

## *Keeping your Online Business Secure*

We hear a lot these days about online security. With new computer viruses breeding every day and hackers seemingly lurking in every corner of the Internet, security has become a major concern.

Security breaches can have a devastating impact on companies and their customers alike. Yet typically we only hear about security threats when large organizations are attacked. Some of the reasons for this are:

- Small and medium-sized enterprises (SMEs) don't have the resources that large companies have to monitor and enforce security – they can be attacked without realizing it
- Because they're not as visible, smaller companies can more readily cover up security breakdowns when they do happen to avoid lawsuits and embarrassing publicity
- The media and the public often overlook small business issues, even though SMEs are the engine of our economy.

Quite often, SMEs don't fully appreciate the extent of the danger posed to their companies when their operations aren't fully secure. When they're faced with a threat as nebulous as Internet security breaches, people find it hard to take it as seriously as it should be.

Yet even though the dangers may not be immediately apparent, they're no less real. Any responsible business understands the need for property or liability insurance. Putting IT security measures in place is simply another kind of insurance.

As a general rule of thumb, SMEs should expect to spend up to 25% of their technology expenditures on security and privacy. They are a critical part of the business planning process, and how seriously you take them is a measure of the credibility of your business.

To make your IT operations secure, you need a well-thought-out strategy. It's not rocket science, and much of it is based on good common sense. When you're mapping your strategy, keep these points in mind:

1. **Training your staff** – the most overlooked, and potentially most critical, of all security-related issues
2. **Physical security** – make sure all entry points are secure, as well as your computers and other hardware, using devices such as wall harnesses, attachments and alarms
3. **Policies and procedures** – have data usage and recovery practices in place, and review them frequently
4. **Hardware security** – includes lockable hard drives and BIOS boot-up passwords
5. **Software security** – for your operating system and all critical applications
6. **Communications** – e-mail and the internet can lay your IT system wide open to any number of threats if you're not prepared
7. **Databases** - internal and customer data is the lifeblood of your enterprise, and if it's corrupted or destroyed through accident or attack, you're toast
8. **Document and record-level security** – includes simple measures such as password-protecting Word documents or Excel spreadsheets
9. **Network security** – firewalls and intrusion detection tools don't let intruders get past your own network's doorstep
10. **Security of the backups** - data backups can be copied or stolen if they're not kept in a secure environment.

How important each of these issues is depends on the business you're running, and how you interact with your customers. Most businesses need to address at least some of these concerns. But regardless of the security strategy, if it's to be effective it must be properly documented, monitored and implemented.

A small business shouldn't be any more vulnerable to security breaches than a large one. After all, it's much easier to secure a small enterprise. All that's needed is information and education – and commitment.

*Claudiu Popa is an e-business management and security specialist at Informatica Corporation in Toronto. He can be reached at [questions@info-corp.com](mailto:questions@info-corp.com).*