiring the bookstore to retain counsel to handle the matter. An event like this can cost tens of thousands of dollars, if not more.



ANOTHER REASON TO FEAR PAPERWORK

A tax accounting firm takes its security very seriously and does everything by the book: firewalls, strong passwords, data security training for employees – the whole deal. They know how important it is to maintain a trustworthy reputation with clients and prospects. Then the unthinkable happens: a large number of fraudulent tax returns are filed by individuals masquerading as the firm's clients, and now its reputation is on the line. The firm hires an investigator to determine what happened. It turns out that a box of W-2 forms – records they are required to keep – was stolen as it was being moved to storage. This single box of old papers was a data breach disaster, full of client names, addresses and Social Security numbers – everything the thieves needed for a successful identity theft heist.

The costs aren't trivial: forensic investigators to identify the cause of the breach, notifying clients of the mishap, legal fees, and a consultant to help manage the message. When all is said and done, the math on this box of old papers can easily top six figures.



ROAMING DATA CAN BE QUITE EXPENSIVE

An ambitious, hard-working employee of a financial planning firm takes his laptop home, with the goal of catching up on a mountain of work over the weekend. It's been a few weeks of long hours, and the quiet commute home offers a great opportunity for a nap. Upon arriving home, the employee realizes he left his laptop on the train. The laptop contains an unencrypted database of over 500 client records – including financial data, Social Security numbers and other personal information.

An honest mistake leads to the need for costly corrective actions, including notifying affected clients and offering to pay for credit monitoring services. In addition, the firm hires a PR consultant to help smooth things over with clients. Replacing the lost laptop was a minor price to pay compared to the cost of dealing with data breach fallout and a tarnished reputation.

TRAVELERS

travelers.com