The slippery slopes of attack and defense

By donalee Moulton

Since 1995 when *Hackers* and *The Net* hit the big screen to popular and critical acclaim, Hollywood has been hammering home the dangers of hacking to box-office success. Truth it appears is not stranger than fiction.

The reality is that cyber threats, breaches and intrusions are all too real. According to a special report prepared by the London, England-based International Cyber Security Protection Alliance Ltd. (ICSPA), on the impact of cybercrime on businesses in Canada, 69 per cent of the 520 businesses surveyed said they had experienced some kind of attack within a 12-month period. In all, 5,866 attacks were reported -- 16.5 attacks per company.

The numbers are not surprising, says George Butters, a certified ethical hacker and chief executive officer of New Media Drive in Fredericton, N.B. “Cybersecurity is an arm’s race. In fact, many refer to it as whack-a-mole: as soon as you stop one threat, another pops up in its place.”

Indeed, high-profile cyberattacks have been front-page news over the past few years. Foremost among those is Target, which crumpled under a malware onslaught from a hacker who infiltrated the retail giant’s point-of-sale system. Data from an estimated 40 million accounts was breached along with details about roughly 70 million individuals. The incident has already cost the company $248 million in expenses. Now a federal judge in St. Paul, Minnesota, has approved a US$10 million settlement offered by Target in one class action lawsuit.

In addition to the increasing frequency and extent of cyber breaches, the risk associated with those attacks is also changing. “The impact of cybercrime has been evolving from cyber fraud to reputational risk. It’s a move from becoming a cybersecurity problem to becoming a business problem,” says Dina Kamal, a partner with Deloitte’s Enterprise Risk Services practice in Toronto.

Historically, a cyber threat has resulted primarily in financial damage, she notes. “It was very manageable. Now it is mostly reputational damage and very difficult to put a dollar sign on.”

Prevention is the best course of action. Companies of all sizes need to invest in enhanced cybersecurity to avoid a successful attack on their data and infrastructure. Such an investment is founded on acceptance of a new reality: cyber threats are only going to escalate. “People have realized they can make a lot of money through digital crime,” says Paul Hanley, KPMG LLP’s Cyber Security Services National Leader in Toronto. “You can make more money via the web and you’re less likely to get caught.”

That means companies need to be prepared. In addition to the lure of easy money, technology is constantly changing, which means a safety protocol or precaution that worked yesterday may be obsolete today. “As businesses rush to capitalize on the promise of [the Internet of Things], digital and big data technology, which inherently create the need to ensure services are provided in a secure, safe and privacy compliant manner, there will be the continued requirement to invest in cybersecurity,” stresses Abhay Raman, cyber risk services leader with Ernst & Young LLP in Toronto.

The best place to start is by addressing a key investment question: What is the best course of action? The answer is either mitigation or acceptance. “There is not third option,” says Hanley. “Ignoring [this] is not an option.”

For most companies, the investment in cybersecurity will start internally with an in-depth review of risks and threats as they are linked to key assets. What is it, in essence, that the bad guys are really after? Organizations have to assess their exposure, says Kamal, and this includes their individual risk and the overall exposure of the industry they work in. “The threats facing a government are not the same as the threats facing a hospital, which is not the same as the threats facing a bank.”

In its 2015 global information security survey, EY discusses the use of advanced cyber threat intelligence noting that different levels of threat assessment and profiling can now be done, building from the basic questions about risk. “More advanced Cyber Threat Intelligence enables you to proactively manage these threats and counter-measures,” the report states.

Be careful not to pat yourself on the back too early or too often, however. Rebuffing numerous cyber threats may not mean you’re well protected. “The constant bombardment of three to four years of numerous attacks and having to react to cyber events can easily provoke complacency,” notes Raman.

A strong record in repelling humdrum typical attacks such as phishing and plugging obvious gaps can lead organizations to think they have “solved” the problem of cybersecurity, when in reality the situation is getting worse, he says. “In reality, most organizations have been putting the foundations for adequate cybersecurity in place, not realizing that this is just the start, and the digital world requires a steady and responsive approach to investment.”

That complacency may be reinforced by the fact that most hacks will not bring an organization to its financial or reputational knees. According to the ICSPA report *Study of the Impact of Cyber Crime on businesses in Canada: Fighting Cybercrime Together*, attacks do not usually result in far-reaching negative consequences for organizations. The study found that among those business affected by some form of breach, only 26 per cent of

respondents said it had a considerable impact on their business. On average, the study concluded, only 17 per cent of cyberattacks cause some or significant reputational damage.

When an attack proves to be more than merely annoying, however, organizations need to be ready. It is essential to have the right tools and capabilities in place. The former may be easier to attain. Today many cybersecurity companies are investing more in R&D to bring optimal cyber protection to market – and they have multiple partners supporting that investment. eSentire, Inc., a Cambridge. Ont., cybersecurity services firm, recently announced that it had secured a total investment of US$19.5 million in venture capital and other funding from five partners including Cisco Investments. The equity investment will enable the company to expand its early success in cloud-based threat intelligence harvesting, sharing and automated protection.

South of the Canada-U.S. border the investment numbers are often much higher. Last year IronNet Cybersecurity Inc., a cybersecurity firm co-founded by former director of the National Security Agency and head of U.S. Cyber Command, raised $32.5 million in a Series A funding round. The capital will be used to "continue developing a comprehensive cybersecurity solution that aims to revolutionize cyber defense for the private sector," according to a release issued by the Fulton, Maryland-based company.

Such R&D is critical, says Butters. "The criminals are doing it, and if we don't, the successful cybercrimes will keep increasing in number and in scope."

Government also has a key investment role to play, notes Hanley. "Everybody needs to do their bit. The government can't ignore this. It's about working collaboratively. That's what the bad guys do."

Work is well under way, Public Safety Canada told *Forensic Accounting and Fraud*. Since its launch in 2003, the federal government has invested $245 million to advance the country's *Cyber Security Strategy*, which included support for cybersecurity research and development activities. Last year an additional $142 million was announced over five years to enhance efforts to help the private sector deal with cyber threats. "This investment helped reinforce federal government cybersecurity capabilities and improve the detection of and response to continually evolving cyber threats," says Public Safety Canada spokesperson Mylène Croteau in Ottawa.

More work is under way, she adds. "We will be undertaking a thorough review of the existing measures to protect Canadians and our critical infrastructure from cyber threats."

The review will be carried out in collaboration with five other federal government departments including national defense and treasury board. Such collaboration – at all levels – is essential, says Butters. "A large part of the problem in Canada is the lack of

coordination: there is no law requiring companies to admit to security breaches; there's no centralized agency collecting and examining these attacks, which are clearly on the increase; few police officers are knowledgeable about electronic break-ins; and many of the threats are coming from offshore, which puts the miscreants outside the jurisdiction of their victims."

While cybercrime is a clear threat to business, organizations and even nation states, it is also an opportunity for lawyers, accountants and other professionals. "Canada has a severe shortage of cybersecurity talent," says Kamal. "There are not enough graduates out of school to hit the ground running."

According to the 39-page ICSPA report, less than one-third of organizations surveyed have a trained crisis management team in place to respond to cybercrime incidents, Specialists are needed in areas such as privacy, cyber forensics, and business continuity, notes Hanley. "There is potentially a big market for cyber experts."

-30-

Sidebar
Organizations not at the ready

According to Ernst & Young's 2015 global information security survey, there are three steps to ensuring a mature cybersecurity process: activate, adapt and anticipate. However, the study, which included a survey of 1,755 people from 67 countries, found that organizations are not taking the action necessary to protect their data, infrastructure and reputation.

- Only 12 per cent of respondents said that the IT security currently in place fully meets the organizations' needs. More than 65 per cent said their company is in the process of making improvements.
- More than two-thirds of those surveyed estimated that the information security budget for their company must increase by as much as 50 per cent to effectively protect the company.
- 37 per cent of respondents said their company has not prepared and implemented a data protection program. In 2014, this figure was 34 per cent.

-30-