

# 2011

## Executive Briefing

### TELUS – Rotman

Joint Study on Canadian IT Security Practices

Breaches • Budgets • Concerns • Threats • Salaries  
Technology • Initiatives • Outsourcing • Mobile • Social Networking  
The Cloud • Applications • Staffing

# 2011

Four years of research and analysis enhances clarity and understanding of the Canadian security landscape, contributing vital insight that helps Canadian organizations to improve their security postures.

Since 2008, TELUS and the University of Toronto's Rotman School of Management conducted annual studies jointly on the state of IT security in Canada. During this period, more than 2,000 IT security professionals have responded to our surveys, allowing us to provide clarity on the Canadian security landscape, especially as it relates to evolving breaches, threats, preparedness, budgets and strategies.

In addition to documenting trends in the IT security environment, each year's study adds a new dimension to the analysis. In 2009, we analyzed the impacts of the financial crisis on IT security. In 2010, we continued to track outcomes of the financial crisis, but we also examined social networking and associated modifications to security strategies as well as the proliferation of mobile devices in the workplace and their impact on security.

This year, we continued our focus on the financial crisis' legacy, social networking and mobile security. But we've also expanded our scope to include an analysis of the three key pillars of a balanced security strategy (people, process and technology) by asking Canadian organizations to rate each pillar as a strength or a weakness within their IT security. We then look at how those perceptions correlate to risk posture, breaches, satisfaction and other critical dimensions.

# Contents

<b>3</b>	<b>EXECUTIVE SUMMARY</b>
<b>5</b>	<b>DETAILED FINDINGS</b>
<b>5</b>	<b>BREACHES</b>
<b>12</b>	<b>COMPLEXITY AND RISK</b>
<b>15</b>	<b>MOBILE TECHNOLOGIES</b>
<b>16</b>	<b>SOCIAL NETWORKING</b>
<b>18</b>	<b>SATISFACTION WITH SECURITY POSTURE</b>
<b>21</b>	<b>TALENT AND COMPENSATION</b>
<b>23</b>	<b>CONCLUSIONS</b>
<b>25</b>	<b>FINAL REMARKS</b>
<b>26</b>	<b>APPENDIX A – SURVEY QUESTIONS AND RESPONSES</b>

## EXECUTIVE SUMMARY

In the four years of the study, breach numbers have continued to rise for the most part, with slight variations for government and public organizations. Beyond examining the incidences of breaches, the breach types represent an emerging point of interest, that hackers are targeting attacks on specific individuals with the intent of financial gain.

The reality of this threat landscape has direct links to the other dimensions of research and analysis in this year's study. Canadian organizations are trying to determine how to allot their IT dollars to security effectively, how to achieve a fluid yet balanced approach to security and how to build and manage their security environments for optimum effectiveness and protection. By examining these dimensions, it is our goal to provide insights that can help to shape the Canadian security discourse while offering benchmarks and direction to Canadian organizations who are navigating security within a paradigm of global threats, mobile work and socially-connected users.

## NEW QUESTIONS FOR 2011

This year, we added some important dimensions to our survey to address the following emerging issues:

1. Breaches in the age of global hacks: numbers, types of incidents and insider/outsider sources.
2. Top concerns from senior management (Compliance vs. Risks vs. Costs).
3. Satisfaction with technologies – are they delivering their proposed value?
4. Further insights into mobile devices in the workplace.
5. How Canadian organizations perceive value for people, processes and technology and how that perceived value correlates to satisfaction and security performance.

Our 52-question survey was administered in the summer of 2011 and received detailed responses from 649 organizations.

## KEY INSIGHTS

### Breaches and Costs

Breach incidence numbers for government and private companies decreased from 2010, whereas those for publicly traded organizations continue to rise, reporting six times the number of breaches experienced in 2008. Nevertheless, the direct costs associated with breaches, for all organization types, fell from 2010 levels. In 2011, breach incidences and direct costs remain significantly higher than prior to the 2008 financial crisis.

The 2008 financial crisis caused a surge in both breaches and their associated costs across Canada. This trend of increasing breaches continued for public and government organizations into 2009 and 2010, but 2011 has seen a reversal for government breaches, but not for public organizations. Breaches in private organizations have fallen since 2009, year over year, into 2011.

Costs associated directly with these breaches, which increased significantly from 2008 to 2009, have reversed for all organization types year over year into 2011. Nevertheless, a longitudinal study across the four years of analysis shows that the number of breaches experienced are still more than twice that experienced in 2008 – surprisingly, six times more for both public and government organizations, but only marginally more for private companies.

### Budgets

As in previous reports, Government IT security budgets continue to lag behind those in the private sector. More than 30 per cent of government organizations report that the IT security component

of their IT budgets was still only in the zero to one per cent range, comparing to 23 per cent of private organizations, and only 5.4 per cent of public organizations. We have cautioned in the past that these limited budgets investments, combined with gaps in compensation and satisfaction, make it increasingly difficult for governments to attract and keep top security talent.

### **Satisfaction and Budgets Relate**

In general, organizations that are most satisfied with their IT security posture allot a large share of the IT budget to security. However, it should also be noted that a sweet spot exists, namely that more than 90 per cent of respondents report satisfaction levels of 'neutral' and better once the security budget reaches five to six per cent. Satisfaction dips slightly in the seven to nine per cent range and then rises again when above 10 per cent. This may be explained by the cross-sectional variation of budgets across specific industries and organization sizes.

### **The Pillars of IT Security: People, Process and Technology**

This year, we asked decision makers to consider the fundamental question of whether the three pillars of their security system, namely People, Process and Technology, can be viewed as strengths or weaknesses. We then gauged the extent to which these responses are related to the effectiveness of the organization's overall security posture. Organizations that view the three pillars as strengths and as critical to their security approach show a high level of satisfaction with their security program. Organizations that indicated any of the three pillars were strengths were more than 80 per cent likely to be satisfied or very satisfied with their overall security posture, with slight advantages towards Processes and People over Technology.

### **Complexity of the IT Security Environment**

We asked organizations to self assess the complexity of their IT security environments, allowing us to examine how complexity correlates with breaches (security performance), satisfaction and outsourcing. We found that government organizations are reporting higher complexity in their IT Security environments than the corporate sector, which may relate to the higher numbers in breaches – as complexity reduces manageability and exposes organizations to risks.

On the other hand, privately-owned companies in Canada are doing a good job of managing the complexity of their IT environments, with an average of six per cent of the IT budget dedicated to information security, and reporting the highest satisfaction levels between industry sectors (High and Very High – 62 per cent Private, 60 per cent Public, 52 per cent Government). Public companies are reporting a balanced distribution between medium and high/very high levels of complexity, as expected – very few publicly traded companies can afford to operate in a low-complexity environment.

We also found that more than 50 per cent of respondents across all levels of complexity outsource some of their IT security capabilities. Half of high-complexity environments have outsourced up to 20 per cent of their IT security capabilities. Outsourcing tends to happen when cost efficiencies can be justified without losing control over regulatory compliance considerations.

As noted above, more complexity adds more risks. This is reflected in the average number of breaches suffered by organizations in different complexity ranges, with the number increasing dramatically for very complex IT security environments.

## DETAILED FINDINGS

### Breaches

The number of breaches experienced by each of the three organization types (public, private, government) is one of the most important trends highlighted in our research. The figure below provides rich insight into how effective IT security efforts have been during the course of the past four years.

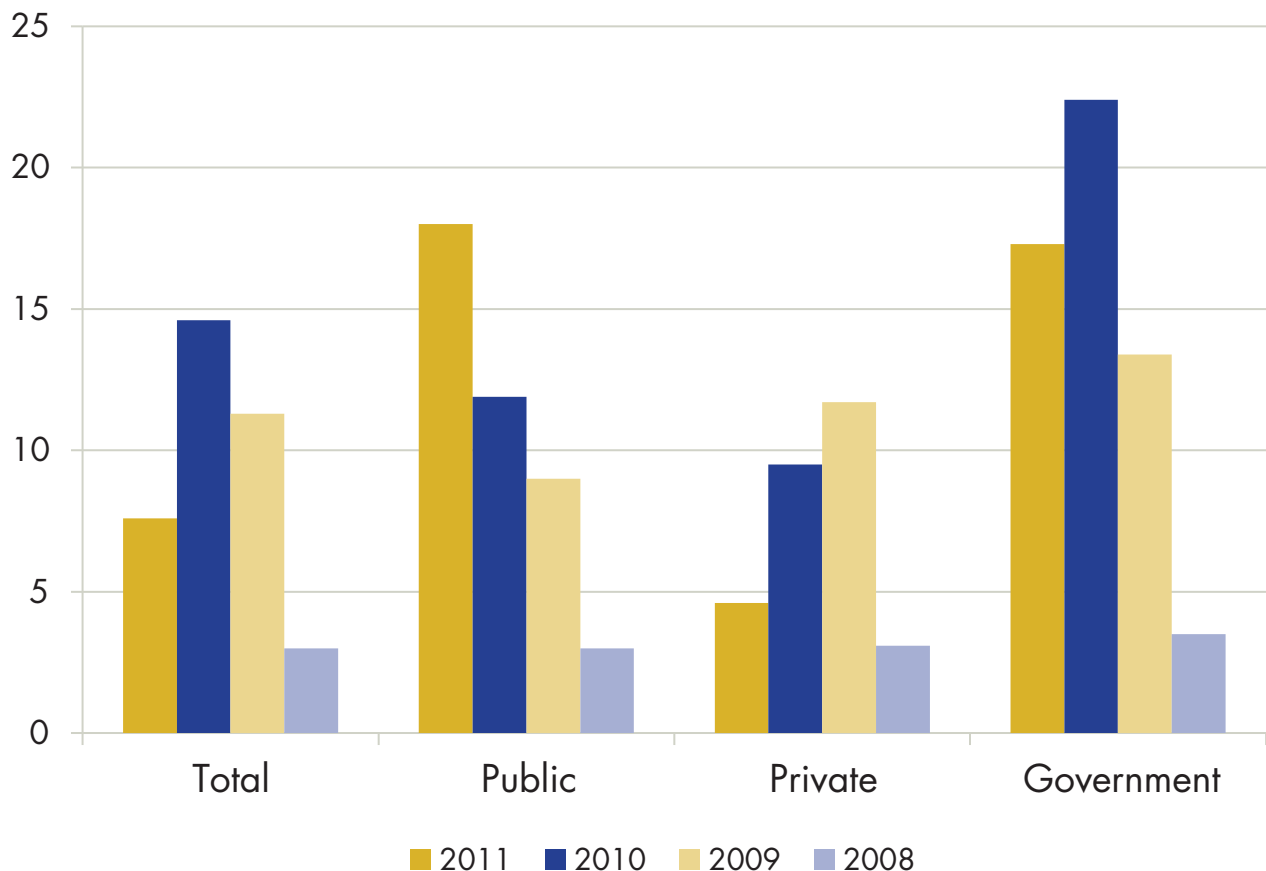
Average Annual Number of Breaches – Per Organization Type				
	Total	Public	Private	Government
2011	7.6	18	4.6	17.3
2010	14.6	11.9	9.5	22.4
2009	11.3	9	11.7	13.4
2008	3	3	3.1	3.5

### Highlights: 2008-2011

#### Data Breach Numbers

1. A significant leap in the number of breaches between 2008 and 2009, which we have linked to the global financial crisis affecting organizational budgets (including security investments) and to a worsening threat environment.
2. This growth in breaches continued through 2010, most pronounced in government organizations, and less so for public corporations. Both sectors are affected by compliance legislation, including privacy and credit card security standards. These regulations mandate the deployment of detective technologies, which increase visibility

### Average Annual Number of Breaches – Per Organization Type



into potential data breaches (and allow for their remediation). With increased visibility comes increased reporting.

In contrast, *private organizations saw a reduction in breaches reported between 2009 and 2010.* Likely, this reduction is caused by reduced investment in detective technologies by private organizations; they may be less targeted by attackers, or less inclined to report a breach even if they detected one.

3. *The results for 2011 show that both government and private organizations have been able to reverse the trend of increasing breaches that occurred since 2008, whereas publicly traded organizations continue to report increasing numbers.* Public organizations have surpassed government agencies in the annual number of breaches for the first time since the beginning of the study (18 breaches for public companies against 17.3 for government organizations).
4. *The number of breaches across all organization types remains higher than reported in 2008.* In the cases of government and public organizations, breaches in 2011 are reported to be three times greater than those reported in 2008. In the case of private organizations, reported breaches in 2010 are only marginally higher than those reported in 2008.

We expect organizations to be substantially more mature in their ability to detect breaches and manage their compliance requirements now than in 2008. In that context, the current security situation should not be seen as 'worse' than in 2008, but more realistic and reflective of a superior understanding of the risk environment in which they operate.

5. What also stands out is the similarity in the breach numbers across all organization types prior to the financial crisis, and the significant divergences in its aftermath. Prior to the crisis, all organization types reported the same number of breaches, approximately three per organization. *The financial crisis, the emergence of new technologies such as mobile computing and the new strategies employed by attackers has impacted each group very differently.*

### **Attacks Remain Increasingly Focused**

The increase in sophisticated and targeted attacks has been a marked trend in our analysis during the past few years. In addition to opportunistic attacks or incidents caused by a lack of education or employee negligence – which are gradually being treated as an annoyance to be managed by the IT operations team rather than a real threat to be handled by the security office – attacks are becoming focused increasingly on targeting specific individuals and their data. These attacks are reported less frequently as they are much harder to detect and often involve much longer timeframes. In most cases, they seek a continuing information stream that can be monetized or leveraged for political or ideological gains. This trend has been reinforced consistently by evidence coming from TELUS Security Labs, which indicated that one in three threats seeks financial information. The recent paper, *Mitigating Threats that Matter*, provides details on current threat trends based on TELUS Security Labs research and forensic investigations. The data surveyed for 2011 is very similar to that from 2010, indicating that attackers are continuing to be motivated by financial gains.

Breach Types				
Attack/Breach Type Reported – All Organizations	2011	2010	2009	2008
Virus/Worms/Spyware/Malware/Spam	46%	49%	41%	62%
Laptop or mobile hardware device theft	22%	31%	30%	34%
Phishing/Pharming (victim described fraudulently as sender )	20%	21%	14%	27%
Unauthorized access to information by employees	14%	20%	20%	17%
Abuse of wireless network	11%	10%	8%	11%
Bots (zombies) within the organization	9%	13%	9%	8%
Denial of service attack	8%	13%	9%	17%
Loss of confidential customer/Employee data	6%	9%	5%	8%
Password sniffing	6%	6%	3%	6%
Financial/Online banking fraud	5%	7%	8%	8%
Misuse of a corporate application	5%	8%	8%	10%
Social engineering attack	5%	11%	-	-
Website defacement	4%	4%	4%	4%
Theft of proprietary information	4%	6%	4%	4%
Sabotage of data or networks	3%	3%	2%	3%
Identity theft	3%	5%	4%	6%
Smartphone/Phone/Tablet device hacked	3%	-	-	-
Exploitation of your domain name server (DNS)	2%	4%	1%	2%
Extortion or blackmail (ransomware)	1%	2%	2%	2%

We also considered how specific sectors in the Canadian economy are affected by different issues. As the data in the table below indicates, most organizations face the same problems, with a few exceptions worth mentioning: some challenges are more prevalent in government than in the corporate sector. Laptop or mobile device losses and unauthorized access by employees are reported to occur almost twice as frequently in government as in private companies – and both are related to lack of education and awareness.

Privately-owned companies tend to be less impacted in most cases, except on the issue of website defacement. This is interesting, as most security professionals would agree generally on the perception that a privately-owned company can often be too small to be selected specifically as a target. Often senior management misunderstand that, in most cases, automated software that crawls the web in search of vulnerable websites picks targets irrespective of any particular brand.

Breach Types – 2011 – By Organization Type			
	Public	Private	Government
Virus/Worms/Spyware/Malware/Spam	43%	47%	42%
Laptop or mobile hardware device theft	25%	19%	34%
Financial/Online banking fraud	4%	5%	6%
Bots (zombies) within the organization	10%	9%	11%
Phishing/Pharming where your organization was described fraudulently as the sender	22%	18%	24%
Denial of service attack	10%	7%	10%
Sabotage of data or networks	3%	3%	3%

Breach Types – 2011 – By Organization Type			
	Public	Private	Government
Unauthorized access to information by employees	19%	11%	24%
Extortion or blackmail (ransomware)	2%	1%	1%
Website defacement	3%	5%	3%
Loss of confidential customer/Employee data	10%	5%	7%
Abuse of wireless network	11%	11%	14%
Password sniffing	8%	7%	2%
Misuse of a corporate application	5%	4%	9%
Theft of proprietary information	7%	4%	0%
Identity theft	4%	3%	4%
Social engineering attack	4%	3%	14%
Exploitation of your domain name server (DNS)	4%	2%	1%
Smartphone/Phone/Tablet device hacked	5%	3%	2%

### Detection Technologies Have a Big Impact into Breach Visibility

We were interested in the number of breaches reported and the deployment of detective technologies in each organization type. In a cross section, can we see how breaches are correlated with investments in detective technologies?

Breaches in the Past 12 Months: "None" or "Don't Know" – All Organization Types					
	Log Management	SIEM	Network IPS/IDS	Wireless IPS	Vulnerability Scanning/ Vulnerability Management
No Deployment	43%	49%	41%	52%	44%
Partial Deployment	32%	32%	28%	27%	33%
Full Deployment	25%	19%	31%	21%	23%
<i>Improvement in Visibility (No vs. Full Deployment)</i>	<i>172%</i>	<i>258%</i>	<i>132%</i>	<i>248%</i>	<i>191%</i>

To answer this question, we first needed to investigate the visibility of data breaches. We measured that by looking at how many organizations indicated they had 'zero' breaches and how many admitted that they don't know. For the purposes of this analysis, we grouped 'no breach detected' with 'don't know how many breaches,' and compared sectors.

Percentage of Respondents Reporting Don't Know and Zero Breaches				
	Total	Public	Private	Government
2011	34%	33%	33%	34%
2010	18.4%	42%	9.6%	16.5%
2009	37%	34.3%	40.8%	36.8%
2008	34%	37%	25%	40%

A significant number of respondents – one out of three – indicated that they did not detect or were not aware of any breaches in their environment in the past 12 months. Our next step was to evaluate, within this group, which detective technologies are in place, or being implemented, and their effect on the responses. We then assessed how the deployment of specific detection technologies was associated with a reduced number of undiscovered breaches or increased monitoring and visibility into the environment.

Unlike public and private organizations, the share of insider breaches in the government sector continue to rise, growing 28% since 2010 and up 68% since 2008.

Technologies including Security Information and Event Management (SIEM) and Wireless Intrusion Prevention Systems show a dramatic increase in visibility or reduction of 'Don't Know' and 'No Breaches Detected' responses. With the increased adoption of WiFi-enabled devices such as smartphones and tablets in the workplace and the increase of traditional LAN-connected and WiFi broadcasting workstations, it becomes absolutely critical to monitor and enforce access control policies to prevent breaches.

**Insider Breaches Going Down – Except in Government**

Breaches caused or perpetrated by insiders is an issue of significant concern for Canadian organizations. The latest data indicates that 22 per cent of breaches are related to insiders. Across all organization types, there was a surge in the proportion of insider breaches in the aftermath of the financial crisis, but this surge has reversed itself almost completely in the case of private organizations. In the case of public organizations, the surge has stabilized and only slightly reversed. One of the reasons that can explain the increase in insider breaches during a financial crisis is the resulting termination of staff and contractors, who leave their jobs with a wealth of inside information, and who may remove valuable business data as they leave. In times of economic uncertainty, employees may also archive their work-related data as a means to improve chances of finding employment later or because they have a sense of ownership over the data that they created or manipulated at work. As the financial situation normalizes and layoffs become less

prevalent, insider breach numbers go down. Another reason, perhaps in combination with the first, is the reduction in budgets dedicated to protect business data as a result of a financial downturn.

The high numbers of insider breaches in government is the most startling finding from the research. Forty two per cent of breaches in government organizations are perpetrated by insiders. Different from private and public organizations, the share of insider breaches for government continues to rise, growing by 28 per cent since 2010, but up 68 per cent since the start of our analysis in 2008.

Number of Insider Breaches (or share of breaches perpetrated by insiders)				
	Total	Public	Private	Government
2011	22%	27%	16%	42%
2010	25%	30%	19%	33%
2009	23%	29%	28%	33%
2008	17%	17%	14%	25%

We wanted to discover if we could isolate the types of breaches taking place in organizations that have a higher incidence of insider breaches. How would the picture look if we analysed entities reporting the largest share of insider breaches, relative to those reporting the lowest share? Not surprisingly, breaches associated with employee activity (unauthorized access to information, abuse of wireless networks and laptop theft) are the most prevalent. In most cases, organizations could have prevented such breaches if they had stronger access controls and policies governing the use of business applications and systems as well as better education programs.

It is interesting to note that one specific breach type, 'Smartphone/tablet device hacked,' has a *negative* correlation with the number of insider breaches, suggesting that compromised smartphones and tablets are associated with outsiders rather than insiders. This is still a new and specialized type of attack, in which the data from the device owner is also stolen. With the proliferation of personally-owned devices in the workplace, this type of breach may be treated as a personal property loss, to the extent that a company may be capable of removing the sensitive data remotely after the incident.

least regard for established security policies. This is in stark contrast with the message coming from the top that security and risk management are critical to the success of the business. It also increases the incidence of insider breaches with aggravated damage as executives may expose highly sensitive information when a breach happens. The conflict between policy and actions makes the mission to educate users within organizations extremely difficult and creates scepticism among middle managers and front-line staff responsible for the management and processing of sensitive business data.

Type of Breach – Per Incidence of Insider Breaches			
	Low levels of Insider Breaches (20% or less)	High levels of Insider Breaches (61%+)	Difference
Unauthorized access to information by employees	15%	60%	45%
Abuse of wireless network	15%	40%	25%
Laptop or mobile hardware device theft	28%	50%	22%
Bots (zombies) within the organization	10%	29%	19%
Phishing/Pharming where your organization was described fraudulently as the sender	30%	48%	18%
Loss of confidential customer/employee data	5%	19%	14%
Misuse of a corporate application	5%	19%	14%
Virus/Worms/Spyware/Malware/Spam	67%	79%	12%
Denial of service attack	12%	24%	12%
Social engineering attack	5%	14%	9%
Theft of proprietary information	3%	10%	7%
Identity theft	4%	10%	6%
Smartphone/Phone/Tablet device hacked	6%	2%	-4%
Financial/Online banking fraud	7%	10%	3%
Sabotage of data or networks	4%	7%	3%
Password sniffing	8%	10%	2%
Exploitation of your domain name server (DNS)	4%	2%	2%
Extortion or blackmail (ransomware)	1%	2%	1%
Website defacement	9%	10%	1%

### Senior Management and Contractors Causing Too Many Policy Violations

Starting in 2010, we polled organizations on which groups have the highest number of violations against established security policies. The answer, both last year and in 2011, shows that executives exhibit the

Search Policy Violations - By Organization Type				
Group Disregarding Security Policies	Government	Private company	Public company	2010
Executives	26%	19%	21%	21%
Contractors, External Consultants, Partners or Agencies	18%	17%	23%	11%
Administrative Staff	12%	12%	15%	14%
Sales	3%	17%	17%	16%
Management	14%	16%	6%	15%
Information Technology	11%	8%	9%	12%
Operations/Manufacturing	9%	7%	4%	5%
Marketing	6%	5%	4%	7%

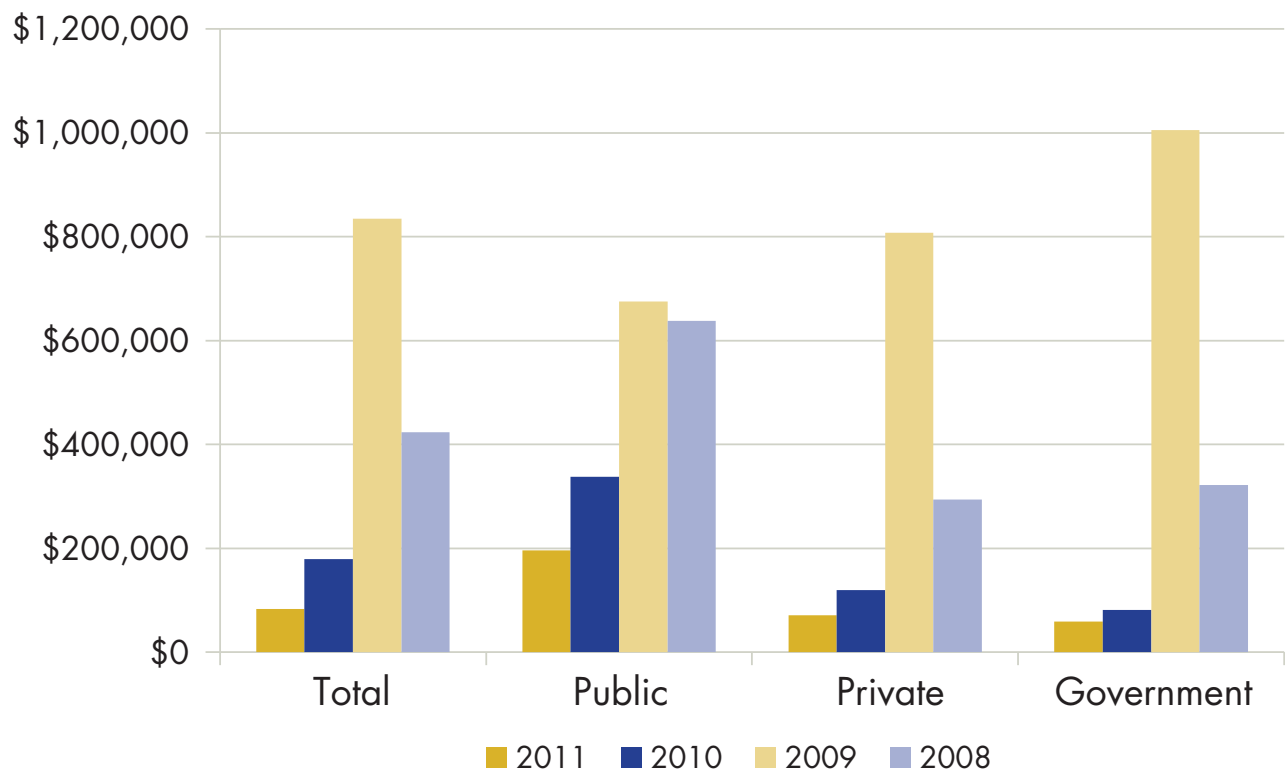
Contractors and external agents also scored high as policy violators (in contrast to 2010). Public companies are reporting more problems with consultants and third parties than with senior management. Considering that austerity measures are still present in many industries across Canada and team sizes have been reduced (not only in security) and outsourcing has increased, it is no surprise that

the additional contractors on-site may not be exposed to the same level of training and supervision as before.

### Costs Associated with Security Breaches

The financial crisis resulted in a surge in security breach costs. However, the significant increase in these costs from 2008 to 2009 have reversed, with

### Average annual loss as a result of security breaches – per organization type



all organization types experiencing year over year reductions in 2011.

These reduced costs should not lure organizations into a false sense of security. As our results continue to show, attacks are increasingly focused, with hackers targeting information that can be monetized or used for political and ideological gains.

The measured costs associated with dealing with security breaches have come down – organizations are far more equipped to keep out nuisance malware and are more effective in dealing with such attacks once they happen. The data suggests that protection technologies are more effective, and that as a whole, the ability of Canadian organizations to contain detected breaches has improved. As a result, the costs associated with such attacks are way down.

Annual Costs of Breaches				
	Overall	Public	Private	Government
2011	\$82,903	\$195,588	\$70,833	\$58,929
2010	\$179,508	\$337,930	\$119,865	\$80,910
2009	\$834,149	\$675,132	\$807,310	\$1,004,799
2008	\$423,469	\$637,500	\$293,750	\$321,429

In contrast, the *unmeasured* costs of breaches continue to rise both for the organization breached and for its customers and partner organizations: costs borne by banks regarding credit card theft, by the customer as it relates to identity theft and by the company vis-à-vis loss of intellectual property. This trend of falling measured costs with rising unmeasured costs can be attributed to the externalization of financial impacts to third parties, which alters the dynamics of accountability in the event of a breach event.

## COMPLEXITY AND RISK

### Complexity in the Environment Increases Risks

As organizations build a larger IT footprint and acquire more servers and platforms to support their businesses, security demands increase accordingly and complexity becomes an issue. With increasing complexity in IT environments comes increasing risks: 100 per cent of reported losses above one million dollars happened in medium (40 per cent) or high-complexity environments (60 per cent). At the same time, only six per cent of respondents claiming zero losses manage very high complexity infrastructures. We can also see in the table below how complexity can be correlated strongly with losses as a result of data breaches.

Average Losses	
Complexity of IT Environment	Average Annual Loss
Very Low	\$31,451.79
Low	\$57,954.77
Medium	\$69,708.22
High	\$144,444.53
Very High	\$169,047.76

Complexity introduces risk. This 'law' in IT risk management is reflected in the average number of breaches suffered by organizations in different complexity ranges, with the number increasing dramatically for very complex IT security environments.

Average Breaches	
Complexity of IT Environment	Average Number of Breaches in the Past 12 Months
Very Low	3.88
Low	3.34
Medium	7.45
High	9.58
Very High	26.96

### Government Managing Highly Complex Environments

Privately-owned companies in Canada are doing a good job of managing the complexity in their IT environments, with an average of six per cent of the IT budget dedicated to information security. Private companies also report the highest satisfaction levels between sectors (for High and Very High levels: [62 per cent Private], [60 per cent Public], [52 per cent Gov]). Public companies are reporting a balanced distribution between medium and high/very high levels of complexity, as expected – very few publicly traded companies can afford to operate in a low-complexity environment.

How Complex is your IT Security Environment (By Number of Servers)?			
Complexity of IT environment	Publicly traded company	Private company	Government
Low, Very Low	7%	35%	10%
Medium	49%	45%	30%
High, Very High	44%	20%	59%

Government reports the highest complexity in its IT infrastructure, but also responds with much more confidence, highlighting technology as a key point of strength in the 'People/Process/Technology' comparative question of the study.

### Outsourcing is Becoming Prevalent in High-Complexity Environments

Outsourcing to a third party remains an important economic driver affecting security decisions in

IT environments with a high degree of complexity reported 26 breaches in the past 12 months compared to three breaches for much more simple environments.

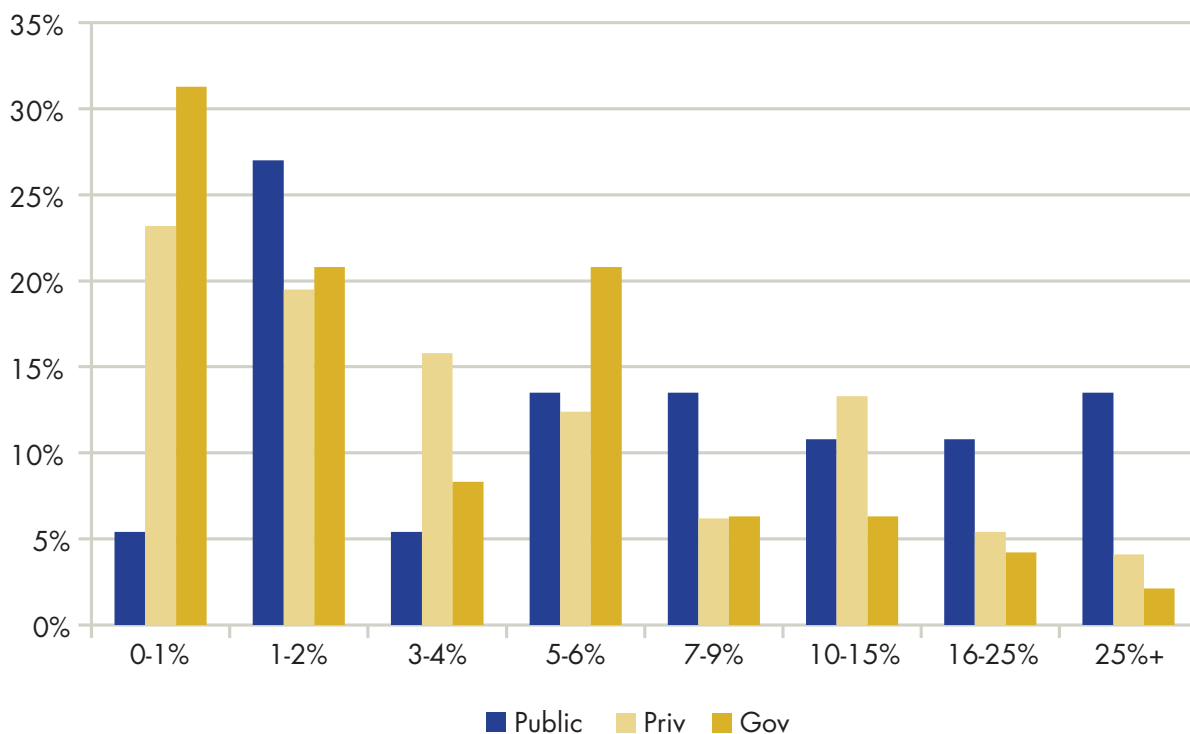
most organizations. When we compare complexity levels with the decision to outsource and how much organizations should be outsourcing, a few observations emerged. More than 50 per cent of respondents across all levels of complexity outsource some IT security capabilities (less complex environments outsource less), and half of high-complexity environments have outsourced up to 20 per cent of their security capabilities. Outsourcing the management of certain IT services to an expert third party is adopted widely as a technique to reduce costs and headcount needs, with the indirect benefit of reducing complexity.

Percentage of Security Capabilities Outsourced					
Complexity of IT Environment	None	1-20%	21-40%	41-60%	61%+
Low, Very Low	42%	35%	7%	5%	12%
Medium	28%	48%	12%	6%	5%
High, Very High	27%	52%	12%	5%	5%

### Budgets Increasing for Public Companies

We have seen IT security budgets fluctuate since the financial crisis. What is of note is that government budgets have seen the smallest variations but remain lower than those in both the public and private sectors. What is also of interest is the continued growth in the number of security breaches in public

## Share of IT Budget allocated IT Security, per Sector



companies, which have been accompanied by increased budgets in that sector. It is likely the case that these investments are a reaction to the breaches and the challenges posed by the increasing complexity of these environments.

In contrast, the proportion of organizations reporting IT security budget allotments of more than 10 per cent of the IT budget is highest for public organizations and smallest for government organizations, with private companies presenting a more balanced distribution of budget allocation.

Share of IT Budget Allocated to Security, Averages

	Overall	Public	Private	Government
2009	6.81%	8.16%	6.79%	5.69%
2010	6.44%	6.78%	7.35%	4.41%
2011	6.13%	9.39%	5.95%	4.56%

More than 30 per cent of government organizations responding in 2011 indicated that their IT security budget is between zero and one per cent of their IT budget, which compares to less than 25 per cent of private organizations and only five per cent of public organizations.

## MOBILE TECHNOLOGIES

### A Business Opportunity and a Security Threat

The vast majority of organizations in Canada embraced mobile technologies such as smartphones several years ago as a way to increase productivity and employee collaboration. The next step, as seen in the past two to three years, has been the introduction of tablets and personal mobile devices in the business environment, changing the dynamics and perceptions around IT security significantly. In many environments, personal smartphones and tablets are simply not allowed, as the IT organization does not have the means to monitor them and enforce policies as they would on corporate laptops and desktops. In some environments, organizational cultures, along with IT, are starting to accept personal smartphones and tablets – a practice described as “bring your own device” (BYOD).

Most business leaders would agree that there are many benefits for introducing these devices. First, users simply like using them, elevating morale. Second, the organization already supplies a computer (laptop or desktop) and a corporate smartphone, and users become confused between using the corporate device or their personal device in different circumstances and usually chose whatever is convenient. Handling one device is simpler and, again, more convenient and perhaps less expensive as users pay for their own smartphone. Finally, tablets are starting to replace laptops in many scenarios, sometimes with a positive trade-off between less computing power for more mobility and flexibility.

Although business leaders may see these benefits, security professionals are still tasked with protecting the company’s data, and introducing a new platform that is not always managed or owned by them may pose a new set of challenges. We have asked security professionals how they perceive the

Mobile technology is seen as both an opportunity and a threat by 80% of senior management.

introduction of these devices in their organizations, with three possible answers: business opportunity, security threat or both.

View Proliferation of Mobile Devices, Tablets	Government	Private Company	Publicly Traded Company
An opportunity	13%	38%	29%
A threat	7%	6%	7%
Both	80%	56%	64%

The majority of security professionals in Canada recognize both aspects, while a significant number see the opportunity with no threat (especially in private firms), and only a small minority recognizes a threat with no real opportunity.

### Loss of a Device is the Primary Concern

When there is a perceived threat, most respondents are concerned about the loss of a mobile device carrying unprotected business information. With 22 per cent of organizations reporting lost mobile devices (see Breaches above - the second most common type of security incident), this represents a legitimate concern.

A silver lining exists in the fact that technologies enabling the remote blocking, wiping or encryption of mobile devices are becoming available in the market. Other concerns are linked to the integration of mobile devices within the existing IT infrastructure,

such as controlling access points, managing the risk of information leakages and new application ecosystems (such as unsafe applications downloaded from the online store).

Devices contain corporate data and may get lost	40%
Devices are yet another entry point into our network	26%
Enables increased information leakage or near-real-time disclosure of company information	17%
Devices are hard to integrate into our existing security technologies and operations	15%
We do not trust the security management of the application ecosystem	10%
Physical security concerns related to location based services	9%

## SOCIAL NETWORKING

### One in Four do not Have Policies Governing Social Networking

While 25 per cent of organizations surveyed do not have any articulated policy to guide the use of social networking (LinkedIn or Facebook) in the workplace, those who do communicate the policy to staff as a business decision (91 per cent). This dialogue between management and staff illustrates how the prevalence of social networking in our personal lives is spilling into the workplace. Management clearly views establishing a use policy as critical to the safe adoption of social networking by employees in the workplace. One in three organizations in Canada decided to have regular communications with staff on this matter, reflecting the importance on the proper use of social networking in a business context.

Approach to Communicate Decisions Regarding Social Networking	
We have not provided communications to employees on the policy	9%
We held one in-person or online session, meeting or event to communicate when the policy was first implemented	18%
We provided one email communication when the policy was first implemented	40%
We hold regular in-person, online sessions or email updates as we continue to adapt our policy	32%

### Social Networking Policies are Well Received in 72 Per Cent of Cases

Employees generally have a positive attitude toward social networking policies communicated by management. Three out of four organizations indicate a strong positive response in such cases, and even when the response is not so positive, only five per cent experience significant incidents of non-compliance. This reflects the fact that most employees are willing to comply with a policy as long as they understand what the policy is, what risks it can pose to the organization and the business reasons behind a policy.

### Policy for Social Networking Received by Employees

We have received strong negative feedback regarding our policy from many employees, with many attempts to circumvent our policy	5%
We have received negative feedback regarding our policy from some employees, without many attempts to circumvent our policy	9%
Some employees accepted and follow our policy	14%
The majority of employees accepted and follow our policy	72%

A large number of respondents indicated that employees use social networking on a personal level, perhaps justifying why other companies block it for productivity reasons. The matter is too complex to be analyzed by numbers alone, and organizations should consider questions of culture and work style that best reflect their situations. Those organizations investing in their own social networking presence should be cautious about blocking their staff from accessing social networks, as it may seem contradictory to the proposed brand value of being in the social space.

Majority of employees are willing to comply with a policy as long as they understand what the policy is, what risks it can pose to the organization and the business reasons behind a policy.

with senior security executives (a video of these roundtable discussions is available on [www.telustalksbusiness.com](http://www.telustalksbusiness.com)), is that most organizations do not monitor 100 per cent of the possible channels used to access social networking websites. When an organization only blocks a social

### Approach to Dealing with Social Networking (more than one answer possible)

	Government	Private	Public	Overall
Employees use for personal purposes	26%	39%	26%	35%
Employees use for professional purposes	29%	34%	19%	31%
Employees use to engage customers	14%	21%	13%	19%
We block access to social networking for security reasons	24%	14%	19%	16%
We block access to social networking for productivity reasons	22%	15%	15%	16%
We block access to social networking to protect our brand	10%	4%	10%	6%

### Blocking Social Networking for Security Reasons: Still not Working

Last year we found a significant negative correlation between organizations blocking access to social networking for security reasons and the number of breaches experienced in past 12 months. The reason, confirmed in subsequent interviews and discussions

site partially, for example, via the corporate web browser, the user may feel encouraged to use an alternate method, such as a smartphone or tablet to access the site. In such cases, the policy is actually *forcing* users to access non-trusted sites, using a technology that is not monitored or controlled by the enterprise security program.

In 2011, we re-tested and confirmed this phenomenon.

Block Social Networking for Security Reasons (Yes)	10.3 incidents in last 12 months (average)
Block Social Networking for Security Reasons (No)	7.2 incidents in last 12 months (average)

## SATISFACTION WITH SECURITY POSTURE

### Two out of three Canadian Organizations Satisfied with Security Posture

In the past, the results of our analysis were clear in indicating that satisfaction with IT security was not correlated to bigger budgets, meaning that satisfaction was not just about spending. Further, we found inflection points – organizations indicated an optimum level of satisfaction when allocating approximately five to seven per cent of the budget to IT security. Satisfaction increased again with a 10 per cent allocation. In describing top performers, we demonstrate that there are several aspects of an optimal IT security strategy beyond spending that include strong governance, education, awareness and other ‘soft’ factors.

Satisfaction with Security Posture			
Percentage of IT budget spent on security	Dissatisfied, Very dissatisfied	Neutral	Satisfied, Very satisfied
4% or less	19%	33%	48%
5%-6%	9%	24%	67%
7%-9%	9%	30%	61%
10% or more	6%	11%	83%

It is clear that moving from a security budget which is less than five per cent of the IT budget to one that is in the five to six per cent range results in a significant increase in satisfaction levels. In contrast, moving into the seven to nine per cent range does

not yield a significant increase. The average budget allocation in Canada is 6.13 per cent, suggesting that approximately 91 per cent of respondents have a neutral or positive perception of their security posture, with two out of three having a positive stance.

Satisfaction with Security Posture			
	Dissatisfied, Very dissatisfied	Neutral	Satisfied, Very satisfied
Government	18%	30%	52%
Private company	11%	27%	62%
Publicly traded company	14%	26%	60%

Satisfaction levels, as in previous years, are lower in government agencies than in the corporate sector. Still, 82 per cent of respondents in government have a neutral or positive attitude towards their security posture, and the number is only slightly better in public corporations (86 per cent) and private companies (89 per cent). Considering that the majority of participants across all sectors are satisfied or very satisfied, and that budget allocation has remained stable for government and lowered for private companies, we conclude that Canadian security professionals are finding more efficient ways to manage their budgets and derive value from security dollars.

### Reliance on People, Process and Technology

We now enter into new territory in our multi-year research: the analysis of the relative strengths of People, Process and Technology in security strategy. A comprehensive security strategy must balance these three elements; over-investing in one to the detriment of the others is considered unwise and possibly dangerous. We now test these assumptions and compare the extent to which organizations value

People, Process and Technology. More specifically, we asked organizations to rate on a scale of one to five the extent to which they view each of these pillars as strengths or weaknesses within their IT security.

**Government and Corporations Relying on Technology for Protection**

Government organizations convey strong confidence in the technology pillar, with 57 per cent of respondents considering this a point of strength. At the same time, only 29 per cent of respondents in government agencies consider people as a strong link in their security chain (38 per cent consider this pillar a weakness).

Public companies communicate the same confidence in technology, with 61 per cent marking technology as a critical point of strength. Public companies report the highest level of reliance on people (49 per cent) among all of the three sectors. Private firms have a somewhat balanced distribution, with less reliance on technology and a neutral position in regards to their people.

More than 80% of respondents who are successful in managing risks communicate that all three pillars of information security – People, Process and Technology – are absolutely fundamental to their strategies.

	People			Process			Technology		
	Weakness	Neutral	Strength	Weakness	Neutral	Strength	Weakness	Neutral	Strength
Public	24%	27%	49%	20%	34%	46%	14%	25%	61%
Private	23%	41%	36%	17%	38%	44%	15%	37%	48%
Gov	38%	33%	29%	30%	28%	42%	16%	27%	57%

Organizations that rate any of the three pillars as a point of strength are more than 80 per cent likely to report that they are satisfied with their IT security posture: 81 per cent for people, 83 per cent for process and 80 per cent for technology.

People			
Satisfaction	Significant weakness, Slight disadvantage	Neutral	Significant strength, Slight advantage
Dissatisfied, Very dissatisfied	31%	4%	8%
Neutral	35%	41%	10%
Satisfied, Very satisfied	34%	55%	81%

Process			
Satisfaction	Significant weakness, Slight disadvantage	Neutral	Significant strength, Slight advantage
Dissatisfied, Very dissatisfied	39%	6%	5%
Neutral	40%	43%	12%
Satisfied, Very satisfied	21%	51%	83%

Technology			
Satisfaction	Significant weakness, Slight disadvantage	Neutral	Significant strength, Slight advantage
Dissatisfied, Very dissatisfied	45%	9%	6%
Neutral	34%	47%	14%
Satisfied, Very satisfied	21%	44%	80%

The other extreme is also of interest: when each of these three pillars is viewed as a weakness. Only 34 per cent of organizations reporting people as a weakness indicate that they are satisfied with their security posture. This is significantly higher than the 21 per cent who indicated process and technology as weaknesses. We can conclude here that a lack of satisfaction with people can be overcome far more easily than when process and technology are weaknesses. To that end, gaps in people-related areas of information security are best addressed by education and awareness.

### Education and Awareness as Key Enablers of Strong Security

The importance of education and awareness in security management is one of the main conclusions that has emerged consistently from our studies. That is, even in the presence of effective technology and process, employees that lack education in security practices or are unaware of risks can expose the company to risks inadvertently resulting in a greater possibility of breaches. As such, awareness training is critically important. In the following table, we consider the relationship between the frequency of awareness training and the extent to which an organization indicates that they are satisfied with their IT security posture.

Frequency of Awareness Training				
	Never	Upon hiring only	Up to once a year	Quarterly or more
Dissatisfied, Very dissatisfied	51%	8%	25%	16%
Neutral	27%	18%	36%	19%
Satisfied, Very satisfied	16%	15%	37%	32%

The results show that *not* delivering awareness training and education has a clear impact on satisfaction with the security posture. More than half of dissatisfied respondents never receive any training. In sharp contrast, the majority of satisfied respondents benefit from regular training.

### Security in Application Development Correlated Strongly to Satisfaction

Those organizations that are ranked highest in terms of their IT security satisfaction and performance all integrate security into the application development lifecycle. Often organizations do not plan for or architect good security into their applications and just hope that good security outcomes will emerge. As the results below show, low satisfaction with the security posture is nearly three times more likely when there is lack of security in the development life cycle.

Satisfaction with Security Posture	Security is Not a Part of our Development Lifecycle Practices
Dissatisfied, Very dissatisfied	32%
Neutral	21%
Satisfied, Very satisfied	11%

## TALENT AND COMPENSATION

Last year, we detected a trend in salaries, in which senior management (Director titles and above) were earning more than in the previous year, while managers and frontline staff were earning less. This year, we have seen a similar trend, except that the dividing line moved upwards: only CIOs and Vice Presidents involved in information security are reporting higher earnings than in 2010, while all other positions are now reporting lower compensation packages.

Title	2010 Overall	2011 Overall
CIO	\$141,999	\$165,000
VP IT/Security/Risk	\$97,500	\$122,166
CISO/CSO	\$115,950	\$115,000
Director	\$113,940	\$103,062
Manager	\$101,535	\$83,011
Security Analyst/ Consultant/Auditor/ System Administrator	\$94,408	\$87,479

Our note of caution from 2010 still stands – while it is important to attract the best talent for strategic positions and compensate properly, execution of the security strategy and tactical implementation of projects and initiatives is critical to the success of a security strategy.

Salaries for executive positions (CIO and VP) are similar between government and private firms, while public companies report higher compensation for

While it is important to attract the best talent for strategic positions and compensate properly, execution of the security strategy and tactical implementation of projects and initiatives is critical.

those roles. Government agencies tend to employ more security-savvy CIOs than other sectors, while public companies fill a CISO or CSO position with that level of seniority. The difference in salaries for CISOs between these sectors is negligible.

Directors, managers and security staff tend to have similar levels of experience, with slightly more seniority in government agencies. While the government employs more experienced professionals in general, the highest earnings are found within public companies. This creates the risk of talent leakage from our government agencies into the corporate sector. The government sector could be facing significant challenges in the event of talent churn in light of this year's findings around IT security complexity. With the most highly complex security environments, government faces a higher level of risk, and cannot afford to be losing security professionals skilled in both the strategic and execution aspects of risk management.

Title	Overall	Government	Private	Public
CIO	\$165,000	\$150,000	\$155,000	\$200,000+
VP IT/Security/Risk	\$122,166	N/A	\$110,900	\$136,250
CISO/CSO	\$115,000	\$111,666	\$130,000	\$110,000
Director	\$103,062	\$117,272	\$93,224	\$139,999
Manager	\$83,011	\$94,933	\$74,516	\$109,333
Security Analyst/Consultant/Auditor/System Administrator	\$87,479	\$87,043	\$87,565	\$90,357

Title	Experience (Years) in Security		
	Government	Private	Public
CIO	12.5	10.0	5.0
VP IT/Security/Risk	N/A	9.5	6.9
CISO/CSO	6.5	8.0	12.5
Director	7.9	6.6	6.0
Manager	7.3	6.7	6.2
Security Analyst/ Consultant/Auditor/ System Administrator	7.7	7.8	7.8

### Security Headcount Keeps Shrinking, Average Security Team now at Three

In 2010, we reported that organizations were much more likely (50 per cent) to report teams of one to five full-time employees (FTE) and much less likely (12 per cent) to report team sizes of six to 10 FTEs. The greater use of outsourcing in the previous year (2009) kept staff temporarily to oversee transitions, and once those transitions were complete, those staff were either redeployed or reduced.

Average Headcount Dedicated to Security				
	Overall	Private Companies	Government	Public Companies
2011	2.9	2.1	4.8	6.5
2010	4.9	3.6	5.3	7.1
2009	8.3	5.9	6.9	16.4

This year respondents have reported even lower staffing numbers, with three out of four respondents in government reporting less than five FTEs dedicated to information security. This number is 87 per cent

in private companies and 58 per cent in public organizations. Some respondents reported zero resources dedicated to protect sensitive data (17 per cent in government, 43 per cent in privately-owned companies and 14 per cent in publicly traded companies). In these cases, the security and risk management functions are carried out by IT and other groups as part of their mandates.

Apparently the austerity measures taken by many organizations in terms of hiring freezes and staff reductions persisted even after the worst of the downturn passed, with many security teams learning how to deliver more with less, in addition to some level of outsourcing of security operations. A detailed look at industry sectors in Canada shows that the Utilities, Financial and Technology sectors invest more heavily in human capital within IT security.

Industry Sector	Average IT Security Headcount
Utilities	10.0
Finance Services and Insurance	7.0
Information Technology and related services	6.8
Educational Services	5.6
Professional, Scientific, and Technical Services	5.6
Health Care and Social Assistance	4.1
Information (Publishing, Broadcasting, Communications)	3.3
Retail and Wholesale Trade	2.6
Manufacturing	2.1

Transportation and Warehousing	1.6
Mining, Agriculture, Forestry, Fishing and Hunting	1.1
Construction, Real Estate, Rental and Leasing	0.7

Since 2009, we have detected a trend of shrinking team sizes. These professionals are tasked with the design, communication and enforcement of information security and risk management policies within their organizations.

With the cost of breaches going down, a strong satisfaction with the security policy and the number of insider breaches also decreasing (except in government), it seems that these teams are successful in meeting their goals. There are two main obstacles hindering these professionals – one technical and one behavioural. Technically, attacks are becoming more sophisticated (as discussed in the Breaches section of this paper) and security infrastructures are becoming more complex. Behaviourally, management and staff are violating security policies in general, and the introduction of social networking and mobile devices further complicates and intensifies the incidences of those violations.

## CONCLUSIONS

### Breaches Splitting into Low-Level Security ‘Noise’ and Deeply Targeted Attacks

Breach numbers decreased from 2010, except in publicly traded companies. Organizations are adapting and becoming better at managing security incidents, which is reducing overall breach costs. The direct costs associated with breaches, for all organization types, also lessened from 2010 levels. In many cases, the perception of what a breach really means is shifting, with some basic types of incidents being transferred to IT operations to handle, along with other system performance roles. The security function is left with the sophisticated and targeted attacks – those focusing on the human element including phishing and social engineering, which can exploit the data available on social networking sites. TELUS Security Labs researchers have also observed this trend, finding that one third of malware has targeted financial data. And our forensic investigations group reports that more than 50 per cent of cases investigated in the past 12 months are related directly to targeted and personalized attacks on specific individuals. These incidents are much more challenging to handle by victim organizations, and cost quantification becomes less clear.

### Balanced Budgets Beat Big Budgets

In the past four years, security budgets have decreased consistently as a result of the 2008 financial crisis and persisting austerity measures that affect resource allocation. Operating in this type of environment, practitioners have learned to deliver more value with fewer dollars, as we have seen from high satisfaction levels and lower breach numbers. Security executives are more efficient in managing investments in IT controls, with more than 90 per cent of respondents reporting acceptable satisfaction with a security budget that is five to six per cent of the overall IT budget.

Security dollars are better spent on integrating security in the development life cycle of information systems and education and training for management staff. With all sectors indicating a strong reliance on technology in security management, it is time to focus on human behaviour – more risk awareness in general and when using social networking/mobile computing as well as motivating senior executives to lead by example with security policy adherence.

### **People, Process and Technology Linked Intrinsicly with Success**

More than 80 per cent of respondents who are successful in managing risks communicate that all three pillars of information security – People, Process and Technology – are absolutely fundamental to their strategies. These results are unquestionable and validate the philosophies of in-depth and layered defence against attacks as well as the balancing of strong technical capabilities, intelligent risk decisions and the right level of processes and procedures in the workplace.

This finding is relevant beyond the theoretical point. Managers in business are advised to consider carefully how they invest in each pillar, the current and desired levels of maturity and process formality within their organizations, the number and frequency of team education sessions and what should be communicated in their security policies. These are critical decisions that can make security an enabler or an obstacle when pursuing the business' goals.

### **Employees are Prepared to Embrace Social Networking, if Management is Ready to Guide Them**

When a decision governing the usage of social networking in the workplace is made and communicated to staff, 72 per cent of respondents indicated a positive reaction with acceptance and compliance. Social networking is a well-established trend in our society at large. The only decision

the business can make is to embrace it or attempt to block access. Although there may be several reasons to block, security is not a very effective one. Organizations attempting to block access to social networking for security reasons are facing more breaches than those that don't, showing that proper dialogue with employees will yield more results than enforcing a technical embargo.

### **The Complexity of IT Environments Presents a Critical Challenge**

A large number of organizations are reporting high levels of complexity within their IT environments, led by government entities. This complexity is justified by the emergence of new technologies such as Identity and Access Management solutions, mobile technologies and mobile security management, web application and next generation firewalls and new developments in email and database encryption.

Although many of these technologies present benefits in terms of risk mitigation in their individual areas, when viewed in aggregate, they introduce a new level of complexity into the security environment. The paradox is that complexity reduces manageability and exposes organizations to new risks – proven by the number of breaches increasing dramatically in highly complex environments.

When security headcount remains the same (or lessens) while new technologies are introduced, challenges are bound to arise. Team performance and morale are affected, and the value derived from technology investments degrades. For this reason, security technologies that require less headcount for management and deliver value are marked with the highest levels of satisfaction among respondents. We saw this trend in 2010, and it continues into 2011.

## **Mobile Technologies Present a Huge Opportunity, with Immediate Risks to be Managed**

Canadian security professionals acknowledge the business opportunity presented by new mobile technologies including smartphones and tablets, and they are ready to embrace them. At the same time, many recognize that as a new technology, considerations around risk management and the secure integration with existing systems must be weighted.

The loss of mobile devices with business information was the primary security concern (as well as one of the primary causes of data breaches in 2011), followed by a number of integration and data leakage questions. Still, one in three respondents in Canada consider them a new opportunity with no associated material threats, considering mobile devices as a new entry point into their infrastructure that must be managed properly like any other.

## **FINAL REMARKS**

Our research process captures the cumulative knowledge of security practitioners in Canada (more than 600 in 2011 and more than 2,000 since 2008). The aggregate information, or collective wisdom, shared by the security community during the years offers critical perspectives that are essential to managers making security and risk decisions. Security leaders have a reliable starting point and an evolving discourse from which they can examine and analyse their environments, investments and strategies based on uniquely Canadian insights and trends.

### **The Relevance of Canadian-Specific Research**

When TELUS and the Rotman School of Management embarked on this joint effort in 2008, there was a significant void in Canada regarding the state of IT

security. Studies available at that time were U.S. or globally focused. As a result, Canadian IT security managers were forced to make decisions based on insights that were not linked directly to the Canadian environment, but rather to environments in other countries. In using non-Canadian studies, IT managers had to assume implicitly that Canada's risk profile, preparedness and governance structures were the same as in other countries, particularly the U.S.

At the time, there were many reasons to expect that the Canadian environment would have unique characteristics, and more specifically would differ in many ways from that in the U.S. For example, the U.S. has a much larger private sector role in Health Care relative to Canada. The U.S. has thousands of banks, whereas the Canadian market is dominated by the Big Six Banks. Regulations and compliance requirements are also very different in the two countries. As such, risk profiles and preparedness would likely be very different. Furthermore, given differences in reporting requirements, reported breaches and actual breaches would be very different, as would the associated costs. Our analysis has confirmed our instincts, showing that Canada is not the same as the U.S. In fact, the differences are abundant.

When IT managers make decisions based on non-Canadian data, which is not an accurate reflection of the Canadian landscape, the strategies deployed and outcomes achieved are sub-optimal. Furthermore, as the threat environment and preparedness change through time, vulnerabilities can emerge, and only with clarity on the state of the Canadian environment can optimal proactive strategies be deployed.

## APPENDIX A – SURVEY QUESTIONS AND RESPONSES

1. What is the ownership/legal structure of your organization?

Government	14.79%
Private company	65.02%
Publicly traded company	14.02%

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

Information (publishing, broadcasting, communications)	4.41%
Information Technology and related services	26.68%
Finance Services and Insurance	8.25%
Professional, Scientific, and Technical Services	6.14%
Government	6.72%
Educational Services, Services densenement	6.14%
Health Care and Social Assistance	4.80%
Retail and Wholesale Trade	6.91%
Manufacturing	6.14%
Utilities	2.88%
Transportation and Warehousing	2.30%
Mining, Agriculture, Forestry, Fishing and Hunting	1.92%
Construction, Real Estate, Rental and Leasing	5.57%
Other	11.13%
Utilities	2.47%

3. How many employees does your organization have?

1-49	44.88%
50-249	12.42%
250-499	4.66%
500-749	5.43%
1,000-2,499	7.30%
2,500-4,999	3.42%
5,000-9,999	4.97%
10,000-19,999	4.81%

20,000-49,999	4.66%
50,000 or more	3.57%
Don't Know	1.24%

4. What was your organization's annual revenue last year? (If government organization, please choose your organization's total budget)

< \$1 million	33.53%
\$1 million-\$24 million	20.23%
\$25 million-\$99 million	8.09%
\$100 million-\$499 million	7.13%
\$500 million-\$999 million	4.24%
\$1 billion-\$1.99 billion	3.47%
\$2 billion-\$10 billion	5.59%
> \$10 billion	2.70%
Don't Know	15.03%

5. What percentage of your employees uses at least one of the following devices/technologies to access business applications/data: iPhone, iPad, Playbook, Android, tablets, Windows Phone 7

0%	12.47%
1-5%	23.36%
6-10%	12.93%
11-15%	6.58%
16-25%	7.71%
26-50%	7.26%
>50%	23.58%
Don't Know	6.12%

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

Chief Executive Officer	10.34%
Chief Technology Officer	2.76%
Chief Information Officer	0.92%
Chief Security Officer	0.92%
Chief Information Security Officer	0.69%
VP of IT or Security or Risk Management	2.53%
Director	12.87%
Manager	21.61%
Security Analyst, Consultant, Auditor	13.56%
System Administrator	11.26%
Other	22.53%

7. Do you have any formal IT certifications, degrees or diplomas? (Please select all that apply).

CISSP	8.63%
CISM/CRISC	2.77%
CISA	4.31%
Privacy	1.69%
Business Continuity/Disaster Recovery	3.70%
SANS (Systems Administration Networking and Security)	3.85%
Forensics/Incident Response Handling	1.85%
MBA	7.09%
PhD/Doctorate	1.54%
Degree, Computer Science/Engineering	33.28%
Degree, Economics/Finance/Business	13.56%
Degree, not in business or technology	13.56%
Other	30.74%

8. How long have you been employed in an IT security capacity?

< 1 year	19.83%
1-3 years	16.53%
4-6 years	14.05%
7-9 years	11.40%
10 years or more	38.18%

9. How long have you been with your current employer?

< 6 months	4.52%
6 months to 1 year	7.02%
1-3 years	21.84%
4-6 years	17.63%
7-9 years	12.32%
10 years or more	36.66%

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

< \$40,000	10.54%
\$40,000-\$49,999	7.29%
\$50,000-\$59,999	9.15%
\$60,000-\$69,999	8.99%
\$70,000-\$79,999	8.68%
\$80,000-\$89,999	8.22%
\$90,000-\$99,999	6.82%
\$100,000-\$119,999	11.94%
\$120,000-\$139,999	5.58%

\$140,000-\$159,999	3.41%
\$160,000-\$179,999	1.40%
\$180,000-\$199,999	0.47%
\$200,000 or more	1.86%
I prefer not to answer this question	15.66%

11. What information sources do you rely on to keep your security and threat awareness current? (Please select all that apply).

Security vendor feeds	59.58%
Social media (such as blogs, Twitter, LinkedIn)	39.08%
Free alerting and advisory services	43.87%
Conferences and events	41%
Paid subscriptions to alerts, advisories and threat details	31.42%
Internal mailing/knowledge base	41.38%

12. Which statement below best describes your approach to updating your security infrastructure?

We respond only to known security incidents in our environment	18.16%
We wait for security related content from our technology vendors	27.93%
We solicit special security related content from our technology vendors	14.26%
We occasionally seek specialized security related content from third party security organizations	20.90%
We subscribe to specialized security related content from third party security organizations	18.75%

13. Which of the following best describes your process to monitor and act on new threat information?

We don't actively monitor for new threats	17.50%
We occasionally review new threat information but rarely act	18.27%
We monitor for new threat information and routinely act	45.00%
We have a rigorous procedure to review and act on new threat information	19.23%

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

0 FTEs	34.89%
--------	--------

1 FTE	28.72%
2-4 FTEs	18.09%
5-10 FTEs	7.45%
11-25 FTEs	4.47%
26-50 FTEs	2.13%
>50 FTEs	4.26%

15. Which of the following C-level executives (or equivalent in government) does your organization have? (Please select all that apply.)

Chief Security Officer (CSO) or Chief Information Security Officer (CISO)	25.86%
Chief Risk Officer (CRO)	10.54%
Chief Compliance Officer (CRO)	11.88%
Chief Privacy Officer (CPO)	12.26%
None	62.84%

16. Which of the following functions do you currently outsource? (Please select all that apply).

Security program development/management	16.48%
Management of firewalls/VPN/IPS/email and web security	23.56%
Management of web application firewalls	19.96%
Monitoring of security events (log Management/SIEM)	15.71%
Management of endpoint antivirus	15.90%
Management of servers/applications security	16.67%
Security testing of networks and infrastructure	21.46%
Vulnerability management	12.45%
Testing of software and applications (including web)	19.35%
Security awareness training	11.30%
IT audit	23.56%
Identity management and authentication	7.66%

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

Very dissatisfied	5.17%
Dissatisfied	7.85%
Neutral	25.86%
Satisfied	35.63%
Very satisfied	20.31%
Not Sure/Don't Know	5.17%

18. How would you rate your organizations security performance across the following three dimensions:

	People	Processes	Technology
Significant weakness	8.85%	6.56%	3.69%
Slight disadvantage	17.50%	14.09%	11.65%
Neutral	37.31%	35.91%	34.37%
Slight advantage	22.50%	31.27%	34.95%
Significant strength	13.85%	12.16%	15.34%

19. Considering your IT security environment, staffing, budget, and mandate, how would you rate the overall complexity in your IT environment?

Very Low	9.83%
Low	17.53%
Medium	42.20%
High	21.58%
Very High	8.86%

20. How many security devices, appliances or management servers does your organization have in its environment?

0	8.01%
1-5	44.34%
6-10	15.82%
11-25	9.57%
26-50	7.23%
50-100	4.88%
100-499	4.10%
500 or more	6.05%

21. How many staff in your organization are assigned to managing your security devices (including full time employees and contractors)?

0	13.87%
1-5	63.87%
6-10	7.42%
11-25	3.71%
16-25	2.73%
26-50	2.54%
50 or more	5.86%

22. How concerned is your organization about each of the following issues? Please rate level of concern on a scale of 1 to 5.

	1 - Least Concerned	2	3	4	5 - Most Concerned
Managing risks from third parties (i.e. business partners, suppliers and collaborators)	15.28%	15.28%	29.44%	26.07%	13.93%
Managing security of new mobile technologies	11.46%	13.26%	27.42%	31.24%	16.63%
Managing security of new social networking technologies	10.61%	12.87%	27.77%	33.63%	15.12%
Disclosure/loss of strategic or sensitive data	4.50%	6.08%	20.95%	29.28%	39.19%
Compliance with regulations and legislation	8.45%	10.05%	25.80%	23.74%	31.96%
Understanding and accountability of user actions and access	5.43%	12.44%	28.96%	33.94%	19.23%

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

	Not Interested	Evaluating	Planning	Deploying	In place
Security awareness program for employees/contractors	19.20%	20.09%	16.96%	8.04%	35.71%
Linking general IT staff performance evaluations to security objectives	36.12%	20.99%	17.83%	7.22%	17.83%
Creating business-level security metrics	24.26%	21.32%	23.13%	9.30%	22.00%
Requiring suppliers, business partners or other third parties to agree to organization's security/privacy policy	23.09%	18.83%	14.35%	9.64%	34.08%
Integration of security into software/application development	20.00%	18.43%	20.22%	13.71%	27.64%
Criminal background checks for all staff	29.55%	14.32%	10.91%	6.82%	38.41%
Creating security and privacy policies	10.66%	14.51%	15.87%	12.24%	46.71%
Creating a vulnerability management program	20.14%	24.89%	18.55%	10.41%	26.02%
Implementing a strategy or policy for security of virtualized and cloud-based applications or infrastructure	26.35%	25.90%	19.14%	9.91%	18.69%
Monitoring or auditing usage of social media	24.38%	24.15%	18.74%	9.48%	23.25%
Conducting regular risk assessment exercises	21.54%	23.36%	18.82%	7.94%	28.34%
Implementing a strategy or policy addressing data loss prevention	14.55%	20.00%	20.45%	11.82%	33.18%
Implementing a strategy or policy for securing new mobile technologies (e.g. iPad, Playbook, Android, tablets, Windows Phone 7, BlackBerry)	17.69%	26.53%	24.49%	12.70%	18.59%

24. Please rate the following challenges, on a scale of 1 to 5, that your organization faces when trying to deliver on security objectives:

	1 - Trivial	2	3	4	5 - Significant Challenge
Lack of resources or funding	10.49%	11.16%	24.11%	25.22%	29.02%
Insufficient support from the business or senior management	19.86%	18.74%	29.80%	18.06%	13.54%
Lack of awareness from employees	12.58%	17.30%	34.38%	21.35%	14.38%
Constrained timelines	12.02%	16.33%	31.75%	25.17%	14.74%
Unclear or conflicting objectives or approach	17.35%	18.95%	34.47%	18.49%	10.73%
A compliance-only focus	21.04%	19.00%	35.07%	14.03%	10.86%

25. On a scale of 1 to 5, how would you rate the following attributes of your security environment?

	Very Low	Low	Neutral	High	Very high
Risk Management Capability (Budget, awareness, resources, etc.) (1 is very low, insufficient, 3 is neutral 5 is very high, proficient)	13.42%	12.75%	43.18%	21.48%	9.17%
Compliance Mandate (Number of, complexity and stringency of regulatory requirements that apply to your organization) (1 is none or simple, 3 is neutral, 5 is very high or stringent)	22.47%	11.69%	38.65%	13.26%	13.93%
Threat Landscape (Sensitivity of business data, exposure to threats, etc.) (1 is very low, little exposure, 3 is neutral 5 is very high, actively targeted)	24.94%	13.26%	37.53%	14.83%	9.44%

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

<1%	17.46%
1%-2%	16.33%
3%-4%	10.43%
5%-6%	11.79%
7%-9%	5.67%
10% -15%	9.75%
16%-25%	4.54%
> 25%	3.63%
Don't Know	20.41%

29. How often does your organization conduct security awareness training for employees and other stakeholders (both inside and outside IT)

Never	22.15%
Upon hiring only	13.70%
Less than once per year	11.87%
Once per year	21.00%
Once a quarter	13.01%
Once a month	6.16%
More frequently than monthly	5.25%
Don't Know	6.85%

27. How important are the following in driving your organization's IT security investment?

	1 - Least Important	2	3	4	5 - Most Important
Legislation/regulations	19.59%	10.83%	23.04%	22.12%	24.42%
Security breaches that have occurred in our organization	13.82%	16.13%	24.88%	20.05%	25.12%
Security breaches that have occurred at competitor, client, supplier or affiliate organizations	16.20%	21.76%	26.85%	23.84%	11.34%
Increased concern over potential losses or activities by employees such as use of wireless devices, remote access, social networking, etc.	10.85%	12.70%	28.41%	30.02%	18.01%
Customers/shareholders/stakeholders demanding better IT/information security from us	17.78%	17.32%	26.79%	20.79%	17.32%

28. Please allocate portions of your security budget against the following areas:

Education and training	20.25%
Technology/infrastructure/systems/licenses	37.51%
Staff/permanent contractors	28.97%
External services (managed services, ethical hackers, IT	16.49%

30. Which group within your organization violates your security policies the most? Please select one:

Administrative staff	13.51%
Contractors, external consultants, partners or agencies	17.54%
Executives	19.43%
Information Technology	8.29%
Management	14.93%

Marketing	5.21%
Operations/Manufacturing	7.11%
Sales	13.98%

31. Please estimate what percentage of security breaches come from insiders in your organization:

None	25.38%
Up to 5%	15.29%
6-10%	8.87%
11-20%	4.28%
21-40%	4.59%
41-60%	4.89%
61-80%	7.03%
81-100%	7.95%
Don't Know	21.71%

32. Did your organization experience and identify any of the following types of information security breaches in the past 12 months?

Virus/Worms/Spyware/Malware/Spam	57.09%
Laptop or mobile hardware device theft	27.20%
Financial/online banking fraud	6.51%
Bots (zombies) within the organization	12.45%
Phishing/pharming where your organization was fraudulently described as the sender	25.10%
Denial of service attack	9.20%
Sabotage of data or networks	3.64%
Unauthorized access to information by employees	17.43%
Extortion or blackmail (ransomware)	1.34%
Website defacement	5.75%
Loss of confidential customer/employee data	6.90%
Abuse of wireless network	14.94%
Password sniffing	7.85%
Misuse of a corporate application	6.51%
Theft of proprietary information	4.21%
Identity theft	3.83%
Social engineering attack	6.51%
Exploitation of your domain name server (DNS)	2.30%
Smart phone/phone/tablet device hacked	4.02%
Other	5.94%

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

None	20.00%
1	13.02%
2-5	33.26%
6-11	10.00%
10-25	4.19%
26-50	1.63%
51-100	1.86%
>100	1.86%
Don't Know	14.19%

34. 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?

0\$	35.83%
< \$100,000	33.49%
\$100,000 to \$249,999	3.51%
\$250,000 to \$499,999	3.51%
\$500,000-\$999,999	0.94%
\$1 million-\$2.99 million	1.17%
Don't Know	21.55%

35. What role does security play in your infrastructure/ systems development or acquisition? (Please select all that apply).

Security starts with the requirements/design phase	36.97%
Security is tested prior to production deployment	31.80%
Security is tested post production deployment	22.41%
We rely on the vendor or integrator to provide us with secure systems	24.90%
Security is not yet part of our development lifecycle practices	17.05%

36. Managing the vulnerability life cycle, the process that starts with vulnerability detection and concludes with remediation, is a challenge for many organizations. Please evaluate your organizations average time to address each stage of the vulnerability life cycle:

	Don't Know	One week or less	More than one week but less than a month	One to three months	More than three months
Decide on an appropriate fix for a discovered vulnerability	12.03%	43.40%	24.53%	15.80%	4.25%
Engage the business to get approval for the change	13.81%	25.00%	6.43%	16.67%	38.10%
Implement the selected fix for a discovered vulnerability	12.29%	26.00%	7.09%	17.02%	37.59%
Retest to confirm the vulnerability has been correctly fixed	15.95%	22.14%	7.86%	12.86%	41.19%

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

None	26.90%
1-20%	37.14%
21-40%	9.05%
41-60%	4.29%
61-80%	1.43%
>80%	4.05%
Don't Know	17.14%

38. When working with security vendors or partners, please rate the major frustrations your organization has experienced on a scale of 1 to 5.

	1 - Non-issue	2	3	4	5 - Critical challenge
Value received does not match my investment	30.41%	13.14%	31.39%	16.30%	8.76%
Business requirements are not clearly articulated or understood	27.21%	19.61%	27.94%	18.63%	6.62%
Too many points of coordination or decision makers	34.72%	15.16%	28.12%	15.65%	6.36%
Poor communications during project execution or delivery	30.73%	17.56%	28.78%	16.34%	6.59%
Consensus is not formed around project outcomes	33.01%	17.60%	32.52%	11.25%	5.62%
Projects are over budget or over time	32.51%	16.26%	28.33%	11.82%	11.08%

39. For the specific technologies you currently use, how satisfied are you with their effectiveness?

	1 - Least satisfied	2	3	4	5 - Most satisfied
IPSEC based VPN	6.45%	7.10%	39.03%	28.06%	19.35%
SSL VPN	5.33%	8.46%	31.97%	31.03%	23.20%
Anti-Virus (on the desktop or servers)	4.30%	8.35%	27.59%	34.94%	24.81%
Email Security (anti-spam, anti-malware)	3.85%	7.69%	26.92%	35.38%	26.15%
Storage/Hard Disk Encryption	5.52%	11.63%	34.59%	25.58%	22.67%
Email Encryption	10.06%	16.35%	32.70%	24.21%	16.67%
Database Encryption	8.79%	14.98%	33.88%	25.08%	17.26%

	1 - Least satisfied	2	3	4	5 - Most satisfied
URL/Content Filtering	6.71%	13.72%	34.76%	26.52%	18.29%
Identity and Access Management (including PKI)	7.77%	13.85%	39.53%	23.99%	14.86%
Network based Access Control (NAC via network)	12.29%	11.60%	37.20%	25.26%	13.65%
Endpoint Security (NAC via desktop)	11.50%	12.89%	37.28%	24.74%	13.59%
Firewalls	2.35%	6.79%	22.98%	38.64%	29.24%
Web Application Firewalls	5.97%	9.75%	35.53%	29.87%	18.87%
Log Management	9.74%	15.91%	39.29%	20.45%	14.61%
Security Information & Event management (SIEM)	7.53%	16.10%	42.81%	19.18%	14.38%
Network Intrusion Prevention/Detection	7.50%	11.25%	34.69%	27.19%	19.38%
Wireless Intrusion prevention (WIPS)	14.38%	13.73%	37.25%	19.93%	14.71%
Application Security Assessment Tools (web/code)	10.60%	17.31%	43.82%	18.37%	9.89%
Two-factor authentication (tokens, smartcards, biometrics)	8.16%	13.61%	39.80%	21.43%	17.01%
New Mobile devices security (iPhone, iPad, Android, Windows Phone 7, tablets)	17.30%	20.44%	35.53%	19.50%	7.23%
Vulnerability Scanning/Vulnerability Management	8.05%	16.44%	42.28%	21.48%	11.74%
Patch Management	6.83%	12.42%	45.03%	22.05%	13.66%
Data Leakage Prevention	10.42%	14.58%	45.83%	16.32%	12.85%
Next Generation Firewall	9.29%	12.86%	52.14%	16.07%	9.64%

40. What specific technologies will you deploy for IT security in the next 12 months?

	No Deployment	Technical Evaluation	Pilot	Limited Deployment	Full Deployment
IPSEC based VPN	48.33%	10.33%	7.33%	12.00%	22.00%
SSL VPN	39.22%	9.80%	10.78%	11.11%	29.08%
Anti-Virus (on the desktop or servers)	20.61%	9.70%	6.97%	9.09%	53.64%
Email Security (anti-spam, anti-malware)	23.99%	9.35%	7.17%	9.35%	50.16%
Storage/Hard Disk Encryption	33.12%	11.78%	9.87%	16.88%	28.34%
Email Encryption	39.81%	14.42%	9.40%	14.73%	21.63%
Database Encryption	43.23%	10.23%	9.57%	16.50%	20.46%
URL/Content Filtering	36.72%	12.46%	10.16%	13.11%	27.54%
Identity and Access Management (including PKI)	43.52%	12.29%	12.29%	13.62%	18.27%
Network based Access Control (NAC via network)	42.05%	14.90%	13.58%	13.91%	15.56%
Endpoint Security (NAC via desktop)	43.19%	17.28%	12.96%	11.30%	15.28%
Firewalls	23.82%	8.46%	7.84%	9.09%	50.78%
Web Application Firewalls	35.33%	9.67%	11.00%	13.00%	31.00%
Log Management	35.18%	15.96%	11.40%	15.31%	22.15%
Security Information & Event management (SIEM)	42.72%	14.57%	10.93%	16.23%	15.56%
Network Intrusion Prevention/Detection	31.82%	16.56%	12.01%	11.69%	27.92%
Wireless Intrusion prevention (WIPS)	39.27%	16.17%	15.51%	11.22%	17.82%
Application Security Assessment Tools (web/code)	44.33%	13.33%	13.67%	14.67%	14.00%

	No Deployment	Technical Evaluation	Pilot	Limited Deployment	Full Deployment
Two-factor authentication (tokens, smartcards, biometrics)	47.10%	12.26%	14.19%	11.94%	14.52%
New Mobile devices security (iPhone, iPad, Android, Windows Phone 7, tablets)	31.87%	19.38%	18.75%	15.63%	14.37%
Vulnerability Scanning/Vulnerability Management	38.44%	13.03%	14.33%	16.94%	17.26%
Patch Management	32.56%	11.30%	13.62%	17.28%	25.25%
Data Leakage Prevention	40.73%	19.21%	11.92%	14.24%	13.91%
Next Generation Firewall	46.41%	18.63%	13.40%	9.80%	11.76%

41. What is your approach to dealing with social networking/media sites such as Facebook, Twitter or LinkedIn? (Please select all that apply).

Employees use for personal purposes	43.10%
Employees use for professional purposes	7.66%
Employees use to engage customers	23.75%
We block access to social networking/media for security reasons	20.50%
We block access to social networking/media for productivity reasons	19.73%
We block access to social networking/media to protect our brand	6.90%

42. How well received is your security policy for social networking by employees?

The majority of employees accepted and follow our policy	57.00%
Some employees accepted and follow our policy	11.55%
We don't have a policy communicated to employees at this time	19.41%
We have received negative feedback regarding our policy from some employees, without many attempts to circumvent our policy	8.11%
We have received strong negative feedback regarding our policy from many employees, with many attempts to circumvent our policy	3.93%

43. Which of the following best describes your approach to communicating to your employees regarding the decisions behind your social media/networking policies and how to properly use these sites in the workplace?

We do not have a security policy for social media/networking	25.56%
--	--------

We have not provided communications to employees on the policy 7.02%

We provided one email communication when the policy was first implemented 29.57%

We held one in-person or online session, meeting or event to communicate when the policy was first implemented 13.53%

We hold regular in-person, online sessions or provide email updates as we continue to adapt our policy 24.31%

44. Which of the following security concerns affect your decision to use the Cloud to run applications? (Please select all they apply.)

The companies hosting Cloud services may unlawfully share information. 34.87%

When you use the Cloud, you may not know exactly where your data is hosted. 44.06%

In the event of a disaster on the part of the of Cloud provider, you are concerned about the providers ability to manage the necessary complete restoration. 38.70%

There is no real way to know that the data is erased or destroyed even if you instruct the provider to do so. 44.25%

Other 9.77%

45. What are your key security concerns with new smartphones (such as iPhone, Android, or Windows 7 powered devices)? (Please select the two that you are most concerned about)

Devices contain corporate data and may get lost 49.62%

Devices are yet another entry point into our network 32.18%

We do not trust the security management of the application ecosystem	12.84%
Devices are hard to integrate into our existing security technologies and operations	18.58%
Enables increased information leakage or near real time disclosure of company information	21.46%
Physical security concerns related to location based services	11.30%

46. Which mobile device platforms, deployed with the appropriate security technologies, do you think are secure enough for your business? Please select all that apply – must choose at least one:

Windows Phone 7	16.09%
Android	18.39%
iPhone/iPad	31.42%
Blackberry/Playbook	58.43%
Others	2.68%
None of the above	6.32%

47. Which of the following best describes your company's policy on usage of tablets in the workplace?

We include tablets in our business processes	17.86%
We allow personal tablets in the office, but only for personal use	8.93%
We are in the process of implementing tablets into our business processes	25.00%
We don't have an established policy on the use of tablets in the workplace	48.21%

48. How much time is needed from your staff to respond to security-related incidents associated specifically with smart devices (such as iPhone, Android, or Windows 7 powered devices)

None	38.52%
Less than 1 man-hour in effort per week	31.38%
1 to 10 man-hours in effort per week	23.21%
11 to 20 man-hours in effort per week	3.32%
21 to 50 man-hours in effort per week	1.28%
> 50 man-hours in effort per week	2.30%

49. Has your company delayed or withheld embracing the emerging smartphone and tablet technologies due to security and privacy concerns? If so how much have you delayed?

We have not delayed	53.75%
Under 3 months	13.18%
More than 3 months but less than 6 months	9.04%
More than six months but less than a year	8.27%
A year or more	15.76%

50. Which of the following best describes your policy on monitoring and surveillance of employees' usage of mobile devices including laptops?

We do not monitor the data or usage by employees	59.90%
We only monitor during business hours	17.04%
We monitor 24/7	23.06%

52. How do you view the proliferation of smart devices and tablets in the workplace for your company?

A threat	6.30%
An opportunity	32.24%
Both	61.46%

## ABOUT THE AUTHORS

### NEIL BEGIN

Neil Begin is the Program Director at TELUS Security Labs, leading multiple research and development programs. Neil was one of the founding creators of TELUS Security Labs Vulnerability Research Service and he helped to create the Malware and Application research services. He leads the Labs' Custom Security Projects and Shellcode Exploit Services and has created a SIEM Content Development service, providing product management, device support and correlation rules to SIEM vendors and the enterprise. Neil brings 19 years of technical and project innovation working with global enterprises across North America. He has extensive experience in service development, project leadership and information security.

### RAFAEL ETGES

Rafael Etges is the Director for Security and Risk Consulting Services for TELUS Security Solutions. Rafael brings 17 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 27001-x, COBIT/COSO, ITIL, PCI-DSS) and regulations (Sarbanes Oxley, Bill 198, PIPEDA and international privacy laws).

Rafael is a research associate in the doctoral degree program at Henley and Rotman business schools. His research focuses on issues of consumer and societal trust in the online capabilities of corporations and government, influenced by data security and privacy breaches. He also examines the allocation of budgets within security programs to protect sensitive intellectual capital as a critical decision-making point within information risk management.

### WALID HEJAZI

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 to find new ways to understand their market data, providing them with perspectives that have allowed them to optimize their marketing activities, reduce their inventory holdings and develop criteria that ensures successful location selection. Walid has also consulted for several branches of Canadian government on diverse themes including the competitiveness of the Canadian economy and international trade.

## SURVEY DESIGN TEAM

- Yogen Appalraju
- Hernan Barros
- Neil Begin
- Rafael Etges
- Walid Hejazi
- Ryan Wilson

## **ADDITIONAL MATERIAL AND RESOURCES:**

- An electronic copy of the executive briefing is available at:  
**[www.telus.com/securitystudy](http://www.telus.com/securitystudy) or [rotman.utoronto.ca/securitystudy](http://rotman.utoronto.ca/securitystudy)**
- Regular updates will be available at  
**[www.telus.com/securitystudy](http://www.telus.com/securitystudy)  
[www.telustalksbusiness.com](http://www.telustalksbusiness.com)**

If your senior leadership team is interested in a briefing session with one of the authors, please contact either Rafael or Walid:

### **Rafael Etges**

Director, Security Services  
TELUS Security Solutions  
[rafael.etges@telus.com](mailto:rafael.etges@telus.com)

### **Dr. Walid Hejazi**

Professor of Business Economics  
Rotman School of Management  
[hejazi@rotman.utoronto.ca](mailto:hejazi@rotman.utoronto.ca)

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

VPN • Anti-Virus • Public Key Infrastructure • Encryption  
Content Filtering • Patch Management • Identity and Access Management  
Network Access Control • Endpoint Security • Firewalls • Log Management  
Web Application Firewalls • Two-factor Authentication (tokens, smartcards)  
IPS • SIEM • Vulnerability Scanning • Data Leakage Prevention

2011 TELUS-Rotman Joint Study on Canadian IT Security Practices



TELUS Security Labs