with Brent MacLean

SECURITY TRENDS TO WATCH

In 2010, social networking sites, dedicated phishing attacks and exploitation of people's economic status are just some of the dangers companies must watch and plan for when they examine their IT security strategy

Security has become synonymous with life, particularly when it comes to our increasing use of technology. Whether you are using a Microsoft Word file or surfing the Internet, the potential for virus, malware, spyware, identity theft or just plain destruction of information has become a real threat to our computing experience.

As such, computer security is an inherent philosophy that must be integrated into every computing environment, whether it is at home or business. Hackers, crackers, script kiddies and espionage are real threats and will continually evolve and expand at an alarming and exponential rate.

More and more of the "invisible bad guys" want access to our individual systems and collective corporate networks, and as our society's economic troubles continue (e.g., unemployment rises), we see the continued exploitation of the financial crisis to scam people with fake financial transactions services, bogus investment firms and fraudulent legal services. Here are just some of the more important cyber crime trends to watch out for in 2010:

- **Social Networking Sites.** Cyber criminals no longer deliver threats solely via spam. They are taking advantage of sites like Facebook and MySpace.

- **Personalized Threats.** Continued expansion of malware in languages other than English. Cyber criminals have come to realize that by diversifying into a global market they can access even larger pools of valuable identity and confidential information.

- **Targeting Consumer Devices.** We expect increased attacks involving USB sticks and flash memory devices used in cameras, picture frames and other consumer electronics.

- **Security Software Scams.** The malware underworld is using mail stream practices in an effort to "sell" security software that is either misleading or outright fraudulent.

- **Abusing Free Web-Hosting & Blogging Services.** Websites, such as Geocities, Blogspot and Live.com allow anyone to create a public website for free, without the authentication necessary when purchasing a domain name website. This gives spammers the opportunity to run their underground business with minimal expense. Spam from do-it-yourself social-website-hosting providers arrives at its destination with far greater frequency than links pointing to domain names assigned by legitimate registrars.

- **Browser-Based Attacks.** Cyber criminals will increasingly attack via web browsers as they are the least protected and therefore, easiest way to transfer malware.

- **Breaches of Confidential Data.** Information that is managed by partner and subsidiary companies of bigger companies will be exposed more frequently, forcing an overhaul of data security practices.

- **Localized Phishing Campaigns.** Online scammers will increasingly target specific communities, especially on university campuses, where professional looking e-mails claiming to be associated with the school's financial or scholarship department will be blasted to all the students at the school.

- **Increase in Forging and Abuse of Free E-mail Services.** The free e-mail services have started to allow accounts to send mails with arbitrary "from" addresses. This has increased the usability of these services significantly to businesses, but has also increased the "abusability" by spammers.

Today, cyber crime and Internet fraud are extremely high profile, although detecting and enforcing these novel and destructive criminal activity continues to pose enormous challenges for traditional and conservative forensic techniques and business intelligence technology.

This has now become a daunting task for computer forensic analysts, as the volume of data that has now come into play is of such magnitude that it is crippling to most contemporary analytical tools. One possible solution is educating and enforcing the human component to help minimize the destruction until technology comes up with faster, more reliable avenues to catch up to this cancer that is infecting our nation at a remarkable rate. ■

Brent MacLean is the founder and CEO of J.B. MacLean Consulting (www.jbm.net) and Canadian Intelligence Solutions. He has more than 22 years of experience in network, security, and infrastructure design and troubleshooting.