Soundbytes

Your time's gonna come

If hackers and viruses don't get you first, your insurance company will

WHEN MANAGEMENT at Creative Internet Concepts, a small firm in American Fork, Utah, fired a 33-year-old employee last February for dealing in pirated TV shows and movies, they must have believed a very big risk had walked out the door. Unfortunately, the worst was yet to happen.

The former staffer hacked into CIC's network from his home PC and changed a key password, locking himself and all of the company's employees out of its computer network. The five-day shutdown cost the firm $100,000 – a big price to pay for such a simple lapse in security.

Let's face it: your organization is more reliant upon computer networks and applications than ever before. And that means an "insignificant" computer problem can inflict significant business damage. Unfortunately, most entrepreneurs continue to ignore computer security shortfalls that leave them vulnerable to system crashes, hacker attacks, virus outbreaks and even internal sabotage. If that doesn't worry you, this should: soon, your insurance company will deny coverage for any business interruption caused by a computer security or reliability problem – unless, of course, you've implemented sophisticated safeguards against such threats.

Two recent headlines show just how much damage can be done:

"Computer glitch disrupts Air Canada Jazz"
–National Post

"Hard drive theft affects 650,000"
–Edmonton Sun

You might dismiss these incidents as "big business" concerns. But consider what happened in each case. The day before Air Canada announced the potential sale of Jazz, the discount carrier's whole reservation system went down for six hours. The culprit? A single failed hard drive. Who'd want to buy an airline that didn't have a rudimentary backup system in place (or people who'd put one in)?

In the second case, several multibillion-dollar corporations had entrusted customer data to the company, ISM Canada, a division of IBM; all of it was on the stolen hard drive. Will companies give their business to this organization again?

A recent U.S. government study shows that, even in the wake of September 11, few small and medium-sized enterprises have implemented adequate computer backup and recovery procedures. Another survey by Gartner Group, a Connecticut-based IT-research firm, suggests most firms don't fix known security flaws in their computer applications, leading Gartner to predict that 90% of cyberattacks through 2005 will exploit holes for which a software patch will have been available.

It's easy to believe you won't be a target – after all, hackers are after big business, right? That's a mistake. In minutes I could go on the Net and download an automated hacker program, which scans the Net for unprotected corporate networks. The program doesn't distinguish between big-business and small-business systems; it merely reveals any systems ripe for hacker havoc.

Computer viruses also are equal-opportunity destroyers. Yet only a third of companies update their antivirus software regularly, according to a survey by the U.S.-based National Cyber Security Alliance, a joint business-government initiative born out of the anti-terrorism effort. Viruses don't know or care what kind of businesses they damage – they are far too dumb for that.

Which brings me to my key point: indifference to these issues might soon hurt your bottom line, even if your business is not directly victimized. In a news article shortly after one recent virus attack, Yahoo! reported that "hacker insurance... is expected to explode from a $100-million sideshow into a $2.5-billion behemoth by 2005."

If you expect any computer-related insurance coverage, including business continuity insurance, you can be sure your insurance provider will demand convincing evidence you're doing what's necessary to avoid potential problems. Without that evidence, you'll be denied coverage.

Insurers know a bad risk when they see it. If they're not going to take it, neither should you. P

Jim Carroll, FCA, is a speaker and author of 32 books, including *Get a (Digital) Life: An Internet Reality Check*. You can find him at www.jimcarroll.com or e-mail him at jcarroll@jimcarroll.com.

Safety sources

Top 10 threats and how to protect your company:
www.hp.com/sbso/advice/articles_networking5.html

Best security practices for SMEs:
www.sans.org/rr/homeoffice/best_practices.php