2009 Rotman-TELUS Joint Study on Canadian IT Security Practices

This is the second in a series of annual studies that the Rotman School of Management and TELUS are undertaking that seek to develop a better understanding of the state of IT security in Canada, across industries, provinces, and businesses of all sizes.

Study and executive summary available at
telus.com/securitystudy or
rotman.utoronto.ca/securitystudy

Dr. Walid Hejazi
Professor of Business Economics
Rotman School of Management
hejazi@rotman.utoronto.ca

Alan Lefort
Managing Director
TELUS Security Labs
Alan.Lefort@telus.com

Table of Contents

SUMMARY OF KEY FINDINGS

2009: A Challenging Year for Security

In 2008, TELUS and the University of Toronto's Rotman School of Management jointly developed an annual study to provide clarity on the state of IT security in Canada. Responses from 300 IT and security professionals allowed us to understand for the first time how Canada differed from the US in terms of the threats it faced and how prepared Canada was to deal with those threats, in terms of people, process, and technology.

The 2008 study was also unique in that it sought to understand the broader business context of security. By focusing on how people, process, and technology interact to yield superior results, we discovered some key best practices of top performers. These practices included a stronger focus on communication and risk management, a greater focus on protecting applications and how to optimize budgets.

Upon conclusion of the 2008 study, we set a 2009 goal to validate and expand on our many findings, but something happened to change our focus. In late 2008, the economy experienced a serious crisis with lasting effects across all business. The magnitude of the downturn forced us to rethink our approach to the 2009 study.

To ensure that our survey would bring to light all of the effects of the financial crisis, we held eight focus groups across the country with over 50 security executives and practitioners. Their insight helped to shape our survey and gave us a much needed context to interpret the 2009 results, post-crisis.

After our focus groups, we no longer wondered whether or not we would observe changes in security year over year. That was a given. Rather, we focused our study on a better understanding of where changes were occurring and what impact those changes would have on Canadian organizations. As it turns out, the impacts were significant. Although organizations generally maintained their commitment to security, the crisis has amplified the threat, both from the outside and within. As a result, the gap between threat and preparedness has grown significantly.

Breaches are up significantly; annual costs are up; single breach costs down

Breach measures are important because they reflect the hardest, most impacting indicators that tell how well an organization's security program is performing. This year we focused on three measures: number of breaches, annual loss due to breaches and individual breach costs. Respondents reported a much higher number of breaches, offset partially by lower costs per breach, resulting in higher annual costs. Specifically:

- Annual losses from breaches have increased to $834,149 per organization up from $423,469. This increased most for government and private companies and increased minimally at publicly held companies.
- The average number of annual breaches reported has increased to 11.3 per year, up from 3 in 2008. Government led in this category while publicly held organizations increased least.
- The cost per breach has decreased across all types of organizations. For example, publicly traded organizations decreased breach costs to $75,014 in 2009 down from $213, 926 in 2008.

While the increase in reported breaches is significant, there is some good news. Yes, threats are up, but it is partially because organizations have improved their capabilities to detect unknown security events. Organizations are also improving their response to breaches, which has lowered individual breach costs.

Canada catching up to USA in terms of breaches

Last year we noted that Canada had caught up with the USA in terms of security investment, driven by requirements to comply with Canadian regulations such as PCI and PIPEDA. This year Canada has caught up in a less than desirable category. We compared our 2009 breach statistics with those from the USA's Computer Security Institute's (CSI) annual computer crime survey. Our comparison showed that across most categories Canadians reported equivalent or higher amounts of breaches. Specifically:

- Financial fraud (Can 14% vs. USA 12%)
- Sabotage (CAN 3% vs. USA 2%)
- Virus / malware (CAN 70% vs. USA 50%)
- Wireless abuse (CAN 15% vs. USA 14%)
- Misuse of applications (CAN 13% vs. USA 11%)

Most breaches Are Up: led by unauthorized Access by Employees

In 2009, the number of breaches increased in 12 of the 17 categories surveyed and decreased in three. The five fastest rising breach categories are:

1. Unauthorized access to information by employees (up by 112%)
2. Bots within an organization (up by 88%)
3. Financial fraud (up by 88%)
4. Theft of proprietary information (up by 75%)
5. Laptop or mobile-device theft (up by 58%)

The Five breach categories that remained constant or declined each are:

1. Password sniffing (down by -17%)
2. Phishing and pharming (down by -15%)
3. Denial of service attacks (down by -6%)
4. Sabotage of networks (no increase)
5. Exploiting DNS (no increase)

Insider breaches almost double in 2009, now comparable to USA rates

In 2008, Canadians reported that about 17% of breaches were related to insider activity, while the USA statistic was about 60%. In 2009, this has increased to 36% in Canada and decreased to 44% in the USA, based on the latest CSI survey.

Disclosure or loss of customer data remains top Issue

To understand what drives security programs and spending, we asked respondents to rank 10 prevailing security issues. Their top 5 concerns for 2009 are:

- Disclosure or loss of confidential data
- Compliance with Canadian regulations and legislation
- Business continuity and disaster recovery
- Loss of strategic corporate information
- Employee understanding and compliance with security policies

Organizations cite damage to brand as biggest breach concern

Canadian organizations continue to report damage to brand as the most significant impact of a breach. Organizations cited the following as their top five costs associated with breaches:

1. Damage to brand or reputation
2. Lost time due to disruption
3. Lost customers
4. Regulatory actions
5. Litigation

Growing threat has rendered most security budgets inadequate

In 2009, the average security budget was 7% of the IT budget. Top performing respondents spent at least 10% and several spent 15% or more of their IT budget. Spending alone did not guarantee a better posture. In 2008 we found that a budget of at least 5% correlated with high satisfaction in security posture. In 2009, we found that high satisfaction with security performance required at least a 15% investment. This shift is mirrored by a significant increase in number of breaches suggesting that the effect of security budgets, often planned a year in advance, is highly sensitive to sudden and major changes to the threat environment.

Budgets were reduced by 1/10th due to the financial crisis

The financial crisis that began late in 2008 and intensified during 2009 prompted organizations to make several fiscal adjustments. According to respondents, the financial crisis had impacted their security program, mostly in budgets and outsourcing. We observed that:

- Respondents reported an average security budget decreases of 10%
- 25% reported a budget increase in 2009.
- 20% of respondents reduced their reliance on outsourcers and contractors.
- 75% reported no changes to headcount.

Overall, the budgets adjustments were challenging, but not severe. Had it been any other year, their impact might have been minor or negligible. In 2009, the significant surge in the number of breaches served to magnify the effects of the budgetary adjustments.

Organizations rewarding formal education more than certifications

Notwithstanding the budgetary adjustments, the security profession is well compensated. Near half (46%) of respondents earned more than $100,000 annually, falling into our high earner category. High earners were most prevalent in IT, communications and media, finance and insurance, and government organizations. Within the high earners, we found a wide range of salaries. For example, directors averaged $132,000 nationally, $118,000 within the government sector, and close to $160,000 in finance, IT, and communications.

For high earners, formal education pays more than certifications and experience alone. Similar to our 2008 results, high earners are much more likely to have a university degree, and twice as likely to have a business degree. Professional designations like the CISA and CISM designations still appear to command a modest premium but much less so than a business degree.

Earnings gap between government and private sector could lead to brain-drain

In 2008 we observed the potential for a migration of talent from government to the private sector because of a large compensation gap. This gap is slightly larger in 2009. About 35% of security professionals working in government earn over $100,000 per year, compared to 47% of those working in private companies and 57% in publicly traded companies.

High-performing security programs have strong governance and education

A higher satisfaction with security posture continues to be driven by greater focus and investment on process. In 2009, education is a new driver for performance. Organizations that use educational programs to promote awareness of security risks are almost twice as likely to be highly satisfied with their security posture.

Other links between governance and high performance include:

- The adoption of business-level security metrics increased the perceived value of the security function by 47%.

- Awareness programs for staff and third parties were associated with a 45% to 55% higher satisfaction with security posture.
- Organizations that link staff evaluations to security goals (accountability) are twice as likely to be high performers.

Application security practices not keeping up with evolving threats

In 2008 we found that top performers invested more in application security and were much less likely to experience several classes of breaches. This year, we focused on how Canadian organizations secure their applications and learned that:

- More than half of the respondents gave some consideration to security in their development lifecycle.
- The focus in Canada is predominantly towards after-the-fact security activities, such as testing, rather than embracing the concept of "build it secure."

Based on the reported increase in application-related breaches, attempts to secure applications are falling behind.

Organizations seemed to be focused on testing with certain types of testing yielding better results:

- Code reviews result in the greatest satisfaction with security
- Independent testing teams with direct access to authority are most effective.

On-shore security outsourcing increases

Our 2008 report linked security outsourcing and with better satisfaction with security posture. This year we speculated the financial crisis might accelerate a movement to outsourcing, yet it grew marginally. Still we did observe a few important differences in 2009. For example:

- Slightly more organizations are willing to outsource (62% in 2009 versus 60% in 2008) and those who do are outsourcing a greater percentage of their security budget
- Privacy concerns are driving a policy shift that favors outsourcing security to Canadian service providers
- Publicly traded companies are more willing to outsource to the best-value provider regardless of location

Overall use of security outsourcing continues to mature in Canada. Respondents are spending more of their budget to procure services such as security testing and perimeter security. As in 2008, organizations that outsourced security were less likely to report a breach.

Cloud security concerns similar to classic outsourcing; it's about trust

An emerging trend in IT is the use of cloud- or utility-based computing to provide services and infrastructure to the business at an optimized cost. Despite the cost advantages and the clear cost pressures imposed by the financial crisis, organizations will not rush to adopt cloud technologies until policy and governance concerns are addressed. The top three concerns with security services in the cloud were:

1. Location of the data.
2. Connecting business-critical systems to security mechanisms outside the full control of the business.
3. Technical challenges associated with security in multi-tenant environments.

Respondents were least concerned about application availability, suggesting that the alternate method of providing service is more accepted in terms of performance. Overall cloud computing is viewed similarly to outsourcing and similar trust issues must be satisfied prior to adoption.

Technology investments focus on fighting malware

Our study surveyed respondents on 23

technologies looking at current adoption, future plans and satisfaction.

One key finding is that in response to the continued threats of viruses, malware, and bots, organizations are focusing their resources where breaches are highest: malware. We observed an increasing investment in the following technologies:

- e-mail security (ranked 1st in usage)
- Anti-virus (ranked 2nd in usage)
- Patch management (ranked 4th in usage)
- Content and malware filtering (ranked 5th, up 6 spots from 2008)
- Vulnerability detection and management (ranked 9th, up 7 spots from 2008)

Organizations favor protecting applications versus fixing them

Although malware related breaches are on the rise, so are targeted attacks. Unlike 2008, organizations are starting to pay more attention to protecting applications and the proprietary data they hold. In 2009, use of technologies that prevent or deter application level attacks has increased. These include:

- Two-factor authentication
- Web application firewalls
- Database encryption
- Public Key Infrastructure

Technologies aimed at fixing application flaws are used less often. Application security assessment tools have the third lowest satisfaction level (21st out 23 technologies), likely due to a lack of skill sets and staffing to remediate applications.

Insider threats up, low satisfaction holding up investment

Given the surge in insider breaches, we expected technologies aimed at detecting and preventing internal abuse to be more common in 2009. Not so, in some cases the use of these technologies decreased while others gained marginally.

Several detective technologies have low satisfaction levels in common. According to our focus groups, technologies which automate detection but not response can overburden security teams. In 2009, staffing increases were uncommon and organizations struggled with deploying more detective technologies. These technologies include:

- Data leakage prevention (ranked 23rd in Satisfaction)
- Log management (ranked 22nd in satisfaction)
- Security information and event management (ranked 20th in satisfaction)
- Wireless intrusion prevention (ranked 19th in satisfaction)
- Network based access control (ranked 18th in satisfaction)

Conclusions

With the threat landscape evolving, Canadian organizations are finding it difficult to maintain their security posture, especially with the current financial challenges. In 2009, top performers overcame these difficulties by:

- Managing the complete breach life-cycle, ensuring that improvements in detection and remediation are accompanied by improvements in prevention
- Developing flexible security programs with strong core capabilities and the ability to adjust to a rapidly changing threat environment
- Increasing focus on education and awareness across IT, development and employees to ensure security risks and responsibilities are understood by all
- Balancing technology spend with staffing to ensure that lack of resources does not impede deploying and using much needed technologies

COMPLETE STUDY

Introduction

Collecting, storing and processing information is an increasingly important activity for businesses, governments, and non-profit organizations. Therefore, securing that information is critical to the success of such organizations. Real or perceived vulnerabilities in an IT security system can undermine user confidence, discouraging them from using the services of that organization. Conversely, an organization can leverage well structured, effective and secure IT systems as a competitive advantage. This study seeks to understand how Canadian organizations can secure their IT systems and enable these systems to provide them with a competitive advantage.

Why a Canadian study?

There are many global and USA surveys that consider the state of IT security, but not one is focused exclusively on Canada. In our interactions with senior IT executives in 2007 and early 2008, it was clear that many felt that existing studies were not accurately portraying the Canadian situation. Many felt that IT security strategies in Canada may differ from those in the USA because of the structural differences in the Canadian economy could. Specifically:

- The USA has a private healthcare system; Canada has a public one.
- The USA financial system is thousands of banks with fierce regulation and oversight; Canada has six large banks that dominate the banking industry and operate under government charter.
- There are cultural differences in Canada with regards to government and the role it should play as compared to the USA.

Given these obvious differences, we felt that Canadian attitudes towards security and the approaches to managing security risk needed to be understood. For that, a dedicated study that focused on Canadian inputs and issues was needed. With this mandate, TELUS Security Labs and the Rotman School of Management began a joint-study in early 2008 to examine the state of IT security in Canada. This partnership is committed to conducting an annual study that seeks to enhance the understanding of IT security from many dimensions, including vulnerabilities, preparedness, budgets, satisfaction, compliance, and best practices. This current document is the outcome of the second study in that series. The results are compared to those in the USA where applicable.

This year’s study was shaped by the 2008 findings and the financial crisis

The 2008 Rotman-TELUS Joint Study on IT Security Practices provided clarity on the state if IT Security in Canada and the dimensions in which Canada differed from the USA. And the findings of the 2008 study actually led to many new questions that needed answering. Questions involving the security of information systems and business applications, questions about cloud computing, breaches and countermeasures. Furthermore, the recent financial crisis posed new questions of its own. What would happen to budgets, staffing, outsourcing, technologies and initiatives? Could changes in these areas affect how well organizations could prevent and respond to threats and vulnerabilities? All of these questions are precisely what this second study will answer.

To answer all of the previous questions, this year's study was enhanced in several ways. Many new questions and areas of analysis were introduced. For example, a great focus was placed on understanding the impact of the current financial crisis to the state of IT security in Canada.

The following sections provide the results of that survey, and a detailed assessment of those results. It it is our hope that the report therefore will allow Canadian security executives and practitioners us to better understand existing and coming trends and formulate strategies and best practices that will improve their security postures.

In addition to the analysis provided in the study, the full set of responses is provided in appendix A.

Respondent Information

The 2008 Rotman-TELUS study analyzed the responses from 300 respondents in Canada across different geographies, industries and organization types. In 2009 we intensified our efforts so that we could increase the number of respondents and improve the representation across Canada and across several verticals. These efforts included:

- We hosted cross-country round-table discussions with IT security officers in Vancouver, Edmonton, Calgary, Toronto, Ottawa and Montreal. These round-table discussions were both specific to certain regions as well as to certain industry sectors such as government, finance, energy and utilities and others. These round-table discussions were attended by representatives from all organizational levels, from security analysts and technical experts to senior vice-presidents and compliance officers.
- We presented extensively at conferences across the country and collected feedback from attendees, as well as encouraged participation in the 2009 survey.
- We focused our resources on increasing general awareness so that potential respondents would understand the value of becoming more involved and sharing their perspectives.
- We administered the survey and all communications in both French and English, to promote participation from all regions of Canada.

All of these efforts paid off, as there was a 60% increase in responses over 2008 which provided access to the views of 500 Canadian organizations (with 100 employees or more).

About respondent organizations

Organizations across Canada responded as follows:

- **Organization type**: Government organizations are most highly represented with 35% of our population, followed by publicly traded companies at 31%. Private companies represent 27% of the sample and not for profit organizations represent 6%.
- **Geography**: 55% of respondents were from Ontario, 16% from Alberta, 12% from Quebec, 10% from British Columbia. The aggregation of all other regions in Canada and organizations with an international presence represented 7% of the sample.
- **Global Headquarters location**: 83% of the respondents had their headquarters in Canada, 11% in the USA, 4% in Europe (including UK), and the remaining 3% in Asia and other locations.
- **Operational reach**: when asked about where the organization does significant business (with the option to mark more than one region), 96% of respondents marked Canada, 41% the USA, 24% Europe (including UK), 13% Japan, 19% Asia (excluding Japan), 14% Latin America. 10% of respondents also marked “Other Regions”.
- **Annual revenue size (or budget size for government organizations)**: Organizations with less than 1 million Canadian dollars (C$1M) account for 1% of the sample, 10% have a revenue/budget of up to C$24M, 11% between C$25M and C$99M, 14% between C$100M and

C$499M, 8% between C$500 and C$999M. 10% of respondents report between C$1B and C$1.99B, 13% between C$2B and C$10B, and 13% of respondents have a revenue/budget higher than 10 billion Canadian dollars.

- **Number of employees**: Organizations with less than 100 employees represented 31% of respondents, 16% have between 100 and 500 full time staff, 7% between 500 and 999, 18% between 1,000 and 4,999, 6% between 5,000 and 9,999, 8% between 10,000 and 19,999, 6% between 20,000 and 49,999 and 9% had more than 50,000 employees.

Note: Organization with less than 100 employees participated in the survey but their responses were not included in some of the breakdown examinations conducted in this study. This separation was necessary to allow the analysis to be consistent with the 2008 study and capture year-Over-year trends. Also small organizations have significantly different behavior patterns than medium and large organizations, sometimes adding elements of randomness to the analysis. The investigation of their security practices will receive a separate, dedicated treatment in a forthcoming report.

This year's sample size of 500 is comparable with most North American and global surveys produced in the field of information security and IT risk management. To contextualize the level of participation and willingness to openly discuss issues around information security in Canada, we must consider the overall size of the Canadian economy against that of other countries. Canada's economy is approximately one-tenth the size of the US economy and Canada is the smallest member of the G7 group (with GDP comparable to Spain's). When we look at the number of survey respondents, the relative representation of Canadian IT and security professionals is quite high.

This willingness was also reflected in the level of participation and discussions held with security officers in focus groups and round-table discussions across Canada (Vancouver, Calgary, Edmonton, Toronto, Ottawa and Montreal). We also benefited from the involvement of representatives from several industries through vertical specific sessions for the Finance, Utilities, Government and Health Care verticals, as well as the participation of industry associations.

About the Security Professionals that Responded

Survey questions were designed to allow the research team to gather and compare perspectives from different geographies, industries and organization types. We also profiled security professionals in different organizations, looking to understand their roles, responsibilities, experiences and backgrounds.

Professionals from all provinces and territories except Prince Edward Island and the Northwest Territories participated in the survey, as well as representatives from 21 industry types including the federal, provincial and municipal government levels. The diversity in the respondent population allowed us to understand how information security differed, tactically and strategically, by region, by experience level and by industry.

The highest industry representation came from Information – Publishing, Broadcasting Communications and IT (14%), Finance and Insurance (14%), and Government (25% - Municipal 13%, Provincial 6% and Federal 6%). Respondents filled positions in their organizations from CEO (C-Level titles corresponded to 9%) to security analyst (19%) or system administrator (12%). 20% identified themselves as being a director or higher position. 59% reported being a manager or individual contributor.

The survey also asked the security professional about their role in the organization. During our focus groups it became evident that roles and mandates assigned to security professionals were very diverse and their opinions reflected that diversity. *Table 1* below shows the different roles assigned to security professionals in Canada in each organization type.

Table 1: Mandate of security professionals by ownership type

Security Role	Government	Private	Public
Security Operations	36%	26%	37%
IT/Security Audit	36%	31%	44%
Policy Development	40%	27%	32%
Forensics/Incident Handling	27%	16%	27%
Risk Management	35%	24%	34%
Management, Security Programs	33%	24%	27%
Security Architecture	34%	25%	34%
Secure Development	18%	12%	22%
Physical Security	17%	15%	16%
Regulatory Compliance	27%	19%	27%
Identity and Access Management	35%	18%	33%
Privacy	24%	16%	16%
Loss Prevention	19%	6%	7%

Regarding the reported earnings of security professionals in Canada, the average salary for respondents identifying themselves as Chief Information Security Officers was $116,000, while for a Chief Security Officer it was $96,000. Individuals claiming a Director title had an average salary of $132,000, while a Manager or IT or Security earned $103,000. Security analysts reported earnings of $89,000.

A key question that we wanted to answer was: where do respondents spend their time and attention? According to respondents:

- Security professionals working in the government are becoming more involved in the development and management of security programs than professionals in the private sector. This variation can be explained by the increased attention in the government sector to budgetary revisions and resource optimization programs, integration and data sharing initiatives between government agencies in Canada as well as new provincial and federal-level electronic and online services (which also relates to the higher level of government involvement with privacy programs in Canada).
- Unlike private companies, publicly traded companies and government entities assign their security staff in a very similar manner. The allocation of time and resources follow a similar pattern for security architecture, regulatory compliance, risk management, incident response, security architecture, physical security, identity and access management and security operations. This similarity suggests that government entities are aligning themselves with the same industry practices used by large enterprises and corporations, without losing sight of their unique requirements and objectives to its constituents.
- Generally, professionals from private companies reported less involvement with the security domains listed above. The responses from private companies may indicate that the responsibility for these domains is not centralized on the security function and may be shared with or wholly owned by the IT function or another group.

- Publicly traded companies have a higher involvement with IT and security audits, and audit response. This is understandable given the additional regulatory pressures and scrutiny from stakeholders that public companies face.
- Government entities dedicate a significant amount of attention to policy development when compared to public and private companies. This reflects a more formalized work environment and the requirement to demonstrate that proper protocols are followed, which does not necessarily reflect in higher satisfaction levels or less breaches, as we will see in the subsequent sections of the report. Government's attention to policies and procedures is consistent with their commitment to managing security programs and privacy initiatives.
- Professionals from public companies are spending more time to promote secure development practices within their organizations in comparison to private companies and government. The cause for the attention dedicated to secure systems development may be attributed to the fact that public entities are more involved with internal and external audits, which tend to raise audit gaps around the software development lifecycle. In addition, their revenue streams are becoming more dependent on complex business information systems, on a larger scale than private companies. Government entities tend to concentrate on the protection of sensitive data and privacy instead of revenue streams.

Profile of a high earner in security

As in our 2008 study, we felt it was important to understand how salaries in Security varied and why. We felt that Organizations looking to grow teams would benefit from an understanding of what skill sets and experiences were collectively valued most in Canada. Following the methodology used in the 2008 study, we focused our analysis on "high-earners" which we defined as professionals earning more than $100,000 annually. We then looked at education, certifications, experience and other elements that could be factors in salary differences.

About half (46%) of respondents earned more than $100,000 annually. The highest concentration of high earners was found in IT, Communications and Media, Finance and Insurance, and Government organizations. To further understand the difference in compensation within these industries, we compared the average salary for a Director responsible for information security in each one of them. While individuals claiming a Director title had an average salary of $132,000 nationally, the same title within the government sector would earn approximately $118,000. The compensation would be closer to $160,000 in the Finance and the IT and Communications industries.

If we examine compensation packages across some of the Canadian provinces, a Director in Ontario would earn $134,000 while a Director working in Alberta would earn $118,000 and $82,000 in British Columbia. *Table 2* shows the annual salary distributions between different organization types in Canada.

Table 2: Annual respondent salary by organizational type

Annual Salary	Government	Private	Public
<$100,000	65%	53%	43%
$100,000 or more	35%	47%	57%

As expected, higher positions had higher compensation packages, with 22% of high earners having a Director title, and 14% holding a C-level position. In addition, high earners shared the following characteristics:

- They are much more likely to have 10 or more years of experience in information security or related fields.
- They are likely to have a Business Continuity Planning (BCP), CISM or CISA certification. The CISSP certification could no longer be associated with high earners (a change since the 2008 survey).
- They are likely to possess a university degree.
- They are likely to possess a business or technology degree.
- They are *slightly less likely* to possess a college diploma or IT infrastructure, networking or security vendor certifications.
- They are *much less likely* to possess a privacy certification.

The price organizations pay for offering lower compensation packages

To better understand the impact of offering lower compensation packages to security personnel, we isolated the organizations in which the respondents reported earnings of less $100,000 and looked for common elements. Generally, the respondents from these organizations reported an average of 6 years of experience in information security or related fields. This is significantly less than the experience of better-paid security officers, who are more seasoned and are likely to have handled more security incidents before.

Turnover is another factor. Entities that offer lower compensation packages tend to face a much higher rate of turnover. 3.5% of respondents from higher paying organizations reported high or very-high staff turnover rates, while respondents from lesser paying organizations reported high or very high turnover 8.5% of the time. High turnover often results in low knowledge retention, low staff morale, lack of continuity in key initiatives, inconsistency of service, and greater risk of security incidents related to disgruntled employees. Notably, better-paying organizations were less likely to report insider breaches.

We also observe that higher paying organizations tend to have larger teams of full-time staff devoted to information security. This finding is explainable in that larger teams of well paid professionals will show stronger performance than smaller teams of underpaid staff.

Application Security

In 2008, we noted that top performers focused more on the protection of business information systems and applications, and that this focus was associated with both higher satisfaction and less breaches. For the 2009 survey we wanted to understand what practices organizations have around securing application and what results these practices generate.

Overall, we found that Canadian organizations are implementing secure development capabilities yet they favour after-the-fact detective and corrective measures more so than preventative controls. Respondents also reported that they are testing the security of their software more regularly. We also found that a properly designed secure software development lifecycle yields better results than relying on a singular focus on testing.

We found that the approach to and emphasis on securing application varies and that compliance plays a significant role in these decisions. Respondents with a greater compliance focus invest more time and effort on traditional security initiatives such as network security and encryption and a result spent less time on securing their software development life cycle.

More than half of respondents report a focus on secure development

With increased breaches related to applications in Canada in 2009 (see forthcoming section on breaches), application security is a rising area of concern that continues to mature in Canada. Of the Canadian companies surveyed, an average of 54% formally includes security at some point within their software development lifecycle.

Table 3: Existence of formal secure SDLC practices

Formal Approach to Secure Development	54%

While there was no major variation across organizational types (government, privately held or publicly traded), publicly traded companies were somewhat ahead while government lagged behind. As discussed in the respondents profiling, publicly traded companies tend to allocate more of their security professionals time to application security which correlates well with the greater likelihood of having a formal approach to secure development.

Table 4: Existence of formal secure SDLC practices by legal entity type

	Government	Private	Public
Formal Approach to Secure Development	51%	55%	57%

The more a Canadian organization does internal application development, the greater the likelihood that they will not include security as a formal element within their SDLC. Based on our focus group discussions, the most likely explanation is that organizations willing to outsource will have a greater level of rigour around their development processes (and impose that via requirements or outsourcing contracts). Conversely this indicates a lower level of diligence in managing the security risk introduced by internal development teams. There is also a sugestion that organizations assume their developers will do the right thing intuitively when it comes to building applications securely or that there is less control over internal development teams.

Table 5: Existence of formal secure SDLC practices by external development

Applications Developed Externally	Formal Security in SDLC
80-100%	43%
60-79%	33%
40-59%	25%
20-39%	14%
0-19%	21%

Compliance focusing organizations away from application security

Organizations following a compliance program are less likely to incorporate security into the SDLC than those operating without one. It is likely that compliance programs are causing organizations to focus on other aspects of security such as network perimeters and virus prevention.

Most compliance regulations, such as PCI-DSS or Bill C-198, or IT security and governance frameworks, such as COBIT or ISO27002, include the security of applications as one of several control areas. Many frameworks and regulations are designed with completeness in mind, and tend to emphasize breadth versus depth (a “checklist approach”). Accordingly, the distribution of countermeasures from organizations that primarily look for compliance is reflective of that approach. However, risk distributions are rarely linear, and the latest breach statistics show that application security is a targeted area. This gap in the deployment of security in the SDLC becomes apparent within organizations that are more focused on compliance. Organizations that tend to prioritize security based on the frequency and magnitude of risks tend to spend proportionally more resources to secure applications.

Table 6: Existence of formal secure SDLC practices by compliance driver

Has Compliance Program?	Has Formal Security in SDLC
Yes	37%
No	85%

More Canadian organizations are implementing security into their software development lifecycle but not all efforts are equal. More than half of the surveyed companies have some form of application security practices. This is promising, but the effectiveness of those efforts varies greatly. For several organizations there is less of a focus on security in the earlier stages of development (during requirements, design or implementation phases) and more a focus during post-development activities (post coding or post deployment of the application).

Table 7: Focus of secure software efforts

Preventative Approach	41%
Detective Approach	60%

Across all types of organizations we noted this bias towards finding the vulnerability after it has been created rather than a focus on preventative activities that reduce the likelihood of building vulnerability code.

Table 8: Focus of secure software efforts by legal entity type

	Government	Private	Public
Preventative Approach	44%	36%	42%
Detective Approach	56%	64%	58%

Organizations that focus on preventative aspects of security in the SDLC ultimately have a greater overall satisfaction with their information security posture.

Table 9: Satisfaction by secure software focus

	Less Satisfied	More Satisfied
Preventative Approach	36%	65%
Detective Approach	56%	44%

As explored in the breaches section, organizations that direct their security officers to invest more time in applications security tend to experience fewer breaches.

Four out of five Canadian organizations test their applications

Four out of five (82%) Canadian organizations employ some form of security testing of their applications, with many organizations performing testing as an ongoing formal part of their development lifecycle. Across all three legal entity types, the use of application testing is almost the same.

Table 10: Performance of application testing by legal entity type

	Government	Private	Public
Performs Applications Testing	78%	87%	86%

Those organizations that do not test their application security as part of their development lifecycle also tend to experience a lower overall satisfaction with their security posture.

Table 11: Satisfaction by use of application testing

	Less Satisfied	More Satisfied
Performs Application Testing	44%	57%
Does Not Test Applications	58%	43%

Organizations that test the security of their application portfolio frequently report higher satisfaction with their overall security posture. Manual penetration testing is a mainstay of evaluating the security capabilities of an application. Most organizations test at least once a year, and 30% of respondents test more often.

How you test matters

The type of testing method used also affects the improvement of an organization’s overall satisfaction with its security posture:

- Preventative approaches (such as code reviews) correlate with more satisfaction than detective approaches (such as penetration testing).

- Automated vulnerability testing alone has the least impact on satisfaction with overall security posture, although satisfaction increases with frequency.

Table 12: Testing type ranked by contribution to satisfaction

Testing Type	Ranking
Automated Code Review	1
Manual Code Review	2
Manual Penetration Testing	3
Automated Vulnerability Testing	4

This ranking is likely driven by tradeoffs between costs, sophistication and coverage of the testing type.

The level of independence and authority of the application tester is just as important as the method of testing. Relying on internal development teams to perform security testing and communicate the results to management tends to generate lower remediation actions than using external auditors.

the success experienced by those respondents using audit teams to perform their testing is noteworthy. This appears to reduce the likelihood of a breach. A likely explanation is not that audit teams are necessarily more skilled or adept at identifying vulnerabilities. Rather, audit teams are more effective at ensuring that issues get management visibility and therefore get the required resources to address the issues.

Table 13 demonstrates how a testing team's authority and independence from development relates to application-related breaches. Table 13 tells us that greater independence likely leads to broader disclosure of potential issues or flaws. It also suggests that the ability to command action or remediation of findings is just as important if not more so than the technical ability to find flaws.

Table 13: Testing entity versus experienced breaches

Testing Team	Authority (Access to Senior Management.)	Independence (Degree of Separation from Development)	Likelihood of application-related breaches
Internal Development Team	Lowest	Lowest	49%
Internal Security Team	Low	Low	41%
Internal Audit Team	High	High	19%
External Audit Team	Highest	Highest	14%
External Security Consultant/Contractor	Varies	Varies	35%

IT Security Budgets

How much an organization spends on security overall is one of the best indicators of how much security is seen as a business issue. We also understand that the level of spending can be influenced by so many factors. Organizations may rely on IT to differing degrees or may handle sensitive information more so than offers. Notwithstanding those nuances, data regarding budgets allows us to ask the questions that CIOs and CSOs ultimately must answer: Am I spending enough and, if so, what level of security am I getting for that spend?

To better understand IT security budgets, we focused our questions in three key areas:

- How is the budget structured and sized?
- How is the budget spent and correlated to measurable benefits to the organization?
- What impact did the global financial crisis of 2008/9 have on Canadian organizations in terms of budgeting, staffing, and planned-versus-executed initiatives?

Budget distribution

The majority of respondents have their security budgets as part of the overall IT budget and the majority of security officers report that security is part of the IT function. The average IT budget was reported to be at 7.9% of the overall organizational budget, and the average security budget was 7% of the IT budget, or a little over half a percent of the organization's total budget allocation.

33% of respondents reported that their security budgets were less than 3% of the overall IT budget, 40% indicated that their budgets were between 3% and 9% of IT spend, and 25% indicated that 10% of the IT budget was dedicated to security.

The distribution of security budgets also vary with each organizational type (government, publicly traded and privately held). *Table 14* below shows a breakdown of security budget allocation per organizational type.

Table 14: Security budgets by organizational type

Share of IT Budget spent on Security	Government	Private	Public
< 1 %	16%	24%	10%
1% - 2%	12%	20%	13%
3% - 4%	24%	12%	15%
5% - 6%	18%	15%	20%
7% - 9%	12%	2%	10%
10% -15%	8%	10%	23%
16% - 25%	8%	12%	3%
More than 25%	0%	5%	8%

An observation made in last year's study and confirmed this year is that publicly traded companies are twice as likely to spend 10% or more on Security compared to government organizations. This may be a concern given that government organizations are storing sensitive information related to critical infrastructure, and private data from Canadian citizens such health care records .Finally 25% of private companies spend 10% of more of the IT funds in information security, and almost half of them (44%) spend less than 3%.

To understand the impact of security spending on performance, we correlated budget data with overall security satisfaction and found that 61% of unsatisfied respondents spend less than 3% of the IT budget in security, while 50% of the very satisfied respondents spend 10% or more. Although higher satisfaction can be correlated with funding, just putting more dollars into security does not guarantee a better posture, as almost half (48%) of respondents that spend 10% or more in security did not report good satisfaction with their security postures. This association is also more evenly distributed as we look at the mid-range budgets of 3% - 9%. 20% of the satisfied and very satisfied respondents spend 5-6%, and another 20% of the very satisfied respondents spend only 3-4%.

To be satisfied requires funding, but just funding alone does not guarantee satisfaction. Last year we looked at the interaction between budget and satisfaction. Once they reached 5%, budgets would start to consistently correlate with higher satisfaction levels (80% or higher). This inflection point has increased to 15% in 2009. This shift is accompanied by a three-fold increase in the number of breaches reported by organizations in 2009. This suggests that the level of budget required to drive satisfaction is highly sensitive in changes to the threat environment.

Table 15: Satisfaction with security posture by security budget as a percentage of IT budget

Share of IT Budget spent on Security	Total Satisfied
< 1 %	27%
1% - 2%	53%
3% - 4%	53%
5% - 6%	58%
7% - 9%	33%
10% -15%	46%
16% - 25%	86%

Security staffing dependent on size and ownership type

10% of respondents (half of which are in privately-owned companies) reported having no dedicated full-time employees dedicated to information security, including IT security operations, audit and policy functions. 48% of the organizations indicated that they have a small team (1-4) of security professionals. 18% of respondents have 5 to 10 professionals in their security teams, 4% have 11 to 25 and 6% have 26 to 50 security staff. Roughly 13% of responding organizations have teams with more than 50 professionals, mostly in the public sector.

The approximate size of security teams in Canada is 6 to 10 professionals for government organizations and private companies, and 20 to 30 professionals for public companies. *Table 16* below shows the breakdown of team sizes per organization types.

Table 16: Size of security team by organization type

	0 FTEs	1 to 4 FTEs	5 to 10 FTEs	11 to 25 FTEs	26 to 50 FTEs	More than 50 FTEs
Government	10%	56%	18%	6%	4%	6%
Private	16%	51%	16%	7%	7%	2%
Public	5%	30%	23%	2%	7%	32%

Compliance most effective justification for funding projects

In terms of driving investments for security initiatives, regulatory compliance is the most successful approach to justifying budget allocation. Other drivers follow, in descending order of relevance:

1. Security Breaches;
2. Risk from Employee Activities (such as usage of wireless devices, remote access, etc);
3. Risk Management Concerns (related to potential losses);
4. Media (reporting of security breaches);
5. Clients demanding better security;
6. Security breaches affecting competitors or third parties; and
7. Security as a potential competitive advantage.

From this list there seems to be a pattern around the threat-related negative drivers (security breaches, violation of regulatory compliance) receiving higher priority than business-related positive drivers (competitive advantage, client demands) when security officers advocate for funding.

The 2009 financial crisis

The 2009 subprime mortgage crisis was prompted by a striking rise in mortgage foreclosures in the United States, with major adverse effects for banks and financial markets around the globe. Canada was not invulnerable to the financial crisis and our capital markets suffered, especially during the initial months of 2009. Global auditing and consulting companies warned that the pressures brought on by the financial crisis could significantly increase vulnerabilities to data breaches and that the budgetary cutbacks driven by cost-reduction initiatives would increase their exposure to security risks. As with most global studies, these estimations were based on observations of the reaction of USA-based organizations to the effects of the crisis, and by educated guesses of the future impact on the Canadian entities.

To validate these assumptions, we asked about the actual effects of the financial crisis on IT security budgets, outsourcing strategies, and staffing decisions. The response was visible but hardly dramatic, and most organizations responded with cautionary but level-headed measures.
Regarding security budgets being affected by the global crisis, 75% of responding organizations reacted by applying budgetary cuts to their security expenditures, while 25% actually *increased* their security investment.

50% of the respondents reported minor adjustments where only 10% or less of their budget was affected (most of them adjusting downward). 20% reported moderate cuts of 10%-25%, and less than 10% applied severe cuts of 50% or more. *Table 17* shows a detailed analysis of the reactions of Canadian organizations to the 2009 financial crisis. In all industry sectors, the highest response rates were within minor to moderate levels.

Table 17: Response to the 2009 financial crisis, by organization type

Effect of 2009 Crisis on Security Budgets	Government	Private	Public
Severe Budgetary Cuts: 50% to 100% of the original budget for contracts or projects related to security and privacy was cut.	4%	13%	12%
Major Budgetary Cuts: 25% to 49% of the original budget for contracts or projects related to security and privacy was cut.	6%	11%	15%
Moderate Budgetary Cuts: 10% to 24% of the original budget for contracts or projects related to security and privacy was cut.	15%	21%	23%
Minor Budgetary Cuts: Less than 10% of the original budget for contracts or projects related to security and privacy was cut.	42%	29%	38%

Effect of 2009 Crisis on Security Budgets	**Government**	**Private**	**Public**
Minor Budgetary Increase: original budget increased by less than 10% for contracts or projects related to security and privacy.	27%	21%	10%
Moderate Budgetary Increase: original budget increased by 10% to 24% for contracts or projects related to security and privacy.	6%	3%	2%
Major Budgetary Increase: original budget increased by 25% to 49% for contracts or projects related to security and privacy.	0%	3%	0%
Average Budgetary Impact	4.6% (Cut)	6.6% (Cut)	10.8% (Cut)

When asked about outsourcing decisions during the financial crisis, 64% of respondents did not change their strategies, while 5% reduced headcounts in their outsourcing contracts and 16% indicated that their outsourcing relationships were reduced significantly.

Finally, staffing decisions did not suffer major impacts. 74% of organizations did not change their staffing decisions for information security in 2009, and only 10% reported laying off part-time personnel, consultants or contractors.

Although Canadian organizations responded to the crisis by revising their budgets and increasing diligence levels when managing their capital and operational expenditures, the dramatic budgetary cutbacks did not materialize in Canada as most analysts predicted.

IT Governance

In the 2008 study we noted that in addition to budgets, the level of governance and maturity in risk management processes, communications and the frequency and quality of assessments contributed to the levels of satisfaction with the security posture within organizations. Satisfaction with the security posture was a key metric used in the 2009 study to qualify organizations as high performers. We examined what IT governance areas were receiving the most attention from organizations that reported higher satisfaction levels, and found several common elements around the "people" aspect of information security (education, awareness, establishing metrics and measuring performance) to have some weight.

Governance initiatives had a strong influence over satisfaction levels, for all items surveyed, and the top initiatives that are correlated with the highest satisfaction increases are security education for general staff, third parties and IT personnel (including developers and architects), the development of business-related security metrics and the linkage of security objectives to personal evaluation criteria (personal accountability for information security).

Table 18 below cross references governance initiatives (at the different stages of deployment) with the overall satisfaction with the security posture of the organization. A recurring pattern in the table is that satisfaction levels become stronger as the organization reaches later stages in the deployment lifecycle for these initiatives. This is likely because the benefits of each initiative are not fully experienced until projects are near the final stages of completion.

Table 18: Respondents satisfied with security posture - per initiative stage

Governance Initiative	Not Interested	Evaluating	Planning	Deploying	In Place	Overall Satisfaction
Security awareness program for general employees	27%	29%	46%	39%	73%	52%
Security awareness program specific to IT staff	21%	34%	42%	53%	71%	50%
Security awareness program specific to developers and architects	34%	46%	33%	64%	80%	46%
Linking general IT staff's performance evaluations to security objectives	35%	36%	61%	83%	82%	46%
Creating business-level security metrics	43%	44%	41%	58%	90%	47%
Security awareness programs for customers	42%	46%	70%	51%	84%	42%
Requiring suppliers, business partners or other third parties agree to organization's security policy	38%	53%	42%	48%	65%	27%
Integration of security into software/ application development	50%	31%	50%	68%	63%	13%
Requiring suppliers, business partners or other third parties to agree to organization's privacy policy	43%	36%	50%	55%	62%	19%
Security training for third parties (contractors, volunteers, co-op)	38%	48%	50%	85%	84%	46%
Mandatory tests after security awareness training	41%	47%	50%	80%	83%	42%
Criminal background checks for all IT and Security staff	29%	48%	33%	50%	67%	38%
Creating a security policy	50%	23%	33%	53%	62%	12%
Creating a privacy policy	50%	29%	26%	70%	60%	10%

Top initiatives for 2010 are security awareness, accountability and metrics

Although only 11% of respondents claimed to have business-level security metrics is in place, this is ranked as a top initiative by organizations in Canada. 29% of responding organizations are planning to deploy them in the next 12 months. This level of interest can be explained by the need to demonstrate value of information security under budgetary pressures.

Security awareness for customers is also driving for the top spot in 2010. This positioning is a function of the increasing availability of automated self-service portals for customers that enable new online and B2C business transactions. These operations rely heavily on the usage of customer-owned identities with credentials to business systems and data, which exposes organizations to new risks. These risks demand that customers receive proper education for two main reasons, firstly they are now actively participating in business transactions, and secondly due to liability limitation purposes. Security awareness is being driven mostly by the Finance, IT and Government industries.

A common theme around the top priorities is a shift towards understanding security in a broader concept of risk management. Increasing involvement of customers and suppliers in the value chain is redrawing the security function to understand risks inclusive of all stakeholders. Managing these risks also requires measurements of business-related metrics (another top priority for 2010). Another noteworthy top priority also reinforces personal metrics and the accountability required for proper business-related risk management.

While third party conformance is high (‘requiring suppliers, business partners or other third parties agree to organization’s security policy’), the intention to train is low. This reflects organizations’ desire to manage the risks associated with them without fully assuming the costs or internalizing the compliance risks (outsourcing tie-in).

40% of the responding organizations do not believe that criminal background checks are necessary. This is a concern, especially when we contrast this level of interest with the increase in insider-related breaches (33% of reported breaches are insider related). Only 25% of organizations in Canada do criminal background checks. 10% are planning to implement this practice next year.

Finally, only 13% of respondents plan to formalize security processes into their software development lifecycle (SDLC) - the lowest ranked priority.

Table 19: 2009 initiative rankings

	Not Interested	2009 in place	Doing in next 12 months	Priority Rank
Security awareness programs for customers	43%	13%	29%	1
Requiring suppliers, business partners or other third parties agree to organization’s security policy	35%	25%	29%	1
Creating business-level security metrics	38%	11%	29%	1
Linking general IT staff’s performance evaluations to security objectives	53%	12%	25%	4
Creating a security policy	12%	47%	23%	5
Security awareness program for general employees	21%	35%	22%	6

	Not Interested	2009 in place	Doing in next 12 months	Priority Rank
Security awareness program specific to IT staff	25%	43%	21%	7
Creating a privacy policy	12%	52%	18%	8
Security awareness program specific to developers and architects	44%	31%	15%	9
Mandatory tests after security awareness training	54%	15%	15%	9
Requiring suppliers, business partners or other third parties to agree to organization's privacy policy	38%	27%	14%	11
Security training for third parties (contractors, volunteers, co-op)	56%	13%	13%	12
Integration of security into software/ application development	35%	35%	12%	13
Criminal background checks for all IT and Security staff	40%	25%	10%	14

A comparison of the 2008 and 2009 initiatives reinforce the trend towards a more strategic view of information security and risk management. When we contrasted the 2008 and 2009 priorities we found that organizations are continuously paying more attention to the outside entities that partner with them (suppliers, customers) and managing risks outside of their traditional sphere of influence.

Table 20 below shows a detailed view of the top 10 prioritized security initiatives in 2009 against the same ranking in 2008.

Table 20: Prioritization of security initiatives: Top 10 in 2009 vs. 2008

Security Initiatives	2009 Rank	2008 Rank
Security awareness programs for customers	1	6
Requiring suppliers, business partners or other third parties agree to organization's security policy	1	9
Creating business-level security metrics	1	3
Linking general IT staff's performance evaluations to security objectives	4	1
Creating a security policy	5	7
Security awareness program for general employees	6	2
Security awareness program specific to IT staff	7	-
Creating a privacy policy	8	13
Security awareness program specific to developers and architects	9	5
Mandatory tests after security awareness training	9	10

Half of organizations do not have a dedicated security officer

Subsequent to last year's analysis of the allocation of senior resources to manage information security, compliance, and other elements of risk management, the survey measured Canadian organizations on how they structure their information security functions. As indicated in *Table 21*, the dedicated security function is most commonly found in publicly traded companies, and less so in privately owned companies.

While these numbers are not surprising and similar relative positioning was found in the 2008 study, the 2009 numbers do show some change. These changes can be attributed to a significant raise in the number of responses since the 2008 study, adjustments made in how questions were worded driven from feedback provided in our focus groups and round-table discussions, and more clarity in the available choices for survey answers.

For government and publicly traded organizations the situation has not changed much since last year, however private companies reported a stronger response to the question related to dedicating a security officer to information security (25% in 2008 to 44% in 2009. The private-company reaction may be attributed to the way the question was worded last year ("Do you have a CISO/CSO function?" versus

"Do you have a dedicated Security Officer?"). A number of private companies may have a dedicated security officer without the recognition of a CISO/CSO.

Table 21: Likelihood of having a dedicated security officer by ownership type

	Government	Private	Public
No dedicated Security Officer	44%	56%	32%
Has Dedicated Security Officer	56%	44%	68%

Additionally, with a higher number of respondents in this year's survey, it is possible to analyze a breakdown of the different levels of responsibility and authority that a security officer or similar role would have in the organization. 56% of the respondents reported that their organization did have a dedicated security function. *Table 22* shows the breakdown in each ownership/legal structure. Most organizations have security officers at the manager or director level, except for publicly traded companies who respond with a significant dedicated VP-level presence. This is understandable given that the regulatory pressure for these organizations is perceived as higher, and risk management decisions are closely monitored by internal and external auditors, market analysts and shareholders. For those reasons, it is expected that publicly traded companies would have the best ability, from the senior management sponsorship point of view, to implement a security program or respond to regulatory requirements. This positioning is also highly correlated to the fact the publicly traded companies are highly concerned with compliance issues.

Table 22: Management level of the security head per ownership type

Management Level of Security Head	Government	Private	Public
Vice President level	10%	17%	46%
Director-level	41%	31%	24%
Senior Manager	6%	14%	9%
Manager-level	36%	33%	16%
Team lead	8%	5%	6%

Security function still reporting into IT

Regarding security reporting, most security functions report to the CIO with the second preferred position being the CEO or similar level (across all industry sectors in Canada). This reporting profile, shown in *Table 23* below, is consistent with the one we found in 2008.

Table 23: Area security function reports into per ownership type

	CEO	Finance	HR	IT	Risk Mgmt	Other
Government	18%	4%	1%	65%	2%	10%
Private	30%	6%	0%	44%	8%	11%
Public	29%	12%	3%	49%	0%	7%

This distribution shows that information security is still perceived primarily as an IT issue in Canada, and explains the fact that many organizations attempt to manage security risks by focusing their attention and resources in the deployment of technological controls.

There is also lack of clarity around the actual mandate of the CIO, who in most cases, despite the title, is responsible for the custodianship and risks related with the protection of business information without being the owner of the same information. Organizations that assign the management of security closer to the CEO tend to see the question of security as one of information management, and information being business-related, a business mandate at the highest level.

Interestingly, while the vast majority of organizations assign the security function as an IT-reporting function, IT companies and media groups tend to position security very close to the CEO. This makes sense when one considers that information is their core business, so managing information risks become a matter of competitiveness and survival to these entities.

The mandate of the security function varies by type of organization and Industry

During the focus group discussions and round-table discussions with security officers that took part in the preparation stage of the 2009 survey, several participants articulated specific requirements, assumptions and perceptions that reflected the reality of each specific industry vertical or ownership structure. Security functions in some organizations have a strong mandate in the deployment of technical controls, while other organizations rely on IT to deploy these controls following the policies developed by the security function.

With that perspective in mind we asked respondents about the mandate of the security function on their specific environments. *Table 24* shows a breakdown of the responses per ownership type. Approximately one third of respondents reported that their security function handles Business Continuity and Disaster Recovery Planning. The other two thirds reported that the function is handled by a separate function in the organization such as a dedicated department or a governance body represented by a Steering Committee or Council. Audits and audit response is also handled by one third of survey participants, except for the private sector, which is less affected by external audits and regulations than the public companies or government entities.

The domain of security operations (managing security of networks, applications and other elements of IT infrastructure) is shared between security and IT, with about half of the accountability mandated to the security function. Likewise, the ownership of compliance monitoring and reporting is co-owned by a complex partnership between the security function and several other entities like Internal Audit, Risk Management, Privacy, HR, Finance and others.

Table 24: Mandate of the information security function

	Government	Private	Public
Audit Function	31%	24%	32%
Compliance	41%	34%	47%
Risk Management	35%	31%	39%
IT Security, Network and Applications	61%	43%	55%
Physical Security	17%	19%	25%
Loss Prevention	20%	15%	28%
Safety and Personnel Security	9%	14%	17%
Business Continuity/Disaster Recovery	29%	31%	34%

The composition of these organizational partnerships in Canada varies greatly, and the way individual responsibilities are allocated fundamentally defines the risk culture, appetite, and thresholds in each organization. For example, the highest levels of response for the security function to own Business

Continuity and Disaster Recovery are with sectors related to critical infrastructure and natural resources such as Utilities, Transportation, Agriculture, Mining, and Forestry. Over 50% of those respondents identified that mandate as their own versus the 20% (or less) of all other sectors except other government organizations. As expected, the assignment of fraud and loss prevention to the security function are concentrated within the Retail, Transportation, Natural Resources, Finance, and Government entities, while Finance and Health Care assign the ownership of audits and the protection of electronic records to its security departments.

Regulatory compliance

Regulatory compliance is by far the most relevant driver for security budgets and the implementation of security and risk management programs in Canada. The Canadian landscape is also influenced by the USA regulatory framework, but is still distinct. Canada's approach to privacy is more closely aligned with the Commonwealth countries than to the USA. For example, our PCI-DSS validation requirements and deadlines are handled differently from those in the USA and Europe, and our health care system is governed by very specific requirements for safeguarding health records. *Table 25* below shows the regulatory requirements faced by organizations in each ownership type.

Table 25: Regulatory requirements by ownership type

	Government	Private	Public
Sarbanes Oxley (USA)	5%	11%	40%
Bill 198	13%	13%	35%
Privacy Act	47%	26%	45%
Canadian Bank Act	5%	5%	17%
Personal Information Protection and Electronic Documents Act (PIPEDA)	37%	25%	41%
PCI-DSS	27%	18%	28%
Other Industry Regulations (FFIEC, NERC, FERC, PHIPA, HIPAA)	17%	14%	20%
Breach Notification Laws	10%	10%	10%
Special Information Security Laws	11%	5%	9%
Other	11%	3%	2%
Don't Know	7%	6%	4%

A persistent theme, and also consistent with last year's study, is the Canadian concern with privacy. Both public and private sectors register a high awareness of privacy regulations and their requirements, although this awareness is not always reflected in strong privacy programs or investments in privacy controls. Our analysis indicates that the industry is monitoring the evolution of privacy regulations in Canada. However the mobilization of resources to mitigate privacy risks will require additional enforcement and punitive measures.

With regards to shifts in regulatory concerns from 2008 and 2009 responses, the following points are worth of attention:

- Privacy remained the top compliance area for all respondents in both years.
- Publicly traded companies remained 100% consistent in their priorities since 2008.
- Government organizations and private companies, which are not directly affected by Sarbanes Oxley (SOX) requirements, lowered the relative importance of this regulation in 2009. This is likely caused by an increase in education around different regulatory regimes and better understanding of the compliance requirements that affect them. Still, Bill 198 (the Canadian version of SOX) was registered as relevant for some respondents in government entities and private companies.

- More government organizations and private companies are becoming aware of PCI-DSS in Canada. This industry regulation was perceived more as a public company, retail-based compliance standard in the past. However, the rising number of breaches involving credit cards and the resulting pressures from the card brands in Canada on partnering organizations to meet compliance is driving merchants and service providers across all industries to respond.

Table 26 below shows the ranked relevance of differing regulations to Canadian organizations.

Table 26: Regulatory priorities in 2008 and 2009 by ownership type

	Government		Private		Public	
	2008	**2009**	**2008**	**2009**	**2008**	**2009**
Sarbanes Oxley (USA)	4	8	4	6	3	3
Bill 198	6	5	3	5	4	4
Privacy Act	1	1	1	1	1	1
Canadian Bank Act	8	8	6	8	7	7
Personal Information Protection and Electronic Documents Act (PIPEDA)	2	2	2	2	2	2
PCI-DSS	5	3	5	3	5	5
Other Industry Regulations (FFIEC, NERC, FERC, PHIPA, HIPAA)	3	4	7	4	6	6
Breach Notification Laws	7	7	9	7	8	8
Special Information Security Laws	6	6	8	8	9	9

The awareness of regulatory requirements is not only driven by the privacy laws, and 83% of respondents indicated that their decision-makers have an adequate, good, or very good understanding of the information security requirements for compliance with the regulations and legislation affecting their organizations. This trend is stable and consistent with the 2008 study. A breakdown of ownership type shows the public companies leading with 92% of respondents reporting high levels of understanding and commitment from senior management to compliance.

The uniqueness in the Canadian regulatory framework is sometimes not fully understood by organizations that receive their security strategy and policies from foreign countries. When considering compliance strategies, we inquired if respondents have analyzed their security requirements in detail. We also asked if the preferred approach for remediation was to search for common controls between different regulations (optimizing resources by addressing common elements), or to handle each regulation in isolation. Responses surfaced the following findings:

- Organizations that define their policies locally or without a centralized security function had the lowest levels of planning with 25% disclosing that they have not yet analyzed their security requirements in detail.
- Organizations that receive their security policies and direction from abroad had revised their requirements, but reported that the preferred method of meeting compliance is to handle each requirement in isolation. This is most likely caused by the need from a foreign entity to increase control and approach the problem using a compartmentalized plan.
- Finally, organizations that had a centralized and Canadian security function defining their policies and strategy reported that their approach to meeting compliance requirements was more likely to be centered on finding an optimal point in common controls and mitigating them first.

IT Security Breaches

For security professionals, breaches are very important to understand and quantify. On the one hand, in the aggregate they help to quantify where threats are most prevalent and where the risks are most perceived. On the other hand, in the singular they test an organization's preparedness to prevent, respond to and mitigate risks. Often, breaches and their associated costs and likelihood of occurrence are used to establish a baseline for how much to invest and a benchmark with which to measure security performance and progress.

Our study in 2008 established a Canadian benchmark for breaches. We were able to quantify likelihood, cost and nature of breaches that Canadian organizations experienced. We learned that the annual loss due to breaches was close to $400,000 and that on average organizations reported three breaches per year. We also noted that Canadian organizations were less likely to report several types of breaches than their American counterparts. This was most acute for insider-abuse breaches where Canadian organizations were 1/3 as likely to report them compared to Americans.

The 2009 study allowed us to ask several questions. To begin with, it provided context for our 2008 results. Did our findings from 2008 hold true for 2009 and to what degree? So we looked at year over year trends. 2009, however, was not directly comparable to 2008. Our 2009 survey was administered during a period of significant economic downturn characterized by rising unemployment and high economic uncertainty. So we had to ask ourselves: How are breaches affected in 2009 by all of these underlying economic changes? To that end, we added several questions to our 2009 survey that would allow us to better understand these issues and answer the questions that arose since the analysis of the last study.

Number of breaches per organization has increased significantly in 2009

Table 27: Estimated number of annual breaches

Organization Type	2009	2008
Private Company	11.7	3.1
Publicly Traded Company	9.0	3.0
Government	13.4	3.5

In 2008, we estimated that organizations experienced on the order of 3.0 to 3.5 breaches per year. Publicly traded companies reported the lowest amount of breaches and government the highest, although the difference was only about half a breach. In 2009, respondents reported a significant increase in the number of breaches, ranging from a three-fold increase in breaches at publicly traded companies to an almost four-fold increase in government organizations and privately held companies. The spread between government organizations and publicly traded companies also widened significantly going from .5 breaches to 4.4 breaches.

The significant increase in the number of breaches and the widening spread between government and industry poses some interesting questions. What caused the great increase in breaches and why did it increase much more in government than it did in publicly traded companies?

Annual losses from breaches up significantly in 2009; Government hardest hit

As would be expected from a more than three-fold increase in the number of breaches, annual losses attributable to breaches are up across all types of organizations in 2009. This year, the annual loss per major incident or breach for all companies grew to $834,149 compared to 2008 when it was $423,469, a year over year increase of 97%. While every type of organization suffered an increase in breach costs, the increase was most pronounced in government organizations that more than tripled their average annual cost of breaches. Private companies also demonstrated a significant increase in annual breach costs, increasing to $807,310 up from $293,750. Publicly traded companies hardly showed an increase at all, with average breach costs only increasing by 6% year over year.

Table 28: Annual loss from breaches by organizational type

Organization Type	2009	2008
Private Company	$807,310	$293,750
Publicly Traded Company	$675,132	$637,500
Government	$1,004,799	$321,429

So what caused breach costs to increase in private companies and government organizations but not publically traded organizations? We believe that a primary difference is a focus on compliance. According to our results, compliance has become a much stronger driver for private companies and government organizations in 2009 compared to 2008. For example, in 2009 privately held companies listed complying with Canadian compliance requirements as their greatest security concern, while in 2008 it ranked sixth among their concerns. Similarly complying with USA regulation has moved up 4 spots, ranking 5th among security concerns in 2009.

So how does compliance lead to higher breach costs? According to commentary from our focus groups, compliance initiatives tend to favor detective controls, focusing more on monitoring and earlier detections of anomalous behavior and activity. If a corresponding increase in prevention and response capabilities does not follow this enhanced detection capability, organizations will not offset their greater discovery of breaches that come from a more rigorous and exhaustive approach to monitoring for security issues. In the case of publicly traded companies where compliance programs are mature, the gap between detective and preventative controls is not as great.

Costs of individual breaches down significantly

Although the number of breaches increased as did the annual loss from breaches in 2009, individual breach costs trended in the opposite direction. Across all types of organizations, the estimated cost per breach has gone down year over year, ranging from an 18% drop in government to a 65%reduction in publicly traded organizations. Given the relative similarity between the types of breaches reported by all three types of organizations, the much more significant reduction in per-breach costs for publicly traded companies suggests a greater ability to handle security breaches.

Table 29: Estimated cost per breach

Organization Type	2009	2008
Private Company	$69,103	$94,758
Publicly Traded Company	$75,017	$213,926
Government	$74,985	$92,364

2009 Breaches up significantly in 12 of 17 categories, led by data-related breaches

Table 30: 2009 vs. 2008 trend analysis on reported breaches

Type of Breach	2009	2008	% change
Virus/worms/spyware/malware/spam	70%	62%	13%
Laptop or mobile hardware device theft	53%	34%	56%
Financial fraud	14%	8%	75%
Bots (zombies) within the organization	15%	8%	88%
Phishing/pharming where your organization was fraudulently described as the sender	23%	27%	-15%
Denial of service attack	16%	17%	-6%
Sabotage of data or networks	3%	3%	0%
Unauthorized access to information by employees	36%	17%	112%
Extortion or blackmail (ransomware)	3%	2%	50%
Web-site defacement	6%	4%	50%
Loss of confidential customer/employee data	10%	8%	25%
Abuse of wireless network	15%	11%	36%
Password sniffing	5%	6%	-17%
Misuse of a corporate application	13%	10%	30%
Theft of proprietary information	7%	4%	75%
Identity theft	7%	6%	17%
Exploitation of your domain name server (DNS)	2%	2%	0%

So if the number of breaches reported per year increased substantially, what types of breaches most account for those increases? In 2008 and 2009 respondents were asked to indicate the types of breaches their organization had experienced in the last 12 months. *Table 30* provides those responses and measures the year over year change per breach type. Out of 17 breach categories there was a significant increase in 12 categories, with year over year increases ranging from 13% to 112%.

Perhaps the most interesting increase occurs in the category *unauthorized access to information by employees*. In 2008, we remarked that it was interesting that in this category Canadian organizations reported a much lower percentage of breaches (66% lower) than their American counterparts. This year, unauthorized access to information by employees has more than doubled, from 17% to 36% of organizations reporting this breach type, a 112% relative increase year over year.

The second highest increase year over year involves botnet-related breaches. The number of organizations that reported dealing with botnets has nearly doubled from 8% to 15%. This growing prevalence of botnets is consistent with our threat and vulnerability research at TELUS Security Labs. Over the last 18 months our Labs have observed a growing sophistication in the methods that botnets use to spread, infect, and evade detection. We have also observed that the variants of botnets are increasing rapidly, making detection and removal harder for technology vendors. As a result, the number of bot-infected computers continues to rise at a global level.

The third highest increase can be observed in the financial fraud category, which has increased by 75% relative to last year. In the last 12 months, much has been written about large-scale theft of credit card data in North America. Our data suggests that the less sensational methods of financial fraud are increasing as well. The fraud reported in our spanned public and private sector and ranged from companies having 250 employees to those with over 50,000. Organizations should no longer assume that because they are small and not-well known that they are safe from these types of breaches.

Theft of proprietary information is tied for third place in terms of year over increases with 7% of organizations reporting theft of proprietary information, up from 4%.

It is worth noting that the four top areas of increase in 2009 are related to data in some way. Clearly the nature of breaches continues to trend towards financial gain and less towards mischief and disruption.

This year's results were not all bad news in terms of breaches. Some types did not go up and some even declined. Phishing and pharming related breaches are down by 15%. Denial of service attacks have declined marginally whereas data sabotage and DNS related breaches have remained constant.

Theft of proprietary information highest in publicly traded organizations

Given that breaches are up fairly significantly across most categories, we wanted to know if this was a blanket increase or did some types of organizations fare better or worse than others? We broke up the breach categories by different organizational types to answer that question and observed several interesting differences.

Table 31: 2009 types of breaches by legal entity

Security Breaches	Government	Private	Public
Virus/worms/spyware/malware/spam	74%	61%	73%
Laptop or mobile hardware device theft	50%	51%	59%
Financial fraud	4%	18%	22%
Bots (zombies) within the organization	18%	12%	12%
Phishing/pharming where your organization was fraudulently described as the sender	25%	14%	28%
Denial of service attack	12%	16%	20%
Sabotage of data or networks	3%	2%	3%
Unauthorized access to information by employees	33%	39%	36%
Extortion or blackmail (ransomware)	0%	6%	3%
Web-site defacement	8%	4%	6%
Loss of confidential customer/employee data	13%	8%	8%
Abuse of wireless network	11%	22%	14%
Password sniffing	4%	8%	5%
Misuse of a corporate application	11%	12%	16%
Theft of proprietary information	1%	4%	16%
Identity theft	3%	4%	14%
Exploitation of your domain name server (DNS)	1%	0%	5%

For example:

- 60% of publicly traded companies reported a breach related to mobile or hardware theft while only 50% of government or privately held companies reported the same.
- Wireless breaches were most prevalent in privately held companies at 22% of respondents, when compared to twice that of government (11%) and about 50% more prevalent when compared to publicly traded companies (14%).
- 16% of publicly traded companies reported theft of proprietary information, which is 4 times higher than privately held companies (4%) and 16 times higher than government (1%).
- Theft of identity information is reported most in publicly traded companies at 14%, which is over 3 times more frequent than in government and private industry.

In 2009 Canadians reporting as many Breaches as American counterparts; insider breaches gap has narrowed

In 2008, when compared to their American counterparts from the 2007 CSI survey, Canadian respondents on the whole indicated they had experienced less breaches (Table 32). For 2009, we compared the Rotman-TELUS 2009 findings with the most recent CSI survey from late 2008, and found that in several categories Canadian organizations are just as likely, and in some cases more likely, to report breaches as their American counterparts.

Two categories that are worth noting are those of virus/malware and abuse by employees/insiders. In the case of virus/malware, Canadians are 40% more likely to report a breach related to viruses and malware than their American counterparts, a significant increase over 2008. In the abuse by employees and insiders breach category we see the gap between Canada and the USA narrowing to an 8% difference at 36% and 44% respectively, compared to our 2008 survey when the gap was 42%.

Table 32: Comparison of security breaches in Canada and in the USA

Breach Type	RT 2009 (CAN)	2008 CSI (USA)
Denial of service	16%	21%
Financial fraud	14%	12%
Web-site defacement	6%	6%
Theft of IP	7%	9%
Sabotage	3%	2%
Virus / malware	70%	50%
Abuse by employees / insiders	36%	44%
Abuse of wireless networks	15%	14%
Misuse of application	13%	11%
Bots	15%	20%
Password Sniffing	5%	9%

30% of breaches are by insiders, with Government organizations having a slightly higher percentage

Based on last year's finding that insider breaches were lower in Canada, we wanted to find out this year if they were lower across the board or if some types of organizations experienced a greater amount of insider breaches. So we asked respondents what percent of breaches they had observed had come from insiders. As can be seen in Table 33 below, insider breaches are fairly similar across the types of organizations with government organizations leading private industry by about 10%. Also of interest is that in the two highest-ranking categories, *61-80%* and *81-100%*, government organizations are in the lead, suggesting that in 28% of government respondents insider breaches are not the exception but the norm.

Table 33: Percentage of insider breaches by legal entity type

% of Breaches from Insiders	Government	Private	Public
6% to 10%	10%	3%	7%
11% to 20%	6%	14%	5%
21% to 40%	13%	17%	12%
41% to 60%	10%	9%	22%
61% to 80%	13%	11%	2%

% of Breaches from Insiders	Government	Private	Public
81% to 100%	15%	9%	12%
None	17%	23%	17%
Up to 5%	17%	14%	22%
Weighted average	33%	28%	29%

Organizations with high numbers of remote workers report lower breaches

Table 34: Breaches by amount of staff working remotely

% of Staff working remotely	% reporting Virus / Worm Breaches
0-25%	69%
26-50%	65%
50% +	52%

Another question we asked ourselves was what drove a greater prevalence in breaches from viruses and malware in 2009. One thought was that perhaps a movement towards telecommuting may have affected the breach statistics. So we compared the breaches, the percentage of an organization's staff working remotely, and our results to determine if a relationship existed. What we found was quite the opposite of what was expected. As the percentage of remote workers increased, the prevalence of virus/malware breaches decreased.

Given the counter-intuitive nature of the finding we decided to dig a little deeper. In enumerating the possible factors that could account for the lower amount of breaches, we decided to look at security-awareness training. We hypothesized that perhaps in anticipation of the greater loss of control, organizations with higher levels of remote workers might invest more time in security awareness training. So we looked at the prevalence of security awareness programs by percentage of staff working remotely.

Table 35: Security awareness training by percentage of staff working remotely

% of Staff working remotely	Security Awareness program for Staff
0%, 1-5%, 6-10%, 11-15%, 16-25%	53.42%
26-50%	66.67%
50% +	61.54%

As can be seen in Table 35 above, organizations with more than a quarter of their personnel working from home are 20% more likely to have a security awareness program for their employees. We believe that it is likely that organizations with large remote workforces focus more on security awareness training, resulting in a lower incidence of virus/malware related breaches. There is some doubt in the security community about the effectiveness of security awareness programs. This result provides evidence that security awareness programs can have a positive impact.

Lack of incident response preparedness points to under-estimation of and under-response to breaches

Table 36: Annual cost of breaches by incident response preparedness

Incident Response Process Testing	Annual Cost of Breaches
Yes	$773,535
No	$412,912

Given the unexpected relationship between remote workers and breaches, we decided to look for other possible relationships that could affect breaches. Given that we had asked questions about whether organizations had an incident process and how frequently they tested, we decided to look at the annual cost of breaches for those who tested versus those who did not. And yet again, the result was counterintuitive at first glance. From Table 36 above we can see that those organizations who have an incident response process and test it frequently report a higher annual cost of breaches. We believe the explanation for this result is that the greater the focus on incident response process the more formal the response, increasing both the activity related to handling breaches and the ability to accurately estimate the complete cost of a breach. So in summary, doing it right takes longer, leads to deeper analysis, and more formal remediation which leads to higher costs.

Outsourcing security does not increase Insider breaches

Table 37: Percentage of insider breaches by outsourcing practices

Outsourcing part of Security	% of Insider Breaches
Yes	31%
No	35%

One final question the team posed regarding breaches related to outsourcing and whether or not outsourcing security results in a greater amount of insider breaches. This question arose during one of our focus groups. One participant was concerned that outsourcing security could result in a greater focus on outsider threats. As can be seen in Table 37 above, organizations that outsource some element of their security report that a smaller percentage of breaches are caused by insiders. One interpretation of this result could be that outsourcers do in fact focus on external threat more and hence under-report insider related breaches, but that would be inconsistent with the compliance-driven focus on data and user-accountability reported by study participants in 2008 and 2009. For that reason, we believe the above table strongly suggests that the likelihood of insider breaches does not increase when outsourcing parts of security.

Compliance leaps to forefront as top issue for privately held companies

To better understand the lens through which breaches and technology investments were perceived, we asked respondents to make two key lists:

- Rank their concern for 10 current security issues.
- Rank potential breach impacts.

We then took these rankings and broke them down by organizational type and compared them to last year's rankings, looking for changes in priority.

Privately held companies now list compliance with Canadian regulations and legislation as their most important concern in 2009, up from 2008 when they ranked it sixth. This was perhaps the most interesting and surprising change in the rankings that we observed. A common view among security practitioners was that compliance was strongly associated with the stronger audit requirements of publicly traded organizations.

In looking for a better explanation, we reviewed our focus group commentary and looked at the responses to other compliance questions. We believe this shift can be explained, at least partially, by two factors. First, the data pointed to an increasing adoption of the Payment Card Industry Data Security Standard (PCI) across several industries and organizational types. Organizations seem to be realizing that PCI is not a retail standard but rather a standard aimed at any organization that processes credit cards. The second contributing factor is that organizations held to high compliance requirements are passing on those requirements to third parties contractually. This comment was frequent in our panel discussions.

Table 38: Ranking of security issues of concern by organization type for 2008 and 2009

	2009			2008		
Security Issues	**Government**	**Private**	**Public**	**Government**	**Private**	**Public**
Managing risks from third-parties, i.e. business partners, suppliers and collaborators	8	9	8	4	8	5
Managing security of wireless and mobile devices	4	6	9	1	5	9
Disclosure / loss of confidential customer data	1	2	1	2	1	1
Compliance with Canadian regulations and legislation	3	1	3	3	6	2
Compliance with USA or other foreign regulations and legislation	10	5	5	9	9	5
Accountability of user actions and access	7	8	7	8	4	7
Employees understanding and complying with security policies	5	7	6	6	7	7
Business continuity / disaster recovery	2	4	4	5	2	3
Loss of strategic corporate information	6	3	2	6	3	4
Managing data in the cloud (cloud computing)	9	10	10	n/a	n/a	n/a

Although slightly less surprising, but equally important, the issue of greatest concern to 2009 respondents was the disclosure or loss of confidential customer data. This was also true in 2008, although there are some minor changes. It is now the top issue for government organizations while it was the second most important issue in 2008. Conversely, it is now the second most important issue for privately held companies, while it was the first most important issue in 2009.

Another interesting change in priorities relates to Business Continuity and Disaster Recovery Planning. In 2008 it was ranked as fifth in terms of priorities. It is now the second most important issue for government respondents. This is likely driven by the H1N1 outbreak and the pandemic planning discussions that were prevalent in the first half of 2009. In the private sector, concern with BCP and DRP has fallen slightly compared to 2008, but is still considered important ranking as fourth.

Managing risks from third-parties is a concern that has fallen in ranking across the board: down by 3 spots in publicly traded companies and by 4 spots in government. At first glance this could seem that organizations are saying that they don't believe that third parties represent risk, but we interpret this differently. We believe that this lowered concern is accounted for by the notion that organizations are becoming better at holding their partners accountable. Essentially, organizations are opting out of managing the third-party risk and opting to transfer the risk to the third parties via stronger legal and contractual agreements that better outline security policies and obligations.

Damage to brand remains chief breach concern

Given the significant changes in the amount and nature of breaches in 2009 and in the economic climate, we wanted to understand how the impact of breaches might have changed. To that end we broke down the 2008 and 2009 respondents by organization type and compared them year over year.

In doing so, we found that concerns remained fairly consistent year over year, with a few interesting exceptions.

According to Table 39 below, *Damage to Brand* remains the chief breach concern in 2009 for publicly traded companies and government. According to the underlying data, the gap between the top concern and those that rank second is much stronger this year than in 2008. We believe that the uncertainty of the economy has heightened awareness of the effects that a high-profile breach can have on organizations. This is reinforced by respondents from publicly traded companies which rank *Loss of Market Valuation* as their second highest breach impact concern, up two spots from 2008.

Another interesting change from last year is that private companies now rank *Lost Time due to Disruption* as their key concern, compared to 2008 when the chief concern was lost customers. We believe this reflects a heightened concern with operational efficiency in 2009 resulting in private organizations having to do more with less. For security this resource tension is corroborated by the increase in annual breaches and the slight decrease in staffing and budgets reported for 2009.

Litigation is falling as a key concern, dropping to fifth in ranking of concern 2009, down from fourth in 2008. This is accounted for mostly by the drop in priority in government respondents. While in 2008 it was their second most important breach concern, in 2009 it falls to fourth. We believe that this drop is reflective of a more mature understanding of the legal implications of a breach in Canada and not a lessening concern with legal obligations.

Table 39: Breach impact concerns, 2009 vs. 2008

Breach Impacts Concerns	2009 Priority Rankings				2008 Priority Rankings			
	All	Government	Private	Public	All	Government	Private	Public
Damage to brand reputation or image	1	1	2	1	1	1	2	1
Lost time due to disruption	2	2	1	5	3	4	3	5
Personal accountability	7	5	8	8	-	-	-	-
Litigation	5	4	5	7	4	2	5	6
Regulatory action	4	3	6	4	5	3	6	3
Lost customers	3	8	3	3	2	6	1	2
Cost of new equipment / services required	8	7	7	9	8	7	7	8
Cost to compensate customers / damaged parties	6	6	4	6	6	5	4	7
Loss of market valuation (share price)	9	9	9	2	7	8	8	4

Security Technologies

Security technologies are perhaps the most important element of an organizations toolkit for fighting security breaches. They are the enforcement of good process and policy. Yet not every technology is adopted by organizations. Some technologies are more prevalent than others.

In 2008 we wanted to better understand the technologies organizations have in their arsenal, which is why we focused on more than technology adoption rates. We also asked respondents about their satisfaction with the technologies they had in place in order to discern possible barriers to broader adoption. Finally, we compared the 2008 results with the results from a compatible USA survey to give our results a benchmark of sorts. And here is what we found:

- Canadian technology adoption was on par with the USA across several technologies
- Technologies that focused on detection without an automated response had much lower satisfaction levels due to a pressure cooker effect
- Compliance, an unexpected strong driver in Canada, resulted in the adoption of several technologies

In 2009, we evolved our 2008 survey. We realized that respondents attached several shades of meaning to the word deploy when asked: what technology do you plan to deploy in the next 12 months? Did deploy mean evaluate, pilot, a limited deployment or perhaps organization-wide? So, for 2009 we decided we would provide more precise options and a better definition for what we meant by the terms “deploy” and “in place”. We also expanded our categories to better mirror how the industry classifies technologies. For example, we split the log management category into log management and SIEM.

These changes provided extra clarity and avenues of analysis, yet also complicated our ability to compare 2009 to 2008. Our 2009 results are slightly lower than 2008 across most technologies. This begged the question: could technology deployments contract within just 12 months? While we attribute some of decrease to the new choices and precision in terminology, we believe some of the drop can be attributed to lower satisfactions in 2008 leading to some abandonment in 2009.

How has security technology usage changed in 2009?

Given the changes in breaches observed in this year’s study, did organizations respond by changing their technology profile? Equally important, were these changes observed across industry types? To answer these questions, we broke up the technology adoption rates by legal entity and compared to the 2008 adoption rates and cross-referenced the different adoption levels with major changes in satisfaction.

Table 40: Security Technology utilization by Legal Entity for 2009

Technology	Public	Private	Gov	2008 Results
IPSEC based VPN	85%	80%	82%	90%
SSL VPN	84%	79%	84%	
Anti-Virus	98%	100%	100%	100%
Email Security (anti-spam, anti-malware)	100%	100%	100%	99%
Public Key Infrastructure	67%	69%	59%	73%

Technology	Public	Private	Gov	2008 Results
Storage / Hard Disk Encryption	75%	56%	61%	82%
Email Encryption	58%	48%	49%	73%
Database Encryption	57%	53%	49%	65%
URL / Content Filtering	92%	84%	87%	85%
Identity and Access Management	77%	67%	74%	86%
Network based Access Control (NAC via network)	45%	52%	55%	82%
Endpoint Security (NAC via desktop)	43%	45%	52%	
Firewalls	100%	98%	97%	100%
Web Application Firewalls	67%	58%	61%	-
Log Management	77%	78%	71%	92%
Security Information & Event management (SIEM)	68%	56%	55%	
Network Intrusion Prevention / Detection	80%	73%	77%	92%
Wireless Intrusion prevention (WIPS)	49%	52%	40%	87%
Application Security Assessment Tools (web/code)	56%	64%	48%	72%
Two-factor authentication (tokens, smartcards)	77%	63%	55%	59%
Vulnerability Scanning / Vulnerability management	84%	69%	72%	75%
Patch Management	90%	89%	100%	82%
Data Leakage Prevention	43%	46%	55%	72%

Overall we found that technologies that have lower adoption rates in 2009 compared to 2008 have one key characteristic in common: low satisfaction. As a result they seem to be less integrated in the environment and are likely still in evaluation or pilot modes. These technologies include Storage/Hard Disk Encryption, Email Encryption, PKI, Log Management and Data Leakage Prevention. Still some technologies did make year over year progress, and within that group we found some common themes.

Encryption a key focus of publicly traded organizations

In 2008, respondents indicated that encryption was a key focus of their technology focus in 2009. This year we see that publicly traded companies lead or are close to leading in deployments of Encryption technologies. For example, 75% of publicly traded organizations are utilizing hard disk encryption compared to only 61% in government and only 56% in privately held companies. Similarly publicly traded organizations lead adoption in database encryption and email encryption. Along with privately held organizations, publicly traded companies are more likely to utilize PKI, a key building block for many encryption technologies.

Patch management leading vulnerability management in deployments

Patch Management utilization is up by 11% in 2009, led by government organizations. Interestingly, publicly traded organizations report less usage of patch management and greater usage of vulnerability management. Since both technologies aid in managing the security of systems, we feel that publicly traded organizations prefer to use vulnerability management technologies as they allow organizations to take preventative or corrective measures in anticipation of a patch, lessening the time an organization is exposed and reducing the likelihood of compromise.

Vulnerability scanning and management is also up in 2009, slightly less than patch management. Quite opposite to patch management, Vulnerability management is less used in government and privately held organizations and up most in publicly traded companies.

Preventing application breaches preferred over detecting application flaws

This year, we added Web application firewalls (WAF) to our survey of technologies. Overall about two thirds of respondents use WAFs with publicly traded companies indicating the high usage and government organizations the lowest. In 2008, we noted that government organizations were not investing enough to protect applications and in 2009, government continues to lag in terms of technologies that secure applications. Government organizations are least likely to employ application testing tools, two-factor authentication, and WAFs. Governments also seem to be more focused on compensating for security deficiencies as opposed to fixing security flaws. This is indicated by the gap between WAF usage (61%) and application security tool usage (48%).

Detective technologies see sharp decline, satisfaction tells the story

Given the surge in insider breaches, we expected technologies aimed at detecting and preventing internal abuse to be more common in 2009. Not so, in some cases the use of these technologies decreased while others gained marginally. To better understand what could cause this discrepancy, we looked at the satisfaction levels year over year and compared them. Given the effect that the increase in breaches would have on satisfaction we opted to compared relative rankings, to determine how relative satisfaction levels had changed. Doing so yielded some interesting insights.

Table 41: Technology Satisfaction Ratings & Rankings, 2009 vs. 2008

Technology	2009 Rank	2008 Rank	YoY Change
Email Security (anti-spam, anti-malware)	1	5	+4
Anti-Virus	1	6	+5
Firewalls	3	1	-2
Public Key Infrastructure	4	14	+10
SSL VPN	5	1	-4
IPSEC based VPN	6	1	-5
Storage / Hard Disk Encryption	7	17	+10
Two-factor authentication (tokens, smartcards)	8	6	-2
Email Encryption	9	19	+10
URL / Content Filtering	10	13	+3
Identity and Access Management	11	22	+11
Web Application Firewalls	12	n/a	n/a
Endpoint Security (NAC via desktop)	13	6	-7
Patch Management	14	12	-2
Database Encryption	15	18	+3
Vulnerability Scanning / Vulnerability management	15	19	+4
Network Intrusion Prevention / Detection	17	10	-7
Network based Access Control (NAC via network)	18	6	-12
Wireless Intrusion prevention (WIPS)	19	11	-8

Technology	2009 Rank	2008 Rank	YoY Change
Security Information & Event management (SIEM)	20	14	-6
Application Security Assessment Tools (web/code)	21	23	+2
Log Management	22	14	-8
Data Leakage Prevention	23	19	-4

As can be seen in *Table 41*, several detective technologies have low satisfaction levels in common. Upon seeing this pattern we were curious as to why detecting more breaches would make security practitioners less content. We found a satisfactory explanation in our focus group notes. According to a few participants, technologies which automate detection but not response can overburden security teams. This statement, coupled with pressure in 2009 to minimize or reduce staffing levels left organizations struggling with the management of detective technologies. These technologies include:

- Data leakage prevention (ranked 23rd in satisfaction)
- Log management (ranked 22nd in satisfaction)
- Security information and event management (ranked 20th in satisfaction)
- Wireless intrusion prevention (ranked 19th in satisfaction)
- Network based access control (ranked 18th in satisfaction)

Identity & encryption technologies show highest Increase in satisfaction

Not all technologies dropped in satisfaction levels, however. Several technologies showed a big gain in satisfaction this year compared to 2008. In 2008 we speculated that low satisfactions were a result of a technology's inability to deliver on the promised value or perhaps end-user struggles with technology complexity.

- Identity and Access Management (up 11 rankings)
- Storage / hard disk encryption (up 10 rankings)
- Email encryption (up 10 rankings)
- Public Key Encryption (up 10 rankings)
- Ant-virus (up 5 rankings)

Identity and Access Management satisfaction levels are up significantly, most likely an indication that organizations are starting to see value from Identity Management both in terms of operational efficiencies and in terms of sustaining compliance.

Encryption technologies as a group have improved significantly in their satisfaction rankings. The increase in usage noted earlier on is likely related to technology improvements which make deployment and management easier for organizations, which also results in greater satisfaction. Additionally, we feel that compliance initiatives are creating a stronger more defined mandate for encryption making it easier to define and measure success, again leading to higher satisfaction levels.

Finally, we noted a decent increase in satisfaction in Anti-Virus, increasing 5 rankings to the number 1 spot. Although, we don't believe organizations have struggled to deploy and operationalize Anti-Virus software, we believe that organization did struggle with the effectiveness of their investment in containing the many different types of malware attacks. We believe that this year's increase is reflective of the greater capabilities being included in Anti-Virus clients, which provide greater control, flexibility and security to organizations and provide a broader set of protections against malware.

Technology priorities have shifted in 2009

So we looked at differences in technologies across organizational types and we reviewed how satisfaction level ranking have changed. The final question we asked is how have priorities changed in terms of deployment plans year over year and why. Again, given that 2009 was a challenging year, we focused less on the absolute values of deployments and more on comparing the relative ranking of deployment plans from year over year. In that analysis we found that indeed several technologies experienced shifts in priority, and that these technologies formed two main clusters. Those that increased significantly and were focused on strengthening applications and those that decreased and that were focused on detecting potential breaches.

Malware and threats driving changes in priorities

As can be seen in the list below extracted from *Table 42*, technologies that experienced the greatest increase in terms of adoption plans are focused on strengthening their applications and people against automatic and targeted breaches. For example, patch management and vulnerability management are about reducing the exposure of organizations to known network, operating system and application vulnerabilities. Content filtering is increasingly used to filter out malware attacks that result from internet usage and both two-factor authentication and web application firewalls are being used by organizations to reduce the likelihood that targeted and brute force attacks will succeed against applications.

- Patch Management (+8 rankings)
- URL / Content Filtering (+ 6 rankings)
- Vulnerability Management (+7 rankings)
- Two factor auth (+ 10 rankings)
- Web Application firewalls (+ 8 rankings)

Table 42: Technology Adoption Rankings, 2009 vs. 2008

Technology Adoption			
Technology	**2009 Rank**	**2008 Rank**	**YoY Rank**
Email Security (anti-spam, anti-malware)	1	3	+2
Anti-Virus	2	1	-1
Firewalls	3	1	-2
Patch Management	4	12	+8
URL / Content Filtering	5	11	+6
IPSEC based VPN	6	7	+1
SSL VPN	7	7	0
Network Intrusion Prevention / Detection	8	4	-4

Log Management	9	4	-5
Identity and Access Management	9	10	+1
Vulnerability Scanning / Vulnerability management	9	16	+7
Storage / Hard Disk Encryption	12	12	0
Two-factor authentication (tokens, smartcards)	12	22	+10
Public Key Infrastructure	14	17	+3
Web Application Firewalls	15	23	+8
Security Information & Event management (SIEM)	16	4	-12
Database Encryption	17	21	+4
Application Security Assessment Tools (web/code)	18	19	+1
Endpoint Security (NAC via desktop)	19	12	-7
Email Encryption	19	17	-2
Data Leakage Prevention	21	19	-2
Network based Access Control (NAC via network)	22	12	-10
Wireless Intrusion prevention (WIPS)	23	9	-14

Detective technologies dropping in focus in 2009

Organizations are strongly dissatisfied with detective technologies. This was true in 2008 and 2009 and, as a result, priorities for the next 12 months reflect this. Technologies like SIEM and Wireless IPS which can detect possible security breaches are still considered “noisy” and subject to false alarms. At the very least they require incremental staffing to respond to their outputs, something in short supply for 2009. In the case of network admission control (NAC), concerns about complexity and the need for manual remediation have caused organizations to rethink about the role NAC should play in their security strategy.

- Security Information & Event Management (down 12 rankings)
- Network Admission Control via Desktop (down 7 rankings)
- Network Admission Control via Network (down 10 rankings)
- Wireless Intrusion Prevention Systems (down 23 rankings)

What goes down must come up

When looking at the rankings, some findings were very contrary to our expectations. Specifically, we were surprised by the findings involving Data Leakage Prevention (DLP) and Network Intrusion Prevention Systems (NIPS). Given the increase in breaches overall and specifically those involving insiders, we expected the deployment of these technologies to at least maintain their rankings if not increase significantly. This is what we found:

- DLP is ranked 21st and dropped 2 spots year over year, while those reporting insider related breaches went doubles
- Network IPS went from 4 to 8 given the increase in breaches.

In the case of DLP, we believe that Canadian organizations do not fully subscribe to the idea that breaches from insiders are common and prevalent. Secondly we believe that DLP products are perceived as requiring greater staffing levels to respond to alerts.

Regarding the drop in NIPS, we were perplexed. NIPS as a technology, evolved from IDS which was focused solely on detection. NIPS are deployed as inline technologies that automatically block attacks. We recognized that some organizations still implement or own IDS or have IPS sensors operating in detection only mode. Those organizations would likely be less satisfied and less willing to put NIPS inline. Since we surveyed on the use of NIPS / NIDS the drop in satisfaction and intent might be understood as dissatisfaction with IDS overshadowing the satisfaction with IPS.

Outsourcing

IT outsourcing is a common practice in Canadian organizations. In 2008 we asked a series of questions to determine just how prevalent security outsourcing was. We found that outsourcing of some basic security functions was fairly common, although complete outsourcing was rare. The 2008 study also revealed that organizations that outsourced were more satisfied with their overall satisfaction with IT security.

The previous study However did not provide as much clarity on the details of outsourcing such as what technologies were being outsourced and to what extent. This year our analysis focused on four key themes:

- Understanding the details of what technologies and processes were being outsourced
- Understanding how the 2008 results drove behaviours and performance in 2009
- Understanding the impact of the financial crisis to outsourcing
- Understanding the role cloud-based services would play in security strategies

Privacy and the financial crisis drive security outsourcing

When considering policies towards outsourcing of security functions, there was an increase in willingness to outsource relative to 2008, with fewer organizations reporting a policy against outsourcing. Overall, 63% of respondents (up from 60% in 2008) are willing to undertake some form of security outsourcing.

Table 43: Security outsourcing policy

Does your organization have a policy regarding outsourcing of information security services to a third party?	2008	2009
We do not allow outsourcing of IT security	40%	38%
We only outsource to Canadian companies	17%	24%
We allow outsourcing of security to other countries where we do business	12%	6%
We outsource to the best value provider; location is not a major factor in our decision	18%	22%
We only allow outsourcing to countries with laws and regulations that are as stringent as those in Canada	13%	12%

Within the group willing to outsource, there has been a noticeable policy shift towards outsourcing only to Canadian companies and a shift away from outsourcing to companies in countries with compatible laws and regulations. This shift was led by government entities. This movement suggests a greater awareness or concern on the part of respondents to having data or core capabilities outside Canadian control, reinforcing the continuing concerns with legislation like the USA PATRIOT Act (see *A Note on the PATRIOT Act* below).

At the same time, a shift towards location not being a major factor also appeared (away from only allowing outsourcing to other countries where business activities are performed). While contradicting the move towards Canadian on-shoring, the movement is being led by publicly traded companies. The willingness of public companies to outsource to the best-value provider is likely due to shareholder desire for increased return through greater efficiency in difficult financial times. Publicly traded companies led the budget reductions (see *The 2009 Financial Crisis*).

Table 44: Security outsourcing policy by legal entity

Does your organization have a policy regarding outsourcing of information security services to a third party? (By legal entity type)	Government	Private	Public
We do not allow outsourcing of IT security	41%	41%	31%
We only outsource to Canadian companies	38%	14%	15%
We allow outsourcing of security to other countries where we do business	3%	5%	10%
We outsource to the best value provider; location is not a major factor in our decision	14%	23%	30%
We only allow outsourcing to countries with laws and regulations that are as stringent as those in Canada	4%	18%	16%

Government departments are most stringent in terms of outsourcing only to Canadian companies. 38% of those Canadian government departments that responded will only allow outsourcing to Canadian companies, whereas this is only the case for 15% of publicly traded companies and 16% of private companies.

Satisfaction with outsourcing Is driving deeper reliance on outsourcers

Overall allocation of budget for security outsourcing has remained relatively stable with respect to last year. However, those who do outsource are doing more of it. We observed an upwards shift in budget allocation with a movement from 20-40% range up to the 41% and beyond. This suggests that those who do outsource security are more comfortable with the concept of ceding control, are obtaining acceptable performance and as such as willing to transfer more of their security functions to external providers.

While the shift lines up well with the policy changes observed (likely due to economic pressures) there is a discrepancy between those willing to outsource and those that actually allocate budget. While policy is a key determinant in willingness to outsource, clearly cost and suitability for outsourcing also factor in and may be more important than policy.

Table 45: Share of security budget allocated to outsourcing

What share of your organization's information security budget is spent on outsourced security services? (of those answering other than don't know)	2008	2009
None	44%	44%
Up to 20%	41%	40%
21% to 40%	11%	5%
41% to 60%	2%	4%
61% to 80%	2%	2%
More than 80%	1%	4%

On a per sector basis, publicly traded organizations tended to be the most willing to outsource but as with the other organizational types, most outsourcing is constrained to 20% of the budget. Further analysis revealed no specific differentiators for those organizations willing to outsource the majority of their security (80% or more) although government appeared to be the most willing. In almost all companies that reported outsourcing 80% or more of their security, one or more employees still remained dedicated to security suggesting that even the most aggressive outsourcers recognized that outsourcing does not obviate responsibility.

Table 46: Share of Security budget allocated to outsourcing by legal entity type

What share of your organization's information security budget is spent on outsourced security services? (of those answering other than don't know)	Government	Private	Public
None	45%	35%	28%
Up to 20%	43%	42%	54%
21% to 40%	2%	6%	10%
41% to 60%	4%	10%	3%
61% to 80%	0%	3%	0%
More than 80%	6%	3%	5%

Global financial crisis impacted outsourcing

The world economy is in a significant economic downturn and the strategy literature predicts that companies should increasingly focus on core competencies when faced with such challenges. In other words, companies should increase the extent of outsourcing of activities that are not part of their core competencies.

66% of respondents indicated that outsourcing was not impacted as a result of the crisis, with government respondents reporting the highest at 79% and publicly traded companies the least at 63%. The primary motivation that drove the increases in outsourcing was to reduce headcount, most pronounced in publicly traded companies but not in the government.

While apparently contradicting the upwards shift in budgets, there was some reduction in outsourcing, mostly by those organizations that only allocated a minority portion of their budget to outsourcing. Overall government outsourcing strategies were least affected by the Global Financial Crisis

Table 47: Changes in outsourcing budget by legal entity type

If the level of your outsourcing was affected by the 2009 global financial crisis, please choose the main reason.	All	Government	Private	Public
No, outsourcing was not impacted in our organization	67%	79%	57%	63%
Yes, we were asked to reduce our outsourcing relationships significantly	13%	16%	13%	10%
Yes, our outsourcing relationships were impacted but not significantly	13%	5%	23%	15%
We increased our outsourcing relationships to reduce headcount	5%	0%	7%	10%
We increased our outsourcing relationships to reduce operating expenses	1%	0%	0%	3%
We increased our outsourcing relationships to reduce our capital expenditures	0%	0%	0%	0%

Testing and perimeter security leads outsourcing

Across all sectors, respondents were most willing to outsource testing and perimeter security. These two are good candidates given the expertise required for testing while managing firewalls and IPS technologies is a well-defined activity that can be outsourced with little to no impact on business activities or the internal network.

Table 48: Security outsourcing choices by legal entity type

	All	Government	Private	Public
Security testing of networks and infrastructure	42%	44%	35%	45%
Testing of software and applications (including web)	20%	28%	35%	27%
Management of firewalls	25%	17%	28%	32%
Other	23%	15%	28%	31%
Management of network intrusion prevention systems	22%	17%	29%	24%

	All	Government	Private	Public
Management of local area networks	22%	19%	20%	27%
Management of virtual private networks	21%	15%	22%	27%
Management of servers / applications (in datacenter)	21%	13%	21%	31%
Management of web application firewalls	20%	11%	29%	24%
Management of servers / applications (on premise)	18%	15%	20%	21%
Backups	18%	13%	20%	23%
Management of desktops	18%	15%	19%	20%
Collection of security logs (log mgmt)	17%	11%	24%	20%
Monitoring of security events (SIEM)	14%	8%	24%	16%
Security program development / management	14%	13%	18%	11%

Of note were private sector respondents who outsourced less of their application testing but more of perimeter security, aligning well with the software security practices noted earlier. The private sectors increased use of outsourcing perimeter security management (firewalls and IPS), aligned well with the notion that smaller organizations may not have the full complement of skills required to deliver perimeter security capabilities.

Security in the cloud

An emerging trend in IT is the use of cloud or utility-based computing to provide services and infrastructure to the business. For the purposes of this study we treated cloud computing as a specialized case of outsourcing. In this case, as with traditional outsourcing, different layers of the technology stack are managed and externally hosted, with the only fundamental differences being the on-demand acquisition of services, a differentiated pricing model, and less visibility into risk exposure.

The 2009 survey evaluated the Canadian organizations willingness to make use of security services located off-premises. The key defining attribute of cloud-based security services versus traditional outsourced services are:

- On-demand access.
- A commoditized and standardized solution (little to no customization on a per customer basis).
- Limited or no ability to perform third party audits of the service providers.

If an organization is considering leveraging cloud based solutions to deliver IT services, and is especially exploring using security services, then it is informative to understand the key obstacles to adoption in Canada.

Concerns about security services in the cloud

The leading concerns are the location of the data, followed by lack of control, and then the technical challenges associated with security in multi-tenant environments. The lowest ranked concerns availability (suggesting that the benefits of cloud based services are well accepted).

This ranking suggests that governance is a greater concern than the technological approach of cloud computing. However, while the security of multi-tenant environments is not the highest ranked concern, it is important (to some degree) to over 50% of the respondents.

Table 49: Concern with security services in the cloud in ranked order

Concern	Ranking
We are concerned about the location of our data	1
We are concerned with the level of security in a multi-tenant environment	3
We are concerned with the ability to remove/recover our data from the cloud	5
We are concerned that our availability needs cannot be met with a cloud-based service	7
We are concerned about our ability to audit the environment for compliance with our security needs	4
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	6
We are concerned about connecting business critical systems to security mechanisms outside our full control	2

For government entities, the number one concern was the location of the systems providing the service which reflects their concerns with legislative requirements around privacy as well as issues of using extra-territorial service providers. This supports findings from the 2008 survey, that a significant portion of the public sector (47%) had concerns around the USA PATRIOT Act.

Table 50: Concern with security services in the cloud in ranked order (government organizations)

Concern	Ranking
We are concerned about the location of our data	1
We are concerned about connecting business critical systems to security mechanisms outside our full control	2
We are concerned about our ability to audit the environment for compliance with our security needs	3
We are concerned with the level of security in a multi-tenant environment	4
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	5
We are concerned with the ability to remove/recover our data from the cloud	6
We are concerned that our availability needs cannot be met with a cloud-based service	7

Publicly traded companies were more concerned about systems outside of their full control as were privately held companies. The second-most important concern of publicly traded companies was data location whereas private companies had reservations about the security of multi-tenant environments. Again this reinforces the findings from the 2008 survey on the impact of the USA PATRIOT Act on outsourcing decisions.

Table 51: Concern with security services in the cloud in ranked order (publicly held companies)

Concern	Ranking
We are concerned about connecting business critical systems to security mechanisms outside our full control	1
We are concerned about the location of our data	2
We are concerned with the level of security in a multi-tenant environment	3
We are concerned with the ability to remove/recover our data from the cloud	4
We are concerned that our availability needs cannot be met with a cloud-based service	5
We are concerned about our ability to audit the environment for compliance with our security needs	6
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	7

Table 52: Concern with security services in the cloud in ranked order (privately held companies)

Concern	Ranking
We are concerned about connecting business critical systems to security mechanisms outside our full control	1
We are concerned with the level of security in a multi-tenant environment	2
We are concerned with the ability to remove/recover our data from the cloud	3
We are concerned about the location of our data	4
We are concerned about our ability to audit the environment for compliance with our security needs	5
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	6
We are concerned that our availability needs cannot be met with a cloud-based service	7

Concerns with cloud security vary by role

During round-table discussions it was noted that attitudes towards cloud based service varied depending on the seniority and role of the participant. CEOs concerns focused on location, control and the ability to audit. The CEO-level concerns were shared by other C-level executives with the exception of CSO/CISO respondents who were more concerned around the technical aspects of multi-tenant security rather the ability to audit. The difference between CSO/CISO attitudes and their peers (technical preventative controls versus audits and other detective security approaches) is attributed to differing business priorities associated with the role. Interestingly, CTOs cite the right to audit as their number one concern. This suggests a desire to deploy the same tools and processed used in traditional outsourcing to understand and manage the risks in cloud computing scenarios.

The majority of respondents holding management and operational roles had views aligned with those of the CSO/CISO group in that they also held concerns about the technical aspects of security in a multi-tenant environment.

Managing data in the cloud

While the survey focused on cloud based security services, concerns around generalized cloud usage were the least contentious relative to all security issues of an organization. Please refer to question 50 in *Appendix A* which contains the complete survey questions and responses.

Given the willingness of Canadian organizations to outsource, along with the overall attitudes towards cloud computing at executive levels, it is likely that once an organization is satisfied that their security concerns are addressed, cloud computing is viewed no differently than traditional outsourcing.

A Note on the USA PATRIOT Act

The USA PATRIOT Act has had profound implications for privacy in Canada. When an organization outsources any dimension of its IT or IT security, there is a risk of the information the outsourcing provider has access to will provide that information to a third party. This risk has increased dramatically with the USA PATRIOT Act, where American companies and their affiliates may be required by the USA PATRIOT Act to turn this information over to the Department of Homeland Security. This requirement can potentially alter outsourcing decisions and compliance postures as it can be seen as putting organizations at odds with their obligations under Canadian privacy laws.

In the 2009 survey a decision was made to focus on the broader topic of geographies that had legislation compatible with Canadian requirements rather concentrating on the impact of USA legislation alone. The expanded focus was selected for two reasons:

- With the growth of cloud computing, Canadian companies have a broader number of options for using external service providers, be they “in-the-cloud” or in traditional collocation and hosting data centers.
- The USA PATRIOT Act has not been amended and remains the same on the legislative books.

The exploration of cloud computing concerns and outsourcing policies suggests that compatible legislation is still prominent, as evidenced by two-thirds of all Canadian organizations willing to outsource reporting some concern about the country the outsourcing occurs in. In addition, nearly 40%

of respondents also reported specific concerns about legislative compatibility. Please refer to question 29 in *Appendix A* which contains the complete survey questions and responses.

According to the 2008 survey data Canadian organizations perceive some degree of risk from the USA PATRIOT Act and USA Homeland Security requirements. Approximately 39% of total respondents answered that the USA PATRIOT Act poses a serious or very serious concern. Government respondents indicated the most concern with the USA PATRIOT Act with 47% indicating at least serious concern. Publicly traded companies followed closely behind at 45%, while privately held organizations were much less concerned with less than one third (32%) of respondents indicating concern.

This concern with the USA PATRIOT Act coupled with Canadian policies towards outsourcing suggests that USA service providers that store Canadian data in the USA will continue to find it difficult to capture Canadian customers.

APPENDICES

Appendix A: Complete Survey Results

Please note that survey results in this appendix have been ordered to facilitate their review. The order of question options at the time of survey administration may have differed.

Over 600 responded to this year's survey. The following results have been filtered to organizations with 100 or more employees to facilitate comparisons to 2008 results. This resulted in an analysis of 501 profiles. Note that An analysis of the results for respondents with 100 employees or less is forthcoming.

Q1. What is the ownership/legal structure of your organization:

Government organization	35%
Not-for-profit organization	6%
Private Company	27%
Publicly Traded Company	31%

Q2. Which industry does your organization belong to? Pick one only, choose main revenue source if more than one applies.

Information - Publishing, Broadcasting, Communications and IT	14%
Finance and Insurance	14%
Professional, Scientific, and Technical Services	6%
Municipal Government	13%
Educational Services	7%
Other Services (except Public Administration)	5%
Retail Trade	5%
Federal Government	6%
Health Care and Social Assistance	6%
Provincial Government	6%
Manufacturing, Discrete	3%
Transportation and Warehousing	3%
Construction	2%
Mining	3%
Manufacturing, Process	2%
Administrative and Support Services	1%
Agriculture, Forestry, Fishing and Hunting	2%
Utilities	1%
Accommodation and Food Services	1%
Management of Companies and Enterprises	1%
Wholesale Trade, Durable Goods	0%
Arts, Entertainment, and Recreation	0%
Real Estate and Rental and Leasing	1%
Waste Management and Remediation Services	0%

Q3. What region of Canada are you located in?

Ontario	55%
Alberta	16%
Quebec	12%
British Columbia	10%
USA	2%
Nova Scotia	1%
International	2%
Manitoba	1%
Saskatchewan	1%
New Brunswick	1%
Prince Edward Island	0%
Northwest Territories	0%

Q4. Where is the global headquarters of your organization located?

Canada	83%
USA	11%
Europe (including UK)	4%
Other	1%
Asia (excluding Japan)	1%
Japan	1%

Q5. Where does your organization do significant business?

Canada	96%
USA	41%
Europe (including UK)	24%
Japan	13%
Asia (excluding Japan)	19%
Latin America	14%
Other	10%

Q6. How many employees does your organization have?

1,000-2,499	17%
50,000 or More	16%
2,500-4,999	15%
10,000-19,999	14%
20,000-49,999	11%
5,000-9,999	11%
500-749	8%
750-999	5%
Don't know	3%

Q7. How large is your organization based on annual revenue for last year? (If government organization, please choose your organization’s total budget)

$1 million – $24 million	10%
< $1 million	1%
Don’t know	20%
$100 million – $499 million	14%
$2 billion – $10 billion	13%
> $10 billion	13%
$25 million – $99 million	11%
$1 billion – $1.99 billion	10%
$500 million – $999 million	8%

Q8. What percentage of your employees works away from the office 25% or more of the time and accesses your network remotely? (Either wired or wirelessly)?

1-5%	34%
6-10%	24%
50% +	6%
11-15%	14%
16-25%	11%
0%	3%
26-50%	8%

Q9. How many workstations (laptops/desktops) does your organization have as a percent of total employees?

More than 100%	26%
91-100%	26%
81-90%	8%
71-80%	7%
< 10%	4%
41%-50%	5%
51-60%	6%
21-30%	5%
61-70%	6%
11-20%	4%
31-40%	4%

Q10. Please choose the job title that most closely matches your own:

Manager of IT or Security	29%
Other	21%
Security Analyst	19%
System Administrator	12%
Director	8%
Chief Executive Officer	1%
VP of IT or Security or Risk Management	2%
Chief Technology Officer	2%
Chief Security Officer	3%
Chief Information Officer	2%
Chief Information Security Officer	1%

Q11. Geographically, what is your scope of responsibility in security:

Local or regional responsibility	39%
All of the organization's activities globally	29%
All the organizations activities in Canada only	12%
Responsibility for Canadian headquarters	8%
Other	7%
Responsible for North America (Canada and USA only)	3%
Responsible for Canada and International (USA excluded)	3%

Q12. In your current role, which of the following functions do you perform?

Security Operations	54%
IT / Security Audit	61%
Policy Development	56%
Forensics / Incident Handling	40%
Risk Management	51%
Mgmt, Security Programs	46%
Security Architecture	50%
Secure Development	28%
Physical Security	25%
Regulatory Compliance	40%
Identity and Access Mgmt	47%
Privacy	33%
Loss Prevention	29%
None of the above	9%

Q13. How long have you been in IT security?

10 years or more	32%
4-6 years	23%
1-3 years	18%
7-9 years	17%
< 1 year	9%

Q14. What is the level of the staff turnover in your security organization currently?

Very low – it is rare that someone leaves our group	38%
Low – staff generally stay for more than 5 years	31%
Medium – staff generally stay for 3 to 5 years	25%
High – Staff generally stay for 1-3 years	5%
Very high – Staff generally stay for less than a year	1%

Q15. Do you have any formal IT certifications, degrees or diplomas?

CISSP	32%
CISM	8%
CISA	10%

Privacy	2%
Business Continuity / Disaster Recovery	4%
SANS Systems Administration Networking and Security	9%
Degree, Computer Science / Engineering	30%
Degree, Economics / Finance / Business	11%
Degree, not in business or technology	11%

Q16. Which range contains your current annual salary (including any bonuses)?

$100,000 – $119,999	22%
$80,000 – $89,999	13%
$70,000 – $79,999	12%
$90,000 – $99,999	9%
$120,000 – $139,999	8%
$60,000 – $69,999	7%
$140,000 – $159,999	4%
$50,000 – $59,999	4%
$160,000 – $179,999	3%
> $200,000	2%
$40,000 – $49,999	2%
< $40,000	1%
$180,000 – $199,999	1%
I prefer not to answer this question	11%

Q17. Where is the Information security policy for your Canadian operations determined?

Asia (excluding Japan)	0%
Canadian Headquarters	61%
Don’t know	4%
Europe (including the UK)	0%
Local Canadian operations	28%
USA	7%

Q18. Does your organization have a dedicated information security officer (i.e. CISO, CSO, or equivalent in government)?

No	44%
Yes	56%

Q19. What is the management level of the highest ranking person responsible for information security?

Director-level	31%
Manager-level	27%
Vice President level	22%
Senior Manager	8%
Team lead	6%
Don’t know	4%
Other	2%
Not applicable	1%

Q20. Where does your highest ranking person responsible for information security report to?

IT	54%
CEO	26%
Other	10%
Finance	7%
Risk Management	3%
HR	1%

Q21. Which areas is the information security function accountable for?

Audit	51%
Compliance	71%
Risk Management	62%
IT Security (network and applications)	94%
Physical Security	35%
Loss Prevention	38%
Safety	22%
Business Continuity / Disaster Recovery	56%

Q22. Do any of the following government regulations or industry regulations with respect to information security affect your organization? Check all that apply:

Sarbanes-Oxley (SOX)	31%
Bill 198 (Canadian Sarbanes-Oxley equivalent)	35%
Privacy Act (Canada or USA)	70%
Canadian Bank Act	15%

Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada)	70%
Payment Card Industry (PCI- DSS)	43%
Other Industry-specific regulations (FFIEC, NERC, FERC, PHIPA, HIPAA)	29%
Breach disclosure laws	21%
Special information security laws	15%
Don't know	10%

Q23. How well do key security decision-makers in your organization understand the information security requirements to comply with the regulations/legislation affecting your organization? Pick one:

Our understanding of the requirements is very limited.	8%
We have a good understanding of the legislated/ regulated security requirements that we need to comply with.	30%
We have a very good understanding of the legislated/regulated security requirements that we need to comply with.	28%
We have an adequate understanding of the requirements.	25%

Q24. How efficiently does your organization manage different compliance requirements (check the one that matches closest to your situation)?

Don't know	13%
We have not yet analyzed our regulatory compliance obligations.	12%
We understand our compliance obligations and we treat each regulation as a separate project / set of requirements.	40%
We understand our regulatory obligations and search for projects or approaches that enable compliance with different requirements.	35%

Q25. Does your organization formally measure its IT staff against specific information security objectives (i.e., does their compensation depend in part on achieving security objectives)?

Don't Know	18%

No	61%
Yes	21%

Q26. How often does your organization communicate about security issues, threats and policies to its workforce (including employees, students and long-term contractors)? Pick the ONE frequency that most closely matches:

At least once a month	11%
At least once a quarter	16%
At least once every two weeks	5%
At least once per year	25%
At least twice per year	8%
Don’t know	5%
Less than once per year	12%
Never	3%
Upon hiring only	13%

Q27. Assessing information security risk involves establishing the value of business assets (data, software, hardware), understanding which threats they are vulnerable to, and understanding how well current security measures protect these assets. How often does your organization assess its security risks (including external or internal audits)? Pick one:

Don’t know	15%
Every 6 months	11%
Every two years	7%
Every year	21%
Less than once every two years	11%
Monthly	10%
More often than once per month	8%
Never	4%
Quarterly	12%

Q28. What share of your organization's information security budget is spent on outsourced security services? Pick one:

21% to 40%	4%
41% to 60%	4%
61% to 80%	0%
Don't know	31%
More than 80%	4%
None	24%
Up to 20%	32%

Q29. Which of the following functions do you currently outsource?

Security programme development / management	11%
Management of firewalls	20%
Management of web application firewalls	16%
Management of network intrusion prevention systems	20%
Monitoring of security events (SIEM)	14%
Collection of security logs (log mgmt)	16%
Management of virtual private networks	6%
Management of local area networks	19%
Management of desktops	18%
Management of servers / applications (on premise)	16%
Management of servers / applications (in datacenter)	18%
Security testing of networks and infrastructure	37%
Testing of software and applications (including web)	25%
Backups	16%

Q30. Does your organization have a policy regarding outsourcing of information security services to a third party?

We allow outsourcing of security to other countries where we do business	6%
We do not allow outsourcing of IT security	39%
We only allow outsourcing to countries with laws and regulations that are as stringent as those in Canada	12%
We only outsource to Canadian companies	24%
We outsource to the best value provider; location is not a major factor in our decision	20%

Q31. To what extent is your organization concerned about the following regarding the provisioning of information security services through cloud computing (Security as a Service, Security in the Cloud)?

Concerns	Average Concern
We are concerned about the location of our data	23%
We are concerned with the level of security in a multi-tenant environment	16%
We are concerned with the ability to remove/recover our data from the cloud	13%
We are concerned that our availability needs cannot be met with a cloud-based service	11%
We are concerned about our ability to audit the environment for compliance with our security needs	14%
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	12%
We are concerned about connecting business critical systems to security mechanisms outside our full control	21%

Q32. How many applications does your organization have?

> 1000	13%
1-4	6%
5-9	9%
10-25	15%
26-50	11%
51-100	16%
101-500	26%
501-1000	4%

Q33. How often do you perform the following types of testing on Applications for your critical applications?

	Never	Yearly	Quarterly	Monthly	Weekly
Frequency of Manual Penetration Testing	33%	38%	16%	4%	8%
Frequency of Automated Vulnerability Testing	24%	23%	23%	15%	15%
Frequency of Manual Source Code Review?	54%	21%	10%	6%	9%
Frequency of Automated Code Review?	60%	15%	12%	5%	8%

Q34. Who performs the majority of your application testing? (Please check all that apply.)

Internal security team	29%
Internal development team	32%
Internal audit team	11%
External audit team	8%
External security consultants	18%
Don’t know	7%

Q35. What role does security play in your software development lifecycle? (Please check all that apply.)

Security starts with the requirements analysis phase	27%
Security starts with the design phase	17%
Security is integrated at the coding phase	17%
Security is tested for after coding is complete	22%
Security is tested after being promoted to production	16%
Security is tested on ad-hoc basis as needed	22%
Don’t know	8%
Security testing is not part of our development practices	10%

Q36. What percent of your applications are developed in-house?

0%	5%
1 - 20%	29%
21 - 40 %	16%
41 - 60%	14%
61 - 80%	13%
81 - 100%	13%
Don’t know	8%

Q37. Approximately how many full time equivalent staff (FTEs) does your organization devote to IT security (including IT security operations, audit and policy functions)?

0 FTEs	9%
1 FTE	21%
2-4 FTEs	22%
5 to 10 FTEs	16%
11 to 25 FTEs	4%
26 to 50 FTEs	5%
Don’t know	10%
More than 50 FTEs	11%

Q38. Rate the effectiveness of the following strategies in obtaining funding for information security projects and initiatives from your organization’s business leaders?

Strategy	Average Concern
Explaining the nature and magnitude of the risk	17%
Explaining the nature and magnitude of the threat	15%
Demonstrating Return on Investment (revenue increase, cost reduction)	17%
Demonstrating how the initiative links to business strategy	16%
Demonstrating how the initiative meets compliance requirements	20%
Demonstrating need to follow industry best practices	12%
Demonstrating the need to meet the internal policies and security objectives	19%

Q39. Approximately what percent of your security staff are contractors? (including IT security operations, audit and policy functions)?

< 2%	53%
2 - 4%	18%
5 - 10%	9%
11 - 15%	7%
16 - 25%	4%
26 - 50%	6%
More than 50%	3%

Q40. What percentage of your organization's revenue/funding is spent on IT?

< 1 %	6%
1% - 2%	19%
3% - 4%	11%
5% - 6%	9%
7% - 9%	1%
10% -15%	8%
16% - 25%	4%
Don’t know	34%
More than 25%	6%

Q41. Approximately what share of the IT budget is spent on security?

< 1 %	12%
1% - 2%	11%
3% - 4%	11%
5% - 6%	12%
7% - 9%	5%
10% -15%	9%
16% - 25%	5%
Don’t know	30%
More than 25%	3%

Q42. How important are the following in driving your organization’s IT security investment?

Legislation / Regulations	60%
Security breaches that have occurred in our organization	42%
Security breaches that have occurred at competitors, clients, suppliers’ or affiliate organizations	25%
Media reporting of security breaches	33%
Increased concern over risk management, potential losses	41%
Increased risk from increased activities by employees such as: use of wireless devices, remote access, instant messaging, etc.	46%
See security as a potential competitive advantage	21%
Clients demanding better IT / information security from us	30%

Q43. Was your IT Security budget affected by the 2009 global financial crisis?

Major Budgetary Cuts: 25% to 49% of the original budget for contracts or projects related to security and privacy was cut.	10%
Major Budgetary Increase: original budget increased by 25% to 49% for contracts or projects related to security and privacy.	1%
Minor Budgetary Cuts: Less than 10% of the original budget for contracts or projects related to security and privacy was cut.	36%
Minor Budgetary Increase: original budget increased by less than 10% for contracts or projects related to security and privacy.	19%
Moderate Budgetary Cuts: 10% to 24% of the original budget for contracts or projects related to security and privacy was cut.	20%
Moderate Budgetary Increase: original budget increased by 10% to 24% for contracts or projects related to security and privacy.	5%
Severe Budgetary Cuts: 50% to 100% of the original budget for contracts or projects related to security and privacy was cut.	8%
Very Significant Budgetary Increase: original budget increased by 50% to 100% for contracts or projects related to security and privacy.	1%

Q44. If the level of your outsourcing was affected by the 2009 global financial crisis, please choose the main reason:

Don’t know	26%
No, outsourcing was not impacted in our organization	48%
We increased our outsourcing relationships to reduce headcount	4%
We increased our outsourcing relationships to reduce operating expenses	2%
Yes, our outsourcing relationships were impacted but not significantly	10%
Yes, we were asked to reduce our outsourcing relationships significantly	12%

Q45. Did the 2009 global financial crisis cause your organization to re-consider staffing decisions related to security or privacy? (Check all that apply):

Yes, we had to lay off full time security personnel	5%
Yes, we had to lay off part-time security personnel, contractors or consultants	5%
No staffing changes caused by the 2009 financial downturn	38%
Yes, we increased our full time security personnel	2%
Don’t know	10%

Q46. If you suffered a breach, what is your confidence level that you would be able to detect it?

High	26%
Low	19%
Moderate	41%
Very High	5%
Very Low	8%

Q47. Did your organization experience and identify any of the following types of information security breaches in the past 12 months? Check all that apply:

Virus/worms/spyware/malware/spam	70%
Laptop or mobile hardware device theft	53%
Financial fraud	14%
Bots (zombies) within the organization	15%
Phishing/Pharming where your organization was fraudulently described as the sender	23%
Denial of service attack	16%
Sabotage of data or networks	3%
Unauthorized access to information by employees	36%
Extortion or blackmail (ransomware)	3%
Website defacement	6%
Loss of confidential customer/employee data	10%
Abuse of wireless network	15%
Password Sniffing	5%
Misuse of a corporate application	13%
Theft of proprietary information	7%
Identity Theft	7%
Exploitation of your domain name server (DNS)	2%

Q48. How many Security breaches do you estimate your organization has experienced in the past 12 months?

1	6%
2 – 5	33%
6 – 10	9%
11 – 25	7%
26 – 50	3%
51 – 100	2%
Don’t know	23%
More than 100	2%
None	14%

Q49. How many Privacy breaches do you estimate your organization has experienced in the past 12 months?

1	7%
2 – 5	19%
6 – 10	6%
11 – 25	5%
26 – 50	2%
51 – 100	1%
Don't know	31%
More than 100	1%
None	32%

Q50. How often do you test your Security Incident Response process (or equivalent)?

Annually	25%
Don't know	22%
Monthly	9%
Never / We don't have an Security Incident Response process	35%
Quarterly	8%

Q51. Please estimate what percentage of security breaches come from insiders of the organization:

6% to 10%	5%
11% to 20%	6%
21% to 40%	9%
41% to 60%	10%
61% to 80%	7%
81% to 100%	9%
Don't know	31%
None	13%
Up to 5%	11%

Q52. What types of costs would your organization be most concerned about if there was a major information security breach? Please rank the options below:

Breach Cost	Average
Damage to Brand reputation or image	28%
Lost Time due to Disruption	17%
Personal Accountability	9%
Litigation	14%
Regulatory Action	15%
Lost Customers	13%
Cost of New Equipment / Services Required	8%
Cost to Compensate Customers / Damaged Parties	11%
Loss of Market Valuation (share price)	9%

Q53. Please estimate the total dollar value of losses that your company has experienced due to all breaches (including those not formally disclosed) over the past 12 months?

$1 million - $2.9 million	3%
$3 million - $4.9 million	2%
$100,000 to $249,999	4%
$250,000 to $499,999	2%
$500,000 - $999,999	11%
< $100,000	24%
$0	14%
Don't know	40%

Q54. How concerned is your organization about each of the following issues?

Managing Risks from Third-Parties, i.e. business partners, suppliers and collaborators	8%
Managing Security of Wireless and Mobile Devices	10%
Disclosure / Loss of Confidential Customer Data	21%
Compliance with Canadian Regulations and Legislation	17%
Compliance with USA or Other Foreign Regulations and Legislation	9%
Accountability of User Actions and Access	10%
Employees Understanding and Complying with Security Policies	11%
Business Continuity / Disaster Recovery	16%
Loss of Strategic Corporate Information	13%
Managing data in the cloud (cloud computing)	4%

Q55. Please indicate the status of the following initiatives in your organization:

Security Initiative	Not Interested	Evaluating	Planning	Deploying	In Place
Security awareness program for general employees	21%	22%	15%	7%	35%
Security awareness program specific to IT staff	25%	12%	18%	3%	43%
Security awareness program specific to developers and architects	44%	10%	15%	0%	31%
Linking general IT staff's performance evaluations to security objectives	53%	10%	24%	1%	12%
Creating business-level security metrics	38%	23%	24%	5%	11%
Security awareness programs for customers	43%	15%	22%	7%	13%
Requiring suppliers, business partners or other third parties agree to organization's security policy	35%	10%	26%	3%	25%
Integration of security into software/ application development	35%	18%	9%	3%	35%
Requiring suppliers, business partners or other third parties to agree to organization's privacy policy	38%	21%	10%	4%	27%
Security training for third parties (contractors, volunteers, co-op)	56%	18%	7%	6%	13%
Mandatory tests after security awareness training	54%	16%	12%	3%	15%
Criminal background checks for all IT and Security staff	40%	25%	9%	1%	25%
Creating a security policy	12%	18%	19%	4%	47%
Creating a privacy policy	12%	18%	15%	3%	52%

Q56. What specific technologies do you currently use and how satisfied are you with their effectiveness?

Technology	Do not use	Not at all satisfied	Not quite satisfied	Satisfied	More than satisfied	Very Satisfied
IPSEC based VPN	18%	1%	7%	40%	22%	30%
SSL VPN	19%	1%	5%	41%	26%	28%
Anti-Virus	1%	4%	9%	36%	26%	25%
Email Security (anti-spam, anti-malware)	0%	3%	10%	35%	29%	23%
Public Key Infrastructure	37%	3%	11%	47%	18%	21%
Storage / Hard Disk Encryption	35%	2%	14%	46%	21%	17%
Email Encryption	50%	5%	10%	51%	19%	15%
Database Encryption	46%	5%	14%	43%	26%	11%
URL / Content Filtering	14%	6%	15%	37%	24%	17%
Identity and Access Management	26%	4%	27%	36%	22%	10%
Network based Access Control (NAC via network)	55%	9%	17%	42%	24%	9%
Endpoint Security (NAC via desktop)	50%	7%	14%	40%	27%	12%
Firewalls	2%	3%	6%	31%	32%	28%
Web Application Firewalls	39%	5%	14%	40%	22%	20%
Log Management	26%	15%	29%	31%	15%	10%
Security Information & Event management (SIEM)	42%	12%	24%	38%	15%	12%
Network Intrusion Prevention / Detection	23%	5%	19%	41%	22%	14%
Wireless Intrusion prevention (WIPS)	56%	6%	28%	38%	18%	11%
Application Security Assessment Tools (web/code)	47%	10%	26%	39%	14%	12%
Two-factor authentication (tokens, smartcards)	35%	3%	13%	37%	24%	23%
Vulnerability Scanning / Vulnerability management	26%	6%	21%	36%	25%	12%
Patch Management	8%	7%	15%	41%	22%	16%
Data Leakage Prevention	53%	12%	27%	43%	10%	8%

Q57. What specific technologies will you deploy for IT security in the next 12 months? Please check your level of deployment:

Technology	No deployment (1)	Technical Evaluation (2)	Pilot (3)	Limited Deployment (4)	Full Deployment (5)
IPSEC based VPN	51%	4%	1%	10%	33%
SSL VPN	39%	7%	1%	15%	38%
Anti-Virus	32%	3%	2%	5%	58%
Email Security (anti-spam, anti-malware)	35%	6%	3%	5%	52%
Public Key Infrastructure	52%	11%	4%	14%	19%
Storage / Hard Disk Encryption	42%	14%	7%	18%	20%
Email Encryption	46%	18%	8%	15%	13%
Database Encryption	58%	11%	9%	10%	12%
URL / Content Filtering	38%	10%	5%	13%	34%
Identity and Access Management	38%	16%	9%	14%	22%
Network based Access Control (NAC via network)	40%	17%	10%	15%	18%
Endpoint Security (NAC via desktop)	51%	13%	10%	6%	19%
Firewalls	37%	3%	3%	7%	51%
Web Application Firewalls	47%	10%	6%	12%	25%
Log Management	38%	15%	11%	13%	23%
Security Information & Event management (SIEM)	47%	12%	9%	16%	16%
Network Intrusion Prevention / Detection	37%	9%	5%	17%	32%
Wireless Intrusion prevention (WIPS)	53%	16%	7%	10%	14%
Application Security Assessment Tools (web/code)	53%	17%	9%	9%	12%
Two-factor authentication (tokens, smartcards)	46%	14%	6%	9%	25%
Vulnerability Scanning / Vulnerability management	40%	13%	8%	13%	27%
Patch Management	37%	7%	5%	11%	41%
Data Leakage Prevention	53%	9%	9%	10%	9%

Q58. How do you feel about your organization's overall IT and information security situation?

About the same as last year	34%
Improved somewhat from last year	41%
Improved substantially compared to last year	18%
Much worse than last year	1%
Not sure	4%
Somewhat worse than last year	2%

Q59. How satisfied are you with your organization's overall IT security posture?

Not sure	2%
Not very satisfied	13%
Satisfied	43%
Somewhat dissatisfied	31%
Very satisfied	12%

Appendix B: About the Authors

WALID HEJAZI

Professor of Business Economics, Rotman School of Management

Walid Hejazi is a Professor of Business Economics at the Rotman School of Management at the University of Toronto where he regularly teaches Canada's current and future business leaders in the MBA and EMBA programs. He has published extensively in more than forty business journals and publications. In keeping with the spirit of Rotman, Walid balances his research activities by helping many of Canada's leading organizations leverage research to decide new strategies and initiatives. Recently, he has assisted several large retail chains find new ways to understand their market data, providing them with perspectives that have allowed them to optimize their business activities. Walid has also consulted for several branches of Canadian government, on diverse themes such as the competitiveness of the Canadian economy and international trade. He is currently editor-in-chief of a study being prepared by the Department of Foreign Affairs that measures the economic benefits of Canada's partnership with the EU.

ALAN LEFORT

Managing Director, TELUS Security Labs

Alan LeFort is currently the Managing Director for TELUS Security Labs, a research organization focused on helping more than 50 of the world's leading security companies identify and eradicate critical threats and vulnerabilities. Alan also acts as a senior advisor to several of the top security companies providing guidance on their market strategy and their product roadmaps. Additionally he heads up the product management team at TELUS for security products and services which include managed services, technology integration and professional services.

Prior to joining TELUS, Alan has held senior roles in software development, product management and IT operations. He has also taught several security courses at the professional learning centre of the University of Toronto's faculty of Information Studies.

RAFAEL ETGES

Research Director, TELUS Security Labs

Rafael Etges is the Director for Risk Management Practices for TELUS Security Labs and Program Director for Governance, Risk and Compliance at TELUS Security Solutions. Rafael brings 15 years of consulting experience at major consulting groups in South and North America. Rafael has extensive experience in corporate and IT governance, information security policy development, information security program management and auditing. He is a subject matter expert on several security control frameworks (ISO 17799/27001, CobiT, COSO, ITIL, PCI-DSS) and regulations (Sarbanes Oxley, Bill 198, PIPEDA and international privacy laws).

BEN SAPIRO

Research Director, TELUS Security Labs

Ben Sapiro is the Research Director with TELUS Security Labs responsible for Security Practices. Ben brings over ten years as a security consultant with global clients in North America, Europe, the Middle East and Asia. Ben's security experience includes security audits, ethical hacking, infrastructure work, threat modeling, secure development, secure architecture, social engineering and application testing.

Ben contributes to community efforts on emerging cloud security standards and XML based security reporting languages.