

Security Matters

A Magazine For Small to Medium-Sized Businesses

[Home](#)

[Subscribe](#)

[Links](#)

[Advertisers](#)

[Advertising](#)

[Conte](#)

Resource Centre

[← Back to Retail articles](#)

[What's New](#)

[Security News](#)

[IT Security](#)

[Data Protection](#)

[Product Previews](#)

[E-mail Security](#)

[Business Continuity](#)

[From the Experts](#)

[Q & A](#)

[Corporate Security](#)

[Access Control](#)

[Video Surveillance](#)

[Industry/Sectors](#)

[Commercial](#)

[Retail](#)

[Manufacturing](#)

[Residential](#)

Offense is the best form of network defence

Emerging threats are forcing many businesses to rethink their IT security.

By Stephen Ibaraki

Defending the network against outside threats continues to be a priority for Canadian businesses and the use of anti-virus software and firewalls has become the corporate norm.

As vital as these tools are, however, it's also important to remember that security is not static. Companies need to go on the offense to proactively defend against an increasing array of malicious attacks. Indeed, the threats facing networks are constantly evolving. True, the viruses and worms that seemed so prevalent in the late 1990s haven't gone away. Rather, hackers have added more sophisticated forms of attack to their bag of tricks.

While many attackers were once driven mainly by vanity — to see their creations wreak havoc on the Internet — this motive is changing to one of personal and financial gain. They're employing tactics intended to easily slip past the network and dupe people into sharing personal or sensitive information. For example, "phishing", the process by which an e-mail message, typically delivered as spam, appears to come from a trusted third-party, such as a bank. The message invites an unwitting reader to submit personal data. Once received, this information can then be used by hackers for monetary or other nefarious gains. This shift toward so-called "social engineering" attacks are designed to bypass your defence software by taking advantage of human nature.

To protect against this mix of traditional and emerging threats, businesses must ensure that they are taking the necessary measures to properly defend their networks and their people. The following steps outline how organizations can go on the offense to help shore up their defences:

Think beyond "the wall." Businesses often talk of erecting a barrier around their network to help keep it safe, but this notion can be misleading. Employees using mobile devices to stay in touch with customers or colleagues may extend your network beyond your four walls. Think about all your devices in a secure context when putting together your security strategy, and ensure staff has the means to login remotely in a way that minimizes risk.

Remember the Five Ps: With security moving away from malicious code and toward people, it's critical to remember that security is about more than just technology. Microsoft often talks about the 5 Ps — protection, policies, processes, people and partnerships. One could also add 'proactive' because proactively educating your people about how to work in a way that supports security best practices — whether it's recognizing social engineering attacks or knowing how to craft a password — will strengthen your defences. Also, putting in place clear security policies and guidelines for everyone to follow will help ensure they don't become unwitting victims of hackers.

Find the right vendor and partner: Staying abreast of security trends is challenging enough for the world's largest companies, let alone mid-size businesses, which may have relatively fewer IT resources at their disposal. Check with your software vendor to ensure you are taking advantage of all the security features and resources available in the software you're currently using, such as instant updates or automatic distribution of patches. Also, consult with security experts — whether in the community or a trusted technology partner — to help you craft a security policy that meets your needs.

Where's the weak spot? As the old saying goes, you're only as strong as your weakest link. The same goes for your network. Businesses may invest heavily in protecting sensitive areas, only to leave other areas under-protected. Be sure to balance your defence across the entire infrastructure. An integrated, end-to-end security strategy is more likely to provide the best protection.

Most businesses accept that implementing a security plan is an important part of an overall business strategy. Comprehensive plans go beyond technology, accounting for people and policies, and are updated and revised on an ongoing basis. Taking a proactive approach to defending your organization and remember these critical success factors, will help build a lasting secure culture that will provide a stronghold for years to come.

Stephen Ibaraki is the national president of the Canadian Information Processing Society (CIPS) and a Microsoft Most Valuable Professional with more than 30 years of industry experience