CYBER CRIME CHRONICLES

Brent MacLean www.jbm.net

Putting Cyber-Crime on ice!

Cyber-crime prevention can be straight-forward, when armed with a little awareness and common sense; many attacks can be avoided!. In general, online criminals are trying to make their money as quickly and easily as possible. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target. The tips below provide basic information on how you can prevent online fraud.

* Keep your computer current with latest patches and updates.

* Make sure your computer is configured securely.

* Choose strong passwords and keep them safe.

* Protect your computer with security software.

* Protect your personal information.

* Online offers that look too good to be true usually are.

* Review bank and credit card statements regularly.

Keep your computer current with the latest patches and updates.

One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.

While keeping your computer up-to-date will not protect you from all attacks, it makes it much more difficult for hackers to gain access to your system, blocks many basic and automated attacks completely, and might be enough to discourage a less-determined attacker to look for a more vulnerable computer elsewhere.

More recent versions of Microsoft Windows and other popular software can be configured to download and apply updates automatically so that you do not have to remember to check for the latest software. Taking advantage of "auto-update" features in your software is a great start toward keeping yourself safe online.

Make sure your computer is configured securely.

Keep in mind that a newly purchased computer may not have the right level of security for you. When you are installing your computer at home, pay attention not just to making your new system function, but also focus on making it work securely.

Configuring popular Internet applications such as your Web browser and email software is one of the most important areas to focus on. For example, settings in your Web browser such as Internet Explorer or Firefox will determine what happens when you visit Web sites on the Internet—the strongest security settings will give you the most control over what happens online but may also frustrate some people with a large number of questions ("This may not be safe, are you sure you want do this?") or the inability to do what they want to do.

Choosing the right level of security and privacy depends on the individual using the computer. Oftentimes security and privacy settings can be properly configured without any sort of special expertise by simply using the "Help" feature of your software or reading the vendor's Web site. If you are uncomfortable configuring it yourself consult someone you know and trust for assistance or contact the vendor directly.

Choose strong passwords and keep them safe.

Passwords are a fact of life on the Internet today—we use them for everything from ordering flowers and online banking to logging into our favorite airline Web site to see how many miles we have accumulated. The following tips can help make your online experiences secure:

* Selecting a password that cannot be easily guessed is the first step toward keeping passwords secure and away from the wrong hands. Strong passwords have eight characters or more and use a combination of letters, numbers and symbols (e.g., # $ % ! ?). Avoid using any of the following as your password: your login name, anything based on your personal information such as your last name, and words that can be found in the dictionary. Try to select especially strong, unique passwords for protecting activities like online banking.

* Keep your passwords in a safe place and try not to use the same password for every service you use online.

* Change passwords on a regular basis, at least every 90 days. This can limit the damage caused by someone who has already gained access to your account. If you notice something suspicious with one of your online accounts, one of the first steps you can take is to change your password.

Protect your computer with security software.

Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defense-it controls who and what can communicate with your computer online. You could think of a firewall as a sort of "policeman" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic such as attacks from ever reaching your computer.

The next line of defense many times is your antivirus software, which monitors all online activities such as email messages and Web browsing and protects an individual from viruses, worms, Trojan horse and other types malicious programs. More recent versions of antivirus programs, such as Norton AntiVirus, also protect from spyware and potentially unwanted programs such as adware. Having security software that gives you control over software you may not want and protects you from online threats is essential to staying safe on the Internet. Your antivirus and antispyware software should be configured to update itself, and it should do so every time you connect to the Internet.

Integrated security suites such as Norton Internet Security combine firewall, antivirus, antispyware with other features such as antispam and parental controls have become popular as they offer all the security software needed for online protection in a single package. Many people find using a security suite an attractive alternative to installing and configuring several different types of security software as well as keeping them all up-to-date.

Protect your personal information.

Exercise caution when sharing personal information such as your name, home address, phone number, and email address online. To take advantage of many online services, you will inevitably have to provide personal information in order to handle billing and shipping of purchased goods. Since not divulging any personal information is rarely possible, the following list contains some advice for how to share personal information safely online:

* Keep an eye out for phony email messages. Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary. Additionally, phishing messages will often tell you that you have to act quickly to keep your account open, update your security, or urge you to provide information immediately or else something bad will happen. Don't take the bait.

* Don't respond to email messages that ask for personal information. Legitimate companies will not use email messages to ask for your personal information. When in doubt, contact the company by phone or by typing in the company Web address into your Web browser. Don't click on the links in these messages as they make take you to a fraudulent, malicious Web sites.

* Steer clear of fraudulent Web sites used to steal personal information. When visiting a Web site, type the address (URL) directly into the Web browser rather than following a link within an email or instant message. Fraudsters often forge these links to make them look convincing. A shopping, banking or any other Web site where sensitive information should have an "S" after the letters "http" (i.e. https://www.yourbank.com not http://www.yourbank.com)/. The "s" stands for secure and should appear when you are in

an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner).

* Pay attention to privacy policies on Web sites and in software. It is important to understand how an organization might collect and use your personal information before you share it with them.

* Guard your email address. Spammers and phishers sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures you will be added to their lists for more of the same messages in the future. Also be careful when posting your email address online in newsgroups, blogs or online communities.

Online offers that look too good to be true usually are.

The old saying "there's no such thing as a free lunch" still rings true today. Supposedly "free" software such as screen savers or smileys, secret investment tricks sure to make you untold fortunes, and contests that you've surprisingly won without entering are the enticing hooks used by companies to grab your attention.

While you may not directly pay for the software or service with money, the free software or service you asked for may have been bundled with advertising software ("adware") that tracks your behavior and displays unwanted advertisements. You may have to divulge personal information or purchase something else in order to claim your supposed content winnings. If an offer looks so good it's hard to believe, ask for someone else's opinion, read the fine print, or even better, simply ignore it.

Review bank and credit card statements regularly.

The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing the monthly statements provided by your bank and credit card companies for anything out of the ordinary.

Additionally, many banks and services use fraud prevention systems that call out unusual purchasing behavior (i.e. if you live in Texas and all of the sudden start buying refrigerators in Budapest). In order to confirm these out of the ordinary purchases, they might call you and ask you to confirm them. Don't take these calls lightly-this is your hint that something bad may have happened and you should consider pursuing some of the activities mentioned in the area covering how to respond if you have become a victim.

Top Canadian Cities and Cyber Crime

Quebec residents appear to be among the least susceptible to cyber crime while citizens of Burlington, Ont., were the most susceptible in a list of Canada's most vulnerable big cities, according to a report by security software maker Symantec.

The company used recorded incidents of cyber crime and per capita data on Internet access and computer spending to determine which of Canada's 50 largest cities rank most at risk for online threats like identity fraud.

Burlington was ranked the most vulnerable overall with the most incidents of security incidents, per capita, in three of four threat categories.

Burlington had the worst rates of: computers infected by malware programs, attempted infections, and rates of computers being hijacked to send out spam. Burlington was second worst behind Victoria, B.C., in the fourth category: having a computer co-opted into a so-called botnet, a global network of computers that carries out attacks.

Symantec says higher per capita access to the Internet - through home connections and WiFi hotspots - increases the risk of a city's computers being targeted. Affluent suburb Oakville, Ont., was ranked as sixth most vulnerable because of high rates of Internet access and computer spending, even though the city was 25th in incidents of cyber crimes.

The top 10 most-vulnerable cities on the list also included: Port Coquitlam, B.C., Langley, B.C., Vancouver, Calgary, Markham, Ont., Toronto, Kelowna, B.C., and Kitchener, Ont.

Montreal had the highest ranking of Quebec cities on the list, at No. 25, while seven other Quebec cities rounded out the bottom of the list in places 44 through 50.

In terms of the cities with the highest incidents of actual cyber crimes, Burlington and Victoria were followed by Langley, Port Coquitlam, Kelowna, Kitchener, Thunder Bay, Ont., Fredericton, Vancouver and Windsor, Ont.

Top Executive Security Threats

Sun Tzu, a legendary Chinese strategist born more than 2,000 years ago, taught the importance of knowing both your enemy and yourself:

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

-- Sun Tzu, in The Art of War, Chapter 3, Verse 18

Truer words were never spoken when it comes to information security. To succeed, you must know your enemy as well as your own strengths and weaknesses. The following are six issues of which executives should be aware to protect their systems.

1. Know Your Enemy

The faceless external attacker often plays the villain role in the traditional information-security drama. While such external attackers exist and are a real threat, internal misuse presents a much greater risk and must not be ignored. To truly know your enemy, you must consider and understand both external and internal threats.

2. Understand External Enemies

By definition, external enemies attempt to attack you from outside your corporate boundaries. These attackers may be teenagers in their parents' basements, miscreants in other countries or credit card thieves, among others. External enemies attack your enterprise for various reasons; some are more malicious than others. Many external attackers resemble joy riders who steal cars for the fun of it. These attackers target your network to show off their skills and expertise to their peers. While they often have little malicious intent, they can cause vast amounts of damage to your systems. Politics motivate other external attackers. They may want to deface your public Web site and use it as a venue for their political messages. Such political defacements occur relatively frequently, numbering in the hundreds per year. Other motivations include theft, fraud, corporate espionage and even cyber terrorism. External attackers must be clever to infiltrate your perimeter defenses, but experience has shown that such infiltration is possible and, in some cases, even easy. The external threat includes individual attackers manually probing and penetrating your networks, as well as highly automated attacks such as worm programs. For example, the Code Red worm attacked and compromised hundreds of thousands of hosts around the world in a matter of hours. Skilled attackers can create such worm programs with little effort. The threat from worms continues to grow, and protecting your systems against them is crucial.

3. Defend Against Internal Enemies

Many traditional security approaches concentrate on building and protecting a hardened perimeter to protect against the external threat. This approach would be sufficient if all enemies were external. In reality, concentrating on the perimeter only builds a false sense of security while leaving your organization vulnerable to attack and misuse by those who can hurt you most: insiders. Insiders know what your most valuable information assets are, where they're stored and how to access them. An insider at a credit bureau drove the success of the recently apprehended identity theft ring that stole millions of dollars from individuals around the country (see story). Not all inside enemies are full-time employees of your company. Contractors, temporary workers and former employees may have privileged access to your systems with little control over or oversight of their activities.

4. Know Yourself

In the context of information security, knowing yourself implies understanding your systems and staff as well as the security risks associated with both. If you don't know your own points of vulnerability and risk, it's difficult to protect yourself. Again, too frequently information security initiatives focus on external forces and neglect internal systems, vulnerabilities and threats. Judicious use of risk analysis tools and background checks can significantly improve your knowledge of your company.

5. Be Aware of Regulations and Consequences

Serious consequences exist for ignoring security. The regulatory climate for information security and privacy is increasing. The Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act and various other federal and state regulations are raising the security bar for corporations by requiring minimum security standards to be in place. Companies that don't comply will face significant penalties in the future. For example, a new law in California (effective July 1, 2003) requires businesses that own databases to disclose security breaches if certain personal information was or may have been compromised. Californians can bring civil actions for actual damages and injunctive relief against entities that fail to comply with the law (see story). Businesses also face the possible loss of customer confidence and revenue in the face of a successful attack against their systems. Egghead Software's widely publicized security breach led to a precipitous drop in its stock price and revenue; the business never recovered, and Egghead closed its doors not long thereafter. Customers will not buy from companies that they do not trust.

6. Protect Yourself

Rather than solely relying on perimeter defenses, such as firewalls, to safeguard your enterprise, protect each critical server and data store against misuse. By protecting valuable information assets directly, you achieve protection against both internal and external threats. Proper protection includes using technology products (such as intrusion prevention, anti-virus and access control software) as well as sound security processes (such as security policies and risk analysis). Using products and processes together to secure each critical asset yields the best protection.

Referring to warfare, Sun Tzu taught long ago the importance of knowing your enemy as well as knowing yourself. Information security is no different. Failure to understand the threats to your business and your ability to counter those threats could be catastrophic to your organization.

FIVE MYTHS ABOUT CYBERSECURITY

The Internet is the global communications and information infrastructure that provides the medium for communication and computation that facilitates the provisioning of

numerous applications and infrastructure services, including e-mail, on-line banking, data storage, and quantum computing power. It brings with it promises of economic development and prosperity, scientific discovery, increased political participation, and ever changing social networks through which we are connected in ways once unimaginable.

While many understand the opportunities created through this shared global infrastructure, known as cyberspace, few Americans understand the threats presented in cyberspace, which regularly arise at individual, organizational and state (or societal) levels.

And these are not small threats: a paper presented earlier this year at the World Economic Forum in Davos Switzerland estimated the total losses associated with cybercrime in 2008 exceeded one trillion dollars and the FBI has declared cybercrime to be its highest criminal priority. This threat is silent and stealthy and must be addressed now lest it introduce more fragility of trust in our global economy that, if left unchecked, will challenge our way of life.

The cybersecurity problem is growing faster than the solution, and in order to address the problem, we have to move rapidly along the continuum from denial to acceptance and dispel a few myths along the way.

Myth 1: Consumer protection exists in cyberspace

False. On-line holiday shoppers beware, you are your own protection. On November 30th - or Cyber Monday as on-line retailers have dubbed the Monday after Thanksgiving - the FBI warned consumers of some of the threats presented in cyberspace, including scams intended to trick us into downloading malware or divulging sensitive information. Web browsers and anti-virus software are not necessarily going to protect us. Why? Because in any given day there can be tens of thousands newly introduced viruses or malware that have a shelf life of 24 hours. Today's software simply cannot keep up. And that is not all. Some botnets, such as the Storm botnet, are used to hide phishing and malicious web sites behind an ever-changing network of compromised hosts acting as proxies. And what happens? Well, the average person holds approximately 20 online accounts for banking, internet-based mail, and social networking like MySpace or LinkedIn. The perpetrators obtain credit card data, bank-accounts, passwords and identities with which they then steal and spend your hard earned cash to support their business activities. Are consumers protected? Many companies claim that they are, but have you noticed that your credit card interest rate recently increased by five percent or more? Is this a way to pass the cost of fraud onto consumers? Further, some banks are considering making their customers responsible for protecting their smart phones and computers from becoming infected so that they cannot be used to hijack their accounts. The bottom line is that the on-line industry will find ways to pass the costs of cybercrime through to consumers, which means that it really is every man (or woman) for themselves.

Myth 2: Firewalls and virus scanners protect my computer and my enterprise

False. A recent report by the Ponemon Institute noted that 82% of C-level executives report that their organization has experienced a data breach and many are not confident that they can prevent future breaches. The bad guys are casing our networks to research and discover vulnerabilities in our software and hardware that they can then easily exploit. For instance, the United States intelligence community notes that commercially available virus scanners only clean roughly 35% of malicious code. As we race to embrace, buy, and integrate the newest technology into our lives and businesses do we really understand the vulnerabilities, exposure points, and subsequent risk that is bundled in that purchase? Attackers are exploiting these seams and are becoming more subtle in their methods. For example, multi-media devices like a thumb drive or I-Pod are often used as a delivery mechanism for malware that embeds in our computer or network and later beacons or "phones home" for orders. Sometimes that homing device asks for a map of the computer or network topology and sometimes it sends specific files to its master-controller. Few software programs protect us from the insider threat or socially engineered attacks that are susceptible to human error (like opening an attachment). What should we do? We need to stop buying point solutions or "band-aids" and demand enterprise wide secure solutions. We must increase security testing of networks to lower our operational risk. We must encourage industry to develop more secure software and force its product strengths and weaknesses to be a part of their brand integrity. Why? Our reputation, price-point, quality of service and overall business health depend on it.

Myth 3: My government has the solution and will protect me

Not really. Although the government has a role to play, and President Obama announced his personal commitment to a new comprehensive approach to securing cyberspace in his May 29, 2009 speech on this subject, this problem cannot be solved without active involvement and shared responsibility by both the private sector and other nations around the world. As I prepared the Cyberspace Policy Review for President Obama earlier this year, it became clear that the interdependencies that are shared nation to nation and company to company are not well understood. Further, details on vulnerabilities of and security threats to our infrastructures and information assets tend to be closely held secrets. It is time to knock the complacency out of the system and hold both governments and the private sector accountable for providing a secure and resilient cyberspace. What is this going to take? It takes a commitment to solve the problem followed by resources, new policies, and laws. The world is expecting leadership from the United States. As the original innovators of the Internet, the United States should use our position of strength to build out the security framework and drive the necessary change. For example, we could provide assistance to nations that ratify the Council of Europe's Cyber Crime Convention to curb the expansion of organized cyber crime. We could lean on the private sector and require all entities that provide managed information services to the federal government or providers of critical infrastructure to abide by minimum standards of care. Further, we could urge the urge the G-8 or G-20 to create a Cyber Action Task Force along the lines of the Financial Action Task Force to promote the development of sustainable information communications technology (ICT) and to combat attacks against the security and resiliency of information systems. Finally, we must find ways to create a private-

public partnership to facilitate information sharing and recovery strategies that truly underpin the availability, confidentiality, integrity and resiliency of cyberspace.

Myth 4: Physical assets are more valuable than information

False. While it is true that physical assets have a quantifiable value that can be depreciated over time, information is where the real value lies. As firms continue to embrace information technology to enable efficiency, productivity, and global connectivity, the value of information increases concomitantly and the medium by which it transits or resides matters less and less. Privacy Rights Clearinghouse, which tracks reported data breaches, reports that since 2005, more than 341,742,628 records containing sensitive personal information were involved in security breaches in the United States. Many experts believe that the rate of corporate data breaches may be at or approaching an epidemic level, even though many of those breach are never reported. After all, there is a disincentive for reporting because by the very fact of reporting the breach, it can undermine customer confidence, brand reputation, price point - all of which can lead to cancelled contracts, fines, and law suits, not to mention downward pressure on stock prices. Attacks to corporate information systems (data and infrastructure) are increasing operational risk and revenue risk but few organizations understand the linkage between IT insecurity and enterprise risk management. Corporations need to prepare for technical glitches, outages and security breaches and be able to measure, monitor, control losses. An IT disruption can paralyze a company's ability to produce or deliver its services, connect with its customers, or in simple terms operate. There are at least two bills that have been introduced in Congress this year that would establish standards for developing and implementing safeguards to protect the security of sensitive personally identifiable information (PII). Those bills are laudable for what they seek to achieve, but why limit the reporting to PII and not include breaches that result in the loss of sensitive corporate intellectual property like our next generation weapon systems or IT product lines too? Are they not just as important? We need to create a safe vehicle and then increase reporting of data breaches so as to shine a light on the problem and so that we can bring to bear all of the ingenuity and capabilities of the United States to solve the problem. Barring that, we run the risk that the world just very well may hold us accountable to Article 12 of the Council of Europe's Convention on Cyber Crime, which holds companies civilly, administratively, or criminally liable for acts committed for their benefit either by an executive or as a result of lack of supervision by the executive.

Myth 5: Laws are keeping pace with technological innovation

False. Cyberspace is evolving faster than our understanding of its opportunities and risks. Laws in the United States and around the globe are not keeping pace with the cross sector, multi-jurisdictional, multi-geographic nature of the infrastructure and services delivered through cyberspace. Laws overlap and create conflict as opposed to cooperation, even when our interests are aligned. For example, Europe's definition of data privacy and protection is much different than here in the United States. They have determined that an Internet Protocol (IP) address is private information, whereas in the United States we do not treat that as such. This is important because it limits our ability to

share and store this information across borders-even when it will lead to finding a perpetrator or attack strategy. Data ownership, data handling, data protection and privacy, evidence gathering, incident handling, monitoring and traceability, and the rights and obligations related to data breach, data transfers, access to data by law enforcement or intelligence services all need to be addressed by new laws written for the 21st digital century. For example, neither the Electronic Communications and Privacy Act nor the Stored Communications Act have been updated for Internet communications or e-services that are exponentially increasing due to IT innovations. The stringent requirements under current law for search warrants in cyberspace slow down law enforcement's ability to pursue on-line malicious activities and protect our citizens. This is important because a good portion of the world's cyber attacks are emanating from the United States. In the Cyberspace Policy Review, we identified scores of legal issues that must be addressed in order to facilitate a more secure future. Laws have not kept pace, but if we tap into the strong talent of our law schools to analyze and publish ideas on how best to modernize these out-of-date laws, we just might begin to catch up with the speed of technological innovation.

What now?

These are just five of the many myths about cybersecurity. To get past the rhetoric and start making progress, we must first recognize our vulnerabilities and then take steps to address the threats in cyberspace. And just as those threats arise at individual, organizational and state (or societal) levels, the responsibility for addressing them arise at each level too.

Working together, as individuals, industries, and nations, we can build a pathway to a safe, secure, and resilient infrastructure that will continue to support our daily lives, our national security, and the global economy. We just need to move from denial to acceptance and bury all of the myths along the way.

Article by Brent MacLean

Brent MacLean is a founder and CEO of J.B. MacLean Consulting Inc. and Canadian Intelligence Solutions Inc.
For more information please visit www.jbm.net