Advanced Security in Canada

Industry Profile: 2010 to 2012

CATAAlliance
Canadian Advanced Security Alliance

ISBN 978-2-9812174-0-0

Advanced Security Study – Canada 2010-2012

© CATA Alliance & ScienceTech Communications, Montreal, QC, November 2010

Legal Deposit: Library and Archives Canada, 2010

© COPYRIGHT. ALL RIGHTS RESERVED. REPRODUCTION WITHOUT PRIOR WRITTEN PERMISSION IS FORBIDDEN.

Contents

Figures

1. Foreword: Reflections on Information

* * *

Excerpts from interview with Marc Fournier, Associate Partner

Information Security & Privacy group
PricewaterhouseCoopers (PwC)

* * *

All too often companies consider security as an information technology and communications (ICT) issue, while it is primarily a governance issue. Security is a strategic issue that should be addressed at the CEO level of the company and its board of directors. Unfortunately, most managers and administrators are mainly concerned with the outline of the regulatory outcome of the Sarbanes-Oxley Act (SOX). But otherwise, they delegate security management to the ICT security department. [1]

Security is a strategic issue that should be addressed at the CEO level of the company.

The result is that firms are relatively well informed about the security of their infrastructures. When we talk with our clients about the need to protect their systems, they are generally receptive and we have managed to secure their infrastructures.

Soft security areas are all found on the side of privacy: customer data, credit cards, identity theft, etc.

Everyone knows someone who has experienced a privacy incident, or else someone who knows someone who has been a victim... Gradually, panic wins. The identity theft victim must go through a real ordeal to restore his or her identity with governments, financial institutions, without forgetting Equifax. Five years ago, anyone who had his debit card cloned at a convenience store was stigmatized for life, the bank did not believe him, his credit was undermined, and his name was circulating everywhere. Some had to take a lawyer to get by.

Today things have improved somewhat, because the issue is better known. Thereby, financial institutions are regularly offering insurance against identity theft.

The fact remains that the number one problem that we have to face in security is privacy protection. Except for big players who have a proactive approach to security, the majority of the market continues to do the minimum and simply comply with regulations, and even then not always.

The number one problem that we have to face in security is privacy protection.

[1] Legislation enacted in 2002 in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. It is named SOX after its sponsors, Paul Sarbanes and Michael G. Oxley.

The information society today is very much like the automobile industry of the 70s: we remember the Ford Pinto that caught fire due to a design flaw in the location of its tank. Instead of adjusting the design, for years the company preferred to pay off fines and lawsuits.

Security still is a legal and regulatory no-man's-land in which there is no accountability. In most countries, governments remain passive and private companies do what they want with the information of their customers. It is obvious that this situation can only be transitory. We have two solutions: self-regulation and government intervention.

Security still is a legal and regulatory no-man's-land in which there is no accountability.

The self-regulation solution

The credit industry has decided to self-regulate by establishing the PCI-DSS standard and adding an electronic chip in credit cards and debit cards, to reduce fraud surrounding these cards, including theft of personal information.[2]

The credit industry has decided to self-regulate by establishing the PCI-DSS standard.

Indeed, financial institutions were losing several hundred million dollars a year because of the massive fraud carried out on payment cards. [3]They came together to ask the merchants to update their equipment and adopt best practices of the security sector. The government had nothing to do with these measures. This is a global initiative by an independent body: the Payment Card Data Security Standards Council (PCI SSC).[4]

The fact that large amounts of money were at stake facilitated dialogue between the credit institutions. They have done so because they considered self-regulation as a way to reduce credit card losses, and to avoid government regulation. They know however that this is the end neither of computer fraud nor identity theft.

Credit institutions know that this is the end of neither computer fraud nor identity theft.

To overcome the phenomenon will require growing public pressure, through articles in newspapers, broadcasts on radio and television, and campaigns organized by appropriate associations. When a company is publicly accused of negligence, it may run into considerable problems.

To overcome the phenomenon will require growing public pressure.

The role of government

In the U.S., policy makers have adopted a novel approach: instead of regulating the level of security, they seek to enforce mandatory notification of security incidents that involve sensitive personal data. California has played a precursor role in this regard by enacting in

[2] The Royal Canadian Mounted Police (RCMP) estimates that $408 million the amount of fraud on payment cards (credit and debit) in 2008 - http://www.rcmp-grc.gc.ca/count-contre/cccf-ccp-eng.htm

[3] The Payment Card Data Security Standards Council (PCI SSC) was established in 2006 by VISA, MasterCard, American Express, Discover Financial Services and JCB International - HHTUTUhttp: / / frca.pcisecuritystandards.org /

[4] In July 2003, the California Security Breach Notification Act requires that individuals be notified when a security breach compromises their personal information. A similar law was passed in four other states and is under preparation in 18.

2003 the obligation to disclose incidents, since then several states have followed suit.[5]

Now, the U.S. federal government is on the verge to adopt legislation on data breach notification.[6] This legislative approach is different from what has been done for years by such organizations as CERT that emphasize research, tool development and training, but do not address typical cases: here is how the latest incident happened, what was done, and why...

The U.S. federal government is on the verge to adopt legislation on data breach notification

The forthcoming laws on disclosure will require any company to notify its customers of a security breach to the database storing unencrypted sensitive personal information (social insurance number or driver's license, birth date, names of parents, etc.). A database compiling security breaches already exists in the U.S. and data is available online and can be searched by company, industry or region.

These privacy bills will force every corporation, public agency, or voluntary association leader to seriously address information security issues.

In my opinion, this is a very interesting model for American security industry companies; because the government directly speaks to the user community and lets it know where to go without dictating it how to get there.

Canada does no such thing. Besides, we hear very little about security in Canada. There is Personal Information Protection and Electronic Documents (PIPED) Act, but it does not require companies to notify security breaches.[7] As a result, the large majority of incidents go unreported.

Canada does no such a thing. Besides, we hear very little about security in Canada.

Indeed, the federal government is the first to give a bad example. Let us recall the incident of the Passport Canada web site that was closed down because the codes had intertwined. Instead of informing the victims and sharing the information with the industry, the government tried to minimize the incident.[8]

As a result, the large majority of incidents go unreported.

Without regulations requiring businesses – and governments – for data breach notification, there will be no effective protection of personal information.

[5] Introduced in the Senate in August 2010, the project Data Security and Breach Notification Act requires businesses and organizations that manage and store information on consumers, such as their social insurance numbers, to adopt measures and reasonable security policies to protect this information and, in the event of a failure to disclose nationally. It is the latest of a series of projects submitted in the Senate and the House of Representatives.

[6] Act Privacy and Electronic Documents Act came into force in stages between January 2001 and January 2004. It focuses on consumers' consent to the collection, use and disclosure of personal information by businesses - http: / / lois.justice.gc.ca/fr/P-8.6/index.html

[7] The Act on the protection of personal information and electronic documents was enacted by phases between January 2001 and January 2004. It deals with company’s use of personal information and consumer consent to collect, use and communicate personal information.

[8] In November 2007, a Huntsville, Ont., man who renewed his passport online realized that by changing a letter on the url of the electronic form of Passport Canada, he had access to unencrypted personal information from other applicants on the Passport On-Line website. The website had to be closed for three days. "Security Breach Forced closure of online passport application service", CBC, May 25, 2009 - http: www.cbc.ca/canada/story/2009/05/25/passport-online-applications052509.html

Entrepreneurial governance is the heart of security.

Whether as a result of government legislation or a self-regulatory measure, it will ultimately be up to each corporation to invent its own security strategy and deploy tools and processes that are effective. However, in most cases, the corporate governance organization does not suit security needs because it does not provide mechanisms for bringing security incidents to the attention of senior management.

The corporate governance organization does not suit security needs.

In most cases, both the chief information officer (CIO) and the chief security officer (CSO) report to the Vice-President of ICT. When an incident occurs, the two officers accuse each other and in the best case, only the Vice President will be notified. In turn, he will settle the dispute at the ICT department level. This structure prevents the information flow to escalate to senior management.

This structure prevents the information flow to escalate to senior management.

If the CEO and the chairman and board do not know what is happening within their own corporation in the security domain, how can we expect the security industry or fraud victims to know? This is also a major problem in all surveys on security. When the question "How many incidents have you had?" is being asked, the real figures are rarely provided, because the respondent is not aware of the number of incidents.

It is important to divide the security responsibility between governance and operations to ensure that the ICT managers do not conceal incidents. The person in charge of security or surveillance governance needs to be systematically involved in the incident management process so as to make the necessary decisions, such as alerting the law department or senior management. This responsibility does not lie with the ICT department.

It is important to divide the security responsibility between governance and operations.

This organization reflects what is at stake when we address corporate security as information security, not system security. And this is not merely a matter of semantics. The data does not belong to the ICT department, it belongs to the finance department or marketing, in short, it belongs to the service that generates it. This leads us straight to the principle of accountability. Those who generate the data must be accountable for their integrity, their availability, their survivability in order to continue operating the company in case of a major breakdown, and finally their confidentiality.

What is at stake when we address corporate security is information security, not system security.

In the paper age, professionals responsible for accounts payable worked manually. They controlled all the data, whether authorizations for suppliers or issuance of checks. All information was physically located on the same floor at the finance or procurement department.

Now that accounting is computerized, accounts payable professionals are still legally responsible for their records – as before. However, the providers list, payment authorizations, in short all the financial data is located elsewhere, on another floor, in another building, sometimes in another city.

If there is a security incident, the data may fall into unauthorized perhaps hostile hands. The first thing the ICT department should do is to notify the professional responsible for the account. Often this is not the case: the incident is not reported to the department responsible for the record, neither is the senior management.

That is why it is essential to split incompatible tasks within the corporate security department. Supervision must be separated from operations. Our role is to explain to the customer that the ICT department is not in charge of the data, but the professional who initiated the data file, even if the content of the file is not located in his office. Whatever the platform, paper or computer, he is the only one responsible. If someone else in the company decides to add his brother-in-law on the suppliers list and if checks are issued, he is responsible.

The ICT department is not in charge of the data. It is the professional who initiated the data file who is responsible for it.

In this regard, the Quebec Government has developed a governance framework of security that can be considered as a model. In each government department or agency, the CSO is accountable to the deputy minister, not to the CIO. To be effective, any security solution must pass through the split of ICT implementation and surveillance functions. Today, security's main issue is organizational, not technical.

Even if a firm were to install 50 firewalls, as long as the tasks of operational and governance security tools are not entirely separated, security reports will always look upbeat. But the executives will never know what is actually happening. It will take the occurrence of a major incident and an external investigation; to learn that this is not the first such incident, tens of undocumented incidents during the past months occurred. Even then, often, no one wants to say anything.

In some documented cases, the security specialist refused to cooperate and the executives did not dare fire him for fear of a repeat of the municipality of San Francisco situation. In this city, when the administrator of the internal network was fired, he refused to give the password of the system that manages the payroll, email and other critical functions. He was tried and sent to prison, but he still refused to give the password to the ICT manager. Ultimately, the mayor of San Francisco in person had to meet the network administrator in jail, and convince him to hand out the code.[9]

In some documented cases, the security specialist refused to cooperate with the upper management.

[9] Terry Childs is the administrator of the fiber network of the municipality of San Francisco who refused to hand over administrative passwords to his supervisor, the ICT Department Chief Operations Officer under the pretext he was unqualified. He was arrested in July 2008 and sentenced to four years in prison in August 2010. "Former San Francisco Network Admin Terry Childs Gets Jail Time", Digital Communities, August 10, 2010.

Major security trends

For large organizations, the turning point was the tackling of the Year 2000 problem which was accompanied by deployment of ERP systems. Since then, every five years, we enter an update cycle. The current one is a major step forward in facilitating the work, but this facility itself creates new security challenges. From a single terminal, sometimes a simple mobile phone, you have access to all corporate data. In response to this increased risk, the leading developer of ERP systems – SAP, PeopleSoft, Oracle and others – are launching additional applications to better secure transactions.

ERP systems facilitate the work, but this facility itself creates new security challenges.

Moreover, the rapid introduction of the PCI-DSS standard brings new players to become aware of the challenges of data security. With this standard in the retail sector, we see medium-sized companies from 500 to 1,000 employees develop a governance framework and deploy software and hardware security. Most small businesses lack the budget to invest in professional services. The industry should have off-the-shelf solutions, but it has not reached that stage.

The PCI-DSS standard brings medium-sized companies from 500 to 1,000 employees invest in security.

Security standards such as ISO 27,000 are still made to fit big business needs. It is up to security specialists to adapt them to the particular context of a given corporation. In practice, this function is performed by large professional services firms.

There are no ready-to-wear solutions because every client is different. Business processes and physical infrastructure varies from corporation to corporation, some of them receive their customers on their premises, and others go through distributors. There are too many variables in the trade sector to make ready-to-wear solutions possible.

There are no ready-to-wear solutions because every client is different.

At the same time, a small business is often ready to take on more risk than a large one, because it is in a developing stage and its' level of visibility is still low. If an SME has a known security breach, the incident is likely to involve few people and have less impact than if a major bank is being attacked.

Ultimately, security is foremost a matter of risk management that must be considered in terms of governance organization and business strategy.

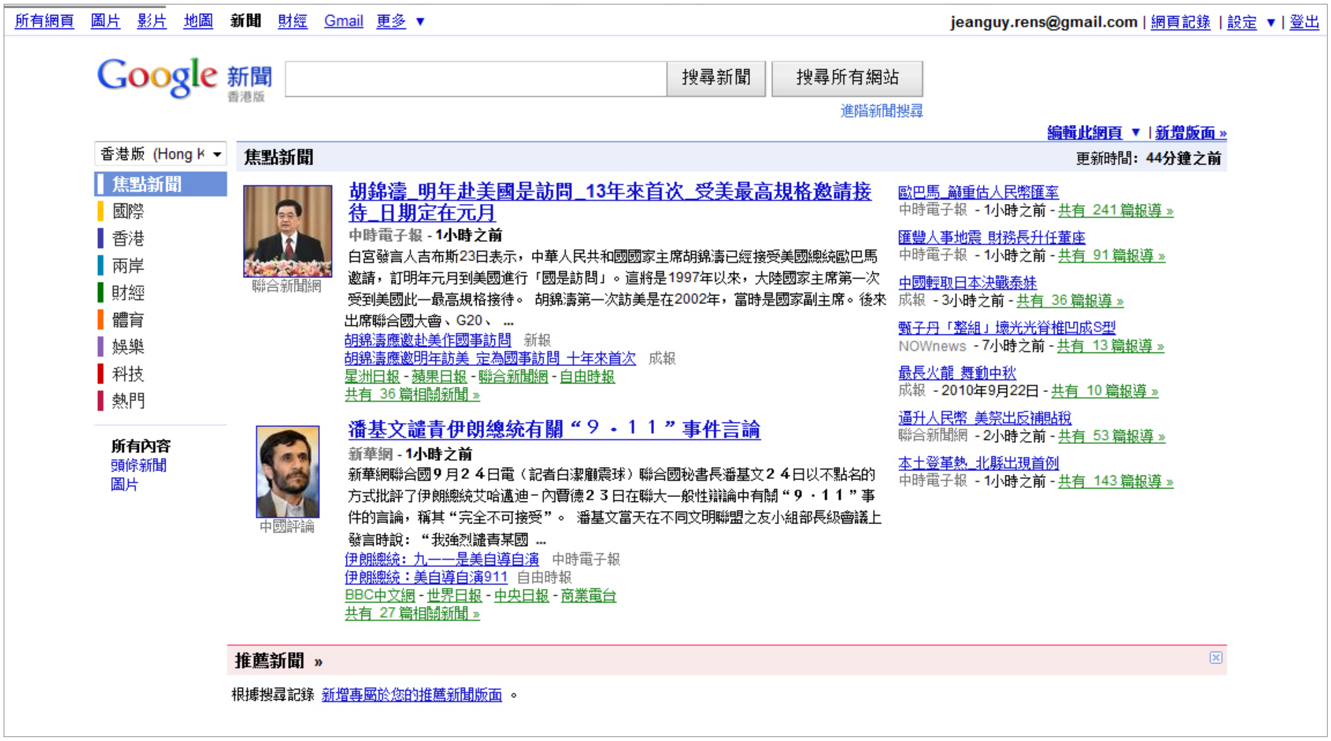
Security is foremost a matter of risk management.

2. Introduction

Information security is the order of the day. Brutal hacking of Google's servers by Internet users based in China, probably linked to its government, has highlighted the weakness of computer security and some highly strategic issues. [10]

For years, many specialists have announced the end of amateur hackers and the rise of professional hackers, criminals involved in organized crime or not, economic espionage, and in the case of attacks reported by Google, espionage possibly from governments.

FIGURE 1 - GOOGLE IN CHINA



焦點新聞 更新時間：44分鐘之前

胡錦濤_明年赴美國是訪問_13年來首次_受美最高規格邀請接待_日期定在元月
中時電子報 - 1小時之前
白宮發言人吉布斯23日表示，中華人民共和國國家主席胡錦濤已經接受美國總統歐巴馬邀請，訂明年元月到美國進行「國是訪問」。這將是1997年以來，大陸國家主席第一次受到美國此一最高規格接待。 胡錦濤第一次訪美是在2002年，當時是國家副主席。後來出席聯合國大會、G20、 ...
胡錦濤應邀赴美作國事訪問 新報
胡錦濤應邀明年訪美 定為國事訪問 十年來首次 成報
星洲日報 - 蘋果日報 - 聯合新聞網 - 自由時報
共有 36 篇相關新聞 »

潘基文譴責伊朗總統有關“９・１１”事件言論
新華網 - 1小時之前
新華網聯合國９月２４日電（記者白潔顧震球）聯合國秘書長潘基文２４日以不點名的方式批評了伊朗總統艾哈邁迪－內賈德２３日在聯大一般性辯論中有關“９・１１”事件的言論，稱其“完全不可接受”。 潘基文當天在不同文明聯盟之友小組部長級會議上發言時說：“我強烈譴責某國 ...
伊朗總統：九一一是美自導自演 中時電子報
伊朗總統：美自導自演911 自由時報
BBC中文網 - 世界日報 - 中央日報 - 商業電台
共有 27 篇相關新聞 »

歐巴馬_籲重估人民幣匯率
中時電子報 - 1小時之前 - 共有 241 篇報導 »

匯豐人事地震 財務長升任董座
中時電子報 - 1小時之前 - 共有 91 篇報導 »

中國輕取日本決戰泰妹
成報 - 3小時之前 - 共有 36 篇報導 »

甄子丹「整組」壞光光脊椎凹成S型
NOWnews - 7小時之前 - 共有 13 篇報導 »

最長火龍 舞動中秋
成報 - 2010年9月22日 - 共有 10 篇報導 »

逼升人民幣 美祭出反補貼稅
聯合新聞網 - 2小時之前 - 共有 53 篇報導 »

本土登革熱_北縣出現首例
中時電子報 - 1小時之前 - 共有 143 篇報導 »

推薦新聞 »

根據搜尋記錄 新增專屬於您的推薦新聞版面 。

September 24, 2010 screen capture (Google China Hong Kong version)

2.1 Trends

In 2003, CATA's first advanced security study identified the convergence between physical and logical security as an emerging trend. This convergence confirmed in terms of technology, has not been transposed on the market not, as we believed at the time, because of administrative barriers within companies, but because of cultural imperatives that have kept it apart.

The field of physical security is separate from information security. Not everything can be digitized. An interrogation ties in policing techniques rather than security logic. Bell is one of the few companies who

[10] In January 2010, Google announced that Chinese hackers had used a loophole in the PDF document format to infiltrate its servers as well as dozen of U.S. companies, including Symantec, Juniper Networks, and Northrop Grumman. This kind of attack against computer systems in large organizations is common, but what is less common is that it was made public. The incident quickly escalated to the highest governmental level with an exchange of notes between the Secretary of State Hillary Clinton and her Chinese counterpart in Foreign Affairs, David E. Sanger. David E. Sanger and Sanger, "After Google's Stand on China, U.S. Treads Lightly ", The New York Times, January 14, 2010.

merged logic functions and physical security in the same service. After years of practice and success in management, the distance between the two groups remains.

The other major trend identified in 2003 was the arrival of products and security services for the SME market. This trend was confirmed by the initiative taken by the major lending institutions to impose PCI-DSS to the retail industry. This initiative has forced SMEs to take security measures that are consistent across the planet.

The new trend that has erupted since 2003 is that of protection of personal data. Even before the advent of the Internet, the issue of personal information collected in increasingly ubiquitous databases, had alerted the public. Now, however, the sudden popularity of social sites belonging to Web 2.0, has attracted hundreds of millions of users to publish individual information. One displays its private life, its date of birth, personal photographs and those of its friends, the name of its employer and, for good measure, one announces when and where they will take a vacation...

It is a wealth of information that opens the door to a whole series of misdeeds, from the outright robbery of the home during a trip to a range of computer crimes such as identity theft, harassment, intimidation, etc. A small French magazine, Le Tigre, published in November 2008 the portrait of an unknown young man taken at random on the Internet and using only public information such as Flickr and a few other social sites, primarily Facebook, the magazine traced his life. All is there to grab: intimate and professional life details of the unknown called Mark L ***, and of his girlfriends and his co-workers. (see box) Within days, the mainstream media got hold of the story that became a national affair, while Mark L *** was trying to erase the traces he had clumsily left in cyberspace - in vain, of course.

The life of Marc L ***

"Happy birthday, Marc! On December 5, 2008, you will be 29. Mind if I treat you like a buddy, Marc? True, you don't know me. But I know you real well. You had the fortune, or misfortune, to be the first Google profile in *Le Tigre*. It's a very simple idea for a column: we take an anonymous person and tell his life using all the tracks he has left on the Web, whether deliberately or not. What's that you say? Is there some message behind this column? Of course: the idea that we don't really pay attention to the private information available on the Internet, and that once it is all brought together, it suddenly makes for a very worrying picture…

So, Marc: Pretty face, shoulder-length hair, a thin face and large curious eyes. I am looking at the picture taken at Starbuck's Coffee in Montreal during your trip to Canada, with Helen and Jose, August 5, 2008. Then you spent a whole weekend in Vancouver. I particularly like this series, because Jose took pictures, and it allows me to see you clearly. You rented a scooter, you went to the seaside, but you did not bathed, just hanging around on the beach. In all, you spent a month in Canada. At the beginning you were alone at the Hotel Central, Montreal. You were there for work…

So in Montreal, you were in an office with Steven, Philipp and Peter, working on architectural plans on two computers, a desktop and a laptop. By enlarging the photo, I can even see that you had a Packard Bell laptop and you used draft pages as mouse pads. I did not say it was exciting, I said we could see it. On August 21, Steven accompanied you to the airport. Back in France, you went to a wedding (Juliette and Dominic), then the following week, you went to the baptism of your niece, Lola, Luc's little sister (who made funny faces with her big glasses)..."

*The portrait goes on for two full pages of the magazine and we discover the life of Marc L *** and his girlfriend Claudia *** R, who works at the Austrian Cultural Center in Bordeaux and who, according to the journalist, "is charming, short hair, nice legs" – everything is real, including Marc's phone number.*

Raphael Meltz, *Le Tigre*, No 28, November 2008 – http://le-tigre.net/Marc-L.html

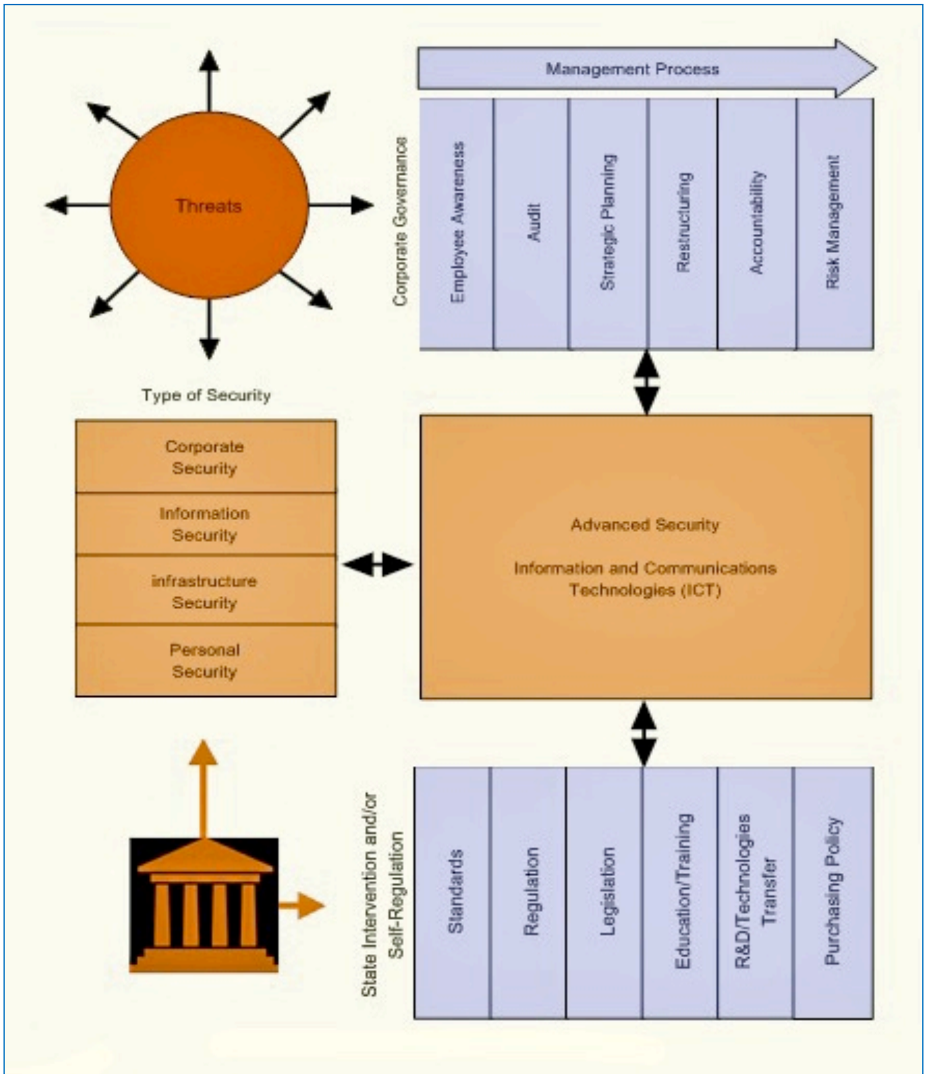
In Canada alone, more than 11,000 people were victims of identity theft in 2009, for a loss of 11 million dollars. If the number of victims remains constant year after year, the losses are increasing, from 6.5 million in 2007 to 10.9 million in 2009.[11]

[11] The sums of money lost by victims of reported identity theft in Canada rose from exactly $6,467,387.75 in 2007 to $10,882, 279.04 in 2009, according to PhoneBusters, also known as the Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit, "Mass Marketing Fraud & ID Theft Activities" Annual Statistical Report 2009, 25 pages.

Another trend: the gradual shift of security from the scope of technology alone to a matter of business management, and that at the highest level - from governance strategy. In fact, in the preface to the 2003 study of CATA, the late Robert Garigue[12] had clearly announced the metamorphosis of security:

> *Security involves an organization's overall management. It must be treated as a business issue and not simply as a question of technology. If we accept this premise, we must be ready to confront a series of consequences that change our entire way of working, and even our way of life, from top to bottom.*

FIGURE 2 – ADVANCED SECURITY BUSINESS ENVIRONMENT



Source: CATA Study – Montreal, February 2011

All indicators show that security goes beyond the scope of ICTs and needs to be redefined as a management function. In doing so, the place of security within firms changes, becomes more strategic and gets closer to upper management and the board of directors. Meanwhile, the importance of security within the state will continue to grow as signalled by permanent legislative activities in the U.S. But Canada

[12] Robert Garigue (1952-2007) began his career in the Canadian Armed Forces where he became one of the theorists behind the concept of cyberwar. Assistant deputy minister in the Office of Information Technology for the Province of Manitoba, then vice-president and head of security to the Bank of Montreal and Bell Canada, he completed a Ph.D. in knowledge discovery at Carleton University. He died in Montreal, at the age of 55.

remains undecided: after years in waiting, the Federal Government has released Canada's Cyber Security Strategy, but it remains unconvincing.[13]

With a paltry $90 million allocated over a period of five years to the task of cyber security, the Canadian government lags far behind its allies: the United States will invest $56 billion for the year 2011 only and $548 million on cyber security research and development (R&D),[14] Britain will spend $1 billion over the next four years,[15] and France has a National Agency entirely on Information System Security with a $120 million annual budget.[16]

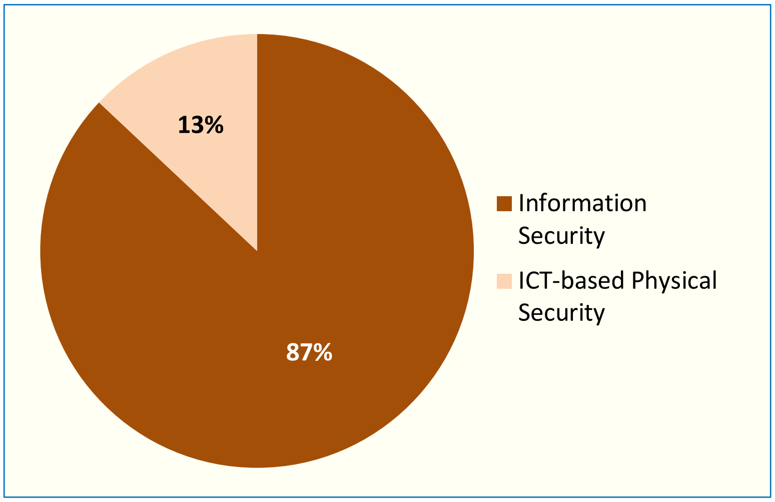
In February 2011, the Canadian government suffered the largest cyber attack of its history. Chinese hackers attacked key federal departments and also cracked into the computer system of the House of Commons, targeting MPs with large ethnic Chinese constituencies. The Communications Security Establishment (CSE) tracked the hacking operation to the Chinese embassy in Ottawa and to computer servers in Beijing. John Thompson, president of the Toronto-based Mackenzie Institute, said: "We need to really improve our defences. This is the A-Team as far as cybernetic intelligence gathering is concerned and we need to develop our defences and countermeasures accordingly."[17]

> All G8 Governments are actively involved in aircraft security associations. Canada is the only exception.
> It is a pity for its presence would contribute to reinforce Canada’s security;
> moreover it would allow emphasizing Canadian companies active in this sector.
> Patrick Patterson, Carillon Information Security

2.2 What is "Advanced Security"?

The term "advanced security" includes firms involved in information security and those who use information technology and communication (ICT) security. This excludes, on one hand, defence and, on the other, private detectives, security officers, companies shielding and safes, conveying funds, etc.

FIGURE 3 – WHAT DO WE MEAN BY ADVANCED SECURITY?



Source: CATA Study – Montreal, February 2011

In the study 87 percent of respondents are companies in the field of information security, while 13 percent use ICT solutions in the physical devices.

Any definition is arbitrary. Thus there are areas of overlap between defence and advanced security solutions. The field of public security (which covers the area of public infrastructure and frontline workers) is the focal point between the defence industry and that of security.

A typical example is provided by Genetec that was a pioneer in fully IP-based security system. Today, Genetec offers IP video surveillance and has extended its expertise in IP security to

[13] The 2010 government policy defines the respective roles of the various stakeholders, encourages public/private partnerships through existing structures and announces a new law requiring Internet service providers to provide police with basic customer identification data. Canada's Cyber Security Strategy, October 5, 2010 - http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf
[14] “White House asks for $548 million in cybersecurity R&D funding”, InfoSecurity, February 15, 2011.
[15] In the UK, the National Cyber Security Programme includes £650 million worth of new investment over four years. “Securing Britain in an Age of Uncertainty”, SITC, Friday, 29 October 2010.
[16] 90 million Euros. “La cybersécurité hissée au rang de priorité nationale », Le Journal du Net, July 9, 2009.
[17] “Chinese hackers targeted House of Commons”, CTV.ca, News Staff, Thu Feb. 17, 2011.

access control and license plate recognition (LPR). As it can be seen, its solution integrates information and physical security on an IP platform.

In summary, there is no clear separation between physical security and information security. The same goes for government systems and commercial systems, and between defence and civilian applications. Internet creates a convergence in cyberspace between previously distinct industries. The world of security redefines itself with changing and sometimes even blurred boundaries but is linked by a strong common thread: the digitization of information.

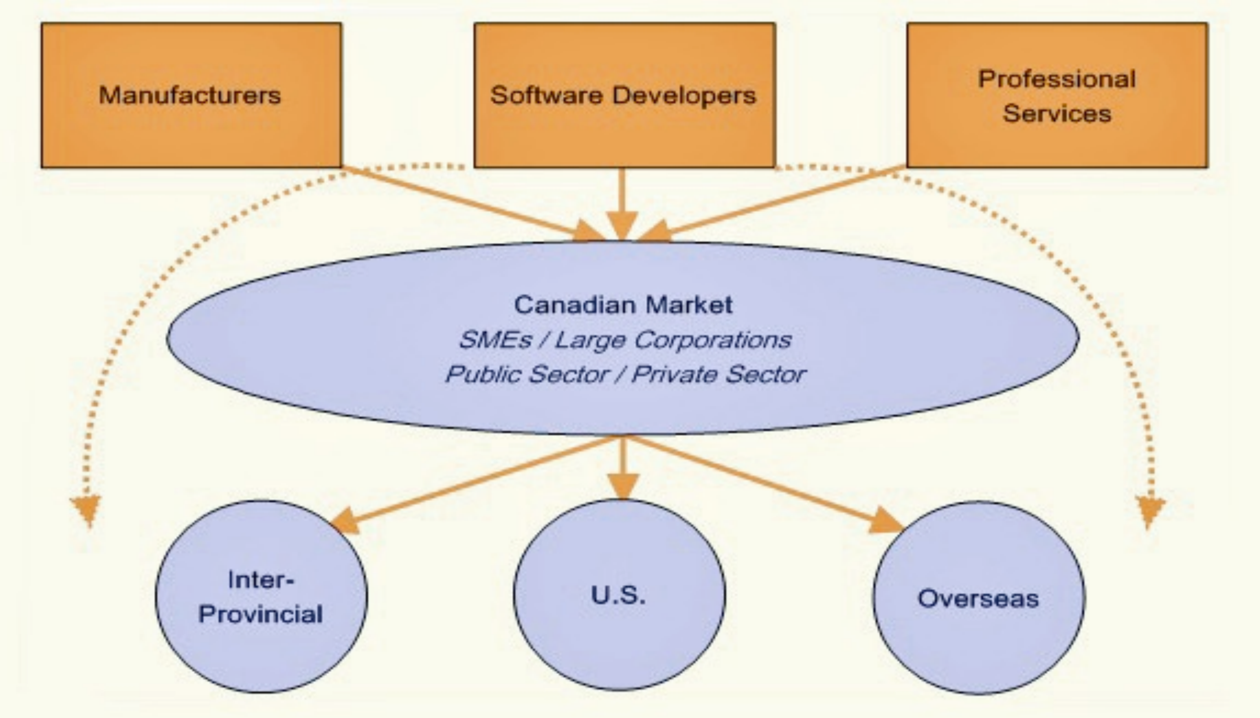
2.3 **Object** and Organization of the study

The study covers hardware manufacturers, software publishers as well as professional service providers. In practice, manufacturers of security equipment are almost always, also software publishers, and both generally provide professional service.

Inversely, providers of professional services have a separate business conduct. Most do not produce products or software: their strength is to be technologically neutral. They can then offer their clients objectivity in their choice of technology platforms.

The professional services firms generally have a closer contact with their customers. The know-how of their employees is their "raw material" and they sell their time, which limit their exportability. In order to export, they must expand outside Canada and in most cases hire local personal. When CGI creates a branch in the US or in Europe, it buys local companies and hires local residents. In this case, can we still speak about Canadian exports?

FIGURE 4 – ADVANCED SECURITY INDUSTRY ORGANIZATION



Source: CATA Study – Montreal, February 2011

On the other hand, whenever large professional services firms such Deloitte, KPMG or PricewaterhouseCoopers (PwC) open offices in Canada, they hire Canadian personal and sell a Canadian know-how. Are they still foreign corporations?

Special attention was paid to advanced security firms markets: they are analyzed by client size (large corporations or SMEs), vertical sector (government, finance, transport, retail, etc.), and of course destinations sites (home province, inter-provincial, U.S., overseas).

The survey conducted by ScienceTech between February and June 2010 is the main source (but not exclusive) of chapters 4 and 5 of this study. Wherever possible, we have clearly separated presentation of results from analysis.

Chapter 3: Industry Profile
This chapter portrays the advanced security companies. Where are they located geographically? What is their size, their age, their structures? Are they specialized companies that do only security (of pure players) or do they have multiple activities? Special attention was paid to the impact of the 2008-2009 financial crisis on business.

Chapter 4: State of the Market
Who are the customers of advanced security firms: large or small companies? In what areas do they work: finance, air or road transport, retail, police and other first responders, etc.? What are the market trends?

Chapter 5: Exports and Growth Strategies
Where do Canadian businesses sell their goods and services? Canadian markets are discussed as well as international. Where do the shipments go outside Canada, and also what are the strengths of Canadian companies and the obstacles they face.

Chapter 6: Research and Development (R&D)
R&D defines much of advanced security. This chapter aims to assess the R & D intensity in each industry segment, the nature of this R & D and its objectives: are R & D activities aimed at creating new products, improving existing products, or opening new markets?

Chapter 7: Financing
Funding is at the heart of the development of any business. This chapter examines the money needs of business and sources of funding.

Chapter 8: Obstacles to Industry Development
Companies identify here what hinders their development: recruitment of qualified personnel, U.S. protectionism, government programs? The lessons of this chapter are both surprising and revealing.

Chapter 9: Conclusion and Recommendations
A concluding chapter addresses the major issues facing the industry. It is based both on survey results and qualitative interviews with industry leaders.

Three appendices are enclosed in the study:

Appendix 1: Case Studies
Companies identify here what hinders their development: recruitment of qualified personnel, U.S. protectionism, government programs? The lessons of this chapter are both surprising and revealing.

Appendix 2: Questionnaire used for the survey (a French version was used in Quebec).

Appendix 3: Acronyms.

2.4 Methodology

The CATA *Alliance's* advanced security project has two inseparable aspects: companies' identification and field survey.

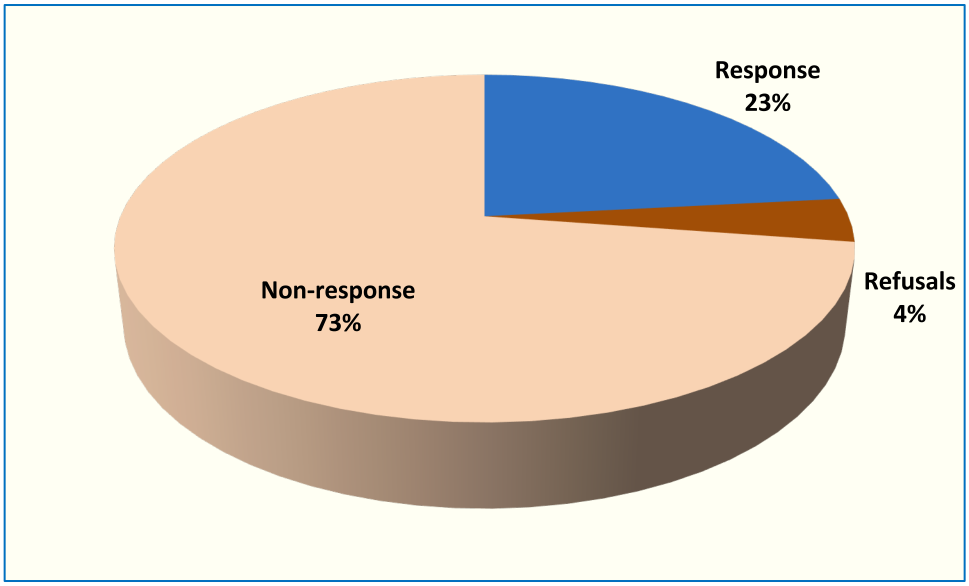
First, advanced security companies had to be identified. Starting with the 2003 database, we performed an exhaustive update mainly through telephone interviews. This work was complemented by a close examination of main security events participants and exhibitors. A first group of some 400 Canadian companies was identified.

CATA *Alliance* also partnered with several security-oriented associations:

- ✓ Association de Sécurité de l'information du Montreal Métropolitain (ASIMM)
- ✓ Canadian Information Processing Society (CIPS)
- ✓ Canadian Security Association (CANASA)
- ✓ Canadian Society For Industrial Security (CSIS)
- ✓ Information Systems Audit and Control Association (ISACA)

Second, the survey was administered in two waves among the 665 retained companies as in the context of the study (February-May, then November). The questionnaire was administered by CATA*Alliance* to all identified companies and the five security-oriented associations did the same with their members. When this step was completed, 155 companies had been contacted, or 23.3 percent of the total population. Twenty seven companies refused to respond, usually because of lack of time. Finally, 483 companies could not be contacted (no response after two months of attempts by e-mail and telephone calls).

FIGURE 5 - A MEDIUM RESPONSE RATE



Source: CATA Study – Montreal, February 2011

Base population went from 698 in 2003 to 665 in 2010, a 5 percent decrease. If we take into account the 42 companies created since 2003, we realize the death rate among the security industry is significantly higher – 11 percent.

What does this decrease mean? Out of the 25 firms that were the subject of cases studies in our 2003 study, four disappeared. We think in particular to Dephy Technologies that was a pioneer in rapid detection and identification of chemical and biological substances equipment aimed at borders and airports. Its team brought together high-level researchers in physics, chemistry, mathematics, computer science, and engineering. Sign@metric had developed a signature-authentication system based on the use of neuromuscular modeling of movements of the arm and hand of the person who is signing. Its technological platform made forgery impossible. Also gone!

In both cases, the companies succeeded a technological breakthrough and created an outstanding product. In both cases, the post-mortem was easy to carry out: marketing did not follow technology advances. However, the whole decreasing number of companies phenomenon cannot be explained just by the disappearance of a few promising start-ups. We must take into account a strong merger-acquisition trend.

Unfortunately, most of the time, Canadian firms are acquired by foreign firms, mainly U.S. but overseas-based as well (such as Cloakware Corporation purchased by South African-owned Irdeto). Even though most jobs remain in Canada, decision making capability is entirely lost and R&D is entailed. There are some exceptions though: when Montreal-based Dessau Soprin purchases Ottawa-based Elytra and its well trained cryptography team; or when Radialpoint merges with ZeroKnowledge.

As a result, there are less advanced security corporations in 2010 than in 2003. But the industry is more concentrated.

2.5 The Study's Production and Funding Team

The study on the advanced security industry in Canada is the result of collaboration and extensive team effort. The study on the advanced security industry in Canada was directed by Jean-Guy Rens, executive director of the CATA *Alliance*, in collaboration with Huguette Guilhaumon, senior partner in ScienceTech Communications Inc. Analysis was performed by E&B Tech's Pierre Bess and DATAPROTECT's Ali El Azzouzi (Casablanca, Morocco).

At the CATA *Alliance*, John Reid, president, enthusiastically supported the project while Cathi Malette oversaw administrative and financial aspects. The study was fully sponsored by the Canadian Advanced Technology Alliance (CATA). In the province of Quebec, the survey was financed by the Government of Quebec and the Economic Development Agency of Canada for the Regions of Quebec. Elsewhere, financing is assured by sales of the study.

2.6 Acknowledgments

CATA*Alliance* and ScienceTech Communications thanks first go to the following of people who took the time to answer our many questions all along the advanced security initiaitive:

Bergeron, Éric	President CEO, Optosecurity
Kokonis, John	Executive Director, Security and Privacy Practice, IBM
Bolduc, Jocelyne	Advisor Economic Development, Government of Quebec (MEIE)
Chouinard, Mathieu	President, In Fidem
Dicaire, Benoit	President, Infrax inc.
Dion, Marcel	President and CEO, Above Security
Doyon, Patrick	Marketing Director, Forensic
Estrela, Marco	Vice-President Sales & Marketing, Virtual Guardian
Fournier, Marc	Associate Partner, PriceWaterhouseCoopers
Galarneau, Pierre	Vice President and Chief Technology Officer, INO
Langlois, Guillaume	Associate Executive Director, Nurun
Meehan, François	President, Cedval
Olivier, Véronique	President, Waveroad Consult
Patterson, Patrick	President, Carillon Information Security
Petrogiannis, Tommy	President Silanis
Piché, Mario	Advisor, Economic Development Agency of Canada
Poellhuber, David	CEO, Zerospam
Reverd, Christophe	President, Auditia
Talbot, Éric	President and co-owner, S.I.C. Biometrics
Tremblay, Charles	Commercial Director, Notarius
Vézina, Guy	Director General, Defence R&D Canada - DRDC

We are grateful to a number of people in the community sector. The advanced security sector is represented by a number of specialized associations that helped us promote the study, and distribute it. From the design of the questionnaire to its analysis, their input was indispensable.

Pepin, François	President, Information Systems Audit and Control Association (ISACA)
Boutin, Michel	President, Metro Montreal Information Security Association (ASIMM)
Marrette, Bob	Executive Director, Canadian Society for Industrial Security (CSIS Inc)
Lane, Greg	President, Canadian Information Processing Society (CIPS)
Edmond, Mona	Marketing Director, Canadian Security Association, CANASA

We would like to thank everyone who answered our questions in the interviews that served as the basis for the case studies. They showed a generosity and patience that are quite remarkable in an industry with a reputation for discretion. In addition, each of the 155 company executives who answered our survey deserves our thanks.

Disclaimer:

The CATA Alliance and the ScienceTech team assume responsibility for any error and omission that may have slipped into this study on the advanced security industry in Canada. Neither the many people who generously contributed to this project nor the partners nor the clients that put their trust in us can be held responsible for the content of this study.

3. Industry Profile

3.1 Age of the Corporations

An analysis of the structure of the industry reveals that advanced security companies are young. Most of them were created after 1995 – the year that the Internet began to be felt on the economy.

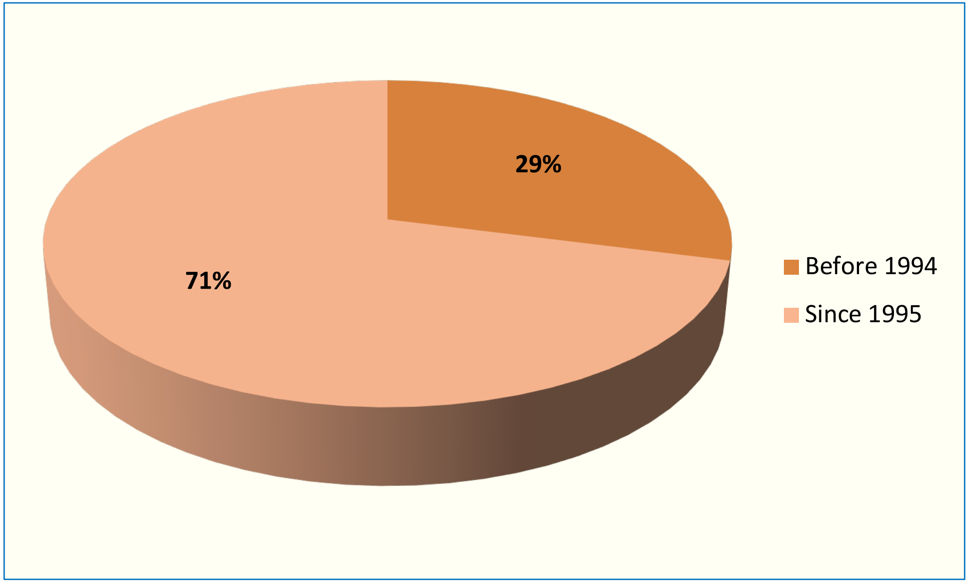
Internet impacted information security – as foreseeable – and also physical security (video surveillance cameras linked to control centres).

Likewise, one has to consider Internet's double impact:

- Firstly, the network helps security management (video surveillance).
- Then, it generates a new vulnerability (computer crime).

FIGURE 6 – MORE THAN 70 PERCENT OF FIRMS ARE "INTERNET CHILDREN"

In what year was your company established?



Source: CATA Study – Montreal, February 2011

3.2 Size and Nature of the Companies

A – Size of the Company and of the Security Team

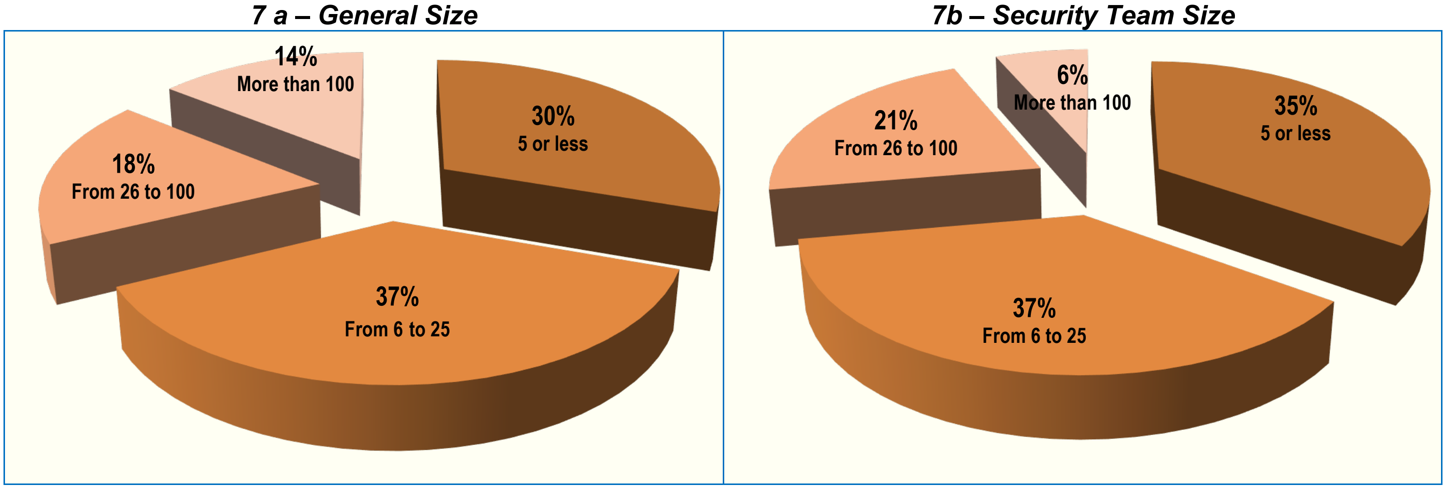
First, it is important to distinguish two different concepts: the size of companies that perform advanced security and the size of teams of specialists that work in security. Indeed, a security specialist at DMR may well operate within a small team of about thirty people, but his work environment cannot be compared, for example, with that of a company such as Cryptocard in Ottawa, which also employs 30 people.

Indeed, DMR's security team is integrated in a company that counts 1,400 employees in Canada and 170,000 in the world (including the parent company Fujitsu). The Canadian team has the support of an entire ecosystem of security professionals located in 70 countries. Cryptocard's 30 employees can only rely on their own resources to innovate, find new customers, sell ... and make ends meet. Two worlds are at play here.

The study's main finding is that the security industry is composed of small businesses and teams. The vast majority of companies (67 percent) have fewer than 25 employees (Figure 7a). The proportion rises to 72 percent (Figure 7b) when you take into account only the employees assigned to security. Security is therefore a matter of very small teams working in very small businesses.

FIGURE 7 - SIZE OF THE COMPANY

How many full-time employees currently work for your company?



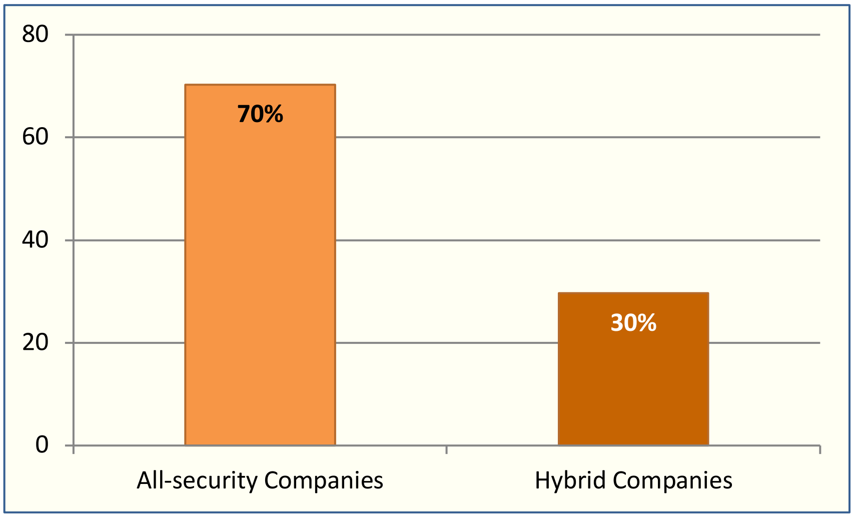
Source: CATA Study – Montreal, February 2011

> There are many more consultants and micro firms in Quebec than in Canada. This is explained by the important lay-offs in many IT firms in recent years. Those unemployed specialists and engineers opted for consultation.
>
> *Marc Fournier, Associate Partner, Price Waterhouse Coopers*

B – Hybrid Companies and Pure Players

There are many more security firms that are specialized than diversified (70 percent of specialists for 30 percent of hybrids). Pure players are mostly SMEs, only six companies have more than 100 employees and only one has over 500 employees (Entrust). Conversely, some companies have hybrid teams that are relatively large, even though security represents less than 1 percent of their revenues. (Deloitte, CGI, Bell).

FIGURE 8 –THERE ARE MORE PURE PLAYERS THAN HYBRID COMPANIES...

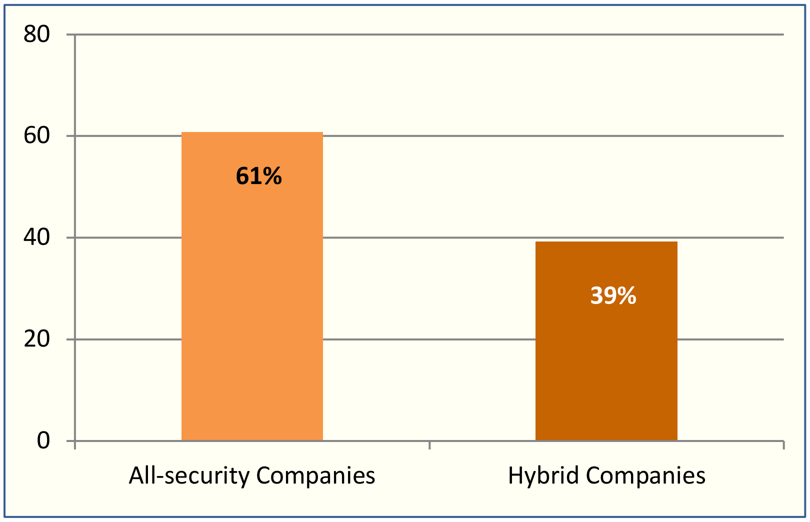


Source: CATA Study – Montreal, February 2011

In terms of employment, pure players still outclass hybrid companies (slightly more than 60 percent all-security companies against nearly 40 percent hybrids). Some hybrid companies even are among the major players in the advanced security sector. Many of these large hybrid companies are marketing commercial security related products and services originally developed to complement their traditional offering. An example of this type of company is Deloitte or PwC which consider information security as an extension of business services.

All the major pure players (100 employees and more) are located in Ontario. It is to be noted the interesting growth of Montreal-based Silanis that still counts less than 100 employees but has been very successful on the U.S, market.

FIGURE 9 – ... BUT HYBRIDS TEND TO BE BIGGER



Source: CATA Study – Montreal, February 2011

> The only way to increase the number of our employees would be to sell outside Quebec but to do that you need revenues and our sales in Quebec do not generate surpluses.
>
> *David Poellhuber, CEO, Zerospam*

C – Main Types of Activities

More than two-thirds of respondents are service providers. Indeed, most software editors are also service providers.

The strength of the Canadian Advanced security industry lies in the software editors. This does not mean that professional service does not create value. Enhancing business processes, reducing operating expenses and eliminating waste to introduce more efficient practices, delivering increased earnings from production rises or winning new markets: this adds value.

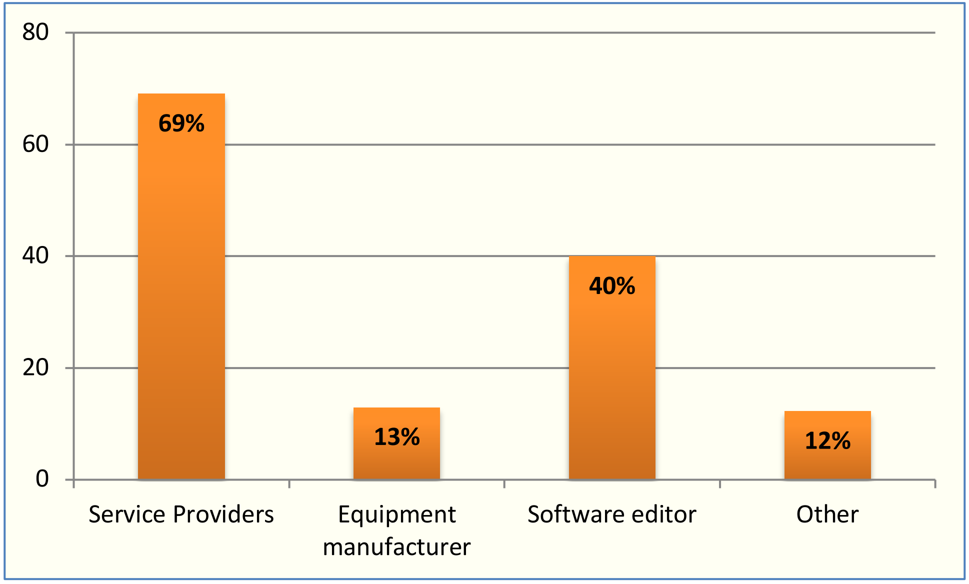
However, the operational mode of a professional services firm is to be under contract. The company sells its expertise by billing the work time of its human resources. On the contrary, a software publisher or equipment manufacturer proceeds in two steps: First, he invests (infrastructure and R&D) and then markets its products.

This two-step process enables software vendors and manufacturers to separate the profits from the work and billed time. If R&D remains dependent on work time, marketing activities and sales are to a much lesser account. Insofar as the innovation corresponds to a market need and the marketing of the product is effective, the software vendor or manufacturer enters a virtuous circle of pure value creation – R&D investment result in superior customer satisfaction which in turn will improved sales, and some of these profits can be reinvested in R&D thereby initiating another iteration of a virtuous cycle.

It is to be noted that more than 70 percent of the Canadian software editors are based in Ontario. Besides the well-known firms such as Entrust and Certicom, there is also the ecosystem of innovative SMEs created by Research in Motion (RIM) to secure the Blackberry and its servers. These large firms are the engine fuelling demand for even greater innovation. It can be said that Ontario's advanced security industry has entered this virtuous circle of pure value creation.

FIGURE 10 – COMPANY ACTIVITIES

How would you define your company? [Multiple answers are allowed.]



Source: CATA Study – Montreal, February 2011

Analysis

Ontario could become the growth engine of the Canadian security industry as a whole. But this would require a better coordination at the national level. Most local SMEs are not linked to the industry leaders so when they run short of cash flow they seek to be purchased by U.S. companies. As a result, the industry seldom reaches a critical mass, R&D remains low and the decision-making control is lost. Networking between advanced security innovative SMEs should be encouraged.

D – Activities Details

Many companies indicated that they covered the full range of security activities. These are mainly professional service providers whose raison d'être is to offer as wide a range of services as possible. Some firms, however, are specialized in cryptography, biometrics, backup systems or IP surveillance, but they are the exception. Service providers are management consultants or advisors in ICT and offer increasingly outsourced services, mainly because clients find it difficult to manage this activity.

Software publishers and manufacturers of equipment – that are also often both publishers and manufacturers – represent another reality. For example, in 2003, authentication was the activity of choice for the Canadian industry. Such an activity covers a range of technologies such as biometrics, cryptography and smart cards.

IP surveillance is still popular, along with a new activity: mobile security. Some companies are mainly oriented towards software and products related to defence. However, they are diversifying their offers towards civil security through the applications for first responders, whose needs are similar to those of defence. This is the case of optical detection software, for example.

One noteworthy point is the frequency of training activities among service providers, independent software vendors and equipment manufacturers. Is the market experiencing confusion vis-à-vis security? The surveyed companies made it clear that to sell security services and products, one needs not only to educate clients, but also to train them.

In addition, computer security issues now relate to a much more complex process of management and governance. Legislation and regulation on the protection of personal information are constantly evolving. As a result, security and training go hand in hand.

Electronic Security

The World Economic Forum places Canada third in the world for the number of secure Internet servers per capita. The security software market is the fastest growing in Canada. Its value was estimated at over $300 million in 2006, and its annual growth was 12.1%. It was expected that the expenses related to security would experience a compound annual growth of 10.75% over the next five years to reach a value of $ 440 million in 2010.

Vincent Butaye, Walloon Agency for Export and Foreign Investment (AWEX), May 2010.

3.3 A Centralized Industry

The heart of Canadian security is in Ontario, which has 341 businesses, more than half of the entire industry compared to 149 in Quebec or 22 percent of the industry (see Figure 11). In general, we can say that the situation is comparable to 2003.

The number of Canadian companies fell about 5 percent between 2003 and 2010. The province most marked by the movement of rationalization and concentration of the industry is Quebec. Everywhere else, except the Atlantic, there has been no more than a levelling.

FIGURE 11 – INDUSTRY PROVINCIAL DISTRIBUTION

Regions	2003		2010	
	Cies	%	Cies	%
Ontario	342	49.0	341	51.3
Quebec	181	25.9	149	22.4
British Columbia	72	10.3	70	10.5
Prairie	66	9.5	62	9.3
Atlantic	37	5.3	42	6.3
Territories	0	0	1	0.2
Canada	698	100	665	100

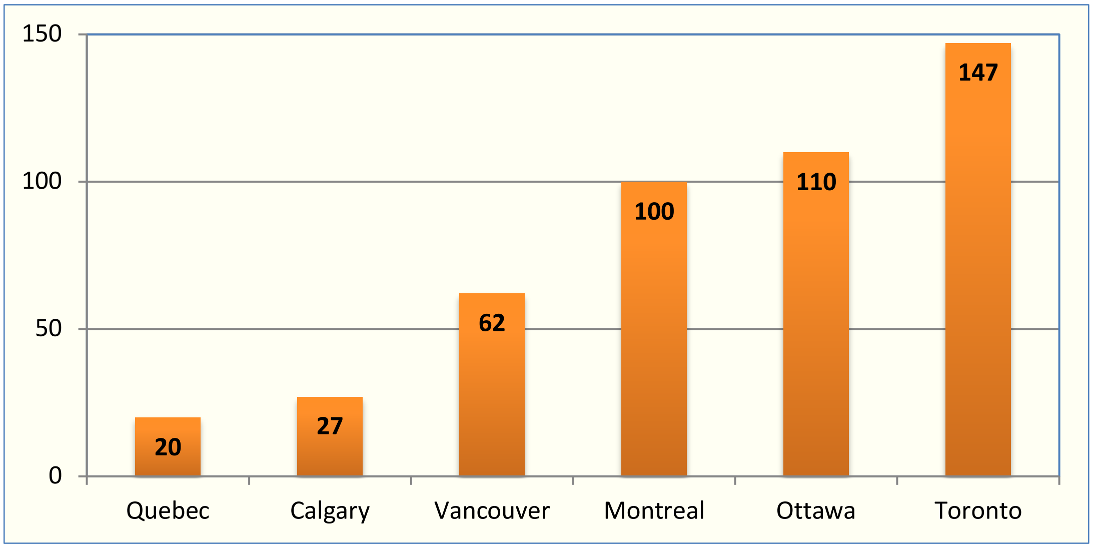
Source: CATA Study – Montreal, February 2011

About 70 percent of the advanced security industry is concentrated in the following six cities: Toronto, Ottawa, Montreal, Vancouver, Calgary, and Quebec City (see figure 12). Advanced security companies are naturally clustered around their primary markets i.e. very large businesses, banks and government agencies.

However, in 2003 these same six hubs accounted for close to 80 percent of the industry. This decrease may be due to the new extension of the security market towards SMEs.

Strategic security hubs (Toronto, Ottawa, and Montreal) compete between themselves and on the international markets. Secondary hubs (Vancouver, Calgary, and Quebec City) face a tougher competition and focus on selected niche markets.

FIGURE 12 –SECURITY INDUSTRY HUBS[18]



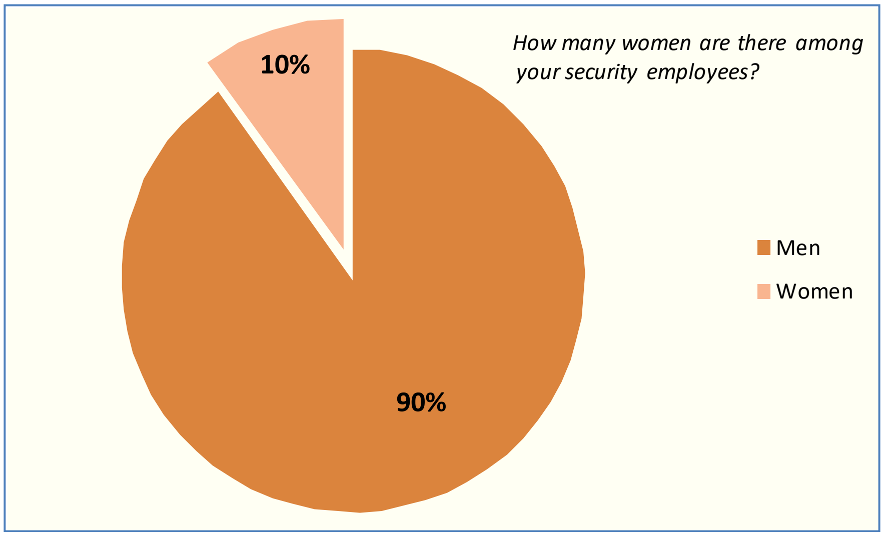
Source: CATA Study – Montreal, February 2011

3.4 An Abnormally High Gender Gap

With 10 percent of jobs, women are virtually absent from the Canadian advanced security industry.

However, the sub-sector of the Advanced Security is not homogeneous. More than half of women security experts are found in companies with 100 employees or more. At the other end of the scale, there are almost no women among the self-employed consultants.

FIGURE 13 - WOMEN ARE UNDER-REPRESENTED



Source: CATA Study – Montreal, February 2011

[18] All figures refer to the urban community in these cities. Toronto includes the 25 member municipalities of the Greater Toronto Area; Montreal includes 48 municipalities, members of the Metropolitan Community; Ottawa includes 11 municipalities that were merged in 2001; Vancouver' includes 21 municipalities of Metro Vancouver; and Quebec City includes the 28 municipalities of the Quebec Metropolitan Community (CMQ). Only Calgary has been regarded as an independent entity.

Analysis

It is known that women are underrepresented with a meagre 30 percent presence in the ICT industry and even less if it is a high-level position. But why does advanced security only attract 10 to 12 percent of women in its ranks?

It seems easier to attract women to become a police officer than to work in computer security. The United States has 100,000 women in charge of policing, i.e. 12 percent of all services. But their proportion was 25 percent in federal agencies and police forces in major urban centres.[19]

The women employment rate in the security industry (10 to 12 percent) should be compared with that of police forces in major centres (25 percent) for advanced security firms are mostly located in urban centres (see 3.3 - *A Centralized Industry*).

This comparison indicates that women do not shun "repressive" environments. The causes for the lack of attractiveness of the sector can be found in the structure of employment, for example, its lack of job security, time constraints, or in the culture of the ICT industry. This situation is not going to change unless government provides a comprehensive strategy with incentives.

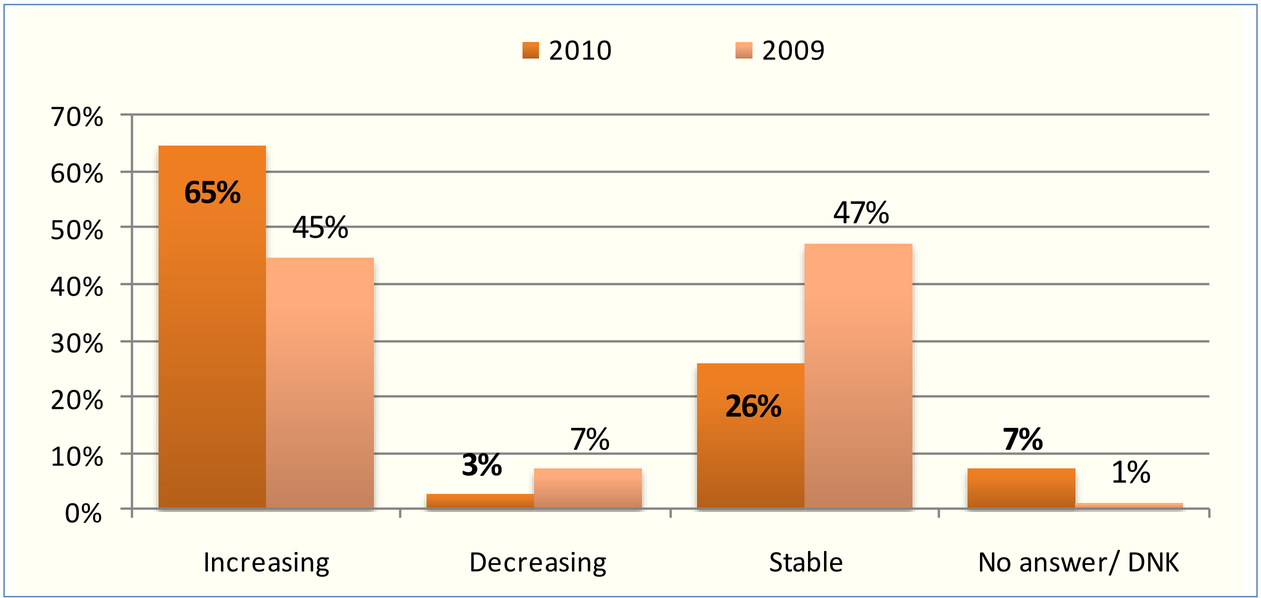
3.5 Financial Crisis Impact upon Employment

The financial crisis of 2009 had a limited impact on advanced security. Only 7 percent of Canadian companies say they experienced a decrease in the number of employees in 2009, while 45 percent say they registered an increase. The financial crisis has mainly resulted in job stability (47 percent).

In 2010, security firms were confident in their forthcoming sales and more than two-thirds of companies (65 percent) were hiring.

FIGURE 14 – VARIATIONS IN THE NUMBER OF EMPLOYEES

In your company, is the number of employees increasing? Decreasing? Stable? Do not know (DNK)?



Source: CATA Study – Montreal, February 2011

[19] Lynn Langton, Statistician, "Women in Law Enforcement, 1987–2008", Bureau of Justice Statistics, U.S. Department of Justice, Washington, June 2010.

Our sales in Europe have protected us from recession but the bottom line is stable, not increasing.

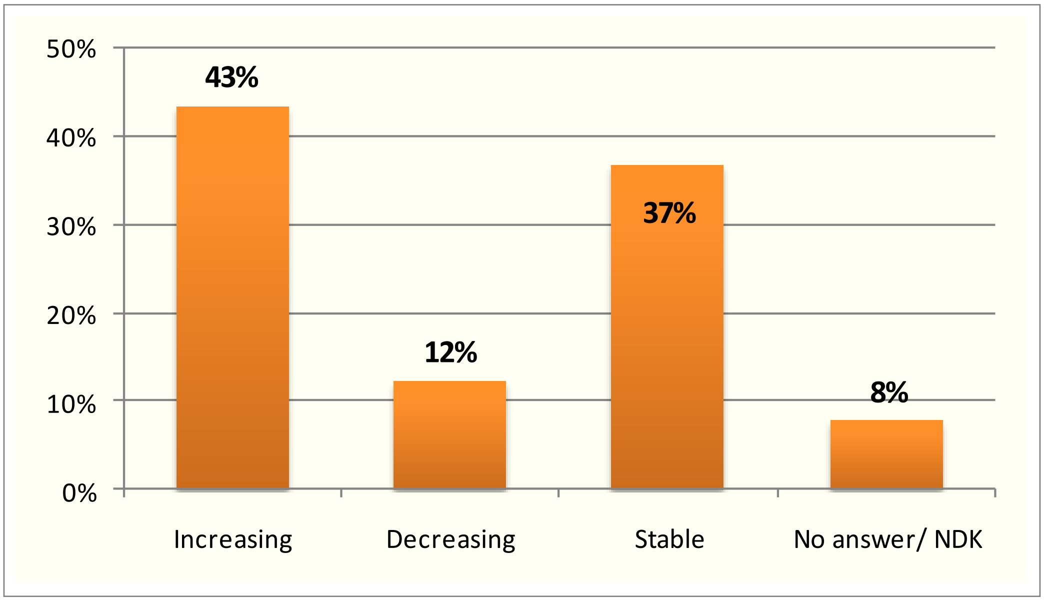
Éric Bergeron, President, Optosecurity

3.6 Financial Crisis Impact upon Sales

Similarly, 43 percent of Canadian firms have increased their turnover in 2009 even though a financial crisis was ongoing. These results confirm the employment figures: the crisis has had a relatively low impact in the Canadian security industry.

FIGURE 15 – SALES VARIATIONS DURING THE FINANCIAL CRISIS (2009)

How would you qualify your sales in 2009? [security only]



Source: CATA Study – Montreal, February 2011

What are the reasons for such good performance? Part of the answer could be provided by the practice of large consulting firms to resort systematically to outside consultants: the non-renewal of consultants' contracts does not appear in the employment figures.[20]

Large firms are dependent on the signing of important contracts. When they lose an account, a lot of people are let go and start their own firm.

Marc Fournier, PricewaterhouseCoopers

Another possible answer could be the introduction of the PCI DSS security standard that became compulsory at the end of the year. An important segment of the SMEs working with credit card users had to upgrade their payment systems to become compliant with the new standard – and most of them had to call upon a security firm for the first time.

Finally, the 2003 results indicate that 89 percent of respondents said their sales were on the rise - against 43 percent in 2009. This perspective allows us to estimate that the financial crisis has caused a slowdown

[20] A question on temporary employment was asked in the survey (In your company, how many consultants work part time in security?), but it did not produce significant results.

in the growth of the security industry going forward - a slowdown but not a real setback (the percentage of companies recording a decrease of their sales was low - 12 percent).

3.7 Level of Advanced Security Employment in Canada

The surveyed sample accounts for 5,450 skilled workers in the field of security.

Analysis

It is difficult to quantify accurately the total number of people employed in the Canadian advanced security industry. A simple extrapolation gives a population of more than 23,000 people (23 percent of companies responded to this question).

In 2003, by the same method of extrapolation, a number of 21,000 were estimated. Because both 2003 and 2009 were approximations, it is not possible to draw definitive conclusions. However, we can indicate a tendency for security employment to rise slightly over those 7 years.

One cause for this low increase can be attributed to the 2008-2009 financial crisis that slowed its progress – even though it minimally impacted the industry.

The other question, more structured, is the large number of independent consultants or freelancers who are, by definition, difficult to identify and rarely respond to surveys. The 23,000 persons identified are, therefore, the core of an industry that may be somewhat larger.

4. Market Trends

4.1 Size of the clients

When asked who their clients are, more than 80 percent of advanced security firms answered large companies, 53 percent SMEs, and 9 percent micro-enterprises.

Half of the respondents that answered "large companies" also serve SMEs.

What is even more interesting is the emergence of a group of advanced security firms, which only serve SMEs and micro-enterprises: 18 percent of the respondents.

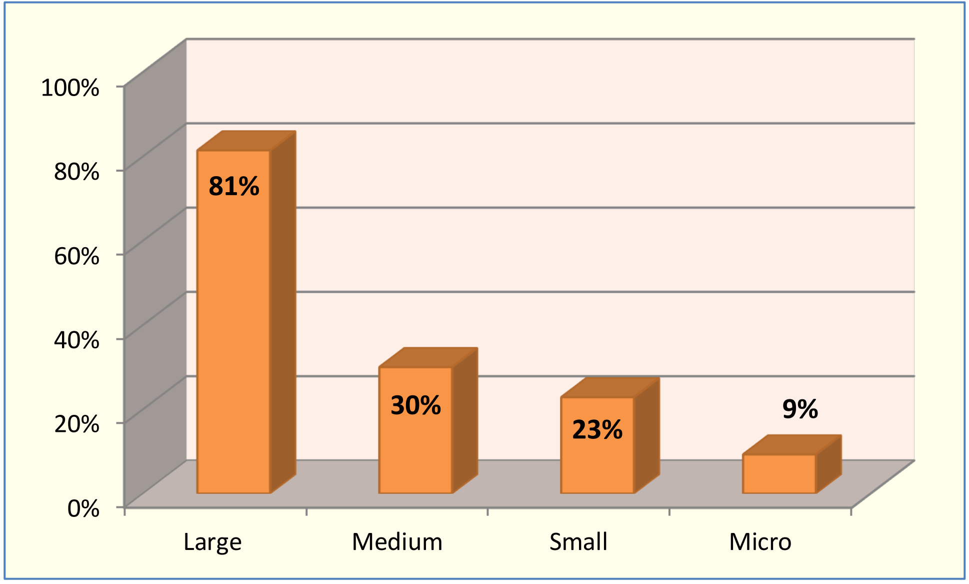
SME Definition

In this report, advanced security companies are categorized under the following employment size ranges:

- Large 500 + employees
- Medium 50-499 employees
- Small 10-49 employees
- Micro 1-9 employees

FIGURE 16 – THE MARKET IS STILL DOMINATED BY LARGE CORPORATIONS

Who are your main clients? [Multiple answers are allowed.]



Source: CATA Study – Montreal, February 2011

Analysis

A market dominated by a few large customers is a clear sign of immaturity. Indeed, large or very large companies are the early adopters of security services. They created teams dedicated to security back in the days of mainframes. The advent of shared access systems has imposed internal security policies. The arrival of the Internet has changed the entire process by opening the system to the outside. Large businesses had to adapt.

On the contrary, SMEs had no concern over security problem until the advent of the Internet for good reason: it was not computerized. For the minority who had acquired desktop before 1995, they were used in standalone mode and when it was connected to private networks, it was through rudimentary systems such as a shared printer used in a common space with special security measures requirements.

Today, the big challenge for security companies in Canada is to penetrate the SMEs market. This is precisely what a minority of advanced security firms is doing.

To win, security companies first need to adapt their offer to this new market. There must be a shift from a product offering high-end completely customized, to an offer based on semi-standardized, affordable and easy maintenance.

That is why the emergence of a minority of advanced security firms serving only the SME is a sign that never fails: the Canadian Security is taking the SMEs turn.

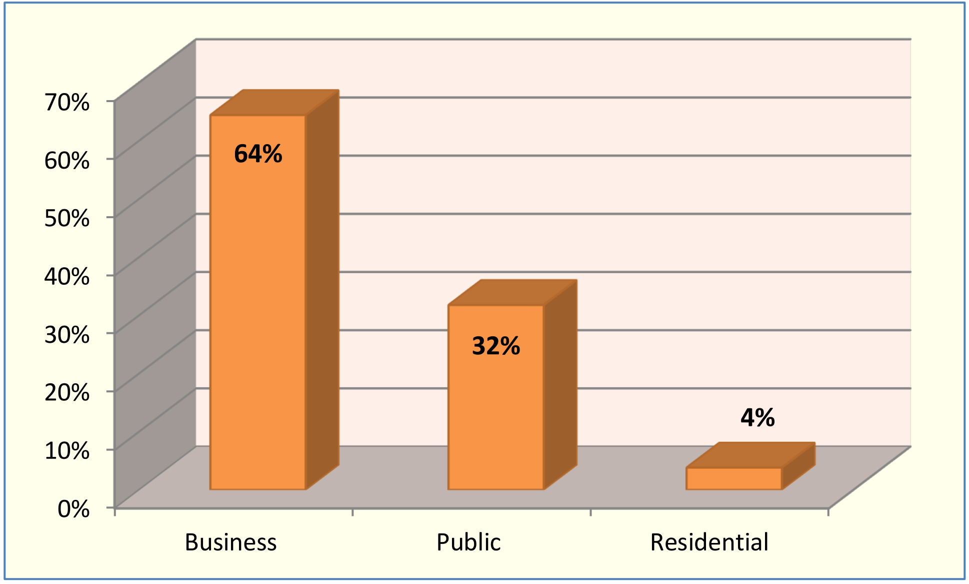
> This allows us to offer a la carte services and to intervene, for example, only on intrusion detection or vulnerability management. We also offer economical packages that bundle services. This pricing flexibility is the solution adapted to the needs of SMEs.
>
> *Marco Estrela, Vice President, Virtual Guardian*

4.2 Main Market Sectors

The advanced security industry mainly sells to the private sector: more than two-thirds of its clients are private companies whilst a third includes public sector organisations. In the private sector, financial institutions dominate the market (banks, insurance, and brokerage firms).

FIGURE 17 – MARKET DISTRIBUTION BY SECTORS[21]

What percentage of your clients work in the... business sector? government and semi-public sector? residential sector? [The sum of the numbers entered must equal 100.]



Source: CATA Study – Montreal, February 2011

This significant public sector presence in the market for advanced security is unsurprising. Security is part of the traditional functions of the State. Well beyond simply maintaining order, security imperative guides the action of the State in a variety of markets: health and education, defence and public security (police and first responders), transportation (ports and airports), local authorities (municipalities,

[21] Percentages do not refer to the number of companies but to the actual level of activities. When a company says 75% of its sales go to the business sector and 25% to the public sector, our graph reflects the rates.

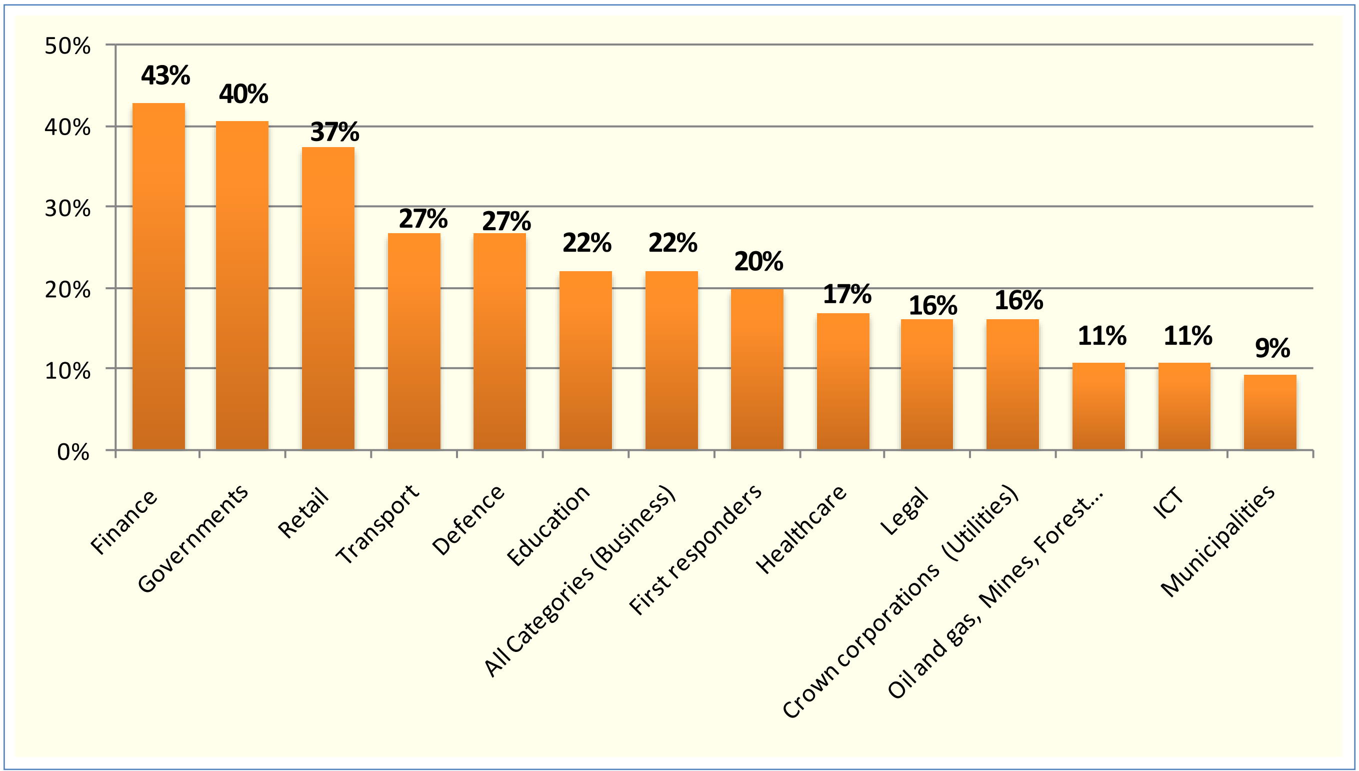
districts/counties), etc. In all its dealings with citizens and businesses, the State and its agencies must ensure the security of transactions and respect for privacy. This is reflected in the market for goods and security services.

The legal sector (lawyers and notaries) is also dynamic and plays a role not only as a market for advanced security, but also as a producer of goods and services. Lawyers and notaries are creating certification centers – Notarius in Quebec, Juricert in British Columbia – that provide registration services which are legally required to validate online identity. But registration service is only the tip of a legal iceberg likely to play a growing role in the security industry and its extension as privacy protection**.**

Secure infrastructure, including energy, may seem underrepresented (10 companies included in the Crown Corporations category), but when viewed with the transport category (35 companies), we realize its importance within the advanced security industry. Note however that this is not an integrated market, but rather a collection of many disparate markets.

FIGURE 18 –FINANCE STILL IS THE FIRST CLIENT OF THE SECURITY INDUSTRY

Within those sectors, please indicate the field in which your clients work.



Source: CATA Study – Montreal, February 2011

> Security is the stepchild of the SMEs. But it is they who are the main targets of pirates who train on SMEs before tackling large corporations such as banks and governments.
>
> *Véronique Olivier, Waveroad Consult*

5. Interprovincial and International Trade, and Growth Strategy

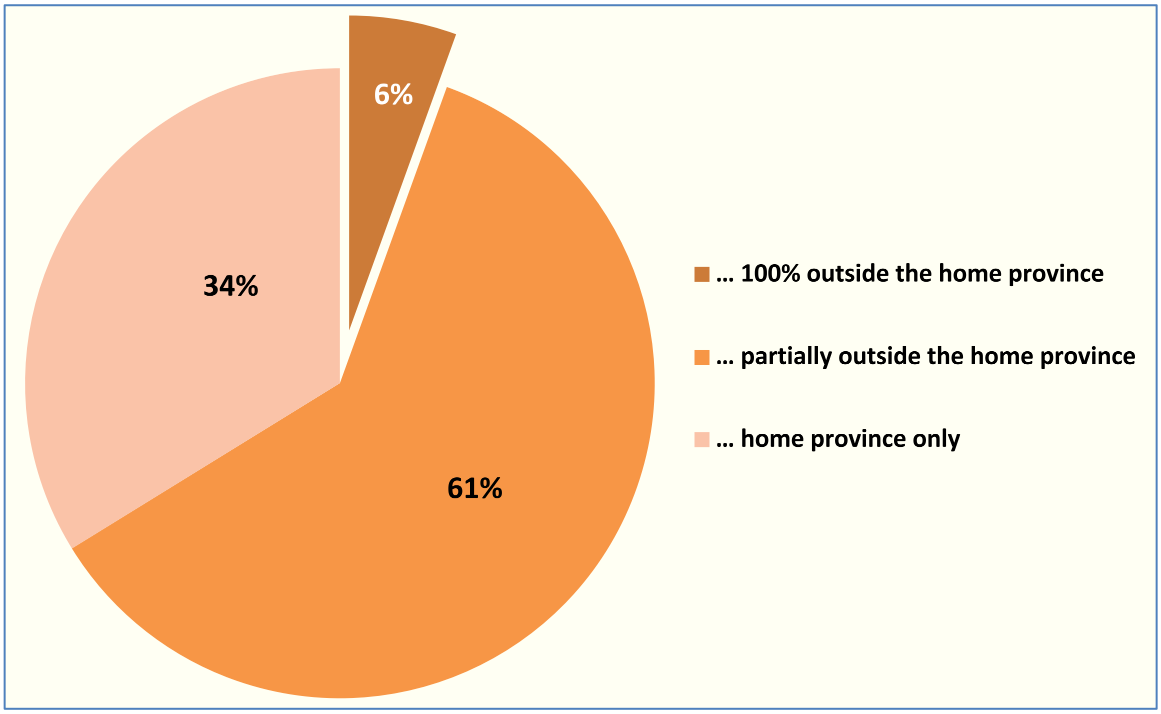
5.1 Domestic and International Trade Distribution

Two-thirds of the advanced security companies export outside their home province (96 companies out of 145 respondents). This result includes shipments towards other provinces (interprovincial trade) and towards foreign countries (international trade). The Canadian advanced security industry is predominantly open to the outside markets.

A small group of eight companies sells all its production outside its home province. It is interesting to note that almost all these companies are based in Quebec (seven out of eight). The typical company in this small group is Silanis who sells electronic signature solution in the United States: This enterprise was founded in 1992 in Canada but does not sell anything domestically. Conversely, 49 out of 145 companies reported only serving their province of origin (i.e. 34 percent of respondents).

FIGURE 19 – AN EXPORT INDUSTRY

What percentage of your sales do you ship to… your home province? elsewhere in Canada? to the United States? to other countries?



Source: CATA Study – Montreal, February 2011

> We only sell outside of Canada. The only reason we are in Montreal is because of the tax credit for research and the good universities.
>
> *Tommy Petrogiannis, CEO, Silanis*

Regarding the intensity of shipments, results should be weighed because the bulk of sales is directed towards the domestic market: in addition to 49 companies that sell only on intra-provincial trade, 39 others will make more than 50 percent of their turnover. Moreover, large professional services firms (PwC, KPMG ...) and large ICT consulting firms (Bell, Telus ...) tend to serve the local market primarily. However, a company such as Deloitte exports 30 percent of its services out of Canada. CGI and Nurun have a world strategy (based on hiring local residents).

FIGURE 20 – SALES VOLUMES BY MARKETS

(Number of companies)

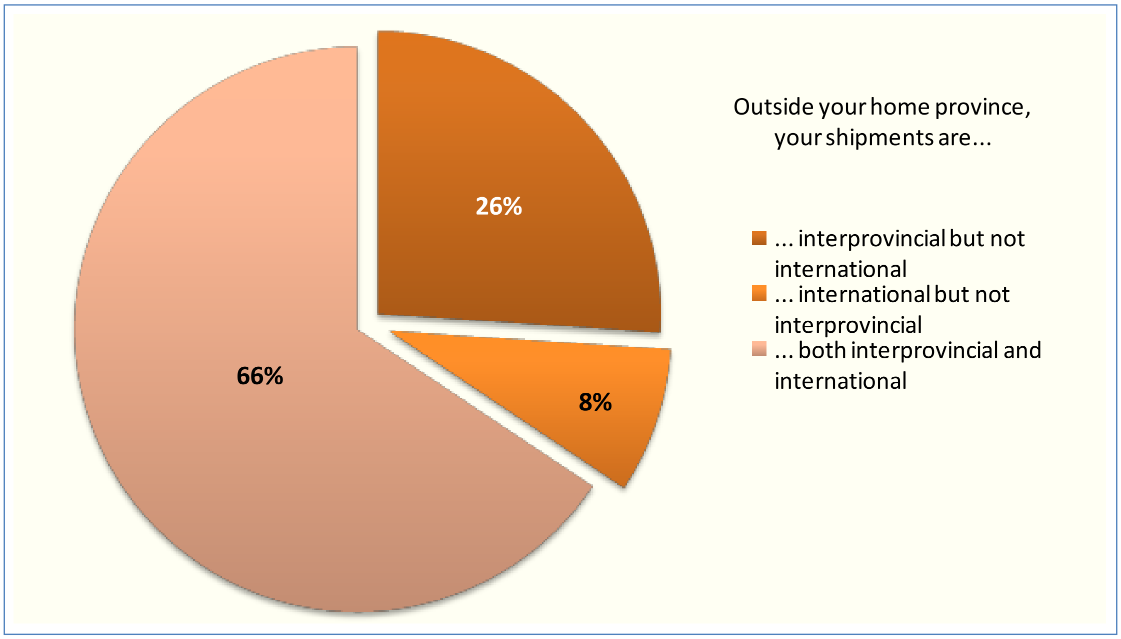
What percentage of your sales do you ship to…	… your home province	… elsewhere in Canada	... in the United States	… other countries
0%	8	56	84	78
1-25%	27	38	27	30
26-50%	22	37	26	27
51-99%	39	13	7	9
100%	49	1	1	1
Total (companies)	145	145	145	145

Source: CATA Study – Montreal, February 2011

If one considers only companies that sell outside their home province, we see that only 8 percent sell exclusively on international markets - without also trading on interprovincial markets.

Conversely, 66 percent of advanced security companies sell both in Canadian provinces and abroad. Sales in other Canadian provinces seem to be a first step to take before facing the international markets.

FIGURE 21 - INTERPROVINCIAL TRADE IS A SPRINGBOARD TOWARDS INTERNATIONAL EXPORTS



Source: CATA Study – Montreal, February 2011

On world markets, Canada is perceived as a worthy partner who offers excellent services. This reputation helps us in our business.

Marcel Dion, CEO, Above Security

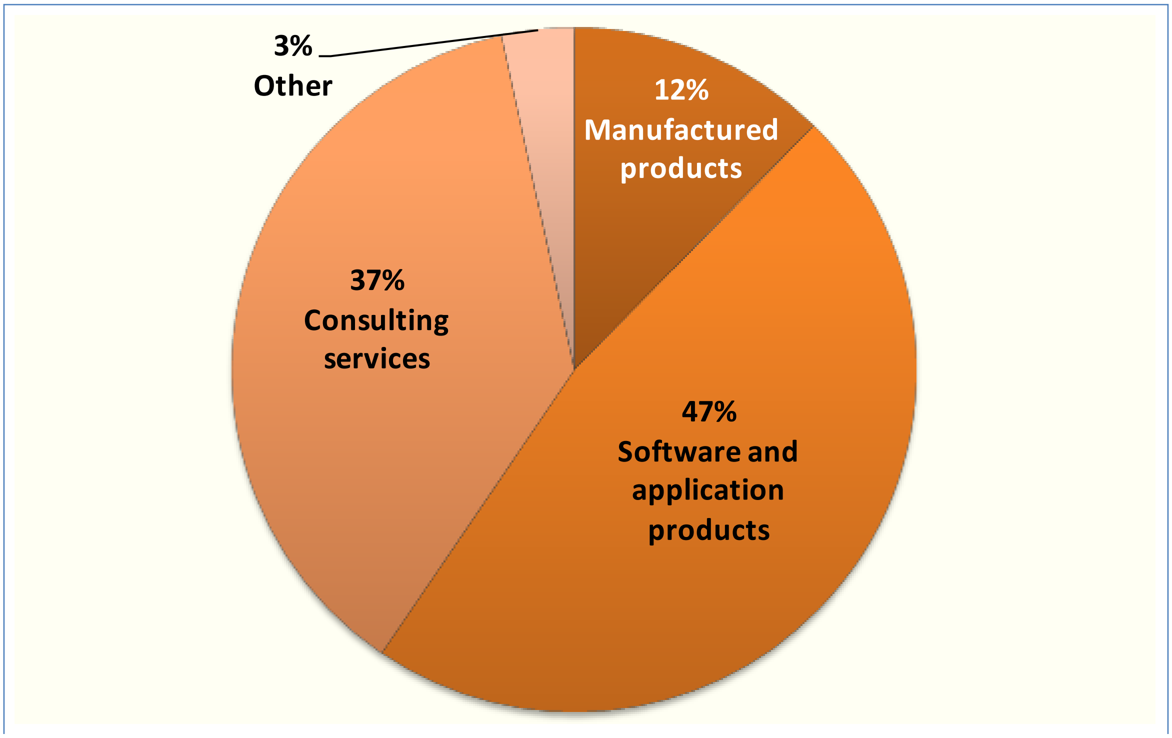
5.2 Nature of Interprovincial and International Trade

Close to 60 percent of interregional and international exports are made up of software and application products (47%) and manufactured products (12%) – whilst consulting services account for only 37 percent even though this sector is the most important in advanced security. (see figure 10 – Company Activities). The proportion of manufactured products is relatively small, as there are not many advanced security manufacturers. However, all manufacturers export.

> We work in the United States and in the Middle East through alliances with firms that complement our services. This enriches our technological know-how because security cultures vary in each country.
>
> *Mathieu Chouinard, President, In Fidem*

FIGURE 22 –SOFTWARE APPLICATIONS DOMINATES EXTERNAL TRADE

For those who sell outside of their home province, what is the proportion of manufactured products? software and application products? consulting services? other?



Source: CATA Study – Montreal, February 2011

Analysis

The relatively large proportion of manufactured products and software applications in the advanced security interprovincial and international trade reflects the “exportability” of these goods – in spite of their intangible nature, software applications behave like hardware products in the value chain. Once developed on a production site, these items can be shipped everywhere in the world under their definitive format.

More surprising is the fact that almost 40 percent of the advanced security interprovincial and international trade is made up of consulting services. This demonstrates the obsolescence of traditional economic theory that says services do not lend themselves to international trade because of their their intangible nature and the impossibility to store them and. Mass digitization information and a large number of processes has transformed the nature of services, as explained very well Statistics Canada:

> *« However, these characteristics have been somewhat influenced by technological changes. Producers and consumers can now more easily exchange services at great distances via telecommunications networks. As well, certain services (ie: tele-health, tele-education and on-line banking) that have traditionally been considered nontradable can now be exchanged electronically. »*[22]

Yet we must distinguish between the unquantifiable, non-storable and non-reproducible tailored service, and all other commercial services. For example, the development of a safety audit or a management plan requires a close interaction between supplier and customer. These are services that do not export easily – unlike commercial services such as financial services, telecommunications, remote maintenance or access to information media.

The very model of a commercial service is the e-SignLive electronic signature developed by Silanis Technology to enable people located in various parts of the globe to certify electronic documents based on the IBM LotusLive platform and available by subscription. The system guides the user step by step through the document to complete and sign (legal contracts, purchase orders, confidentiality agreements, insurance policies, credit applications, etc.). A first version of this service was launched in April 2010 and is currently managed by an independent division of Silanis. Once the incubation period ends, the division may, if necessary, be outsourced and incorporated.[23]

In this way, the electronic signature software which is the staple service of Silanis is transformed into a commercial product and retains all its exportability features.

In Europe – 50 percent of our company sales – our sales strategy is based on a network of resellers and partnerships with physical security firms such as ADT, Prosegur and Accenture.

Eric Talbot, President, S.I.C. Biometrics

5.3 Export Growth Strategy from 2010 to 2012

A slight majority of firms want to develop new export markets in 2010. They are both companies who already have experience in exports and local companies. Large professional services firms are very active in interprovincial trade, but not on the international markets. It is mainly SMEs that target world markets.

Micro-enterprises, almost exclusively, serve the local market.

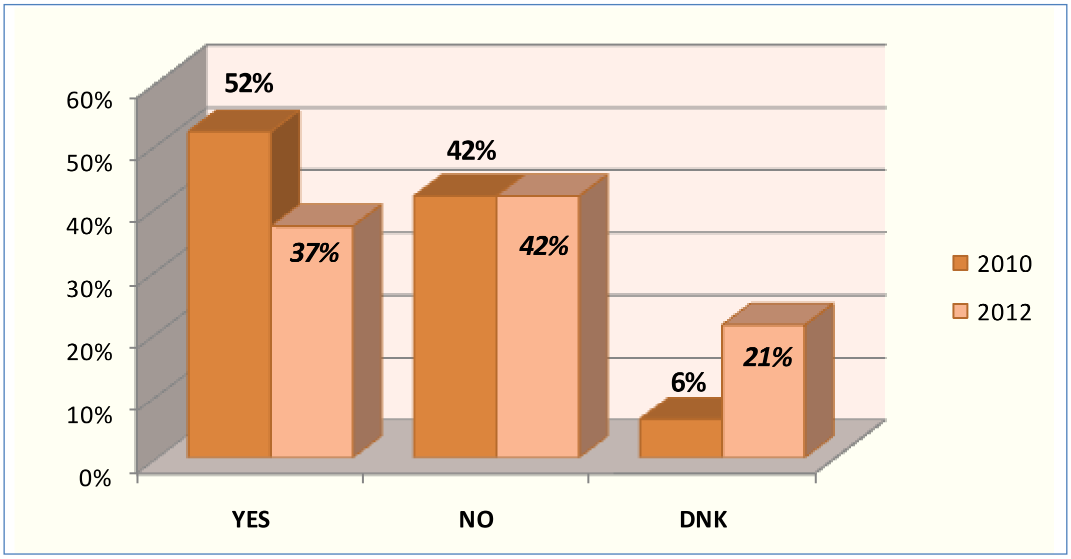
The United States is still the best target market but more and more companies now target emerging markets such as Africa and the Middle East.

Eric Talbot, President, S.I.C. Biometrics

[22] Christine Roy, *The services industries and trade in services*, Service Industries Division, Statistics Canada, August 2001.
[23] See web site e-SignLive - http://www.e-signlive.com/

FIGURE 23 - A MAJORITY OF COMPANIES INTENDS TO INCREASE INTERPROVINCIAL AND INTERNATIONAL TRADE

Are you targeting new markets outside your home province?

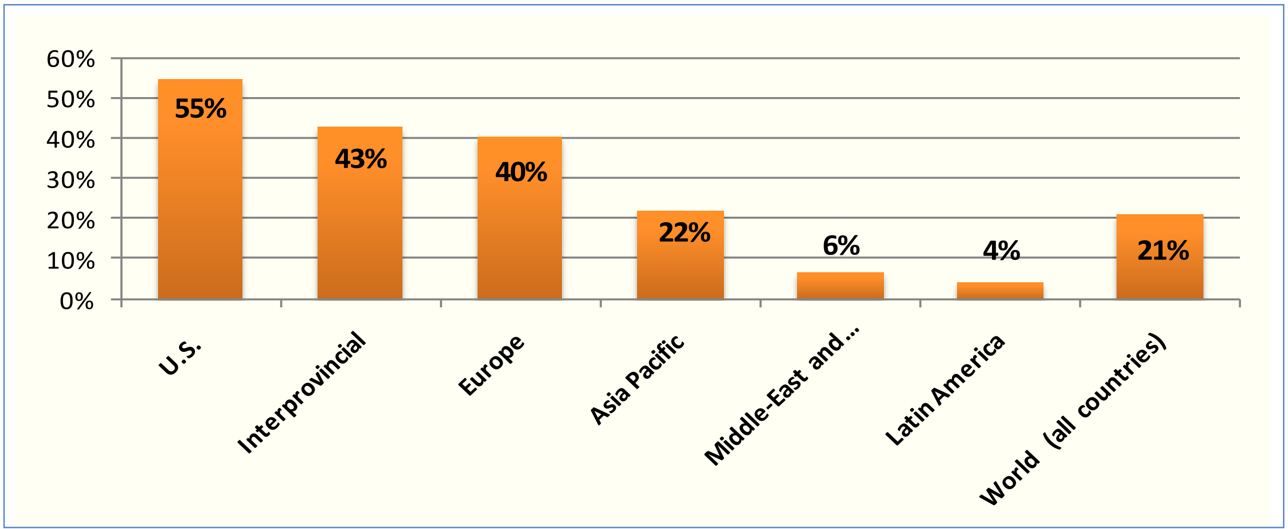


Source: CATA Study – Montreal, February 2011

The United States, Europe and other Canadian provinces remain the destinations of choice for expanding exports. Among the companies that say they want to attack the European market, few of them mention a particular country (Great Britain: 5; France: 3). Curiously enough, the Asia-Pacific region is seldom mentioned by the respondents among the areas of growth.

FIGURE 24 – DISTRIBUTION OF TARGET MARKETS (FORECASTS FOR 2012)[24]

[Multiple answers are allowed.]



Source: CATA Study – Montreal, February 2011

[24] Our question was about 2010 and 2012 forecasts. As most respondents answered the same thing for both years, we merged the answers.

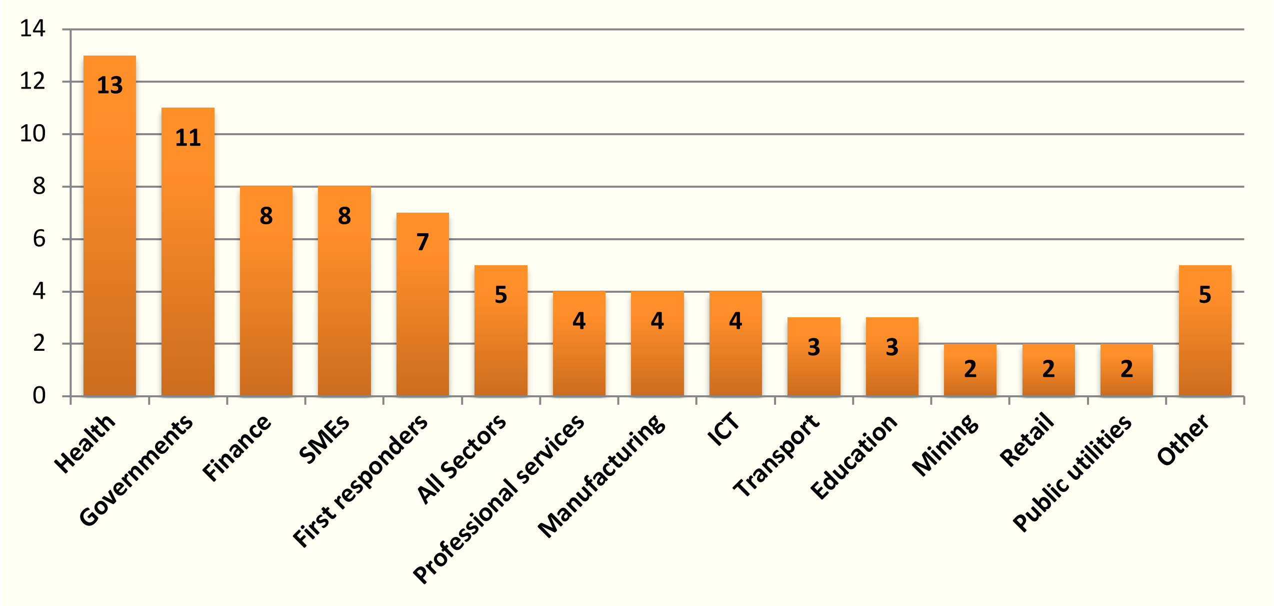
A relatively high proportion of respondents intend to export in the whole world. In a few cases, this means their products actually can be sold on the world market. But in the majority of cases, this only indicates the corporation indecisiveness.

5.4 Market Sector Diversification from 2010 to 2012

Few companies have answered the question on supply diversification (43 respondents), making it hazardous to try to identify a strong trend. Note also that the supply diversification is similar to the current supply (Figure 18 - Finance still is the First Client of the Security Industry), with the exception of health that has strong growth prospects.

FIGURE 25 – DISTRIBUTION OF TARGET SECTORS (FORECASTS FOR 2012)[25]

Are you targeting new markets inside your home province? (please specify what economic sector)



Source: CATA Study – Montreal, February 2011

Eight respondents identified SMEs as an independent market, which is revealing of a new behaviour. Security firms begin to consider SMEs as a homogeneous category with common features all across the economical sectors. One respondent indicated he was designing incident management templates aimed at SMEs to automate incident reporting, management, and analysis at an affordable price.

> An alternative strategy is to systematically attack the SMEs market.
> To address this market, we adopted a strategy that differs from what is used with large companies.
> We offer a package of consulting services at a fixed price through a network of local distributors.
>
> *Benoit H. Dicaire, Founder, Infrax*

[25] Our question was about 2010 and 2012 forecasts. As most respondents answered the same thing for both years, we merged the answers

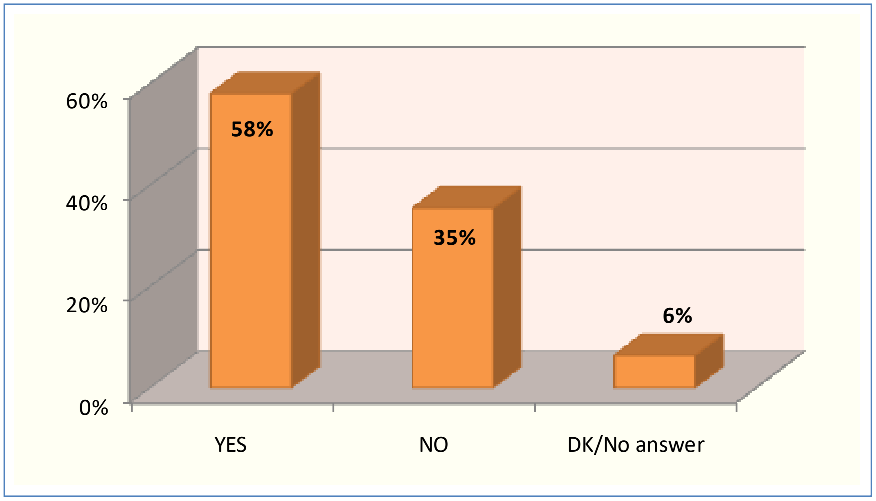
6. Research and development (R&D)

6.1 R&D Volume

Only fifty eight percent of security firms in Canada have R&D programs. This is because the Security industry is dominated by small and micro enterprise (see Section 3.2 - Size and Nature of the Companies). This industrial structure does not induce R & D investments.

FIGURE 26 – A MAJORITY OF SECURITY FIRMS CONDUCT R&D

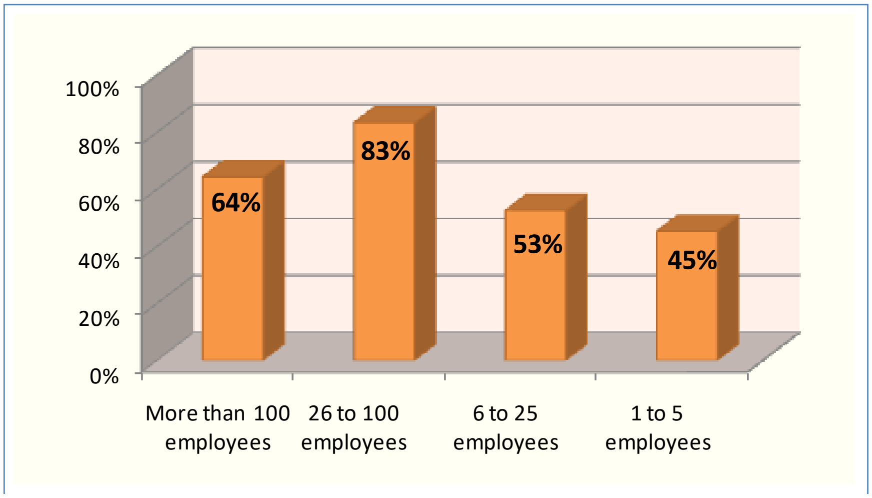
Does your company conduct R&D?



Source: CATA Study – Montreal, February 2011

This situation is aggravated by the fact that only sixty four percent of large companies (more than 100 employees) conduct R&D (figure 27). Many large security firms are professional services multinationals which are not R&D oriented. The bulk of advanced security R&D in Canada lies in the medium-size enterprises segment of the industry (eighty three percent).

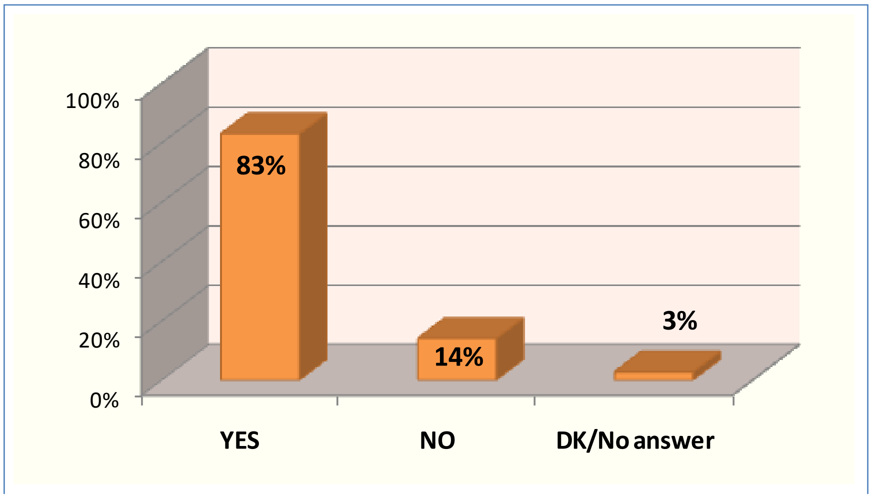
FIG. 27 – R&D IS CONDUCTED BY MEDIUM COMPANIES



Source: CATA Study – Montreal, February 2011

Above eighty percent of advanced security enterprises engaged in R&D export their goods and services. This high proportion indicates the importance of R&D to ensure their success in foreign markets.

FIG. 28 – R&D IS A PREREQUISITE FOR EXPORTS



Source: CATA Study – Montreal, February 2011

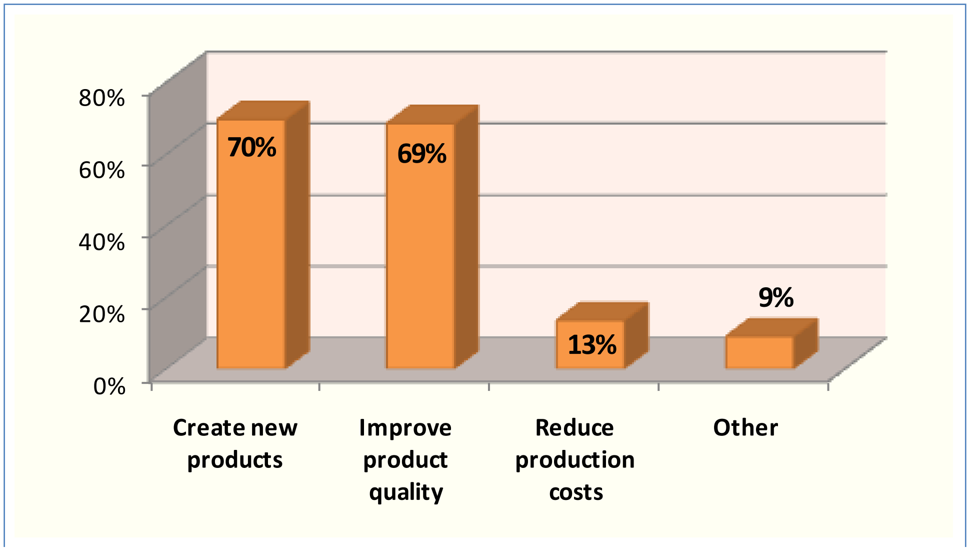
> Five years research and 60 patents issued: we are just starting our operations and we know we have the right solution.
> *Éric Bergeron, President, Optosecurity*

6.2 R&D Objectives

Creating new products and improving their quality are the main objectives of the advanced security R&D. However cost reduction is not a meaningful factor. Commercial factors are never mentioned which may be considered as a lack of maturity of the industry.

FIGURE 29 - R&D OBJECTIVES

What are the principal objectives of your R-D activities? [Two answers are allowed.]



Source: CATA Study – Montreal, February 2011

6.3 Top R&D Trends

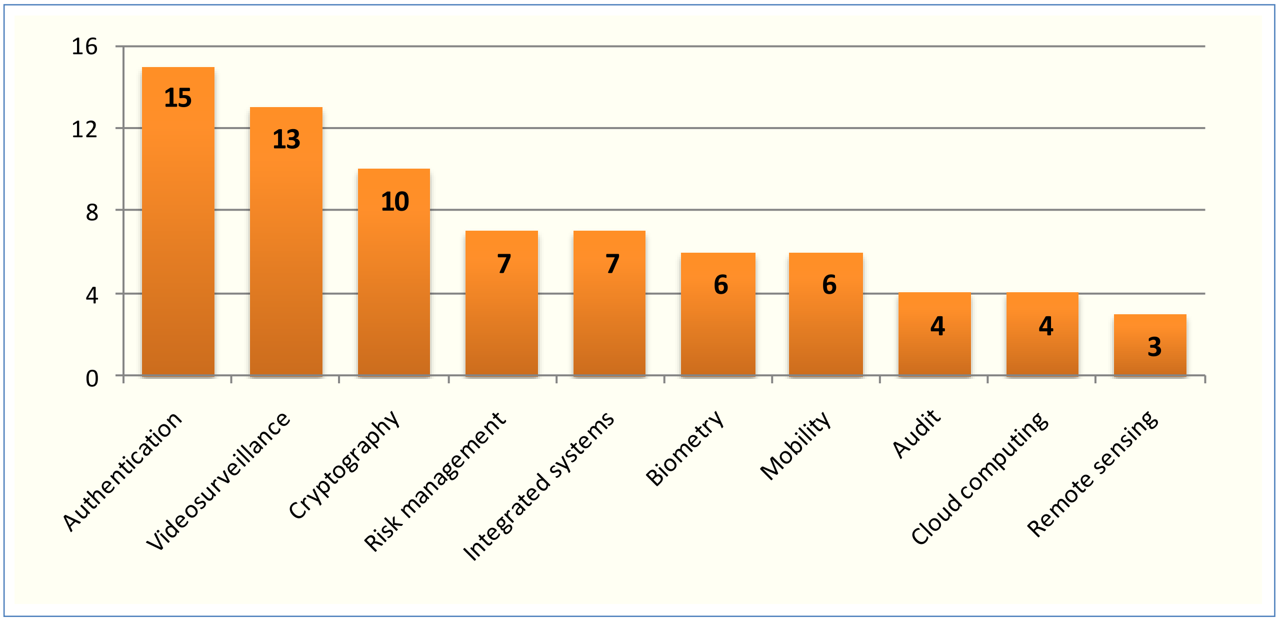
Authentication, IP video surveillance, cryptography and mobility technologies are raising in the Canadian security industry, in terms of R & D. Authentication and cryptography, technologies being sister technologies, can be included in the same category, which would further underscore the concentrated nature of Canadian research.

This indicator denotes a community of interest, but cannot account for the actual weight of research activities in each specific area.

For instance, Entrust invests more than seventeen percent of total revenue in R&D, that is above $seventeen million per year and the firm holds one hundred and twenty five patents granted and pending.[26] This enterprise focuses its R&D approach on identity-based solutions: mainly authentication, fraud detection, digital certificates, SSL and PKI. This indicates that Authentication/Cryptography weigh even more in the advanced security industry that what is suggested in the table below.

FIGURE 30 – R&D 10 TOP TRENDS

Please indicate the research fields pursued by your company?
[Absolute figures. – Multiple answers are allowed.]



Source: CATA Study – Montreal, February 2011

> Zerospam devotes a third of its resources to R&D in particular to keep updated on the manoeuvres of hackers and other Internet spammers.
>
> *David Poellhuber, Zerospam*

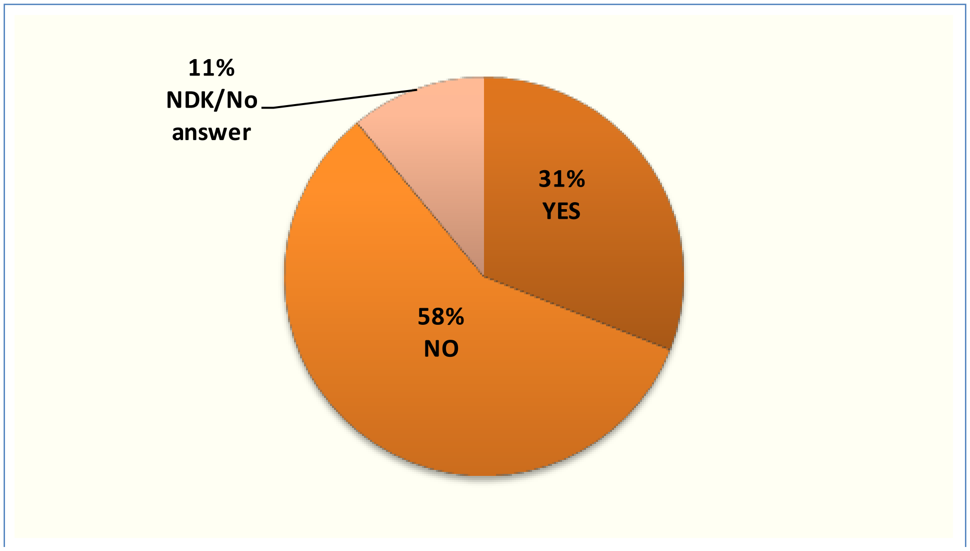
[26] Entrust's total revenue was $98.9 million in 2010 (News release February 14, 2011). R&D expenses have not been revealed since the private equity firm Thoma Bravo acquired Entrust in July 2009. In the 2009 financial statements, R&D expenses were $17.2 million or 17.31 percent of total revenues, and the company announced that "research and development expenses may have to increase in the future". Form 10-Q 2009.

7. Financing

Less than a third of respondents are looking for funding, which is well below the 2003 situation when forty four percent of them said they were seeking funding. Even if one considered the eleven percent of undecided or no answer, such as the entrepreneurs who have abandoned their research funding for lack of venture capital, the results indicate a reduction of funding research.

FIGURE 31 – FINANCING IS NOT A MAJOR ISSUE

Are you looking for financing?



Source: CATA Study – Montreal, February 2011

Despite the low response recorded on the aims of funding research, two themes emerge clearly: the development of new markets (14 responses out of 27) and R&D 9 responses out of 27).

Other reasons mentioned include training, quality assurance, purchasing, accounts receivable, hiring staff and increase cash flow.

> DRDC Valcartier has the scientific and financial resources necessary to encourage companies in defence and security to engage in R & D activities. One of the objectives DRDC Valcartier is to foster public-private synergy in security.
>
> *Richard Delagrave, Deputy Director General, DRDC Valcartier*

8. Obstacles to Industry Development

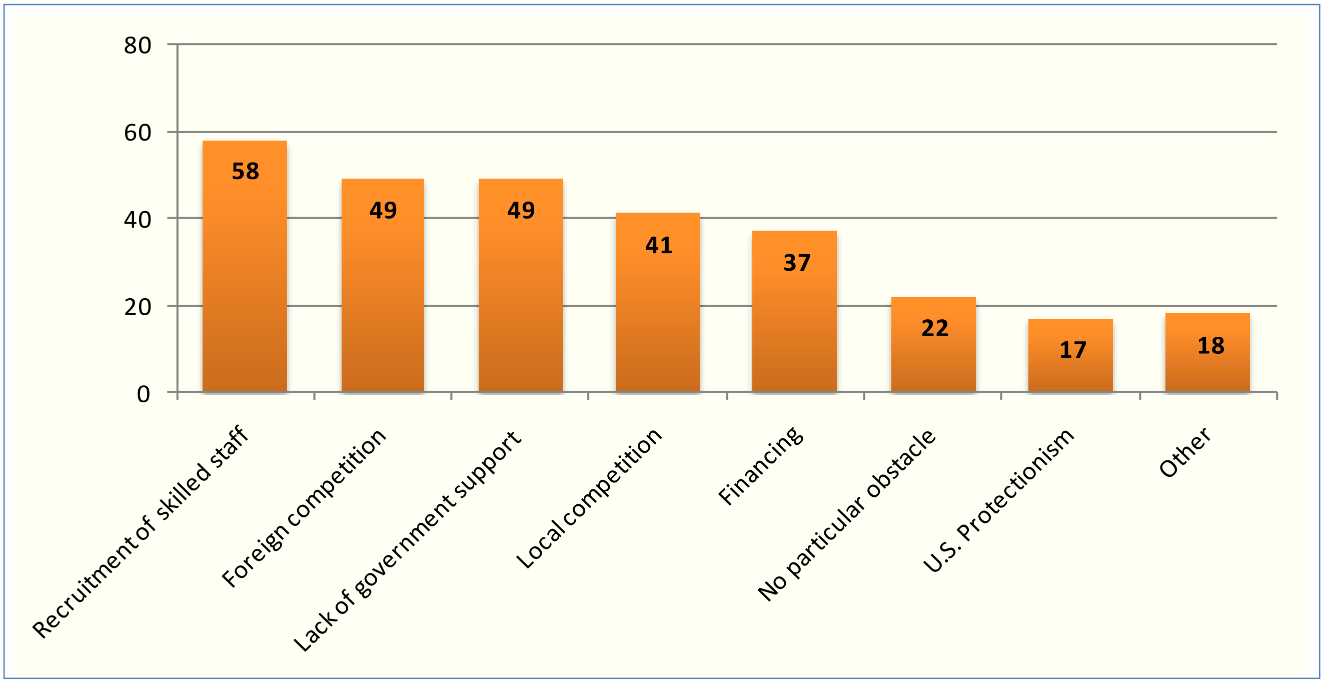
The great obstacle to the security industry going forward is the recruitment of qualified personnel (58 companies). Foreign competition is in second place (which is predictable), tied with the lack of government support (which is less predictable).

The other big "discovery"of this survey is the near absence of the problem posed by U.S. protectionism (only 17 companies have identified it as an obstacle). Taking into account those who claimed to have no problem (22 companies which are all - except one - different from those who responded had no problem with American protectionism) is a strong signal that the industry send on the open U.S. market.

Among those who answered « Other », the lack of awareness was mentioned by five enterprises, which shows the intensity of the issue (contrary to the previously cited issues, this one was not mentioned in the questionnaire). The lack of national and provincial requirements regarding security standards and the obligation to disclose security breaches when they occur is mentioned by three respondents.

FIGURE 32 - RECRUITMENT CHALLENGES

[Absolute figures. – Multiple answers are allowed.]



Source: CATA Study – Montreal, February 2011

Analysis

A – Human Resources

The situation in terms of recruitment has worsened since 2003 when the problem appeared relatively minor (only thirteen percent of respondents identified then the lack of qualified staff as a barrier). What has happened since?

Clearly, advanced security has become a more general concern than in the past, but training has not kept pace. But what training is involved here? In many cases, ICT training is not sufficient. Most cyber attacks originate from within the agencies involved - a mixture of ICT expertise, management experience, and interrogation and investigative techniques are needed.

In addition, the growing importance of professional services within the security sector is a challenge: the counselling service requires experienced staff. One does not sell the service of a young graduate to a business or public administration that already has a highly specialized internal department. There is a demand for experts who are experienced, which remains unfulfilled.

B – Role of the State

The State has a dual role as a user and a legislator on safety and respect for privacy. Some respondents highlighted the legislative void on theft of confidential information, compared to the situation in the U.S. or in European countries. According to them, for lack of such a legislative and regulatory framework, many companies would not make efforts to maintain a safe environment in their ICT infrastructure.

Moreover, many small businesses complain of challenges in doing business with the federal government. This criticism is very similar to what we noted in 2003: public administration tends to favour large companies and in drafting the bidding based on them. It is easier for a government that is by definition large, to deal with a large company than with an SME. The large company has similar structures: a vice-president talks to a deputy, a department head to a general manager and so on.

Yet some large companies are experts in the art of dealing with SMEs. A company like IBM has created an ecosystem of partners from which it draws much of its innovation and enables it to adapt to niche markets where it would otherwise be absent. Research In Motion (RIM) in Waterloo and Ericsson Canada in Montreal have created powerful ecosystem (in which security is present) which plays a large part the future of their smart phones.

The government of the twenty-first century can no longer afford to neglect the SMEs as a source of supply, especially in the security sector as part of their core business (core business). The security industry needs no subsidies, no respondent raised this possibility but it requires partnerships and contracts with a government that adapts to the structures of SMEs.

However, government is often forced to deal with large companies for reasons of universality and coverage. In all cases where the government and its agencies are forced to turn to big business, it should provide in their RFP calls for subcontracting to SMEs.

In fact, the large company already uses the expertise of SMEs to meet the overall needs of the government. This is mainly for government leaders to improve what already exists, not to invent ex nihilo. How could they include such improvements? For example, it is possible to confer in the RFP a formal and visible place for SMEs alongside the main bidders, and thus, throughout the mandate. It is also possible to create campaigns for the SMEs to foster partnerships. In short, we must devise a continued collective action with results that are medium term.

9. Conclusion and tentative recommendations

The development of the advanced security sector in Canada is influenced by three key variables:

- ✓ The development of a range of highly advanced security techniques embedded in the governance of organizations instead of a strictly technological approach;
- ✓ The development of an appropriate SME offer;
- ✓ And the lack of qualified personnel..

9.1 From ICT to governance

Security is fast breaking away from its ICT origin and becoming a governance issue. This transition is accelerated by the decision of the Payment Card Data Security Standards Council to impose the PCI-DSS to the retail sector.

Consequence

Security will soon cease to be a sub-sector of ICT and will become an integral part of governance, management and organizational strategy; in short, it behaves like other activities of professional services (audit, board tax, business management ...).

9.2 Development of a SME offer

The above mentioned Payment Card Data Security Standards Council's decision has finally created a security offer customized to fit SMEs' needs. We announced this change in the 2003 study on advanced security, but the transition has taken longer than expected, due to the lack of incentives.

Consequence

The retail sector has suddenly realized the importance of protecting the privacy of its customers. It is a great step towards greater accountability of business practices. However, the PCI-DSS is applied differently depending on the intensity levels of transactions by traders.

FIGURE 33 – SCOPE OF THE PCI-DSS STANDARD

Level	Transaction volume
Level 1 Criteria	Merchants with over 6 million transactions a year, or merchants whose data has previously been compromised.
Level 2 Criteria	Merchants with 1,000,000 to 6 million transactions a year.
Level 3 Criteria	Merchants with 20,000 to 1,000,000 transactions a year.
Level 4 Criteria	Merchants with less than 20,000 transactions.

Source: https://www.pcisecuritystandards.org/index.php

Only Level 1 merchants are required to perform annual audits by an external auditor and a quarterly vulnerability scan on the external access points (web, email ...). This phased approach is realistic. According to survey participants, it must penetrate security in companies trading with five hundred employees or more (some say a thousand or more). In any case, only the "M" of SME development is affected.

Small business eludes the most compelling aspects of the PCI-DSS in the sense that external auditing is replaced by a self-assessment.

It follows that the PCI-DSS is primarily aimed at companies with more than five hundred employees. We have seen that over eighty percent of Canadian advanced security serves this market (see 4.1 - Size of the customers). However, in the retail sector, these large establishments represent less than one percent of the market. The potential for increasing safety in the retail sector is enormous, but there is little supported by the imposition of the PCI-DSS.

PCI-DSS Standard Summary

The PCI-DSS standard comprises twelve requirements that can be combined into six themes:

- ✓ Build and maintain a secure network
- ✓ Protect cardholder data
- ✓ Maintain a vulnerability management program
- ✓ Implement strong access control measures
- ✓ Regularly monitor and test networks
- ✓ Maintain an Information Security Policy

FIGURE 34 – THE RETAIL TRADE SECTOR IN CANADA

Employment Size Category	Number of Employees	Number of Establishments	Percent Distribution
Micro	1 - 4	50,989	38.9%
Small	5 - 49	77,020	58.7%
Medium	50 - 499	2,991	2.3%
Large	500 +	111	0.1%
Total	---	131,111	100.0%

Source: Statistics Canada, Canadian Business Patterns Database, December 2009.

9.3 Lack of qualified resources

The lack of qualified personnel is undoubtedly an obstacle to advanced security business growth: nearly sixty percent of businesses report having problems recruiting qualified staff (see Figure 32 - Recruitment Challenges).

Consequence

The future of advanced security industry in Canada depends on the availability of qualified staff of international caliber.

To illustrate the critical importance of this factor, we cite the example of Silanis Technology: This company does not sell anything in Canada. Vendors are all located in the United States, its Vice President of Marketing lives in Vancouver and the company is based in Montreal. When we ask the question of the choice of Canada, President of Silanis cites the comparative advantage lavished by tax credits for R & D and the presence of four universities in Montreal where there are "fantastic talent."[27]

Considerable efforts have been made by universities to promote information security, but it is not sufficient, as shown by the results of CATA survey. Furthermore, education is only part of the security

[27] Tommy Petrogiannis, interview, March 9, 2010.

training, the other one being in the hands of enterprises and specialized associations: let us mention the role of ISACA in CISM, CISP and CobiT certification; or CIPS ISP/ITPC certification; no to mention private institutes.

These examples clearly show the existence of a good training infrastructure. What is missing is the political will to mobilize this network as evidenced by the negative signal sent by the closing of the NRC Institute for Information Technology (NRC-IIT) in 2009. Based in Fredericton, New Brunswick, this program was addressing the challenges associated with network security and privacy for distributed systems.

The closure of this important R&D center in information security attests to a lack of strategic vision from government stakeholders.

9.4 Tentative Recommendations

To help develop the industry in advanced security, governments should take into account certain factors:

- ✓ Industry advanced security is a separate area of ICT and its development will contribute further to this specificity.

- ✓ The Personal Information Protection and Electronic Documents Act (PIPEDA) Is a weak framework that does not protect the general public and does not prompt corporations to comply. This narrow and reactive approach to privacy is not up to the international standards and should be completed with a binding legislation requiring mandatory notification of breaches affecting personal data.

- ✓ Safety training should be encouraged in Canadian universities by all means available to the government (scholarships, research funding, government contracts, etc..), including a political awareness of women who are underrepresented in this sector and are a reservoir of untapped labour.

Appendix 1: Cases Studies

Companies profiled in this section were chosen to illustrate the different core businesses and the level of intensity of their activities in advanced security. This is not a list of the top enterprises selected according to a given criteria (whether technological, managerial, or related to sales growth, best practices, etc.).

The size of the case studies varies from one firm to another. A longer case study does not mean the company is more innovating or more interesting than another one described in a short case study. It only reflects the information policies of the various respondents: some were more open than the others, and one must not forget that many security specialists are very reluctant to speak as a result of being so conditioned by their profession.

Case Studies List

- ✓ Above Security
- ✓ Carillon
- ✓ Deloitte
- ✓ Forensic Technology
- ✓ IBM Canada
- ✓ Notarius
- ✓ Nurun
- ✓ Optosecurity
- ✓ PriceWaterhouse Coopers (PwC)
- ✓ Silanis

Above Security

1919 Lionel Bertrand Blvd, suite 203
Boisbriand, Quebec
J7H 1N8
Marisol Litalien
(450) 434-8060
marisol.litalien@abovesecurity.com
www.abovesecurity.com

Interview	Marcel Dion, CEO	
Contact	Marisol Litalien, Director of Communications	
Data	***Founded***	1999
	Headquarters	Boisbriand, QC
	Number of employees in Canada	35
	Employees in Canada	45
	R&D	10
	Products	Network surveillance Security Operating Center
	Clients	80% - companies of 500 employees + 20% - companies from 50 to 500 employees
Mission	Outsourcer, Above Security does not sell software or equipment	
Strategy	Growth through international partnerships	
Means	Reseller training program to accelerate international development	
Markets	Canada, Latin America, Caribbean and Europe	
Advantages/ Issues	Canadian member of FIRST International (Forum of Incident Response and Security Teams).	

Background

Above Security was created in 1999 by Marcel Dion, accountant, and his son Martin Dion computer scientist, each complementing the other’s expertise. They developed a solution for monitoring the security of networks that protects organizations against external cyber attacks and internal fraud.

Applications

Above Security, whose main service is the remote monitoring of computer networks, acts as a strategic partner in managing information risk. Analysts based in a security operation center are ready to get down to the job on a 24 / 7 basis to detect any intrusion and ensure confidentiality of data exchanged on customers' networks.

Sensors installed strategically in information systems do packet level inspection of all traffic and messages circulating on servers, operating systems and applications. Once an intrusion, or any other type of anomaly, occurs, an alarm is transmitted to the security operation center. Above Security then prioritizes the incident and assesses the impact on the operations of the client company.

Above Security detection systems also analyze data issued by the information systems, which allows for the detection of non-conforming use of the internet by internal users, access to pornographic sites, chat nuisance, the use of P2P software, etc.

More than a dozen certified IT professionals work in R & D to incorporate protection systems against cyber threats. When a new threat is detected, the experts at Above Security provide preventive measures as appropriate.

The company had 45 employees in 2010. It also offers professional consulting services or operational audits, technical audits, safety policies, training, business continuity plan, IT recovery plan and compliance with norms and standards such as PCI DSS, WLA: CBS, Basel II and ISO 27001.

Market

The company serves more than 250 large customers in 22 countries: thirty percent in Canada, fifty percent in the Caribbean and twenty percent elsewhere in the world. The clientele is diverse: finance, pharmaceuticals, telecommunications, manufacturing and government.

Above Security's business strategy is based on direct sales for two-thirds and one-third by a network of reseller partners. The company targets priority markets such as Latin America and Europe.

Above Security's revenues have increased each year, including in 2009 during the financial crisis. The president believes that "Canada is perceived abroad as being trustworthy and providing quality services. This reputation greatly facilitates our international business."

Strategy

The company has no funding problem. It relied in the early years on subsidies from Canada Economic Development and Investissement Québec.

Above Security is one of the few and select international providers to be members of the Forum of Incident Response and Security Teams (FIRST). This participation allows the company to be informed instantly, on the latest computer threats and how to fix them. Above Security was sponsored by National Defence Canada to be part of FIRST.

Carillon Information Security

356, Joseph-Carrier St.
Vaudreuil-Dorion, Qc
J7V 5V5

514-485-0789
ppaterson@carillon.ca

Interview	Patrick Patterson, president	
Contact	Patrick Patterson	
Data	***Founded***	2001
	Headquarters	Vaudreuil-Dorion, QC
	Total number of employees in security	7
	Employees in Quebec	7
Mission	Providing services of identity management to the aerospace industry.	
Strategy	Focusing on one customer service by providing a targeted service.	
Benefits & Issues	The commitment of the Government of Canada in the aviation industry does not strengthen its security and the neglect of this important aspect is a major issue.	

Background

Carillon Information Security was founded in 2001 by a group of four professionals to address computer security in the aerospace and air transportation industry. The group was convinced that the aerospace security was a growth market. "Initially, our services focused on public key infrastructure, and then, over the years, we have refocused our offer on identity management" said Patrick Patterson.

Market

In 2001, the clientele of Carillon was exclusively found outside Canada, mainly in Europe. Today, this ratio is more balanced with fifty percent of clients in Canada and fifty percent in the rest of the world.

Strategy

In the identity management area, contracts usually last three to four years. A plan for identity management reduces the number of authentications required to access corporate applications, and the number of calls received by support services to users (e.g., recovery of passwords). Carillon participates actively to the Transglobal Secure Collaboration Program (TSCP) platform to establish and maintain an open, standards-based framework for the defence and aerospace manufacturers and systems integrators around the world. Carillon focus on identity management and helps the TSCP members to reduce the waiting time information, control access to their intellectual property and facilitate compliance with laws governing the export of equipment and technology control.

The competitive advantage of Carillon’s expertise is the aerospace and air transportation community. "We know in depth the laws and regulations of the industry and we are acting as advisers. We are part of industry associations, including the Air Transport Association (ATA) and represent clients with associations like the TSCP and CertiPath, which include major companies in the aviation field, and the U.S. government. "

"All G8 countries, governments, like France, the United Kingdom and the United States, participate actively in the security associations field of aeronautics. Only Canada does not. It's a shame because not only would this presence help to strengthen domestic security, but also because it would highlight the Canadian companies working in the sector. It must be said and repeated: the aerospace industry is a strategic area for Canada and the Government must take an active part in promoting the safety of this industry", concludes Patrick Patterson.

Deloitte & Touche

30 Wellington St W
PO Box 400
Toronto, ON M5K 1B1
(416) 601-6500
amelek@deloitte.ca
www.deloitte.ca

Interview	Adel Melek, Global Leader, Security,Privacy, & Resiliency	
Contact	Adel Melek, Global Leader, Security,Privacy, & Resiliency	
Basic Data	***Founded***	1990
	Head office	Toronto, ON
	Branches	10 Canadian cities (including Toronto)
	Sector	Service provider and integrator
	Technology	All regular InfoSec services including application integrity, vulnerability management, infrastructure & operations security, security management, business continuity planning and identity & access management. Does not provide converged services (i.e. video surveillance).
	Employees (security only)	World: 11,000 Canada: 370
	Revenues	World: $2.3 billion
	Market segments	Private sector (70%) and Government (30%)
	Client location	Canada (70%), USA (15%) and emerging countries (15%)
Mission	- Deloitte takes advantage of its experience in the integration of business, process *and* technology to provide an end-to-end e-Business security solution.	
Strategy	- Security is sold as part of the whole range of professional services provided by Deloitte's enterprise risk practice. - AAs with the rest of the company, the security, privacy & resiliency practice focuses on vertical segments: Financial Institutions, telecommunications and media, health care, real estate, manufacturing, natural resources and public sector.	

Means	- Over 150 Certified Information Systems Security Professionals (CISSP) in Canada - Global leadership in the areas of security management, infrastructure & operations security, vulnerability management, identity & access management, business continuity planning, PKI, PSI, e-Business assurance, Security Products, Digital Forensics and Incident Response - Established references with Canada's elite organizations - 55 Technology Centres in Canada - Central Technology Centres (connected to Global Centre)
Benefits & Issues	- Deloitte has the broadest security services capability in Canada. - Holistic approach that encompasses both security of information and privacy issues. - Regulatory and ethical constraints due to conflicting interests of auditor role and information - Security integrator. - Independent analysts consistently rate Deloitte as a global leader in the security consulting and technology risk management space - Acknowledged leaders in the areas of planning for business disruptions through roundtable series, thought leadership, and media interviews

Background

Deloitte & Touche LLP ("Deloitte") was formed in February 1990 through a merger of two firms, both more than 150 years old (Touche Ross and Deloitte Haskins & Sells Samson Belair). It provides a full range of assurance and advisory, financial advisory, tax, consulting and enterprise risk services, with more than 7,700 people in more than 58 locations across the country (the firm operates in Québec as Samson Bélair/Deloitte).

Deloitte Canada is part of Deloitte Touche Tohmatsu, a global leader in professional services with 170,000 people in over 140 countries. Deloitte Touche Tohmatsu is a Swiss Verein, and each of its national practices is a separate and independent legal entity.

Deloitte is a security pioneer. Its activities go back to the mainframes era – before the merger of the two founding companies it was specialized in mainframe security and ERP security (SAP, PeopleSoft, etc.). In 1993, Deloitte created the security services practice to address network security, and in particular, new issues raised by the Internet.

The Security, Privacy, & Resiliency
Practice counts on 370 security experts divided in two branches:

- Information security: 200 professionals;
- Risk management: 170 professionals.

- The practice relies on the Toronto-based Security Technology Centre which is designed to test application integration, biometric authentication devices and data quality testing. It also holds an inventory of "hacker" tools.

- Deloitte's Security, Privacy, & Resiliency practice is part of the global security network of Deloitte Touche Tohmatsu, with approximately 11,000 people in more than 40 countries (300 CISSPs and 1,000 CISAs). The Canadian Security Technology Centre is connected to a network of eight technology centres located strategically around the world. Their security practitioners are constantly exchanging information on newly released state of the art of tools.

Business Strategy

- Deloitte's Security, Privacy, & Resiliency practice focuses on large size organizations and the high end of SMEs: medium size enterprises with high growth. It divides the market by vertical segments:
- Financial Institutions;
- Public Sector;
- Telecommunications and media;
- Manufacturing;
- Natural resources: oil and gas industry, hydro, etc.;
- Healthcare; and
- Real estate.

More than half of Deloitte's activities are concentrated in the two first segments (financial institutions and public sector).

Nature of the market

Thanks to its ongoing links with the main security users, Deloitte performs a permanent tracking of the evolution of the security market. It estimates the Canadian information security market to US$2 billion in 2010 all components included (hardware, software, system integration, outsourcing, etc.). The market is set to rebound in 2010-2011 after a 2009 drop and grow steadily at a minimum of 5 five percent per year going forward. Canadian information security professional services market is estimated at US$430 million in 2010.

Some of its research is available in free publications such as:

- Cyber Crime: A Clear and Present Danger (the CSO 2010 CyberSecurity Watch survey shows that cybercrime threats to organizations are increasing faster than they can combat them), February 2010.
- http://www.deloitte.com/view/en_US/us/Insights/centers/Center-Security-and-Privacy-Solutions/bcdc005f1e056210VgnVCM100000ba42f00aRCRD.htm
- Cybersecurity: Everybody's Imperative: Protecting our economies, governments, and citizens (cyber culture is growing faster than cybersecurity, so everything that depends on cyberspace is at risk), May 2009. http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/CybersecurityDeloittePointofViewlowres(1).pdf
- Protecting what matters: The 6th Annual Global Security Survey, February 2009. http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/dtt_fsi_GlobalSecuritySurvey_0901.pdf
- Security can't be discounted: 2009 Consumer Business Global Security Study (including retail, wholesale and distribution, consumer package goods manufacturing organizations). http://www.deloitte.com/assets/Dcom-Canada/Local%20Assets/Documents/CB/ca_en_cb_GlobalSecuritySurvey_111709.pdf

Exports

The Security, Privacy & Resiliency practice exports thirty percent of its services outside Canada mainly through the global network of Deloitte Touche Tohmatsu sales force. These exports are equally divided between the USA and the emerging countries located in three parts of the world:

- Caribbean and Latin America;
- Middle-East;
- Far East (mainly China and Thailand).

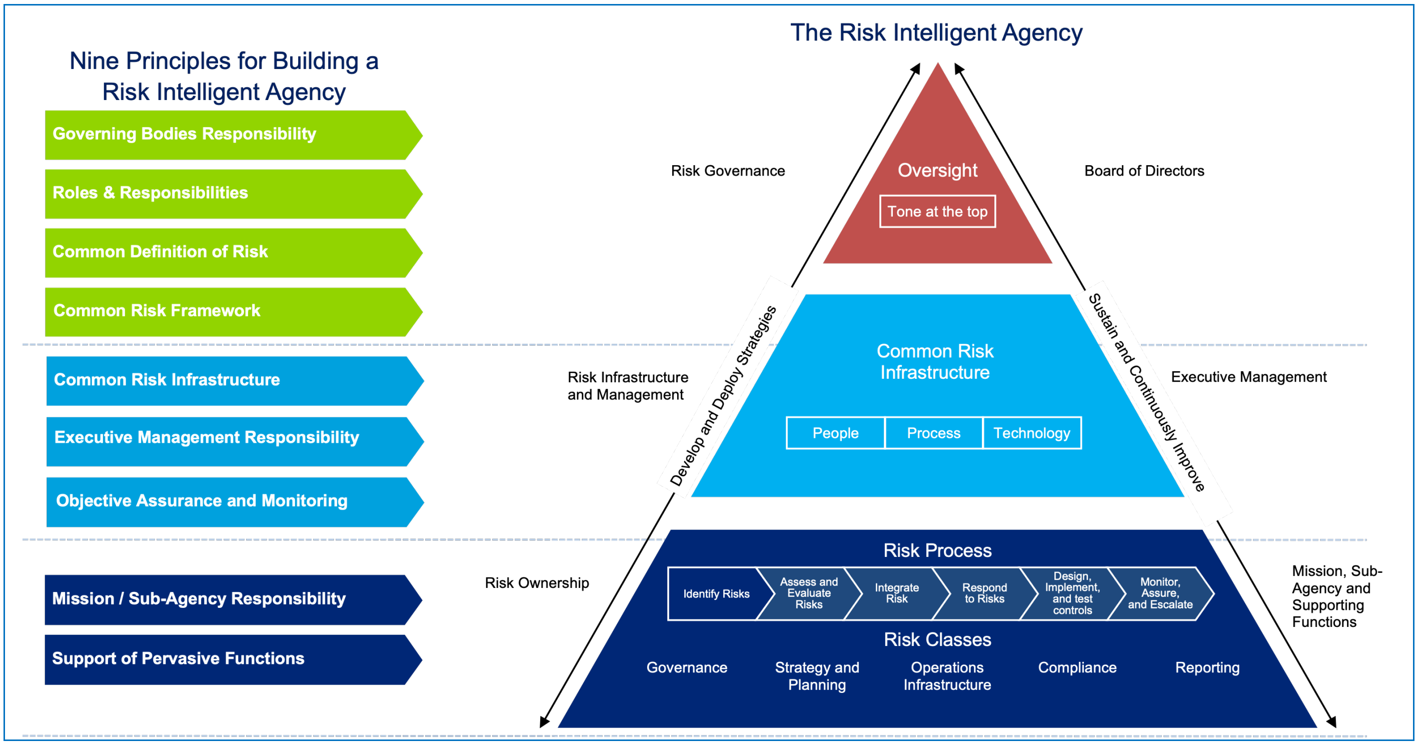
There are no exports to Europe and Japan, which are self-sufficient in security expertise.

Process and Technology

According to Adel Melek, Global leader for the Security, Privacy & Resiliency practice, cyber security cannot be achieved through technology alone. It requires a cultural understanding and a widespread willingness to exhibit secure behaviors.

Deloitte is technology neutral. It distributes products and services from forty seven security vendors. As a system integrator, it manages the entire life cycle of enterprise security and oversight including the development of strategies, policies, directives, standards, procedures, operational procedures, and auditing. Nevertheless, Deloitte remains outside the outsourcing and hosting business.

Deloitte's approach to cyber risk is designed to help agencies develop a comprehensive picture of their current cyber risk profile, supporting their efforts to synchronize multiple security, information and technology risk management initiatives and prioritize efforts based on risk and impact to mission. It's Risk Intelligence Program Methodology applies nine fundamental principles for building a risk intelligent enterprise to transform an organization's risk management capabilities. It is a holistic and unifying approach for building an effective and efficient risk management program that is also scalable to focus on the key areas that can provide an agency with the greatest benefits.


Nine Principles for Building a Risk Intelligent Agency
Governing Bodies Responsibility
Roles & Responsibilities
Common Definition of Risk
Common Risk Framework
Common Risk Infrastructure
Executive Management Responsibility
Objective Assurance and Monitoring
Mission / Sub-Agency Responsibility
Support of Pervasive Functions
The Risk Intelligent Agency
Risk Governance
Oversight
Tone at the top
Board of Directors
Develop and Deploy Strategies
Sustain and Continuously Improve
Risk Infrastructure and Management
Common Risk Infrastructure
People
Process
Technology
Executive Management
Risk Ownership
Risk Process
Identify Risks
Assess and Evaluate Risks
Integrate Risk
Respond to Risks
Design, Implement, and test controls
Monitor, Assure, and Escalate
Mission, Sub-Agency and Supporting Functions
Risk Classes
Governance
Strategy and Planning
Operations Infrastructure
Compliance
Reporting

Source: Adel Melek, Helping Government Manage Cyber Risk, Ontario Critical Infrastructure Assurance Fall Conference, November 2, 2009

Issues

Deloitte tackles security from a management perspective and not as a technology platform. This allows it to sell security services fully integrated in the overall business strategy of its clients, including full compliance with regulatory and legal requirements.

Deloitte notes and deplores the persistence of certain obstacles among Canadian organizations:

- low awareness of senior management to security threats;
- lack of transparency of reporting security incidents (no obligation to report information crimes);

- low adoption of security standards by vendors and users (everybody acts as a security expert, but never submits his or her products and services to world class standards evaluation).

There is one particular constraint to Deloitte’s Security, Privacy & Resiliency practice - as one of the four major financial auditors, Deloitte cannot partner with its clients, or compete against them (for instance, Bell Canada and Telus are being audited by Deloitte and this imposes a limit on its security activities).

Forensic Technology

5757, Cavendish blvd
Cote-Saint-Luc, Qc
H4W 2W8
514-448-2751
patrick.doyon@forensic.com
www.forensic.com

Interview	Patrick Doyon, marketing director	
Contact	Patrick Doyon	
data	***Headquarters***	Montreal, QC
	Founded	1992
	Number of employees in security	200
	Employees	150
	R-D	25
	Clients	Governments
Strategy	The company uses a mixed strategy B2G direct sales and partnerships with resellers.	
Means	Forensic has four offices abroad: USA (Florida), South Africa, Ireland and Thailand.	
Markets	Forensic sells around the world and now tackles to Africa, Latin America and Asia.	
Advantages/ Issues	The ballistic recognition is an area of few players. Forensic is dominant and is always improving its products and services to keep up. The current challenge is to convince institutions of different countries to share with others their database, the aim being to create a global database.	

Background

Forensic Technology pioneered automated ballistics identification in the 1990s and continues to be a leader in ballistics and firearms identification technologies. The firm is an international player as shown by its cooperation with INTERPOL and an ever growing number of police agencies.

Technology

The whole system of identification and analysis of bullets is called IBIS Technology. The system has several solutions including the main the imaging technology, BulletTRAX-3D, used in criminal investigations. Using the latest sensor technology in three dimensions, this recent addition to the line of IBIS solutions gives operators the ability to capture digital images and create 2D topographic models of the surface of a bullet in three dimensions. BulletTRAX-3D system is both easy to use and highly automated. It allows operators, for the first time, to take quantitative measurements of the surface of a ball. No other ballistics imaging system is combined with the latest 3Dtechnology ,which offers ultra precise image quality and proven ability to operate in a network.

A second option offered by Forensic Technology is the correlation server that receives, manages and compares the digital signatures from single images of ballistic evidence. These digital signatures are mathematically compared and classified according to their similarities. This power of comparison allows operators to quickly search through hundreds or thousands of pieces, focusing only on the most likely candidates.

Forensic Technology has also developed the analysis ballistic evidence station most advanced in the world for solving crimes committed with firearms – MatchPoint +. With new visualization tools that allow it to reach informed conclusions, MatchPoint + offers the latest technology to compare and analyze evidence of remote sockets and bullets in two and three dimensions. MatchPoint + also makes it possible to compare digital images in side by side mode or multiple display mode . No other unit of comparison combines both the latest technology with IBIS viewing of high resolution images and the proven ability to operate in a network.

Business Strategy

Ballistic recognition is a market niche in forensic. Forensic Technology's strategy is to bring its customers from 35 countries and 33 centers to share their respective databases. Hosted by Forensic Technology, the database would be the world's largest database of ballistic recognition. "We have a captive market, it's true, but it is a demanding market. Our clients belong to the government sector and most are scientists. They expect constant improvement of our software and our database. It is a great challenge, "said Patrick Doyon, vice president of marketing.

IBM Canada

3600 Steeles Avenue East
Markham, Ontario L3R 9Z7
(905) 316-1278
pmccullo@ca.ibm.com
www.ibm.ca

Contact	Paul McCullough, Business Unit Executive - Public Safety – Public Sector, IBM Canada	
Interview	John Kokonis, Business Unit Executive - Canada – IBM Security Services	
Data	***Founded***	1917 (in Canada)
	Headquarters (SPT Group)	Markham, ON
	Branch	Ottawa, Montreal, Vancouver, Calgary
	Activity	Service provider, publisher, integrator and outsourcer
	Technologies	Identity management and access, application security, compliance of the security, infrastructure and information security.
	Employees	± 4 500 security professionals worldwide, 110 in Canada, including 10 Quebec-based experts in various outsourcing services.
	Revenues	n.a.
	Markets	Financial institutions, public services (electricity), commerce, SME, government.
Mission	- Offer the very best in all areas of security. This end to end approach includes the protection of persons and their identity, data, applications, regulatory compliance and best practices. IBM offers a full range of security solutions, and it allows customers to choose what they need without imposing binding packages.	
Strategy	- The IBM security offering is based on acquisitions. Since 2006, IBM bought 11 security companies. This strategy of vertical integration is complemented by a series of alliances with specialized firms such as PGP (encryption for data protection business).	
Means	- These purchases are guided by the needs expressed by groups of IBM security professionals who work closely with the acquisitions leads.	
- Benefits & Issues	- Every security professional in Canada has access to IBM's worldwide expertise (4,500 specialists); - The cloud computing phenomenon increases corporate vulnerabilities.	

History

In the particular field of security, IBM Canada has a long tradition. The procedures for security and privacy at IBM Canada were established in 1998 by three experts based in Toronto. The acquisition in April 2000 LGS Group, including laboratory Domus Information Security based in Ottawa (Domus was purchased in

1998 by LGS) was an important factor of growth. The Domus laboratory specialized in evaluating standards of security products and cryptographic products.

Platform Technology

IBM claims to be "technologically neutral" in terms of security. Although the company offers a full range of systems, it does not hesitate to provide third-party products to preserve the capital invested by its customers or their preferences.

Its technology platform is constantly updated through a massive investment in R & D, technological and tracking threats. The counter-intelligence and security training work is conducted by IBM X-Force division which comes largely from the company Internet Security Systems (ISS), acquired in 2006. However, it is the X-Force researchers who have identified more threats and vulnerabilities globally (over fifty one percent). Through this monitoring work, X-Force now has a detailed database of 48,000 cases of documented incidents in all areas of security. In all, IBM has 3,000 patents in the field of security.

IBM security offer is based on professional expertise (Tivoli range of services), the solutions to encrypt stored data, applications and processes, services, networks and end systems.

This offer is based on a global infrastructure of nine centers-- Virtual Security Operations (SOC), divided between North America (4), Europe (2), Asia / Pacific (2) and Brand New in Bangalore (India), which allows IBM to provide oversight of the needs of its customers 24 / 7: Mission critical, monitoring of electrical, data processing and management of communication links, as well as outsourcing of certain services (such as intrusion prevention, for example). One of the four SOCs in North America is based in Toronto.

Moreover, there are four IBM Business Continuity centers within Canada (Montreal, Toronto, Calgary and Winnipeg), which are part of a global network of 120 similar centers. Powered by a generator, the Toronto centre has an IT infrastructure connected by direct lines to hosts located in Markham (Ontario), Boulder (Colorado), Gaithersburg (Maryland) and Sterling Forest (New York). In this unparalleled environment under high protection, a hundred workspaces can accommodate clients at any time.

Acquisitions

Globally, IBM is taking leadership expertise through its policy of acquiring companies, which arguably IBM has made a science. Vice President Marketing and Strategy for IBM Rational Software, Scott Hebner said: "IBM Software does not buy a company unless it has already determined that its customers have a need, that the software produced by an external company data fills this need, and that it is more reasonable to buy this company than trying to develop an equivalent system from scratch, or concoct something out of existing products from IBM.

Equally important in the eyes of management is the existence of sufficient overlap with its own products so that "widgets" of the new company can easily fit into the overall activities of IBM's sales. Thus, the company purchased can grow inside IBM faster than if it remained independent. When the company bought has a strong brand, which commands the loyalty of established customers, it may even keep the name that will become an IBM brand.

Most other products are integrated into the division of Tivoli management and security which is itself the result of an acquisition. Tivoli was originally a small Texas company that specializes in managing servers, today it is one of the fastest growing divisions and most profitable of IBM.
The result is a roadmap atypical in the ICT industry where statistics show that only 30 percent of mergers and acquisitions are successful. Instead, IBM manages all of its acquisitions, as evidenced by the shopping list without the security sector:

- July 2010: BigFix, for $ 400 million (estimate), a developer of software solutions for automating the compliance management and security (California);
- February 2010: Initiate Systems, a developer of software for managing data of the company (Illinois);
- January 2010: National Interest Security Company (NISC) for $ 1.3 billion (estimate), a developer of security systems and data mining for defense and intelligence-cons, health and energy (Washington DC);
- September 2009: Guardium for $ 225 million, a developer of security tools for databases (Massachusetts);
- July 2009: Ounce Systems, developer of security tools and vulnerability detection (Massachusetts);
- March 2008: Encentuate, a developer of software for identity and access management (California);
- September 2007: Softech, a developer of security tools and management databases (New Jersey);
- July 2007: Watchfire for $ 100 million (estimate), a developer of security testing tools (Canada); PFPF
- January 2007: Consul, developer of tools for auditing and compliance (Netherlands);
- October 2006: Internet Security Systems (ISS) for $ 1.3 billion, a developer of security tools on the Internet has also given rise to X-Force in 1998 (Georgia).

This strategy was rewarded in February 2010 by SC Magazine (http: / / www.scmagazine.com/) which selected IBM as the best security company at the RSA Conference in San Francisco.

Market

The threat market has shifted to the end systems. Accordingly, priority that was traditionally given to incoming traffic is now given to the outgoing traffic. Customers want to ensure that their databases are accessible only to the right people. They believe that their core activities are now well protected and want to increase the protection of the perimeter.

Each year, X-Force issues a report on global trends and risks in terms of cybercrime. Within this overall picture, the Canadian market is still down compared to the average of industrialized countries. Even the banking sector is relatively undeveloped. One reason for the lack of dynamism of this market could be the lightness of Canadian regulations which are not binding, and little incentive.

IBM Canada primarily serves the Canadian market. Its exports consist primarily of providing services to Canadian companies that have operations abroad.

Issues

IBM is the world leader in the security market. IBM's strength comes largely from its collaborative tools that allow it to quickly mobilize the best specialists in a particular area to address in an online incident even if unusual, to extract the main features and to develop a solution.

To remain at the forefront of the security industry, IBM is reorienting its offer in light of new vulnerabilities such as "cloud computing".

Notarius inc.

1080, Beaver Hall Hill, suite 700
Montreal, QC
H2Z 1S8
(514) 281-1577
http://www.notarius.com/

Contact	Charles Tremblay, Commercial Director	
Data	***Founded***	1996
	Headquarters	Montreal, QC
	Total number of employees	50
	Total number of employees in security	3
	R-D	On-going
	Products	Certification Authority (digital signature); Security Management Information
	Clients	Financial sector, retail, professional, department, national defence, first responders, etc.
Mission	Quebec certification authority	
Strategy	Demonstrate that the electronic signature is not only safe but economical	
Means	Capitalizing on R & D in the field of public key infrastructure and software development related to certification of electronic documents Adobe PDF	

Background

Notarius, the technological subsidiary of the Chamber of Notaries of Quebec, is a non-profit organization established in June 1996. Notarius has established a public key infrastructure to ensure the delivery of a digital signature adapted to various professional practice standards. Indeed, the creation, transmission and archiving of electronic information have changed that. Today, any professional who uses this information carrier must ensure the security and integrity of electronic documents.

Technology

The digital signature is based on public key infrastructure and operates from a technology, known worldwide, called asymmetric key cryptography. Notarius certificates are issued by a CA, registered under the name Center Certification Quebec (CCQ), following an identity verification and validation of professional status of the future owner. The digital signature is personal; a private signature key affixed to an electronic document and which irrefutably confirms the author of the electronic document and protects the integrity against any attempt to change.

Strategy

Notarius is the certifying body of a very large number of professional corporations. It counts among its members a number of Canadian engineering and architect associations. In Quebec, the solution offered by Notarius is not only adopted by Orders and associations, but also by companies belonging to various spheres of activity that want a reliable electronic document that offers authenticity and integrity protection all through the life cycle of the document.

Societies and associations immediately adopt the solution because it is linked directly to their mission of protecting the public. The solution provides insurance that a particular electronic document is indeed the work of a member in good standing or professional association.

"We have always regarded the paper as our competitor", said Charles Smith." In the case of large companies, we had to demonstrate that the solution could easily fit into the business processes and result in savings compared to paper. Do not forget that electronic signature permits you to skip the step of printing paper, binding, archiving originals and scanning, and finally sending, by courier ... which greatly reduces environmental footprint."

Nurun Inc.

330, Saint-Vallier East, suite 120
Quebec, Qc
G1K 9C5
418 627-2001

Interview	Guillaume Langlois, Executive Associate Director	
Contact	Guillaume Langlois	
Data	***Founded***	1985
	Headquarters	Montreal, QC
	Other offices	Quebec
	Total number of employees in security	35
	Employees in Quebec	450
Mission	- The Nurun business unit is committed to accompany its customers in developing their business strategies and contributing to achieve their organizational goals in information technology.	
Strategy	- Attracting, engaging and retaining talent allows Nurun to be the leader in integrating Web-friendly business solutions, design and implementation of business models and innovative business services.	
Advantages & Issues	- Nurun brings a multidisciplinary approach and pragmatic focus in customer service. It aims to provide an integrated view of the organizational, legal, human and technological development of information security. - To accomplish their mission effectively, organizations must now take advantage of new Web 2.0, react quickly to changes in technology and have modern means of communication to interact with their customers and their partners. Nurun's challenge is to implement all these services while ensuring information security.	

Since 1985, Nurun has become known for its expertise in online government sites obtained mainly for the Government of Quebec. In recent years, Nurun consulting is becoming more diversified in the private industry, health and trade online.

"In addition to being recognized on the setting up of security technology solutions, Nurun has a full range of information security services. We offer services including governance, compliance, awareness, risk analysis, identity and access management. Our customers are mainly in Quebec, but we also have clients elsewhere in Canada, the United States, France and China," says Guillaume Langlois.

Optosecurity

505 Parc-Technologique Blvd.
Québec QC
G1P 4S9
418 653 7665
lfrancoeur@optsecurity.com
www.optosecurity.com

Interview	Eric Bergeron, President and CEO	
Contact	Lucie Francoeur, Marketing Director	
Data	***Founded***	2004
	Headquarters	Québec, QC
	No of employees in security	40
Mission	Optosecurity aims to increase security in the world	
Strategy	Setting the standard of excellence in threat detection	
Means	Acts as a leader in the security industry with innovative technology and products and unique solutions in order to establish new standards for threat detection.	
Benefits/ Issues	Canada's R&D policy played an important role in the development of Optosecurity	

Background

Eric Bergeron is an engineer and physicist by training but defines himself as an entrepreneur. He has 20 years experience in start-up management in the technology industry. In 2003, Eric Bergeron saw the opportunity to commercialize a military application developed by the National Institute of Optics (INO) in Quebec City. "The INO had no in-house contractor to develop this technology. So I created a spin-off and for nearly two years I developed the company alone with my own resources. In 2005, I managed to raise $ 5 million investment in venture capital, which allowed me to hire a team of PhD researchers and begin to develop the product with the participation of our first customer, "said Eric Bergeron.

Five years later, imaging X-ray technology has changed mainly because it has become a business application designed for both civilian and military use. Optosecurity has developed the first automatic detection system of threats for carry-on luggage at security checkpoints. The detection solution designed by Optosecurity relies on feature extraction and pattern recognition, although it also serves as a basic analysis of material and many complex algorithms for signal processing. The OptoScreener can be used in all places that require maximum security such as nuclear power stations and control critical infrastructure.

Technological Platform

Optosecurity has filed 60 patents in different countries. The company is the first to offer such a passenger service protection. Over the next few years, the firm will expand its services to the detection of threats in air cargo and port containers.

"We can detect a bottle of nitro-glycerine in the luggage, whilst to the naked eye, the container seems to be filled with water," said Eric Bergeron, who added “that OptoScreener is a system of decision support that improves capabilities of detection systems and conventional X-ray that allows security officers to better identify potential threats, such as weapons and dangerous liquids.”

Products

- XMS Threat Detection Software Suite
Optosecurity’s flagship product, the XMS Suite is a software product developed to complement X-ray imaging systems at the checkpoint with automated threat detection.

- OptoScreener
The OptoScreener system transforms the common checkpoint X-ray equipment of today into a precise automated threat detection system. A standalone system, the OptoScreener integrates the XMS Threat Detection Software Suite - an innovative decision support solution that enables conventional X-ray imaging systems to automatically detect liquid explosives and other liquid threats, bottles and concealed firearms and firearm parts.

- eVelocity Integrated Security Screening (ISS)
The eVelocity ISS software suite offers a network-enabled open architecture that gathers data from multi-vendor X-ray machines located in multiple checkpoints within one remote centralized screening room. Optosecurity’s technology allows the acquisition of X-ray RAW data from any manufacturer’s equipment along with a standard and consistent representation of this data.

- PICASO
PICASO (for Portal Image Contextual Analysis Software) is based on 3D computer vision and contextual visual analysis. It is designed to improve and automate capability body scanners. Using proprietary contextual algorithms, PICASO is aimed better detect anomalies driven by objects hidden under clothing.

Market

In 2010, the company officially went into its first year of commercial operation. Optosecurity does business primarily in the U.S. with clients related to the National Defence sector but also with Nuclear facilities and other high security domains.

PricewaterhouseCoopers (PwC)

1250 Rene-Levesque West Blvd., 28th Floor
Montreal, Qc
H3B 2G4
(514) 205-5001
http://www.pwc.com/ca

Interview	Marc Fournier, Associate Partner, and Maxime Rousseau, Manager, Information Security	
Contact	Marc Fournier	
Data	***Founded***	1849
	Headquarters	New York
	Number of employees	World: 163 000 Canada: 5 200 Security World: 2 300
	Clients	Banks, large corporations
Strategy	Worldwide vigil and governances processes.	
Means	High level professional services.	
Opportunities and Issues	Adapt governance to security requirements.	

Computer security at PricewaterhouseCoopers (PwC) began with the popularisation of accounting software in the '70s. Since then, it has become inseparable from accounting and management.

Early on, PwC – along with the "Big Four"[28]– ensured that the accounting data in enterprises where they acted as auditors remained protected against modification.

Their first mission was to certify the financial statements of clients. Then, with the expansion of computer systems, they sought to help their customers protect themselves, protect their systems and also set up security tools that were effective in terms of access management, compliance regulation and protection of personal information.

The need for protection has evolved and today there are many firms who specialize in security. However, even if a firm like PwC allocates a small share of its resources to security, in terms of numbers, there are globally about 2,300 consultants who specialize in this area. This is much larger number than many firms that are specialized in security.

[28] The expression “Big Four” designates the four world largest professional services companies: Deloitte Touche Tohmatsu, Ernst & Young, KPMG and PricewaterhouseCoopers

Technology Platform

"PwC is a service provider, said Marc Fournier. We do not manufacture or sell any security tool. Our role is to help a client choose the right tool, install and configure it and implement the processes in view of managing the tool and create value. "

Business Strategy

According to Marc Fournier: "The strength of PwC is based on an outstanding feature: We operate in 151 countries on various projects, which means that there is always someone in the world that is capable of performing a mandate. We were able to set up a world monitoring system. PwC's strategy aims at helping its technologically advanced customers to predict the future. "

Nature of the market

"The security market in Canada is still in a transition phase. Some clients think that the risk factor is lower here than elsewhere in the world. But when the same client sees in the newspaper that his competitor is experiencing security difficulties, he begins to react."

Issues

"PwC is entirely oriented towards strategy and tactical processes. Our role is to put security issues on the same level as governance and information strategy."

Silanis

8200, Decarie blvd, suite 300
Montreal, Qc
H4P 2P5
http://www.silanis.com

Interview	Tommy Petrogiannis, President & CEO	
Contact	Tommy Petrogiannis, President & CEO	
Data	***Founded***	1992
	Headquarters	Montreal
	Activity	Electronic signature
	No of employees	Canada: 75 U.S.: 5
	R-D	25
	Revenues	6,2 millions (2009)
	Markets	Private sector: 75%, Government (US) 25%
	Clients	Government, insurance
Mission	Silanis provides solutions to automate approvals – blanket purchase agreements (BPA) – and since 2010, sells licenses of transactional sites.	
Strategy	Silanis has nearly twenty years of experience in the development and deployment of software management approvals. Silanis has specialized in the field of insurance, banking and property management. Strong partnership with IBM. Silanis customers all come from the United States. In the 90s, Silanis worked primarily through direct sales. Then the company changed its business model and now it only works in concert with partners, primarily IBM.	
Means	12 patents filed, 12 patents pending.	
Markets	- Insurance and Financial Services: 75% - Governments: 25%	
Benefits & Issues	- Silanis embodies the "paperless office". The company has computerized all necessary approvals, for example, for buying a house, from the offer to purchase to the submission of final copies to the undersigned. Thus, conclusion of a sale of a property, which could last up to three hours, is now reduced to 15 minutes – because all documents have been previously read, approved and signed by the parties. - Silanis has prevailed against a legal challenge of the process, which confirms the soundness of the electronic signature process and BPA on the legal level.	

Background

According to Silanis President, Tommy Petrogiannis, the heart of business processes is the approval of written documents: "In an office, all documents are now generated electronically and printed for reading or signing thus causing a bottleneck. Organizational management is mostly approval processes that materialize these documents. "

A few years ago, graphics tablets and pen-based computing seemed a solution to the blanket purchase agreements (BPA) issue. Some work was done on computerized tablets in the late 1980s. But the technology never spread outside niche markets. In 1992, Mr. Petrogiannis and his two partners (Joseph Sylvester and Michael Laurie) decided to focus on the validation process of the problem. They created Silanis in 1992 around a software package that facilitates the creation, management, and distribution of electronic documents through the use of an electronic handwritten signature.

The company's second client was Walt Disney Imaging (the first was Ontario Hydro). Since then, Silanis has been working mainly in the United States. A first jump was given to its business in 1997 when the U.S. Joint Chiefs of Staff (JCS), located at the Pentagon, adopted its electronic signature solution (ApproveIt® Desktop) in order to precipitate the workflow of all 1,500 department members.

The second jump came in 2000, when the U.S. Army Medical Command (MEDCOM) equipped its 40,000 employees with Silanis solutions, making it the single largest deployment of approval automation software to date.

Labelled "a company to watch" by CIO Magazine, and recognized by Gartner Research as "the leading producer of electronic signature software," Silanis has established the largest customer base in the industry, with over 1,000 organizations and more than half a million users, within the financial services, Government, manufacturing, health, and FDA-regulated sectors.

For its third milestone, Silanis has created a new division in 2010, Esignlife, currently in incubation, whose mission is to offer to SMEs the electronic signature process hosted on the new business platform IBM LotusLive.

Technological Platform

Silanis main product is the Silanis ApproveIt product family whose aim is to make the electronic signature simple and with the same legal value as a classic signature on paper. The products are tailored to companies' operations; they do not require that business processes are reconfigured.

ApproveIt products are divided into two suites, one centered on electronic approval and the other on-line transactions:

- eApproval (approved online) offers a full range of electronic signature and approval management. These products can be deployed in a specific service for a product line, or can be combined to upload the entire process of approval signatures that was previously on paper.
- eTransaction (online transaction) offers a secure, scalable online registry configurable for financial transactions which include negotiable documents. The products operate together to generate, identify and track the owners of copies and transfers for the life force of all these documents.

Business Strategy

Silanis sells a system aimed at automating and simplifying business process, while increasing productivity and efficiency. Tommy Petrogiannis explains: “Office automation still is a delicate balance between user friendliness and security requirements.” Technology must be transparent to users who do not want to keep downloading certificates or public keys. Silanis monitors the system various processes from a centralized server that remains invisible to users.

Silanis considers that security is not solely based on a technology application. It is the result of a process. Its expertise is shared with the company's clients in order to reorganize and to better plan internal processes and make them legally binding. At the same time, it respects its clients' commercial, legal and technological needs. Thanks to its direct sales force, Silanis can cooperate with its clients in order to select the better solutions for a given corporation and its business environment. Target markets are regulated sectors and geographically dispersed corporations such as governments, finance services, medical, and health care industry and large manufacturing plants.

Market

In recent years, Silanis specialized to finance, particularly in the insurance, mortgages and real estate domains. These are regulated markets, where the complex approval process is one of the foundations of decision making in the organization. "It took several years," says Tommy Petrogiannis, for industries to understand how to integrate electronic signatures into their business processes. Companies interested in adopting automated approvals are now driven by the savings or the need to retain their customers. This is why Silanis is successful in regulated markets and in countries which have legislation governing the acceptance of digital signatures. In addition, PDA process efficiency is now recognized."

Other players in this market include companies developing digital signature software and consulting firms that develop products tailored to their customers.

Many sectors are actively engaged in the PDA process are part of the "early majority". Others, like the health sector are "early adopters".

Issues

The future of Silanis market lies in the laws and regulations that define emerging standards. Several markets have already published standards that support technology from Silanis, and market openings will depend upon the adoption of additional laws or regulations.

Silanis revenues which were at $7.5 million in 2008 decreased to $6.2 million in 2009, a loss of eighteen percent. However, the company has no debt and its financial reserves enable it to consider the future without fear.

"2009 was a very bad year for our customers in the U.S., but now the business has recovered and we believe that 2010 will be a recovery year. New rules taken by Obama in the fields of finance and real estate management will allow us to increase our market share."

Appendix 2: Survey Questionnaire

Canadian Advanced Technology Alliance (CATA*Alliance)*

CANADA ADVANCED SECURITY INDUSTRY

The proposed CATA*Alliance* study will deal exclusively with advanced security – computer security + physical security using information and communications technology (ICT). The study's objective is to develop a strategic perspective of the advanced security industry and its ability to support the domestic market needs, and exports to key markets.

With the cooperation of CED

CONTACT
Huguette Guilhaumon, CATA
Innovation Manager
36 Trafalgar Place, Montreal, QC,
H3H 1T3
Tel. 514.656.3254
Fax 514.313.5751
Email service@cata.ca

With the cooperation of MDEIE

Company Description	
Q.01	**Name** …………………………………………………………………………………… **Surname** …………………………………………………………………………………… **Email** …………………………………………………………………………………… **Telephone** …………………………………………………………………………………… **Title** …………………………………………………………………………………… **Name of company** …………………………………………………………………………………… **Website** …………………………………………………………………………………… **Civic number** ……… **Street/Place/Blvd./Ave.** .... **City** …………………………………………………………………………………… **Province** ……… **Postal Code** …………………………………...
Q.02	**In what year was your company established?*** *[For international corporations: Please indicate the incorporation date in Canada.]* ……………….
Q.03	**How many full-time employees currently work for your company?** *[Data for Canada exclusively.]* ……………….

Q.04 **Of that total, what percentage is allocated to security?**

……………….

Q.05 **In your company, how many employees work:** *[Security employees only]*

In your home province ……………………… Elsewhere in Canada ………………………
In the United States ………………………… Other countries ……………………………..
[Please specify what countries]
…………………………………………………..
…………………………………………………..

Q.06 **How many women are there among your security employees?**
[If you are unsure, please give an approximate percentage.]

In your home province ………..
Elsewhere in Canada ………..

Q.07 **In your company, how many consultants work part time in security?**
[IN PERSON-YEARS EQUIVALENT. For example, if 4 freelancers work 3 months each, this would translate into one person contracted for a 12 month work. You then indicate: 1 consultant. If you are unsure, please give an approximate number of consultants.]

In your home province ………..
Elsewhere in Canada ………..

Q.08 *[Security employees only in Canada]*

In your company, **are the number of employees:**	**Last year** *(2009)*	**In 2010** *(forecast)*
Increasing ………………………………..	□	□
Decreasing ……………………………….	□	□
Stable ……………………………………	□	□
Do not know/Not sure ………………..	□	□

Company Activities

Q.09 **How would you define your company?**

□ Equipment manufacturer □ Service Provider
□ Software editor □ Other (please specify)
….……………..………………….…………
….……………..…………………………….

Q.10 **What main security products or services does your company offer?**
[security products or services only]
1°) ....………………........
2°) ....………………........
3°) ....………………........

Additional products (if any): ....

Market Information

Answers to the following questions will be treated as **confidential**. Information will be used only in an aggregated form in order to perform statistical analyses. Neither CATA nor its partners will use this information; it will not be divulged to any third party.

Q.11

Who are your main clients?
[You can tick more than one answer.]

Companies of more than 500 employees
Companies of 300 to 499 employees
Companies of 100 to 299 employees
Companies of 50 to 99 employees
Companies of 20 to 49 employees
Companies of 10 to 19 employees
Companies of 1 to 9 employees
Individuals

Please specify your clients' main type of business:
[*banks, manufacturers, government departments, police forces, defense, airports, retailers, etc.*]
....
....

Q.12

What percentage of your clients work in the...*
[The sum of the numbers entered must equal 100.]

… business sector? …………
… government and semi-public sector? …………
… residential sector? …………

Q.13

Within those sectors, please indicate the field in which your clients work.
[Do not provide company names only categories. See examples below.]

BUSINESS (banks, insurance, transport, retail, gas stations, lawyers, etc.) ……………………………………………..

GOVERNMENT & SEMI-PUBLIC (government departments, national defense, first responders, municipalities, schools/universities, health, etc.) ……………………………………………..

HOUSEHOLDS (directly to consumers or through alarm companies) ……………………………………………..

Q.14

What percentage of your sales do you ship to…

	0% *Nothing*	**1-25%** *Some*	**26-50%** *Quite a few*	**51-99%** *A lot*	**100%** *All*
your home province	□	□	□	□	□
elsewhere in Canada	□	□	□	□	□
in the United States	□	□	□	□	□
other countries	□	□	□	□	□

Q.15 **For those who sell outside of their home province, what is the proportion of...**
[IN PERCENTAGE. The sum of the numbers entered must equal 100.]

… manufactured products? …………%
… software and application products? …………%
… consulting services? …………%
… other? …………%

Q.16 **How would you qualify your sales in 2009?**
[security only]

□ Increasing
□ Stable
□ Decreasing
□ Do not know yet

Any comment about sales trends?
……………………………………………………………………………………………………
……………………………………………………………………………………………………

Q.17 **Are you targeting new markets inside or outside your home province?**

□ YES, this coming year (2010)
□ YES, within two years (around 2012)
□ NO
□ Do not know/Not sure

If you answered YES, please specify

□ In Canada
□ In the United States
□ Other countries
Please specify what countries?
…………………………………………
…………………………………………

Q.18 **If you answered YES, please specify:**
[Examples of "economic sectors" referred to in this question are: Transport, health, police, law, government departments, etc.]

Outside your home province in 2010 (please specify what province or country) …………………………………………

Outside your home province within 2012 [ditto] …………………………………………

Within your home province in 2010 (please specify what economic sector) …………………………………………

Within your home province within 2012 [ditto] …………………………………………

Corporate Strategy

Q.19 **Does your company conduct R&D?**

YES □ NO □ Do not know □

If YES, how many employees are allocated to R&D?: *[Researcher-year equivalent.]*
……………………………………………………………………………………………………
…………………………………………………………………………… *[then, please go to Q.16]*

Q.20	**Please indicate the research fields pursued by your company?** [E.g. authentication, cryptographic techniques, public key technology (PKI), video surveillance, remote sensing, etc.] ……… ………
Q.21	**What are the principal objectives of your R-D activities?** [Please tick 2 answers only.] □ Improve the quality of your products □ Reduce production costs □ Create new products □ Other If you answered OTHER, please specify: ……………………………………………… ………………………………………………………………………………………
Q.22	*Are you looking for financing?* YES □ NO □ Do not know □ **If YES, for what purpose:** [Please specify if it is for R&D, new markets, promotion or any other] ………………………………………………………………………………… …………………………………………………………………………………
Q.23	**What are the main obstacles facing the Canadian security industry today?** □ Local competition □ Foreign competition □ U.S. Protectionism □ Recruitment of skilled staff □ Financing □ Lack of government support □ No particular obstacle □ Other (Please specify) …………………………………………………………………… ……………………………………………………………………………………………… ………………………………………………………………………………………………

DO NOT FORGET TO RETURN YOUR QUESTIONNAIRE

BY E-MAIL SERVICE@CATA.CA
BY FAX (514) 313-5751

THANK YOU !

Appendix 3: Main Acronyms

ASIS	American Society for Industrial Security
ATM	Automatic Teller Machine
BIS	Bank for International Settlements
CANASA	Canadian Alarm and Security Association
CCTV	Closed Circuit Television
CGEIT	Certified in the Governance of Enterprise IT
CIPS	Canadian Information Processing Society
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CobiT	Control Objectives for Information and related Technology
DES	Data Encryption Standard
ECC	Elliptic curve cryptography
EPPR	Emergency Prevention, Preparedness and Responses
ERP	Enterprise resource planning
FDA	Food and Drug Administration (U.S.)
ICT	Information and communication technologies
ISC	International Security Conference
ISP	Information Systems Professional
ITCP	Information Technology Certified Professional
ITU	International Telecommunication Union
NCRC	National Research Council Canada
OCIPEP	Office of Critical Infrastructure Protection and Emergency Preparedness
Octave	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OSSTMM	Open Source Security Testing Methodology Manual
PIPEDA	Personal Information and Electronic Documents Act
PKI	Public Key Infrastructure
PMP	Project Management Professional
RFID	Radio Frequency Identification
SCC	Standards Council of Canada
SMEs	Small and medium enterprises
SSCP	Systems Security Certified Practitioner
TSCP	Transglobal Secure Collaboration Program
VPN	Virtual Private Network

CATA*Alliance*

About CATA*Alliance*

Mandate and Mission

The Canadian Advanced Technology Alliance (CATA*Alliance*) grows the revenues of its members by creating a collaborative edge -- a chain of expanding value that ripples across Canada's Innovators, Commercializers, Users, and Professionals.

The largest high-tech association in Canada, CATA*Alliance* matches businesses with opportunities across almost every sector, so that we can all do business together. Reaching out from Canada, CATA*Alliance* members are connected with investment and partnership opportunities with the major global companies. As 80% are exporters, CATA's members are the arrow-head for global growth.

Through its "Innovation Nation" program, CEOs come together to catalyze the development of the Canadian business environment. CATA is the foundation for commercialization, market research, networking, events, access to other associations, and professional development, across the nation.

Add your strength to the collaborative edge -- we would like to connect with you!

Support Industry Advocacy and Business Development: Apply for membership today.

Contact :

Cathi Malette:
cmalette@cata.ca
613-236-6550
http://www.cata.ca/

CATA*Alliance*

Advanced Security in Canada 2010-2012

The scope and sophistication of information security attacks on businesses has escalated. Are we protected? Does Canada have a security industry, or even a security cluster? What are its strengths and weaknesses?

In 2010, the Canadian Advanced Technology Alliance (CATA*Alliance*) made a profile of advanced security enterprises in Canada. A survey was send to 665 enterprises and thirty one on one interviews were performed with key executives.

More than 150 enterprises responded. Their names and data are available on the CATA*Alliance website*: http://www.cata.ca

The report contains:

- ✓ Industry profile
- ✓ Market strategies
- ✓ Export trade
- ✓ R&D trends
- ✓ Financing
- ✓ Issues

This report was created for

- ✓ Security industry executives
- ✓ Security goods and services users
- ✓ Public and private investors
- ✓ Government decision-makers
- ✓ Foreign partners
- ✓ Trade press

Print format*:* $**320.00** + taxes
E-book (PDF format): $**280.00** + taxes
50 percent discount for CATA*Alliance* members
Email: cmalette@cata.ca

Commercial contact:
Cathi Malette
Telfer School of Management, Desmarais Building,
suite 6119, 55 Laurier E., Ottawa, ON, K1N 6N5
Tel. **613.236.6550**

Author:
Jean-Guy Rens
36 Upper Trafalgar Place
Montreal, QC, H3H 1T3
Tel. **514.667.2097**

Government of Canada Gouvernement du Canada

Canada

With the cooperation of the Government of Canada and the Government of Quebec

Québec

Legal Deposit:
Library and Archives Canada, 2010
Bibliothèque et Archives nationales du Québec, 2010
ISBN 978-2-9812174-0-0