What every CEO needs to know about cybersecurity: A background paper

By Ray Boisvert
President and CEO
I-SEC Integrated Strategies
Executive summary

Cybersecurity is a significant challenge facing Canadian corporations and the country as a whole. Information technology (IT) underpins every aspect of company operations. The critical infrastructure that we depend on, from payment systems to the electric grid, are managed electronically. The mass deployment of information technologies has generated immense efficiency gains for the Canadian economy. However, everything that is networked is hackable. Cyber-criminals, foreign intelligence agencies, activists and others are attacking corporate and government systems with increasing speed and sophistication. The results can be catastrophic: disrupted business operations, stolen customer data, direct financial losses, compromised intellectual property, physical damage and undermined brand strength.

This paper identifies the key issues that CEOs should be aware of in dealing with cybersecurity. It is organized in a dozen short sections:

1. Examples of prominent cyber-attacks and what the perpetrators were seeking;
2. State of play on cybersecurity and how we got here;
3. Cybersecurity complexities created by the proliferation of mobile technologies;
4. Costs of cyber-attacks to major firms;
5. Individuals inside organizations who knowingly or unknowingly aid cyber attackers;
6. The major types of cyber-attacks and what the perpetrators are seeking;
7. Emerging cyber threats;
8. How companies should prepare for cyber-attacks;
9. Suggested areas of focus for companies during and after an attack;
10. Questions that CEOs may wish to ask their CIOs;
11. Dealing with cyber risks when doing business abroad; and
12. Concluding thoughts on how to mitigate cyber threats.

The two key differentiators between cybersecurity and other enterprise risks are diversity and interdependence. Many types of actors located around the globe are attacking the networks of Canadian-based firms using a dizzying range of techniques. There is no simple or single solution. Cybersecurity demands 24/7 vigilance by a skilled array of professionals, and well-established internal procedures that enable enterprises to address threats as they arise.

Traditionally, firms that have been subjected to attacks have been reluctant to talk about it, for fear of repercussions from customers, shareholders, or the legal system. Unfortunately, this makes it more difficult for other potential targets to anticipate what is coming. The grave nature of cyber threats is encouraging firms and governments to share information as never before. This is not an easy undertaking, as it breaks with established disclosure practices in both the private and public sectors. Much more work is required to ensure that the necessary procedures and protocols are in place. Yet this leap into cross-sectoral and public-private collaboration has already thwarted or reduced the severity of numerous attacks. No firm is an island. Information-sharing is central to ensuring the cybersecurity of our economy and our country.
Introduction

It was a mere 20 years ago that the Internet went mainstream. In the early days, cybersecurity was about locking up laptops holding sensitive data at night. Today, everything is networked. Technology is at the heart of our lives, and information is the foundation of the modern economy. We efficiently sell to customers across the globe. We precision-manufacture our products with electronically controlled machinery. We provide services and customer support online. Twitter is our newsfeed. Our cars, homes and electrical grid are increasingly “smart” and are being connected into the Internet of Things (IoT). The exponential growth of connected IoT devices is eroding traditional network security and opening many more potential avenues of attack.

Everything that is networked is hackable. Criminals, foreign governments, and activists are seeking to compromise company networks and steal their most valuable data. Like the web itself, these threats are global. When the bad actors succeed, they can seriously compromise core business priorities.

There is no easy solution to today’s fast-changing cybersecurity challenges. Many large companies have more devices connected to their internal networks than they have employees. The bad actors may already be inside the firewall. Deliberately or otherwise, “insiders” - employees, contractors or vendors - often play a role in cyber attacks.

Few things can so severely injure a company as a cyber-attack. The consequences can include theft of intellectual property, direct financial losses, disruption of operations, severe brand damage, physical damage to property, harm to people (through attacks on industrial control systems), and ex post litigation. Given the scale and complexity of the challenges, cybersecurity deserves to be a CEO priority.

This guide is intended to provide Canada’s CEOs with an overview of the evolving cybersecurity landscape, and possible mitigation strategies. It also identifies questions that chief executives may wish to direct to their Chief Information Officers.
Welcome to the brave new world

Many of today’s corporate leaders vividly remember Y2K. So-called “experts” predicted that at the stroke of midnight on January 1, 2000, aircraft would fall from the sky and the banking system would collapse. In fact, nothing abnormal happened that day. Most technology experts agree that pre-2000 IT investments likely prevented a number of critical system failures. To many business leaders, however, the threats appeared in retrospect to have been exaggerated and the investments were too steep relative to the risk. For many years afterward, there was widespread skepticism about the seriousness of cyber risk.

This perception has finally begun to change. The cybersecurity challenges of 2014 are sadly not exaggerated. Consider some recent incidents.

In April 2013, a hijacked Associated Press (AP) Twitter account announced that explosions at the White House had injured U.S. President Barack Obama. AP retracted the tweets within minutes, yet the stock market suffered a reported (albeit temporary) loss of $136.5 billion.

A few months earlier, in Europe, an organized crime group, likely facilitated by an insider, physically installed devices on the network at one of Europe’s busiest seaports. For months, criminals controlled important parts of the network, allowing to them “receive” and move shipping containers at will while avoiding law enforcement and scrutiny by the company.

In January 2014, the CEOs of the three South Korean credit card companies bowed in shame before TV cameras and promptly resigned. The reason? An IT contractor working for an independent credit rating firm had managed to steal 104 million pieces of customers’ personal and financial information - affecting half of Korea’s adult population. Lawsuits are now underway and greater regulations are pending.

In 2010, when BHP Billiton sought to acquire Potash Corporation of Saskatchewan Inc., hackers reportedly rifled through the networks of seven leading Bay Street law firms and various federal government departments, looking for information on the case.

Over this past holiday season, hackers launched a high-profile attack on Target Corporation, the large U.S. retailer. They stole at least 40 million customer records and compromised 70 million accounts.

One evening in February 2014, a series of well-crafted “socially engineered” emails arrived in the inboxes of senior staff of Forbes, the business media company. The moment one of those staff members clicked on a link in the email, the attackers gained access to Forbes’ internal network. One million subscriber accounts were compromised.

As these examples illustrate, the cyber world is evolving and hackers are executing attacks in new ways. A key characteristic of this new age is that the balance of power has shifted away from the defender. Today’s attackers combine immense technical prowess with dogged persistence. Some are employed by the militaries and intelligence agencies of foreign countries. Others are associated with criminal gangs based in Europe, Asia, and Latin America. Still others fall into a murky zone between the state and organized crime.
Then there are the “hacktivists”, who count corporations among their favourite targets. They range from individuals seeking to redress a perceived injustice to highly skilled and motivated activists who view corporate activities as a threat to environmental or social sustainability. “Anonymous”, the loosely affiliated international network, is perhaps the most prominent. Its members have attacked banks, government websites and other interests which it accuses of “crimes against freedom of information,” such as seeking to shut down sites that harbour pirated material. In Canada, Anonymous claimed credit for attacks in May 2012 against the Government of Quebec as part of a series of protests against student tuition increases.

Faced with such adversaries, CEOs can no longer take for granted that their companies’ assets are protected by the corporate firewall, ubiquitous virus filters and anti-spam technologies. Nor can all who have access to the network be trusted. Traditional approaches are no longer sufficient to secure the corporate ramparts or its soft internal vulnerabilities.

Today’s cyber attackers can easily collect data on company, vendor and employee practices from half a world away. Victims often aren’t even aware when an attack is in progress. An innocent-looking email that appears to have come from a friend or colleague may invite an employee to a corporate event or encourage recipients to click on a link. As soon as someone does, the hacker gains access to the system and can roam at will. In Target’s case, the attacker managed to get around the company’s defenses by stealing the network credentials of a third party.

“Criminals gained access to [Target’s] networks through a contractor that was servicing heating and air-conditioning systems at several stores”

- KrebsonSecurity.com

Canadian companies are prime targets in this brave new world. As the Canadian Security Intelligence Service (CSIS) noted in its 2014 Annual Report:

Canada’s advanced industrial and technological capabilities, combined with expertise in a number of sectors, make this country an attractive target for foreign intelligence services. Several sectors of the Canadian economy have been of particular interest to foreign agencies, including: aerospace, biotechnology, chemicals, communications, information technology, mining and metallurgy, nuclear energy, oil and gas, as well as the environment. The covert exploitation of these sectors by foreign powers as a means to advance their economic and strategic interests may come at the expense of Canada’s interests and objectives.

Beyond purely seeking profit, hackers are also seeking intellectual property. Top priorities include proprietary industrial designs, processes and practices related to resource management and information related to “valuations” that can affect acquisitions. A number of countries see cyber theft as a legitimate approach to modernization, market assurance and resource access.

And what about the threat from insiders? The cases of Bradley Manning and Edward Snowden are instructive. While Manning was in the military, Snowden worked for Booz Allen Hamilton, a firm with exceedingly high technical capabilities and knowledge of how to prevent cyber attacks. Of course, most employees are not discontented and are loyal to their organizations. Hence corporate executives must simultaneously defend their organizations against threats from without and within, while also encouraging a culture of collaboration.
**Relevant statistics**

<table>
<thead>
<tr>
<th>Who are the victims?</th>
<th>Sources of Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 37% of breaches affected financial institutions</td>
<td>• 76% of network intrusions exploited weak or stolen credentials</td>
</tr>
<tr>
<td>• 24% occurred in retail &amp; restaurant locations</td>
<td>• 69% of breaches were spotted by external parties (9% by customers)</td>
</tr>
<tr>
<td>• 20% of network intrusions hit information &amp; professional services firms</td>
<td>• 41% of cases of IT misuse relate to “unapproved” hardware accounts</td>
</tr>
<tr>
<td>• 20% of network intrusions involved manufacturing, transportation, and utilities</td>
<td>• 66% of all breaches discovered in the 2013 report took months or years to discover (around 4% took over a year to emerge)</td>
</tr>
</tbody>
</table>

Internet-enabled IP theft from UK businesses are estimated at $15.4 Billion (USD), with another $12 Billion (USD) stolen in industrial espionage aimed at contract bids.

- BAE Systems Detica report

**“More than 75 percent of organizations utilize unsecure, personal email accounts to distribute board documents, and almost 50 percent do not ensure board communications are encrypted. But 52 percent of organizations now use a board portal to share sensitive board information.”**

- Thomson Reuters 2013 Board Governance Survey

**“If you’re running critical software on an architecture that has security flaws in it, you’re eventually going to be bitten . . . . Remarkably, 75% of U.S. banks continue to use XP.”**

- CTO, Phirelight Security Solutions, discussing the end of Windows XP support
Where we are and how we got here

The digital age has changed everything, and it continues to do so at an accelerating pace.

For intelligence agencies, the Internet has opened incredible possibilities. Governments around the world are collecting mass quantities of meta-data (“data about data”) at home and abroad. Today’s Internet giants boast multi-billion stock valuations based on their capacity to mine, organize, and monetize data. Some talk of the end of privacy.

While many worry about these trends, the number of Internet-enabled devices around the world continues to grow. So many people are online and so many devices are deployed that the digital divide is fast diminishing. Moreover, the devices we carry are more powerful than ever. People now carry complete office capabilities in their pocket.

Mobile phones are the tip of the iceberg of the digital revolution. Within five years, an estimated 40 billion devices - from “smart” thermostats in your home to sensors on power plants and pipelines - will transmit information over the Internet. By 2020, the Internet of Things will generate an estimated $1.9 trillion in annual global economic output.

“The “SpyEye” malware that successfully infected 1.4 million computers worldwide, while enabling the theft of passwords and PINs, sold for as little as $1,000 per copy”

- FBI.gov

The empowerment of individuals, businesses and governments brings new risks. Information about how to undertake a cyber-attack is easily found online, and off-the-shelf “exploits” can be purchased, tailored and aimed at a target of choice. As a result, the risk environment is sure to worsen.

In the early years of the Internet, state-run intelligence and security agencies owned all significant cyber capabilities. Over time, large numbers of state-contracted proxies, sometimes outside the control of their sponsors in government, began targeting Western companies. According to General Keith Alexander, Director of the U.S. National Security Agency, in very little time the West woke up to the “greatest transfer of wealth in history”. This cyber-based crime covered the landscape of the Internet-connected economy: science and technology, defense contractors, extractive industries, manufacturing, financial services, pharmaceuticals, regulators, government policy centers, and anything linked to markets, evaluations and acquisitions.

Elsewhere, and in permissive environments where the line between government authority and organized crime is blurred, newly empowered teams of hackers have begun to take advantage of tools that used to be found only in the intelligence world.
Alongside the legitimate world of e-commerce, a “dark web” has emerged with actors who operate with a combination of counterculture motives, skills and interests. Typically their intent is to obliterate impediments to access, gaining entry to any institution or company they desire. They do so either for sport or, increasingly, to profit from stolen information, including credit cards and the personal history of employees or customers.

“Malicious hacker activity may result in a ‘cyber backlash’ where reduced consumer trust may costs business $3 trillion by 2020 in productivity and growth”

- McKinsey and Company

Those with the intent to commit terrorism for political, social or religious reasons have also not let this opportunity pass. The attackers might be isolated in a city under siege in Syria, or in a Pakistan village targeted by drones. Hostile regimes around the world have mapped critical infrastructure and key economic nodes, with the intention of disrupting infrastructure or economic systems at times of increased tension or conflict. Owners of key resources that sustain Canada’s fundamental infrastructure are therefore among the likely targets.

Hackers of all stripes have enjoyed significant success so far. Government officials estimate that 80 per cent of North America’s significant organizations have been “surveyed” by hostile actors. A recent survey by the International Cyber Security Protection Alliance (ICSPA) found that 69 per cent of Canadian businesses have been hit by a cyber-attack in the past 12 months. More than a quarter of them said that the impact of such attacks was “considerable”.


Mobile technology - growing ease, productivity and risk

Over the past three decades, technology has made many things smaller, faster and more “personal”. Computing power has moved from large rooms to desktops, laptops and now tablets and smartphones. “Wearable” devices are the next step forward in this trend. Access to data has never been more ubiquitous.

The benefits to business of the mobile revolution are widely understood. But how can companies ensure security for mobile devices and their companies?

A recent BAE Systems Applied Intelligence report notes that 70 per cent of top IT decision-makers see smartphones, tablets and other mobile devices as a “significant security risk”.

Mobile devices are easier to hack into and are typically subject to a lower level of security than personal computers. The recent Applications Security Trends Report 2014 by Cenzik found that 96 per cent of smartphones in the U.S. have at least easily 14 identifiable vulnerabilities (down only slightly from 99 per cent in 2013).

Cenzik identified a number of trends that create opportunities for hackers. These include:

- the rapid emergence of “Bring Your Own Device” (BYOD) policies;
- wider access to cloud services;
- the downloading of unauthorized applications to smartphones;
- the “continued failure of organizations to detect and address exploits around authentication, authorization and session management”;
- privacy violation and excessive privileges appearing in more than 80 per cent of mobile applications; and
- the growing number of vulnerabilities in applications shared with third parties.

Too often, mobile devices are distributed without an adequate associated risk management framework. Treating mobile platforms on par with all other facets of network or IT security is crucial.

The rise of machine-to-machine (M2M) networks will present a new set of challenges. Given the speed at which M2M threats can propagate, it is clear that companies will require new methods of intrusion detection, protection, and response that do not rely on humans.
Hard and soft costs of cyber risk

Cyber breaches tend to have both short-term and long-term consequences. In the short term, firms must thwart the breach, manage the headlines, deal with partners and customers to minimize damages, address internal staff issues and concerns, inform and respond to questions from the board, and reassure markets. Managing these elements effectively can help to contain the damage and shape perceptions about the competence of senior leadership at the firm.

However, the impacts of a major cyber breach do not end when the story slips from the headlines. The longer-term effects can sometimes be more serious, including enduring brand damage and intensified scrutiny from the media, regulators, privacy advocates, investors, and, potentially, law enforcement officials. Given the public’s growing unease about cyber-related abuses, tolerance levels for lapses in institutional preparedness or responsiveness are declining.

In the age of cyber threats, the risk profile for companies is changing. The growing number of attacks against corporations, combined with fears of future attacks on critical infrastructure, has prompted the insurance industry to reassess how it calculates insurability.

BBC News reported recently that underwriters at Lloyds of London were requiring companies that apply for coverage to demonstrate that their systems were adequately protected against cyber intrusion. According to the BBC report, “the majority of applicants were turned away because their cyber-defenses were lacking.”

A complicating factor is that companies are finding it more difficult to contain news of cyber breaches. Details of such attacks are emerging with regularity and governments are increasingly moving to mandate such disclosures through legislation, particularly when personal privacy is involved. Canada has not yet enacted formal breach notification legislation, but a bill to that effect was proposed in the last Parliament and was strongly endorsed by the Privacy Commissioner.
In the past, some took the view that it was cheaper to pay to clean up the mess after a breach than to invest heavily in trying to prevent it. Remediation, however, is no longer a viable strategy. The leaks of customer data from Target Corporation will cost the company more than $500 million simply to replace credit cards. Meanwhile, customers and small banks have filed 68 class action lawsuits, in more than 20 states, alleging that Target did not take proper steps to protect consumer data. Because the breach occurred early in the holiday shopping season, Target’s net income for the fourth quarter of 2013 fell by 46 per cent. The long-term impact on the retailer’s brand is as yet unclear.

Cybersecurity is as much about the human factor as it is about technology. A recent survey of 165,000 U.S. workers by the Corporate Executive Board found that 93 per cent of them knowingly violate policies designed to prevent data breaches. The survey also found that senior executives are the worst offenders. Another source of risk is former employees at all levels who may have the knowledge and the will to break into - or encourage others to break into - company systems. Finding ways to raise awareness within organizations is crucial.
The insider threat

During the Cold War, intelligence services, militaries and the defense industry were obsessed with uncovering “moles”. The hunt was for those believed to have betrayed society for ideological or financial reasons and sometimes to assuage egos or exact revenge.

Today, in an era of reduced corporate hierarchy, mobile communications, e-commerce, on-time delivery and open innovation - organizations tend to rely on a risk-managed approach to information access. More people than ever have access to company information. This can include co-op students, interns and “work from home” staff, to name a few. This increased flexibility can contribute to improved performance. But what are the risks? Are our risk-management frameworks adequate? Are they evolving to address new threats? What is the appropriate balance between access and security?

Context

Once inserted into a network drive, a USB stick can pull down as much as a Terabyte of data - the equivalent of 75 million pages. While performing seemingly innocuous, everyday activities, an “insider” can download everything he or she might desire, or upload a cyber-menace into company systems.

Many attacks blend electronic and physical elements. In 2012-2013, criminals used stolen bank information and increased daily withdrawal limits to withdraw cash from a variety of ATMs in New York City and defraud bank customers. The fraud cost the affected banks $45 million.

The most egregious “insider threat” events have involved highly vetted persons in positions of trust: Canadian Naval Lieutenant Jeffrey Delisle, U.S. Private Bradley Manning and NSA contractor Edward Snowden. Many insiders, however, have no idea that they are being exploited.

Threats led or delivered by an insider can inflict great harm on an organization, as insiders tend to have special knowledge and privileged access. Insiders can also recruit or use others with relative ease. Such orchestrated insider attacks are often difficult to detect. According to the 2013 Trustwave Security Report, “64 per cent of organizations took more than 90 days to detect intrusion.” To address the insider threat often requires new or more sophisticated investments in cyber defense.

Insider facts

- 80% of the malicious acts were committed at work during working hours;
- 81% of the perpetrators planned their actions beforehand;
- 33% of the perpetrators were described as “difficult”;
- And 17% as being “disgruntled;”
- “Insiders” were identified in 74% of cases;
- Financial gain was a motive in 81% of cases, revenge in 23% of cases, and 27% of the people carrying out malicious acts were in financial difficulties at the time.

- Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector, Software Engineering Institute, July 2012
The nature of the threat - a typology

Spear phishing

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are likely to be conducted by perpetrators out for financial gain, trade secrets or military information. After modeling a target from information gleaned through social media mining, telephone calls or other open information, the attacker can then send a “socially engineered” email to a victim. By posing as someone the victim trusts, he or she often accedes to the invitation to confirm an interest or visit a link to a website, accept an invitation, or see a document or photo. Once the embedded link is “hit”, the attackers access the corporate network or personal computer or device. High rates of success continue due to a focus on outside security parameters such as firewalls, while underestimating the impact of trusted, well-meaning staff within.

Watering hole attacks

A two-stage attack designed to target an industry or particular demographic. The first step is to compromise the web site where the target industry’s customers congregate (be it for online shopping or browsing). The second step is to plant malware on the website so that it can infect as many visitors to the website as possible. This type of attack has been successful using vulnerabilities on Google, Microsoft and others. As such, target areas include those that attract high-value clients or where there are high volumes of financial transactions.

Distributed Denial of Service (DDoS) and botnets

Distributed denial of service (DDOS) attacks are the result of many computers all sending traffic to the same destination. Many times these attacks are facilitated by a botnet, which is a large number of compromised computers that are under an attacker’s control and can be instructed to spew traffic at the victim site or service. DDOS attacks are a tool of choice for “hacktivists” and criminal groups. Hacktivists will use them as a “virtual sit-in” to disrupt service to corporations or government entities in order to bring attention to their cause. Criminal groups have frequently used DDOS attacks as a means to extort money from corporations (especially gambling or banking entities) that cannot afford to have their online services unavailable to customers. While there are commercial mitigation strategies that can be purchased, the tools and tactics used by DDOS attackers are continually changing.

Vendor Verification

Canadian companies rely on software and hardware products purchased from third party foreign and domestic suppliers. All vendors have their own unique standards, or lack thereof. Given that a majority of company compromises originate through such external acquisitions, buyers should invoke a “security first” approach during the purchasing process. Equally, it is essential that maintenance contracts clearly spell out how vendors will handle servicing, including “patches” and security updates - but especially “back door” access.
Exploit kits

The Black Hole Exploit Kit (and the newer Neutrino, Cool Exploit, and Angler kits) are web based tools designed to gain access to a victim’s computer through “socially-engineered” (infected) email or spam (phishing) attacks. Like normal software, they are easily purchased or rented from developers. Importantly, the technical skill required to use the exploit kits is minimal. While browsing, these “exploits” load malicious web page content into unpatched browsers. This provides an avenue to access and exfiltrate data.

Point of Sale (PoS) attacks

Any Point of Sale (PoS) system represents an important “sweet spot” for attackers — whether it is the card terminal that performs the reading or the software and operating systems that power them. In retail level attacks, a number of issues contribute to failure: a weak supply chain entry point; lack of effective monitoring and protection on the internal network; and, ultimately, a lack of good security controls on the PoS systems themselves. The current transition from a now unsupported Windows XP operating system will take time and investment. This will leave important gaps and create “soft spots” for attackers moving forward. In the interim, it is critical that companies leverage all of their regular security controls and monitoring techniques on their PoS systems. Effective network segmentation also needs to be applied so that these systems, should they be compromised, cannot exfiltrate the sensitive data they contain. Fortunately, Canada has seen a widespread deployment of debit and credit cards containing chips and requiring PINs, which has resulted in progress in deterring PoS attacks.

Supply chain attack

Supply chains in Canada provide an excellent avenue for attacks by nation states and organized criminals. In large scale hacks, from stealing plans for military weapons systems to sizeable retail credit card information theft, the supply chain is now a most preferred route for both high and modestly skilled attackers. By attacking a less guarded small business, the perpetrator can take advantage of existing trust relationships between the victim and the larger target organization. Larger entities in Canada with more developed capabilities and security-focused resources should establish information sharing and security frameworks for their suppliers and partners. Equally, smaller entities must not leave themselves vulnerable to compromise, which could lead to lost business opportunities.

Leaky systems

In order to not aid attackers, IT teams need to ensure through testing that their networks and databases are not “leaking”.

Data of this nature provides excellent targeting information for Black Hole and other penetration attempts.

Bring Your Own Device (BYOD)

With the sharp increase in Android and other smart phone operating system malware effects, BYODs introduced into the workplace, and then “plugged into” the network, allow for easy and hard-to-eradicate virus contamination from within.
Industrial control systems

Network-connected industrial and environmental control systems are becoming the norm across all industries. Be it machine automation on the factory floor, HVAC controls, or pipeline monitoring systems, each of these become accessible to malicious actors via the Internet if they are not properly managed. Along with the implementation of higher (security-related) supplier standards at purchase, installation or servicing, organizations must treat and defend these systems like any other part of their network.

Encryption and anonymization threat

Employees are increasingly applying their “home internet habits” that include the use of encryption or web sites that anonymize their Internet activities and footprint. Except in cases where inappropriate and possibly illegal material may be accessed and downloaded on the corporate network - including pornography - encryption is used to facilitate banking and other personal matters. However, it is also used by “insiders” or already successful malware implants, to move commercially important data or other business intelligence, out of the organization. By using anonymization tools within the workplace, employees circumvent corporate filters intended to limit the potential to access inappropriate content, including malware, while making it difficult to “inspect” data packets leaving the organization. Employee awareness, limits on options, continuously updated policies and procedures, and advanced security tools that can implement them are necessary.

Extortionware

Last year a cyber-extortion scheme, dubbed “CryptoLocker”, took corporations and individuals by storm. This particular malware variant would infect a target computer, and then encrypt the contents of the hard drive, rendering many files unusable. Once a fee had been paid to the criminal group, the files would be decrypted and restored to their original state. Estimates place extortion scheme profits in one year at $40 million (USD). Given its success, a more potent 2014 model is expected soon.

Low and slow

A sophisticated tactic employed by attackers is called a “low and slow” attack, which takes place over weeks or months. This is done in the interest of thwarting event correlation or intrusion detection systems from picking them out from the data haystack on the network. Primarily, it is applied in the reconnaissance and the exfiltration phases.
**Trends for 2014: a look at what lies ahead**

**Point of Sale (PoS) and Automatic Teller Machines (ATM)**

These attacks are expected to be prominent. The success of the Target (November 2013) and Neiman Marcus (January 2014) attacks are important omens. The PoS and ATM attacks are increasingly achieved by using an “insider” or by attacking a third party supplier - such as a servicing company.

**Increasingly targeted sectors**

Those who support or supply others will continue to be vulnerable. Entities in the chain, rather than the principal target, will be the focus. Otherwise, expect continued growth in data breaches affecting manufacturing, retail and financial areas. Attackers will make critical infrastructure a top priority, and will use successes in targeting data control systems to attack.

**Actors: old and new**

The capabilities of nation states will continue to improve, despite Snowden-related setbacks. Gains made through the Snowden revelations will benefit other cyber criminal groups, terrorist entities, and hacktivists. The technologies in the hands of the aggressor will continue to increase in sophistication, stealth and speed to delivery point.

**Trends in techniques and approaches**

Spear Phishing email will continue to be a source of concern. In addition, “Strategic Web Compromise”, including “watering hole” attacks, and SQL Injections (where malware joins and then hides within the body of the operating system) will emerge. The use of “insiders” to conduct reconnaissance or to deliver the “package” will increase. Finally, mobile applications and devices will be the weakest link in the chain.

**What’s next?**

By sending bogus, pre-determined encrypted emails, attackers can “listen” to a processor's unique decrypting “hum”. After a few emails, the attacker learns how the software decrypts. Of course a “listening post” must be created; hence the risk of “insider” facilitation. Solutions already exist to counteract this threat, but they need to be pushed out into supply chains now as well.
Preparing for a cyber-attack: what can be done in advance?

Being prepared for a spectrum of emerging threats is a key part of a well-managed business risk model. Cybersecurity should be incorporated into that broader risk framework. Companies need to consider what could threaten critical information assets, and what the impact would be if those assets were compromised.

“Basic information risk management can stop up to 80 per cent of the cyber attacks seen today, allowing companies to concentrate on managing the impact of the other 20 per cent.”

- UK Government

What companies can do in advance:

1. Properly identify, in priority order, the most critical information nodes that may be threatened, and place a value on each.

2. Calculate how much risk to those assets the organization is willing to absorb.

3. Remain briefed by subject-matter experts (from inside and outside the company) on technology shifts, and on changes in threat-related activities within your environment.

4. Set strict, rigorous access control policies for prioritized critical areas. Policies should include media (i.e. removable data on thumb drives) and system access (with a particular emphasis on knowing who has administrator or “super-user” privileges).

5. Constantly challenge assumptions. Challenge how safe the leadership team feels about critical assets. Verify employees are following IT and related security policies. Test the robustness of current defences, of the organization and the supply chain, from outside and inside the organization.

Complacency will only assure asset or reputational risks. Do not attempt to protect all areas with equal vigour. Complexity and size will surely defeat any honourable intent.

Prevention and avoidance are the best strategies. When this fails, be in a position to respond effectively to a cyber-attack.
When you are attacked

The best cyber defense practices will not guarantee absolute resilience. At some point, something will get through and you will be attacked.

The executive team’s ability to contain the scope and impact of the attack will be determined by the level of preparation. The better your defences and internal procedures, the harder a target you will be.

Early detection of an intrusion is crucial to effective mitigation. Verizon reported in 2012 that two-thirds of all cyber breaches to which it responded were in the network and undetected for a period of months or longer.

When an attack hits, the practice of consistently testing the network and the existence of an established protocol will pay dividends. An established protocol can limit the potential damage and increase the organization’s ability to detect the attack’s scale and scope. Understanding the “who, what and why” will also help shape the response.

The Business Continuity or Disaster Recovery Plan must focus on ending the intrusion, while quickly assessing the damage - from the impact of lost information to potential legal liability.

Irrespective of early reporting, assume the worst. Be prepared to invoke the crisis plan and deploy a crisis management team.

Limiting liability means containing the damage inside and outside the organization. Consideration of law enforcement assistance, along with advice to or from security intelligence officials, should form part of the options list. This is especially important if a nation state is suspected of being behind the attack, or when national security may be at stake.

Be prepared to reach out to others in a shared business area, as they may have come under the same attack, currently or in the recent past (or may suffer a similar fate in future).

A strong communications approach will be an important asset in achieving some measure of success in difficult times.

---

### Government resources

The Government of Canada offers valuable cyber security information and services to Canadian industry through the Canadian Cyber Incident Response Centre (CCIRC). CCIRC is Canada’s national coordination centre for the prevention and mitigation of, preparedness for, response to, and recovery from cyber incidents. As the single point of contact into the government, CCIRC helps to coordinate the national response to significant cyber incidents with key government agencies, such as CSIS, CSEC, and RCMP. When CCIRC becomes aware of malicious activities, it notifies owners of compromised systems. CCIRC offers:

- **Technical products**: time sensitive information related to specific cyber threats, including detection indicators, mitigation information, and best practices.
- **Operational products**: information about cyber incidents to help support organizations’ operational and security decision-making.
- **Services**: the provision of incident response coordination, mitigation advice, technical analysis and reporting on malware samples, and tailored malware notifications.
Questions for the CIO

Before an attack

1. What are our major IT risks? Do we understand them? How do these compare with other enterprise risks?

2. What is our mechanism for reviewing major IT risks and adjusting defence strategies accordingly?

3. What are our most critical data elements? Where are they held within our enterprise or partner data system? How are we protecting them? What is our approach to cloud computing?

4. Have we evaluated our supply-chain risk?

5. Do we have a social media policy? Are all employees trained on it? How do we monitor its application?

6. Do we have daily cyber threat intelligence/information that is customized for our environment and systems so we can prepare for threats before they strike?

7. What is our response plan in the event of a cyber breach? Do we have access to professional cyber incident responders - internally or through service providers - who can help us manage and contain a breach? Do we know who to call in the government and law enforcement communities for assistance? How would you evaluate our business continuity program?

During and after an attack

1. What happened? What part of our cyber defences failed?

2. What systems have been affected? What parts of our enterprise are implicated?

3. What is the potential impact on mobile or home-based platforms connected to the organization or partners?

4. What is known or understood about the parameters (levels and depth) of the attack?
5. Who are the possible suspect actors behind the attack? Is it possible that insiders were involved?

6. Do we know about attacks with similar parameters within our industry or beyond?

7. What countermeasures are we taking? Who are we working with to fix the breach? What is the timeline for completion and resumption of operations?

8. How are you coordinating with our legal and communications teams?

9. Have all observed elements been recorded for future defensive purposes? Are there evidentiary/forensic elements that should be protected in the event of a law enforcement investigation?

10. What lessons have we learned?
The CEO abroad: understanding the risks and managing the threat

A typical scenario

The corporate executive and spouse boarded the overseas flight looking forward to a break, along with the potential to reach agreement on a joint-venture production facility 10,000 kilometers from home. The opportunity to expand into a foreign market with a well-financed partner was the company’s best hope to secure future growth.

What the executive did not realize, despite some measures to protect the company’s intellectual property and negotiation strategy, was that the host country had anticipated the company’s defensive measures and ongoing vulnerabilities.

To be sure, the executive was conscious of the risks. His corporate laptop had been wiped clean, his phone SIM card had been replaced, and the files on his laptop had been password-protected and re-labeled.

His spouse, however, needed to stay on top of her own business affairs back home, including a complex litigation case with a government regulator. Since this spouse was not involved in the company on an official basis, and had “no secrets”, she traveled with a personal iPhone, a business Blackberry and a company-provisioned tablet.

This was precisely what the host intelligence service was counting on. After the plane landed and the smartphone connected to the closest telecommunication tower, the predators were in. The breach became even more serious when the laptops and tablets connected to the free airport and hotel or airport Wi-Fi networks.

By applying “password guessing” (a technique that often succeeds given the number of people who use easily deduced passwords), or “brute force” software, intruders can gained control of devices and their applications. The intruders then scan the device for social media logins, photo albums, personal emails, and so on.

Often within an hour, a number of important sub-targets will receive what seems to be a legitimate email from the traveling spouse. The emails can include greetings and photos from the trip and a snapshot of the newly targeted victim, perhaps taken at a recent fundraiser event early that year.

Before long, the executive’s network will have been breached because an employee accepted what he or she thought was a legitimate email from the spouse.
Little attention has been paid to cyber based threats affecting executives, engineers, sales staff, public relations leads and others who venture outside of a controlled domain.

<table>
<thead>
<tr>
<th>The CEO abroad: remedies and best practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Do your homework (in advance of business or leisure travel, understand the complexity of local issues, as well as capability and intent)</td>
</tr>
<tr>
<td>2. Be aware of your environment (while on guard, take note of anomalies, recognize new or unexpected threats as they emerge)</td>
</tr>
<tr>
<td>3. You are a target, act accordingly (do not try to search for “bugs”, beware of inducements and approaches after hours)</td>
</tr>
<tr>
<td>4. Be a minimalist (travel with the barest of minimum information and encrypt heavily)</td>
</tr>
<tr>
<td>5. Burn after use (use devices one time)</td>
</tr>
<tr>
<td>6. Accept few gifts (no outside technology)</td>
</tr>
<tr>
<td>7. Leave nothing unattended (hotel safe, company lock-up, safety deposit box)</td>
</tr>
<tr>
<td>8. Be circumspect (cellphone or taxi)</td>
</tr>
<tr>
<td>9. Leverage secure partners (Canadian Embassy)</td>
</tr>
</tbody>
</table>
A way forward

Cybersecurity is a threat to all Canadian enterprises. The only proven tools available for overcoming this grave challenge are information-sharing and investments in mitigation technologies that are rooted in a broader risk-management framework. Traditionally, companies tended not to talk about cyber-attacks. The grave nature of cyber threats, however, is pushing companies to change course and look for safe ways to share information. Attackers are hitting targets with more precision and sophistication than ever before - and when they succeed, they often target other firms in the same sector or community. If a firm learns in advance about the details of a recent attack on a competitor, it can take steps to thwart a similar attack on its own network. It is unlikely to learn such information, however, unless it commits to sharing as well. Government can play an important role in facilitating these exchanges.

Cyber-attackers prefer to go after those they perceive as easy targets. Besides sharing information, investments in cutting-edge security applications are crucial. According to The Economist, global payment-card fraud losses grew by 15 per cent between 2011 and 2012, hitting $11.3 Billion (U.S.). Many U.S. banks, for example, use only magnetic strips on their credit and debit cards – first generation security technology. Consequently, retailers and financial institutions are seeing escalating losses from Point of Sale and other types of “hacks”. By contrast, a strategic decision by Canadian banks to introduce “chip and pin” technology cut the losses through fraud from C$142 million to C$38.5 million between 2009 and 2012.

Similar strategic investments that involve a number of nimble and constantly evolving solutions, from hardware to software, and the applied use of social and personnel-related security layers, will sharply alter the threat landscape.

As centres for secure commercial activity, Canadian businesses will reap the short- and long-term benefits of attracting investment, and increased consumer confidence, along with higher global e-commerce traffic — all the while staving-off litigation and increased government regulation.

Top 10 tips for cybersecurity

1. Acknowledge that cyber threats are as much about people as technology
2. Be environmentally aware: outside and in
3. Sensitize and train staff, then repeat
4. Monitor in tight improvement cycles
5. Link data access to roles (not people)
6. Segment production data from everything
7. Encrypt sensitive data
8. Apply “security zones” to global level data
9. Enforce a mobile device security strategy
10. Update everything security-related, every day