Canadian Centre
for Cyber Risk Management

June, 2015

Cyber Risk Management by Design

An Approach for Managing the Privacy and Security Risks Associated with the Use of Cyber Systems

Douglas Blakey, B. Math
Managing Director
Canadian Centre for Cyber Risk Management
Waterloo, Ontario, Canada

Ann Cavoukian, Ph.D.
Executive Director
Privacy and Big Data Institute, Ryerson University
Toronto, Ontario, Canada

CONTENTS

CONTENTS

FOREWORD

Systems security is often mistaken as the safe means by which to address privacy and data protection. There is no doubt that encryption, firewalls, access controls and the like, serve to protect data from external threats.

Privacy, however, subsumes a much broader set of protections than security alone. Privacy encompasses data minimization, whether it be in the collection of personal information or the use of such information. Think "purpose specification" and use "limitation" as the shorthand for distinguishing privacy from security. However, security of personal information is an essential component of privacy and data protection. Without strong security end to end, there can be no privacy since, personal information will be at risk.

Over the last several years, personal data has gained prominence as an extremely valuable resource for the 21st century, to the point where it has been characterized as the "new oil" of the Internet age. From a Big Data perspective, we must clearly keep privacy at the forefront. Just as *Privacy by Design (PbD)* advocates that organizations take a proactive, positive-sum, win-win approach to managing the personal information in their custody and control, it makes abundant sense that cybersecurity be treated no differently.

Whether it involves technology, business processes or networked infrastructures, the risks of cybersecurity are considerable and must be integrated into an organization's culture. This paper offers such a framework and provides valuable guidance to organizations.

Ann Cavoukian, Ph.D.
Executive Director, Privacy and Big Data Institute
Ryerson University

PART I – UNDERSTANDING THE CYBER RISK PROBLEM

First we build the tools, then they build us. **- Marshall McLuhan**[1]

Global Cyber-Interconnectedness: A Challenge to Our Privacy and Our Security

On January 29, 2014, James Clapper, the Director of National Intelligence for the United States, reported in his annual *Worldwide Threat Assessment of the United States Intelligence Community*[2] that cyber-vulnerabilities are now considered the number one risk facing the United States and its allies, ahead of the likes of terrorism and weapons of mass destruction. That's a sobering thought. How could cyber, something we all now so highly dependent on, rise so quickly to the top?

Global cyber-risk has grown so fast it has become a major threat to our privacy and our security. Economic espionage is the US government's primary concern. But does a threat to Canada's largest trading partner suggest there is also a threat to Canada and its businesses and institutions?

Are Canadian organizations at risk?

According to an August, 2014 report in the Globe & Mail:

> *More than one-third of Canada's IT professionals know – for sure – that they'd had a significant data breach over the previous 12 months that could put their clients or their organizations at risk…*[3]

Canadians may not hear many media accounts directly linking our businesses, non-profit organizations, governments, and other institutions to cyber-breaches. However, there is much evidence which suggests that Canada is just as vulnerable as our American neighbours.

Our world is so highly interconnected on local, regional, provincial, national, and global scales that, essentially, we all live on a common same "cyber-street". Any notion that Canada is not a target, or is somehow immune to cyber-attacks is, in our view, incorrect.

Is cyber-risk predominantly confined to large Canadian companies?

Certainly large Canadian companies face considerable cyber-risk. However they also enjoy economies-of-scale that enable them to effectively manage this risk, should they so choose. Most cyber-incidents targeted directly at large companies are thwarted.

However, the large enterprise's under-appreciated Achilles heel is the (likely) poor degree of security preparedness of its smaller partners, including: suppliers, contractors, and general business partners. Often when a large enterprise is breached, the source of the problem can be traced to a smaller organization to which the enterprise is in some way connected.

A case in point is the infamous Target breach. The CEO of Target, who lost his job after his company's well-publicized breach from late 2013,[4] probably wishes that he had ensured that Target's business partners were managing their particular cyber-risk more effectively. Target was not breached directly. Target was breached through a business supplier that failed to practice good cyber risk management. [5]

Are Canada's small and mid-sized enterprises a target?

In a February, 2015 article from the Globe & Mail, Jordana Divon interviewed Kevvie Fowler of KPMG Canada. He says:

> *Based on what we're seeing, small businesses are still focusing on the bare minimum to meet the compliance requirements to stay in business…As a result, a lot of small and medium enterprises are finding themselves in hot water, warning that Canadian business owners are just as vulnerable to hackers as anyone in the world.* [6]

Looking deeper, according to a report by Armina Ligaya of the Financial Post:

> *Most Canadian businesses are unprepared for cyber attacks, but small and medium-sized businesses are particularly vulnerable…*
>
> *About 60% of Canadian firms do not have a security strategy in place or don't know how to prepare their networks for new mobile or cloud-based models.*[7]

There are many reports and documents which clearly state that small businesses in Canada are at great cyber-risk, and that they are not doing a very good job managing that risk.

What do hackers want?

In a word, *everything*. Although most think that cyber-criminals target specific organizations, the fact is everyone using the Internet is a target. Why? Because it is so easy for hackers to leverage banks of computers to systematically gather large volumes of data from every unlocked door they encounter. For the most part cybercrime is a crime of opportunity. Cyber-criminals take whatever information they can, aggregate it into clusters, and then sell it en mass to the highest bidder.

In 2014 the *Rand Corporation* published a report titled "*Markets for Cybercrime Tools and Stolen Data*"[8]. The authors wrote:

> *These black markets are growing in size and complexity. The hacker market…has emerged as a playground of financially driven, highly organized, and sophisticated groups. In certain respects, the black market can be more profitable than the illegal drug trade; the links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible.* [9]

Essentially, these markets are e-commerce sites for the hackers. Hackers gather as much data as they can, then sell it in bulk. They are not necessarily trying hard to break into locations, they are checking for unlocked doors that are easy to enter, collecting data of any type – personal, financial, intellectual property, passwords, etc., and then selling it. To cyber-criminals, this is a very lucrative business venture.

How do hackers break into so many locations?

There are many ways to break into systems. The world has connected billions of computers, which execute billions of instructions per second, into what is known as the Internet. As a result there are many weak points ripe for security failure. Plugging 100% of the holes, especially after rather than before systems and networks have been assembled and commissioned, is an impossible task.

In 2012 a so-called "good guy" hacker decided to see if he could do a "census" of the entire global Internet.[10] He thought there would be many computing devices which could easily be broken into because they would be using default passwords as set at the factory. He was proven right.

Over the course of a week he created something called a *botnet* – in essence, a network of computers – belonging to numerous owners, and housed at disparate locations – into which he inserted his own computer code. He used the considerable resources of this botnet to scan the complete address range of the Internet for open "ports" - virtual doors in a network's firewall which directly connect to the systems on the inside. He then used his botnet of 300,000 or so hacked computers to scan the entire global Internet.

His resulting "study" gave a fascinating snapshot of Internet use. He was able to assess it from head to toe in roughly 30 minutes. Therefore he was able to plot an Internet census showing changing usage day and night over a 24 hour period.

The good news is that he lacked malicious intent; so upon completion he reversed his work and erased all changes made to the botnet computers, thus leaving them as they had been before he arrived. Regrettably, he published his *Internet Census 2012* paper about how to do all of this publicly on the Internet. Needless to say, hackers have been leveraging his techniques ever since.

Privacy, Security, and Identity Theft on a Grand Scale

In a startling revelation published on October 20, 2014 by Erin Kelly of *USA Today*, Tim Pawlenty, the president of the Financial Services Roundtable and former governor of Minnesota said:

> *About 110 million Americans – equivalent to about 50% of U.S. adults – have had their personal data exposed in some form in the past year.*[11]

These breaches were against US multinationals like Target, Home Depot, and eBay, all organizations, at the time, with a significant Canadian presence. In fact the personal privacy and security of many Canadians was also compromised.

In particular, looking closely at the eBay breach of May, 2014, the CBC reported:

> *EBay Inc. said that hackers raided its network … accessing some 145 million user records in what is poised to go down as one of the biggest data breaches in history, based on the number of accounts compromised.*
>
> *It advised customers to change their passwords immediately, saying they were among the pieces of data stolen by cybercriminals.*[12]

The eBay attack occurred in late February and early March, but was not reported until May, when eBay suggested to all of its customers they should change their passwords.

Further, the Financial Post interviewed Avivah Litan, vice-president and analyst at technology research firm Gartner Inc. about large incidents like eBay's. She said:

> *The fact is [hackers are] collecting a ton of information on all of us…and while it may take some time, eventually they're going to start using all that information.*

That is probably the greatest concern. Months, even years after these data breaches occur, information collected on such a large scale could be organized to create personal havoc for individual Canadians and Canadian companies. Recovering from identity theft is a long term, time consuming, and expensive proposition. It would be far better to avoid the breach in the first place. The question is, how?

Are we asking the right questions?

It seems that every time we close an electronic door, hackers find a new one that we didn't even know existed. Are we taking the right approach to addressing the cyber-problem? Are we asking the right questions?

Modern technology and global interconnectedness has resulted in risks that seemed highly unlikely only a few years ago. In order to protect our privacy, our personal security, and the integrity of the organizations we depend on, we need to think differently.

PART II – CYBER-RISK CONTAINMENT – A BETTER APPROACH

Leave the beaten track behind occasionally and dive into the woods. Every time you do you will be certain to find something you have never seen before.

- Alexander Graham Bell[13]

Be Prepared: There will be Breaches

It is clear that cyber-breaches will happen, sooner or later, to virtually every person and every organization. Price Waterhouse Cooper, in its recently published annual cyber-risk report Managing Cyber Risks in an Interconnected World, stated:

> *As incidents continue to proliferate across the globe, it's becoming clear that cyber risks will never be completely eliminated. Today's interconnected business ecosystem requires a shift from security that focuses on prevention and controls to a risk-based approach that prioritizes an organization's most valuable assets and its most relevant threats.*[14]

In other words, the question is not *if*, but when, a data breach will occur. The entire focus has now shifted to managing the risk rather than just applying a patchwork of technical solutions. The current approach is not working. We need a better way.

Defining Cyber Incidents

According to the U.S. Department of Homeland Security, a cyber incident is:

> *The violation of an explicit or implied security policy. In general, types of activity that are commonly recognized as being in violation of a typical security policy include but are not limited to:*
>
> - *attempts (either failed or successful) to gain unauthorized access to a system or its data, including PII Personally Identifiable Information related incidents*
> - *unwanted disruption or denial of service*
> - *the unauthorized use of a system for processing or storing data*
> - *changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent"*[15]

In other words, cyber incidents are related to either failed or successful attempts to gain unauthorized access to computer systems or data. In fact, cyber incidents defined in this manner are occurring all the time. Attempts to gain access from the public Internet into systems that are behind a business' firewall occur many times every day.

Essentially, hackers never stop knocking on doors to see if they can get in.

When an Incident Becomes a Breach

A data breach is the intentional or unintentional access to secure information by an untrusted, unauthorized actor. Incidents range from a concerted attack by hackers with the backing of organized crime or national governments, to careless disposal of used computer equipment or data storage media.

When an incident catches the attention of the business, either through IT department vigilance or an employee noticing something unusual, the business invokes its security incident response policy and data breach protocol. This is used to determine how severe the incident is and whether in fact it has become a formal breach.

A carefully crafted incident response policy will include steps to insure that certain system log information is not disturbed by the IT department so that it could be used as evidence in a court of law if so needed.

A New Model: The Incident Response Timeline

In today's world, where incidents are constantly bombarding organizations connected to the Internet, we need to rethink our approach to addressing the problem. We need to think in terms of the *Incident Response Timeline*. In other words, serious incidents, which become actual breaches, will occur.

Therefore, we need to prepare well before a breach occurs, we need to know how we will respond in the first 24-48 hours when a breach has been confirmed, and we need to improve what we do after the dust has settled. This way we will learn from the experience and constantly improve defenses through monitoring, evaluation and risk management.

Basic Principles for Addressing Any Risk

According to the International Standards Organization (ISO),

> *Risks affecting organizations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes. Therefore, managing risk effectively helps organizations to perform well in an environment full of uncertainty.*
>
> ***ISO 31000:2009, Risk management – Principles and guidelines,*** *provides principles, framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.*[16]

Although there are other organizations with similar risk management guidelines, ISO 31000 is a clear, simple approach for managing enterprise risk and is suitable for applying to cyber-risk. In its simplest terms, ISO 31000 is a set of industry best practices, which essentially boil down to four ways to manage risk:

1. **Risk avoidance,** such as when an alternative approach is taken which eliminates the risk in question.
2. **Ignoring risk,** which means understanding the risk and choosing to do nothing about it.
3. Risk reduction, which means applying processes, systems, and techniques to minimize the risk.
4. **Risk transfer,** which means moving all or a part of the risk to another party. This is what occurs when an organization buys insurance for example.

ISO 31000 is a simple way to look at risk. When applied to cyber-risk, the approach becomes even simpler. First, risk avoidance is a desirable but not practical cyber-risk option. Organizations would be at tremendous competitive disadvantage without the use of modern computing technology. Second, ignoring the risk is not an option either. The global Internet has too many incessant hazards which could spell the end for many companies.

This leaves two viable approaches for managing cyber-risk. The first is *risk reduction*, which means applying sound risk management principles to reduce cyber-risk to a reasonable and manageable level. The second is *risk transfer*, which is a way to further protect against a major catastrophic loss by way of specialized services and insurance. Noting that risk reduction is never going to completely eliminate the risk, transferring residual risk such as through insurance may make good business sense.

When considering these approaches in terms of the incident response timeline, cyber-risk reduction occurs well before an incident happens, while cyber-risk transfer is applied as a last resort after the incident has become a significant breach.

The Cyber-Risk Paradox: Technology Alone is not the Solution for Managing Cyber-Risk

Most of us intuitively assume that preventing security breaches is the responsibility of the IT department. This is a poor assumption. Even though global interconnection of electronic systems and networks has brought about threats to privacy and security, believing that a silver bullet technical solution will "solve" the problem is wishful thinking.

Technology will only address part of the problem. People must also be considered. And with human nature being what it is, people will make mistakes. This is at the heart of why, to date, we have not been winning the war against cybercrime. In fact, this is one reason why things may be getting worse.

A better approach is to think in terms of *people-process-technology*.[17] This means, from the outset, managing cyber-risk systematically through education and awareness for employees, policy reviews of the processes employees follow, and implementing technology using privacy and security best practices.

Cyber Risk Management by Design (CRMbD)

The idea of implementing protective measures for maintaining information privacy from the ground up was popularized by one of the co-authors through a framework called *Privacy by Design (PbD)*.[18] Privacy by Design simply states that whenever new processes or systems which involve personal information are developed, developers apply best practices for safeguarding that information from the outset.

The result will be better systems in the long run, and which will invariably cost less to operate and maintain. Modern systems need to work for people, not against them. *PbD* becomes an automatic component of the design for all systems that touch Personally Identifiable Information (PII).

Since protecting the privacy of people also involves applying certain security best practices, some elements of security must also be included in *PbD* initiatives. However safeguarding the privacy of people is only one part of the problem. The big picture includes not only the privacy and security of people, but also the security and trust of the institutions people depend on, like companies, governments, and countries.

Therefore, a next logical step in the protection of people and maintaining the reputation of organizations is to develop an approach, from the outset, that enables the protection not only of the people in the organization, but the organization itself. This means implementing a cyber risk management approach right from the outset, i.e. *Cyber Risk Management by Design (CRMbD)*.

PART III – FOUNDATIONAL PRINCIPLES OF CYBER RISK MANAGEMENT BY DESIGN

The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn, and relearn. - **Alvin Toffler, 1970**[19]

The Seven Foundational Principles

Similar to *PbD, CRMbD* includes seven foundational principles:

1. Proactive not Reactive

Cyber Risk Management by Design (CRMbD) means applying cyber risk management best practices before a cyber-breach occurs, not after. For emerging start-up companies, this means establishing a program from the outset before the organization opens its doors.

For existing companies this means making sure the organization begins implementation and constant improvement of their *CRMbD* program as soon as possible.

2. *CRMbD* as the Default Setting

In its most basic form, the first step when creating a *CRMbD* program is to confidently address one crucial question:

When did the company last verify a trial restore of their secure off-site business system backups?

This is not a sufficient condition for a complete *CRMbD* program, but it is an essential first step. Company leadership must know with confidence that they can recover from almost any calamity. Their systems and data, going back to a reasonably recent point in time, *must* be recoverable. Nothing less is acceptable. By default, make certain the organization will survive to live another day.

3. *CRMbD* Embedded in the Organization

All business leaders intuitively make risk management decisions every working day. Managing cyber-risk is no different. Leaders must set the tone from the top. They must maintain oversight for the cyber risk management program in place and they must practice what they preach, thus setting the tone for the rest of the team. By embedding the notion of properly managing cyber-risk into the corporate psyche, every leader and every employee will know their role in maintaining a strong cyber risk management posture for the company.

4. Full Functionality – Positive-Sum, not Zero-Sum

Often, cyber-security threats overshadow the importance of privacy through means that focus solely on security. In any CRMbD, the goal is to achieve both privacy and security, without any trade-offs. There is no need to sacrifice one for the other, no room for half-baked solutions, and no net value in cutting corners. Maintaining a consistent, clear approach will result in the preservation of both the privacy and security attributes of personally identifiable information (PII) in systems.

5. End-to-End CRM – Full Lifecycle Protection

CRMbD is a never ending cycle of constantly reviewing, refining, and improving cyber risk management practices whether it involves data at rest or in motion; and data at collection or at the destruction/end of the lifecycle. This is not an onerous task, and if maintained using practical best-practice approaches for CRMbD solutions, will reduce costs and keep the organization and all of the people it touches reasonably safe and secure.

6. Visibility and Transparency – Keep it Open

The mark of a great organization is an organization functioning at peak performance. This is accomplished by knowing that processes and technology are designed and integrated in such a way as to ensure the existence of appropriate checks, balances, and oversight. If so, then allowing these traits to be known publicly will garner far greater

trust and credibility of the organization.

7. Respect for People

People always come first. Above all else remember why we develop systems and build companies: to improve quality of life. This must always be a primary motivating factor when fostering the growth of organizations. This does not mean "spare no expense". By applying practical CRMbD best-practices, the privacy and security of our employees, our clients, our partners, and everyone touched by the organization may be preserved, allowing the organization to thrive long-term.

PART IV – EXAMPLES FOR INITIATING A *CRMbD* PROGRAM

There are no passengers on spaceship earth. We are all crew. ***- Marshall McLuhan, 1963***[20]

CRMbD for Individuals

Managing the cyber-risks every business faces on a daily basis is a big challenge. For individuals and their families it must be daunting. The tools we develop to make life easier and more enjoyable are evolving so fast and on such a large global scale, the average person is left with a monumental task; figuring out how to manage the privacy and security risks they and their families face.

In today's highly interconnected world we can communicate with family and friends pretty much wherever we are on the globe. So how do we strike a practical balance between ease of use of our digital tools while maintaining our privacy and security? And the key word here is *practical*.

With this in mind, here are four steps that every individual can take, starting right now, to secure and maintain control over their personal information while enjoying the many benefits of modern technology:

1. Assume that everything you communicate electronically about yourself and your family will eventually become public. Therefore do not share any sensitive information that you would not wish to share on a postcard or public notice board.

2. When you use any electronic system, including email, personal computers, smart phones, and the like, invest the time to understand and use the security features behind that system from the very beginning. They should provide a good layer of protection

when used wisely.

3. Guard access to all of your electronic systems by applying wise password and access control practices.

4. When in doubt about steps 2 or 3, invest in professional help. Some systems are easy and intuitive to understand. Others, like home computer networks, can be complicated. Find a trusted professional technical advisor and leverage their skills to assist in your quest for that right balance between modern technology ease-of-use versus maintaining your privacy and security.

Memorize and practice these four basic steps, share them with your family and friends, and carry on enjoying the benefits of modern technology. And do so with the knowledge that you are taking wise steps to protect your privacy and your security.

CRMbD for Start-ups and Early Stage Companies

There are numerous complex tasks every start-up must do to develop a desirable product/service, generate sustainable revenue, and become a thriving business. What many entrepreneurs do not appreciate, however, are the complex cyber-risks they face as their company unfolds and grows. In fact, incubators are prime targets for hackers because of the innovative technologies they develop and the lack of cybersecurity maturity they possess as a fledgling young business. As stated in *The New York Times* by Newman and Stein, "Hackers are aiming at these young, innovative companies with the goal of walking away with an entire business."[21]

These organizations are absolutely at high risk. They also have the best opportunity for instilling a cyber risk management tone and mindset in the business from the very beginning. As employees, processes, and technologies are assembled and the company takes shape, the application of *CRMbD* principles are sure to serve the company well for many years.

As noted in the previous section *CRMbD for Individuals,* the key message is that early stage companies must be practical. There is no need to "boil the ocean" as it were. Rather, by educating employees about cyber-risk, establishing processes with privacy and security in mind, and implementing technology that incorporates proven risk management business practices, the young organization will be poised to flourish and build a strong, extensible foundation. From a business standpoint this makes more sense than haphazardly applying a patchwork of privacy and security measures later.

With this in mind here are three steps every start-up should take to maintain control over their intellectual property, protect scarce financial resources, and build the confidence of their stakeholders:

1. Ensure that every new employee, starting with the original management team, reviews and follows the four steps outlined in the previous section, *CRMbD for Individuals.*

2. Apply the seven Foundational Principles of *Cyber Risk Management by Design* outlined in section III, from the outset, for every business process developed for the company.

3. When developing new technologies for delivery to customers, again, apply the seven *Foundational Principles of Cyber Risk Management by Design.*

Since young companies have so many business pressures vying for limited time and resources, cyber risk management considerations often take a back seat to other priorities. This could very well lead to disaster. It is well known that hackers prey on the start-up company, and as we have seen there are many ways to break into any company. Practicing *CRMbD* from the outset will significantly reduce the risk of becoming the next start-up hacking statistic.[22]

CRMbD for Small/Medium Enterprises (SME)

When it comes to implementing CRMbD best practices, early stage companies have an advantage over their more mature SME peers. They can address the cyber-risks they will face from the outset. Most SMEs are relatively set in their approach for addressing cybersecurity. But what the vast majority do not realize is that effective cyber risk management includes more than just a technical approach. People and the processes they execute must be part of the equation.

Before the SME faces that dreaded media-worthy cyber-breach, it needs to embrace CRMbD principles. This should start now, and it is a very do-able task. But in order to achieve success it requires the direction and commitment from its leaders.

As discussed in the previous two sections, the key is to be practical. By enlightening all employees about how to address the cyber-risks the business constantly faces, by bolstering business processes with the intent of improving privacy and security, and by implementing

technology that incorporates good risk management business practices, the SME will be poised for growth while at the same time maintaining the integrity of the business.

With this in mind, here are four steps that every SME can take to establish a more complete, extensible approach for managing cyber-risk:

1. Establish buy-in from the organization's executive leadership. A more complete approach to managing cyber-risk starts with them. Ensure they fully appreciate the cyber-risks every SME now faces, and that they practice *CRMbD* foundational principles from this point on.

2. Ensure that every employee, starting with the original management team, reviews and follows the four steps as outlined in the section *CRMbD for Individuals.*

3. Review existing business processes to ensure that privacy and security aspects involving people address the full paradigm of people/process/technology. (Third-party organizations exist that can guide the SME through this process in a realistic, affordable manner).

4. Apply the seven *Foundational Principles of Cyber Risk Management by Design* from the very beginning for every new business process developed for the company.

Since SMEs have so many business pressures vying for limited time and resources, cyber risk management considerations often take a back seat to other priorities. This could very well lead to disaster. Ensure that business leadership follows and promotes a *CRMbD* mindset going forward so as to significantly reduce the risk of becoming another hacking casualty.

CRMbD for Large Enterprises

Large enterprises generally have the economies of scale needed to manage the cyber-risk problem effectively. Many cyber incidents directed towards them are being thwarted because most have developed a mature cyber risk management program.

As long as they are applying good cyber risk management practices, they will continue along a strong path and continue to grow. However their main weakness is the cyber security preparedness of their trading partners.

Large enterprises should lead the business world by insisting that all partners verify they are

following good cyber risk management practices. This will benefit the enterprise and show good business leadership. Every organization must protect the integrity of information entrusted with them.

Following are 3 steps large enterprises should take to maintain the confidence of all stakeholders:

1. Verify that their organization is aware of and following the *CRMbD* foundational principles.

2. Ensure that the organization has considered the question "How severely would the enterprise be exposed if one of our trading partners had a significant media-worthy security breach?"

3. Introduce business partners to *CRMbD* for Small/Medium Enterprises and consider mandating that they verify their implementation of smart cyber risk management practices.

By and large most large enterprises are following smart cyber risk management practices. However large enterprises would be wise to ensure that their business partners do so also.

CONCLUSION

There are more than 3 billion people connected world-wide, using powerful computing devices as if they were collectively living and working in the same neighbourhood. This poses severe threats to our privacy and our security, which must be addressed.

Large Canadian enterprises have the economies of scale to address cyber-risk, and many have chosen to exercise that strength. Small to mid-sized enterprises are also a significant target, but many may not yet fully appreciate that fact. And since large enterprises rely on small and medium enterprises as customers, business partners, and suppliers, SMEs have become the exposed soft underbelly for cyber-criminals to exploit.

Hackers tend to be sophisticated and part of well-funded organizations. They want any and all information they can get their hands on. They aggregate whatever they find and they sell it on hacker e-Commerce sites for considerable gain. Everything we do electronically is now at risk. However, we may not be approaching the problem in an effective manner. We are not asking the right questions, and are, by and large, not employing smart cyber risk management practices.

Changing our mindset and improving our approach is the best way to contain cyber-risk. From the outset, we must be better prepared as there will certainly be breaches. By putting ourselves in a position to minimize the damage when a breach occurs, we will be ready to recover quickly and completely. The great cyber-paradox is that technology alone will never be the solution for managing cyber-risk. We must bring all employees into the equation.

Cyber Risk Management by Design (CRMbD) establishes 7 foundational principles for managing cyber-risk: carefully considering the risk, and addressing how to contain it from the very beginning. It also means remembering why we create new companies, build new systems, and develop new technology – to improve the quality of life for *everyone*.

ENDNOTES

[1]Marshall McLuhan, "Marshall McLuhan Quotes", *Goodreads,* Marshall McLuhan Quotes.

[2]James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community", *US Senate Select Committee on Intelligence,* January 29, 2014, Worldwide Threat Assessment of the US Intelligence Community.

[3]David Paddon, "Cyber attacks have hit 36 percept of Canadian businesses, study says", *Globe and Mail,* August 18, 2014, Cyber attacks have hit 36 per cent of Canadian businesses.

[4]Eric Basu, "Target CEO Fired – Can You Be Fired If Your Company is Hacked?", *Forbes*, June 15, 2014, Target CEO Fired - Can You Be Fired If Your Company is Hacked?.

[5]Brian Krebs, "Target Hackers Broke in VIA HVAC Company", *Krebs on Security*, February 14, 2014, Target Hackers Broke in Via HVAC Company.

[6]Jordana Divon, "Cyberattacks an ongoing threat to Canadian small businesses", *Globe and Mail*, February 2, 2015, Cyberattacks an ongoing threat to Canadian small businesses.

[7]Armina Ligaya, "Canada's small and medium-sized firms vulnerable to cyber attacks", *Financial Post,* December, 2014, Canada's small and medium-sized firms vulnerable to cyber attacks.

[8]Lillian Ablon et al, "Markets for Cybercrime Tools and Stolen Data", *RAND*, 2014, Markets for Cybercrime Tools and Stolen Data.

[9]Ibid, pg ix.

[10]"Internet Census 2012", *internetcensus2012*, 2012, Internet Census 2012

.

[11]Erin Kelly, "Officials warn 500 million financial records hacked", *USA Today*, October 20, 2014, Officials warn 500 million financial records hacked.

[12]"EBay cyberattack hit 'large part' of 145 million users", *CBC News*, May 22, 2014, EBay cyberattack hit 'large part' of 145 million users.

[13]Narain Gehani, "Life in the Crown Jewel", *Bell Labs*, 2003, Bell Labs, life in the Crown Jewel, page 12.

[14]"The Global State of Information Security Survey", *Price Waterhouse Cooper,* September 30, 2014, The Global State of Information Security Survey, 2015.

[15]"Report Cyber Incidents", *Homeland Security*, Report Cyber Incidents.

[16]"ISO 31000 – Risk Management", *International Standards Organization*, 2009, ISO 31000 - Risk management.

[17]"An Introduction to the Business Model for Information Security", *ISACA*, 2009, An Introduction to the Business Model for Information Security.

[18]Ann Cavoukian PhD, "Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices", *Privacy by Design Centre of Excellence*, December, 2012, Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices.

[19]Alvin Toffler, "Alvin Toffler Quotes", *Goodreads*, Alvin Tofler Quotes.

[20]Marshall McLuhan, "Statement in reference to Operating Manual for Spaceship Earth", *Wikipedia*, 1965, Statement in reference to Operating Manual for Spaceship Earth.

[21]Craig A. Newman and Daniel L. Stein, "Cyberattacks a Huge Threat to Start-Ups, and Their Investors", *The New York Times,* April 19, 2013, Cyberattacks a Huge Threat to Start-Ups, and Their Investors.

[22]Chad Brooks, "Warning: Business Bank Accounts Aren't Safe from Cybertheft", *Business News Daily*, January 31, 2014, Warning: Business Bank Accounts Aren't Safe from Cybertheft.