Cyber-Enemy at the Gates
By Elaine Wiltshire
The Bottom Line, Volume 23, Number 3, March 2007.
http://www.thebottomlinenews.ca/index.php?section=article&articleid=242

Accountants can play a critical role in driving the security of information, said cyber-security and terrorism expert Andrew Colarik.

Colarik, a Brunswick, Ohio-based author of several books relating to cyber-terrorism, said the security of critical information should be considered in the valuation of a company, just like other assets.

“I would suspect that as more and more companies are breached, it’s going to be part of the equation in valuation,” he told The Bottom Line. “Accountants could actually incorporate that to move the security agenda forward.”

Accountants should be “encouraged to create some kind of valuation or devaluation for security,” he said.

But, according to Toronto accountant Philip Maguire, Colarik’s theory might be missing the mark.

“I’d like to see how you could measure that,” said Maguire, a speaker with the Institute of Chartered Accountants of Ontario and partner at Caledon Mills Consultancy.

“It’s very difficult to measure how (the value) would be effected, particularly if the company has taken steps to address the weakness,” he said.

“If (a security breach) happens next month and the month after next, clearly yes, I would agree that you could ascribe or attribute some value – or devalue – to the company.”

However, recent security breaches could show Colarik may be more in line with the future of valuation.

Maguire said, “When accountants are devaluing a company, they need to look at the marketplace and see whether the market has devalued the company.”

In the case of the recent security breach at TJX Cos. (see related story, Holiday Hackers, page 16), it seems the market has done just that.

Prior to the announcement of the security breach, TJX’s stock hovered just under $30 a share. On January 18, the day of the announcement, the stock price dropped to $29.50 – realistically, not a large hit.

But on February 1, the day after a class action-lawsuit had been filed in the U.S. against TJX after specific cases of credit card and debit fraud had been directly linked to the breach, the stock price tumbled an additional 3.7 per cent, falling over five percent in one week.

Although this price is still on the high-end of the 52 week trend, could this indicate marketplace sentiment with regard to security issues? Are security breaches becoming a real financial threat?

“Your company name is worth more than what you sell,” said Colarik. “If you lose that, you’re done.”

Cyber-attacks can damage more than just a single company. A large-scale attack by a co-coordinated terrorist group could potentially affect a national economy.

“In my definition of cyber-terrorism, there has to be physical harm,” said Colarik. But “economic harm is also part of (a cyber-terrorism) plan.”

Cyber-terrorism has become synonymous with many different types of computer attack, including hacker assaults and industrial espionage – crimes that have fundamentally skewed the original definition.

“There is no cyber-terrorism without terrorism – period,” Colarik said. “If you disconnect the two terms then you have a large net catching lots of dolphin and fish instead of the sharks.”

He said cyber-terrorism must be a “premeditated, politically-motivated criminal activity.” This definition then excludes a disgruntled employee who plants a virus on a company’s computer network or a ‘cracker’ illegally revealing software source codes. The hackers and crackers may be cyber-criminals, but they are not cyber-terrorists.

According to Colarik, cyber-terrorism is more about “facilitating terror” and is being used as a tool to further the terrorist agenda rather than a threat on its own. It’s about communication, co-ordination and intelligence gathering.

“As their skills continue to increase (and they will), cyber-terrorists will commence assaults on high-value targets through the interception of confidential communications, the modification of critical data resulting in physical harm, and the denial of resources in times of crisis used in conjunction with physical attacks,” warned Colarik in his most recent book, Cyber Terrorism: Political and Social Implications.

If the 9/11 attacks had been executed in conjunction with a cyber-attack that disabled medical communication or crippled cellphone networks, the death toll that day could have escalated dramatically, said Colarik.

At the end of 2006, the U.S. government issued a warning that al-Qaeda was calling for denial-of-service attacks against online trading and banking websites. Although nothing came of the threat, it indicates that the terrorist group is exploring the notion of a cyber-attack.

Real protection may be more difficult to achieve than many people realize, said Colarik.

“There are things you can do,” he said. “But the Internet and cyberspace is a collection of dependencies.” Security is dependent not only on individual businesses but their partners, vendors, suppliers, employees, etc.

“In the coming years, organizations will discover that protecting systems through redundancy alone is only effective if the foundational systems are secured. Communication networks can only be protected against attacks if all stakeholders participate,” stated Colarik in his Managerial Guide for Handling Cyber-Terrorism and Information Warfare (co-written by Lech Janczewski of the University of Auckland, New Zealand).

Accountants can play a critical role in protecting a company’s information as advisors and consultants.

Accountants can work with the internal controls of a company to “ensure there is an appropriate IT control environment,” said Maguire.

Both Maguire and Colarik strongly agree that every company should have an information security policy in place and that reviewing it on an ongoing basis is critical.

A security policy is “something that needs to be continually revisited and continually assessed,” said Maguire.

“It’s not like an accounting policy for bank reconciliations, where you can just do it once and leave it. It’s something that needs to be monitored.”

Cyber-terrorism is no longer simply for the pages of a bestselling novel, it’s a real threat with the potential for catastrophic results and everyone in business plays a significant role in protecting a firm’s most valuable property – information.