Globe + Mail Sept 30/99

The misconceptions surrounding on-line security



E-BIZ

JIM CARROLL

One of the most challenging issues that management must confront when it comes to the Internet and electronic commerce is the issue of security. It is dominated by myths and misconceptions.

Most executives have been pummelled by relentless, continuing hysteria over the security challenges that exist with the Internet. The result is that they've become persuaded that "Internet security" is in fact an oxymoron, and conclude that it is still far too risky to get involved with E-commerce.

Consider the all-too-prevalent myth that it isn't safe to undertake a credit card transaction on-line. This is the issue that most people worry about, whether they plan on purchasing an item on-line or building a store on the Internet.

The reality? Most mainstream on-line stores have implemented rather complex forms of encryption, which make the card number and other details inaccessible to all except those folks who might have one or two supercomputers and a fair bit of time at their disposal.

Contrast this to the situation that exists with the terminal device that is used to swipe your credit card in a department store. In that case, your credit card details are usually sent unscrambled to a bank through a regular phone line. This means that any teenager can go into Radio Shack and buy a few parts for a couple of bucks that would let them tap the line and scoff a few credit card numbers.

I don't know about you, but my money is on the kid.

Part of the security challenge with the Internet is simply a behavioural one: People implicitly don't trust technology, but are willing to place blind faith in "waiterware" each and every day. Why is it that so many people remain persuaded that it is risky to place a credit card number on the Internet, yet they think nothing of giving their card to a waiter in a restaurant? After all, that fellow could easily go in the backroom and write down the details, and then use that information for nefarious purposes.

Beyond the issue of credit cards is that of the security of computers linked to the Internet. Executives have widely subscribed to the myth that the Internet itself is inherently insecure, and that it is too dangerous to link corporate networks or resources to the Internet to take advantages of its riches.

This belief is reinforced by what seems to be a never-ending series of news stories about the latest Internet security break-ins. With so many problems reported, the Internet, and hence E-commerce, must be a dangerous undertaking.

Yet what isn't widely reported is that many of the situations where crackers have broken into Web sites or into corporate networks have resulted from the negligence of the site owner or corporate network staff.

In one widely covered event earlier this year, a fellow in Seattle advised the media that he was able to access confidential customer information at a number of on-line stores on the Internet. News stories proceeded with abandon about yet another big security breach on the Internet.

Yet further investigation revealed that the problem came about because those who built the stores didn't read the page in the book about how to properly secure the business. The thing is, if you hire a fellow to put locks on the windows and doors of your home, and he doesn't know what he is doing, your home won't be too secure. Incompetence and negligence in the implementation of software is a poor excuse for security when it comes to the Internet as well.

The fact is, it is quite possible to protect yourself to a highly reasonable degree when you get involved with the Internet and E-commerce, but this means being willing to spend money to do things right.

You can put in place sophisticated security software and methodologies that protect you while conducting business in cyberspace. You can check the validity of your security by hiring "ethical hackers" from organizations such as IBM or Ernst & Young. They'll try to break in to your system to discover any weaknesses. And you can monitor your security over the long run to ensure that you remain up to date in guarding against new challenges.

Jim Carroll is co-author of the new book Selling Online: How to be a Successful E-Commerce Merchant in Canada, *and can be reached by E-mail at jcarroll@jimcarroll.com*