Sweat the Small Stuff

Eduard Goodman
Attorney, Privacy Expert and Chief Privacy Officer IDT911

Losing USB flash drives, using weak passwords and having unprotected networks are among the everyday scenarios that make up most data security breaches. Still, small and mid-size companies appear not to be sufficiently prepared to avert the potentially costly effects of cyber exposures.

When companies think about privacy breaches, the first thing that comes to mind is the classic hack attack against a global corporation. But the bigger threat comes from breaches at smaller companies in the form of a mislaid thumb drive, a stolen laptop or a weak password. In fact, most data security breaches and other cyber exposures are the result of benign, everyday scenarios.

This should not come as a surprise considering that 55% of small and mid-size businesses (SMBs) allow employees to use devices like USB flash drives, but only 23% encrypt customer data, notes a recent study by Symantec.

Dianna Fioravanti, vice president of sales, distribution and underwriting operations at Economical Insurance in Waterloo, Ontario, says that a variety of other, equally ordinary events, such as unprotected networks and breaches, also can put SMBs at risk.

Mobile computing and social media rank high on companies' list of concerns when it comes to risks in the cyber world. But for all these worries, 66% of SMBs polled reported that they would not even know if they had suffered a breach, and fewer than a third (31%) have procedures in place should a breach be discovered. The confluence of risk and lack of preparation is a recipe for disaster.

"I think there's a lot of education around this that needs to be done," Fioravanti says, adding it is imperative that brokers have the tools and information they need to assess and manage their clients' cyber liability risks.

Companies in Canada may not have as many widely publicized cyber exposures as their counterparts in the United States, but that does not mean they have not learned a few lessons from their southern neighbours. It appears the Canadian market has been closely watching what has

Illustration by Greg Hargreaves/www.threeinabox.com

been going on in the United States. Not only does that mean that SMBs in Canada are now more attuned to the potential for privacy breaches, it could also translate into additional compliance mandates from both provincial and federal governments to get in front of what is certainly a growing issue.

The regulatory environment is likely to move toward a mandatory notification requirement in Canada, making it even more critical for firms to have proactive protocols and breach response plans in place.

The main areas of concern in the cyber realm for Canadian businesses are not materially different than those of firms in the U.S. and even the United Kingdom, says Nowell Seaman, manager of risk management and insurance services at the University of Saskatchewan in Saskatoon, and a member of the Risk and Insurance Management Society, Inc.'s board of directors.

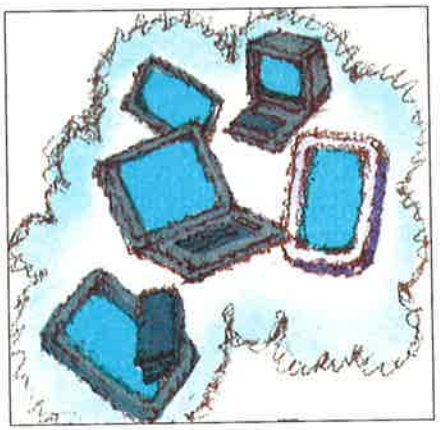
"All firms — whether you're large, small, non-profit or for-profit — should be very concerned with protecting their customers' and users' data and privacy," Seaman says.

But the increasing reliance on IT systems to conduct business and support daily operations, including taking payment information and storing sensitive data, makes the need for a secure and robust technology architecture of even greater importance than it was 10 or even five years ago. Because customers need to be confident that their information is protected, and companies need to know their technology tools will continue to bring money in the door, any systems that have been compromised "would be a very great concern," Seaman says.

SIZE MATTERS

When it comes to privacy breaches and data security concerns, a company's size may be a telling indicator of its risk. A recent study conducted by Verizon and several international security partners shows that larger organizations are less likely to suffer breaches caused by the "exploitation of default or guessable credentials" — Does 1-2-3-4-5 sound like a familiar password? — and "exploitation of insufficient authentication" — such as networks that do not have any passwords.

In addition, the wide availability of automated hacking programs may increase the odds that an SMB will be a victim when a larger company will not. "The amount of effort big companies put into detecting and repelling these programs, using similarly automated defence systems, is staggering," Seaman suggests.



A recent study conducted by Verizon and several international security partners shows that larger organizations are less likely to suffer breaches caused by the "exploitation of default or guessable credentials." Does 1-2-3-4-5 sound like a familiar password?

SMBs typically have fewer resources available to respond to cyber exposures, not only in terms of in-house technology tools and expertise, but also the amount of money they can funnel into breach response. Fioravanti says that SMBs are more likely to need insurance coverage to address things such as the cost to notify customers and to conduct an investigation to determine the extent of the exposure.

There are also less tangible implications that may be more damaging to smaller organizations. "If a large company experiences a breach, its major risk is either the total cost of handling the breach or the potential cost of a lawsuit," Fioravanti explains. "The major risk that an SMB faces is going out of business because customers decide to take their business somewhere else. It's that reputational loss that's really a concern for the small to mid-size businesses."

COVERAGE OPTIONS

As technology platforms have become more sophisticated and companies rely more heavily on them to do business, the insurance industry has responded with improved coverage options. Brokers who may have struggled with client pushback in the past might find more success with today's more comprehensive solutions.

"The cyber insurance products have evolved significantly in the last decade," Seaman points out. "The products and the types of coverage they're offering now seem to be more consistent from provider to provider, and they are filling very important gaps."

Exclusions in traditional policies make the latest dedicated breach coverage options an even better value to SMBs, especially when viewed against the potential cost of an exposure.

Not only were the cyber liability policies of old typically less robust than today's offerings, Fioravanti says many of them were also too expensive for the SMB crowd. Coverage was historically aimed at "larger, global companies, with prices starting at $25,000," she reports. That was prohibitively high for the vast majority of small firms.

Today's products have a much lower barrier to entry, and Fioravanti says that when SMBs compare the price point to the risks they potentially face should a breach occur, "it's a no-brainer for these brokers and clients."

The availability of affordable breach coverage in an increasingly connected world also gives agents a new tool to retain existing accounts and take advantage of new opportunities. "If a broker is not talking about this," Fioravanti says, "they're going to lose the business to somebody else who is."