# 2013 TELUS-Rotman IT Security Study

**Hernan Barros**
Director, Security Solutions, TELUS

**Walid Hejazi**
Associate Professor, Rotman School of Management,
University of Toronto

TELUS®

Rotman School of Management
UNIVERSITY OF TORONTO

# Table of Contents

# Introduction

## The security reality of "yes" and "no" organizations

With the rapid pace of technology innovation, many Canadian enterprises now find themselves navigating unknown waters – a perimeter that is less defined, greater employee control in personal technology choices and a diversified IT sourcing mix that is bringing more partners into the process ecosystem. As a result, there have been inevitable impacts on security, making it even more critical, yet also more complex, to identify and prioritize the right controls in the face of constant and unrelenting change.

Canadian organizations find themselves on an interesting continuum. Some are saying "no" to innovation as a result of security concerns, some are saying "yes," but tempering adoption with security policy, education and awareness, while others are aspiring to move their security environments to a place where "yes" is a distinct possibility. In this continuum, innovation is defined as the adoption of new technologies and processes including Bring Your Own Device (BYOD), cloud computing and social networking.

Responsible "Yes" organizations are open to new technologies and collaborate with their employees to balance security with the business value innovation can bring. However, there are defined adoption parameters. These organizations recognize the criticality of security when embracing any new technology and are integrating strategy, policy, awareness, education and buy in into their processes.

Conversely, "no" organizations lack openness. Whether as a result of fear, lack of knowledge or simply not wanting to embrace change, these organizations are hesitant to contemplate the business value of innovation, citing security and optimum protection as their rationale. Unauthorized access becomes the irony of this approach. Employees will often circumvent blocks or policies in order to access the technology, app or website they want or need to use. This results in less visibility and control for IT, which translates into a less secure environment. This is the rationale for why "No" organizations have a false sense of security (see page 7, sidebar) and are often times less secure than "yes" organizations. "Yes" organizations adopt innovation responsibly, supporting it with strategic security.

## A qualitative approach in 2013

To get a deeper understanding of the security concerns and concepts driving this yes/no continuum, TELUS and the Rotman School of Management at the University of Toronto engaged with Canada's security leaders to talk about their security experiences and find out what keeps them up at night. For the 2013 study, we opted for a qualitative approach, rather than the quantitative approach employed since 2008.

Our goal was to gain a different level of insight, which is more interpretive, reflective and personalized to the individual's experience in his/her role, company and industry. This type of insight provides depth and perspective that both augments and validates the quantitative data that we have collected during the past

four years. It is our aim to enable Canadian organizations and their security leaders to learn from the security experiences, best practices and strategies employed by their peers.

## A qualitative process

During the fall of 2012, the research team held roundtable discussions with security leaders (Director level and above) in Vancouver, Calgary, Toronto, Ottawa and Montreal). In addition, we conducted more than a dozen one-on-one interviews with senior security professionals across the country. In open, forthright discussions, security leaders were candid about their concerns, strategies and approaches.

Our focus during these discussions covered a wide spectrum of discussion points including:

- What keeps senior security leaders awake at night
- How to handle the introduction of mobile devices into the workplace
- The emergence of new technologies including cloud
- Increased engagement with the global economy, and particularly with environments that lack protection for IP
- Significant turnover in the IT security labour market
- The impacts of legislated compliance on organizations from a financial and security perspective
- Security strategies used to address these concerns

In posing the initial question, “what keeps you up at night?,” four central concerns emerged:

- Has my organization been breached, and I don’t know about it?
- How will a breach affect my brand?
- What are my employees doing with corporate data?
- How do I retain my security resources?

Our in-depth examination of these four concerns uncovered several additional sub themes including topics such as innovation, end-of-life protocols, compliance, global expansion, risk vs. preparedness, social networking, BYOD, cloud and complex targeted threats. It is clear from the insights shared in our discussions and analyzed in this report that the widespread aspiration among Canadian security leaders is to move along the continuum towards becoming a “yes” organization – but temper the move with a balanced approach to security. However, the ever-evolving threat landscape leaves some organizations struggling to keep up. With the ability to compare their concerns against those of the leaders profiled in this year’s TELUS-Rotman report, Canadian organizations can gain objective and comprehensive insight to evaluate their risk profiles and those of the organizations in their supply chains. To enhance the insights presented in this year’s study, TELUS and Rotman security experts crafted a list of five comprehensive security recommendations for 2013 (see page 20, Conclusions and Recommendations). With this guidance, Canadian organizations can contemplate the secure adoption of innovation and transform a potentially false sense of security into awareness and proactive action to mitigate information security risks.

# What keeps you up at night?

**"In terms of security, what concerns me the most is the lack of end-user education and understanding about security risk. We can do a lot in the backend with logins, passwords, encryption and those kinds of things, but if you leave a USB stick lying around, if you attach a confidential file to an email or if you succumb to phishing attacks, nothing I do will make a difference."**

## Four key concerns emerge from reflections of Canadian security leaders

With a qualitative approach, we were able to glean executive views on top-of-mind security issues. We began each roundtable discussion and one-on-one interview with the following fundamental question: "what is it about information security that keeps you up at night?" Most participants answered almost immediately, showing a great awareness of and preoccupation with their top-of-mind issues.

In this section, we will explore the four key concerns, which emerged in both the roundtable and one-on-one interview discussions:

- Has my organization been breached, and I don't know about it?
- How will a breach affect my brand?
- What are my employees doing with corporate data?
- How do I retain my security resources?

Below we explore these concerns further as well as why these issues are top of mind. Having an understanding of the context in which these security leaders are operating is critical in order to understand the best strategies that can be deployed to mitigate risks.

> "The thing that keeps me up at night? I think the biggest challenge is people. Security is only as good as the people who adhere to your policies and security measures. Organizations are always at risk if employees aren't aware of security."

# 2.1 Has my organization been breached, and I don't know about it?

Simply because an organization has not identified a major breach, it does not mean a breach has not occurred. The media have been filled with reports of a history of long-standing breaches that were not detected, including Nortel, the Treasury Board and the Department of Finance Canada, TJ Maxx and those profiled in the 2011 McAfee Operation Shady Rat report.[1]

According to a February 2012 Wall Street Journal article, hackers had free reign over Nortel's corporate network for more than a decade. Foreign state-sponsored hackers were suspected of perpetrating the breach by leveraging the passwords of seven top executives, including the chief executive. The article goes on to state that "over the years, [the hackers] downloaded technical papers, research-and-development reports, business plans, employee emails and other documents."[2]

Foreign state-sponsored cyber espionage was also responsible for a major breach in the Canadian government in 2011. According to a February 2011 CBC news report, the attack affected the Finance Department and Treasury Board as well as Defense Research and Development Canada. The two main finance departments prohibited Internet access as a response. It was believed that highly classified information was exposed. The report highlights "executive spear-phishing" as the source where, "the hackers apparently managed to take control of computers in the offices of senior government executives as part of a scheme to steal the key passwords that unlock entire government data systems."[2]

### Pervasive sense of vulnerability

The inevitability of a major security breach was a common concern in many of our discussions. The following quote reflects this sentiment: "When I started this job, I told senior management that we will be breached within the next 18 months, so get over it now."

> "We have all been breached, whether we know it or not."

While there seemed to be a consensus that a breach would occur, there were varied responses around the confidence that security leaders had about their ability to detect it. As one executive put it, "While I don't have any formal metrics telling me that we haven't been breached, my gut tells me we haven't." Another participant echoed the same sentiments. When asked if his organization was experiencing an increase in the number and sophistication of breaches, his response was instructive: "While I don't have any objective measures of that, subjectively, I think the answer is no." The only objective measure he could point to was the increase in the denial of service attacks on the organizations that host his company's websites and customer channels.

> "The presence of data, in even what appears to be well-protected environments, very often means a user is one click away from doing something very dangerous accidentally, and we don't always know how to manage that."


Ironically, global expansion has helped some organizations improve visibility into domestic vulnerabilities and threats. While many organizations note the additional risks associated with deploying global strategies, these organizations report that addressing the new global risk profile proactively has improved security overall.

### Insider breaches often go unreported

People are often the weakest link in an IT security system. The concept of "misplaced emphasis" around security risks was a common thread during our breach-focused conversations. Many organizations are capable of implementing state-of-the-art processes and deploying the best technologies, but people within the organization often create vulnerabilities through their lack of security education and ensuing actions. While most organizations focus their efforts and budgets on protecting information systems from external vulnerabilities and threats, there is often a lack of appreciation of the vulnerabilities from within the organization.

The vast majority of breaches emanate from within the organization, either from malicious intent or from careless, ill-informed actions. According to one of our

## False Sense of Security

In an information-based economy, confidential information, including intellectual property, is often an organization's key competitive advantage. If this information leaks out, competitors can use it, reducing the breached organization's advantage, and ultimately, its profitability. Protecting this information is critical.

But are organizations that don't detect breaches more secure than those that do detect them? While the answer may seem obvious, it is not. Very often organizations have a false sense of security. Managers and C-level executives may feel proud that no security breaches have been detected on their systems. But even though breaches haven't been detected, it does not mean that they have not occurred. Security executives that participated in this year's TELUS-Rotman study were fairly unanimous in their view that their limited ability to detect breaches is a top-of-mind concern. And, one could argue that an undetected breach could have a greater negative impact on an organization than a detected breach since the organization would not be able to identify and remediate the damage.

It must be highlighted that as breaches become more targeted, sophisticated and seek information that can be monetized, the parties perpetrating the breach have incentives to ensure that the breach is not detected. This is very different from hacking of the past, where perpetrators would brag about their bounty. In sharp contrast, the sophisticated hacker of today will use the information for profit, but likely in a strategic way so as not to alert the hacked organization of the breach. Put differently, organizations that never realize that they have been hacked, or are currently in the midst of a long-duration penetration, may have a false sense of security. These types of breaches can undermine the success of the organization's long-term profitability.

participants, a CSO at a Canadian financial organization, "employees are our single greatest threat – it's not malicious, it's just not knowing."

We highlighted the growing trend of insider breaches in the government sector in our 2011 study. Unlike public and private organizations, the share of insider breaches in the government sector continued to rise, growing 28 per cent since 2010 and up 68 per cent since 2008. We saw from our data in previous years, as well as through the insights of this year's participants, that employee breaches, whether intentional or not, are the biggest threat to an organization.

While awareness training is prevalent across organizations, the sophistication and frequency of such efforts vary significantly. It is quite evident that there is awareness fatigue in many organizations – employees simply become immune to security messages. Organizations need to find the right balance for security training and employee education to help to ensure that these initiatives remain effective. There is an optimal frequency and method of communicating with employees that is largely dependent on the organization's risk profile. IT security managers should not assume that their job is done simply because an email was sent out or a pamphlet was circulated with information on risks and mitigating them. Each manager needs to identify the best way to promote continuous awareness.

There is also the issue of delivery of the security awareness message. Explaining the "why" behind the security policy is an effective way to promote employee buy in and compliance. Working with employees so that they understand the rationale behind a security policy helps them follow security protocols. For example, in the 2011 study, we found that social networking policies were well received in 72 per cent of cases, reflecting the fact that most employees are willing to comply with a policy as long as they understand what the policy is, the risks associated with the technology and the business reasons behind the policy.

## If security is inconvenient or an impediment to efficiency, employees circumvent it

Making security convenient is related to the challenges around encouraging employees to "do the right thing" and follow security protocols. There was a consensus among participants that when security is inconvenient and becomes an impediment to efficient employee performance, the likelihood of violating security protocols rises dramatically. The most mature organizations have been working to make the secure approach the most convenient approach. While this is not always possible, IT security managers should consider their policies with this in mind.

Findings from our past studies about social media policy and associated breaches illustrate the importance of making security convenient. In our 2010 study, we found a significant correlation between organizations blocking access to social networking for security reasons and the number of breaches experienced in past 12 months. In 2011, we retested and confirmed this phenomenon (see Diagram 2). Organizations that blocked social networking for security reasons averaged 10.3 incidents in a 12-month period, while organizations that did not block averaged 7.2 incidents in same timeframe. Blocking a social site partially in only one channel (for example, the corporate web browser) can result in employees accessing that site by alternate means (a smartphone or tablet). In cases such as these, 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.

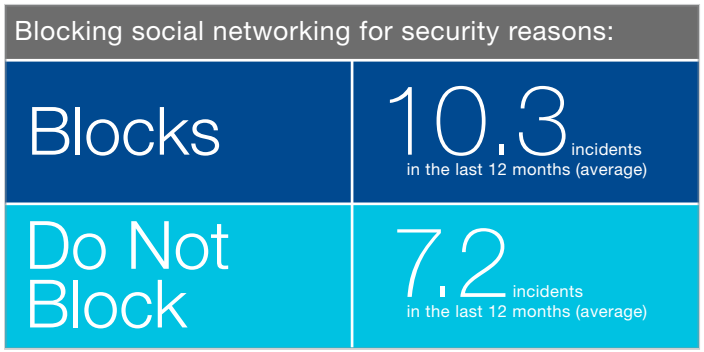



Diagram 2

## "No" organizations face increased risk from employees circumventing policy to use in-demand technology

With the advent of BYOD and public clouds, the risk and probability of a major breach emanating from the actions of employees is expected to increase. As noted above, there is a significant sentiment that security must be convenient. Often employees will circumvent the security policy if complying with it hinders their productivity or is overly inconvenient. For example, we heard many stories where employees were using public clouds because sharing documents according to the company's security policy was too much work.

There is an increased awareness of unauthorized use of new technologies. There was also a sentiment among the participants that "yes" organizations were more secure than "no" organizations. The feeling was that when security managers turn down requests from employees to use a new device, a new technology or public cloud, employees go ahead unmonitored and actually create more risk for an organization (Diagram 3). One participant told us, "employees are going to do it anyway, so we have to figure out how to allow the use of these new technologies." Many organizations were in some sense embarrassed in admitting that they are "no" organizations. The vast majority strives to be a "yes" organization.

"Yes" organizations work with employees to enable innovation securely, and in the process, make the organization more secure. They do not let security inhibit innovation. Rather, they understand that security must enable innovation and drive efficiency. However,

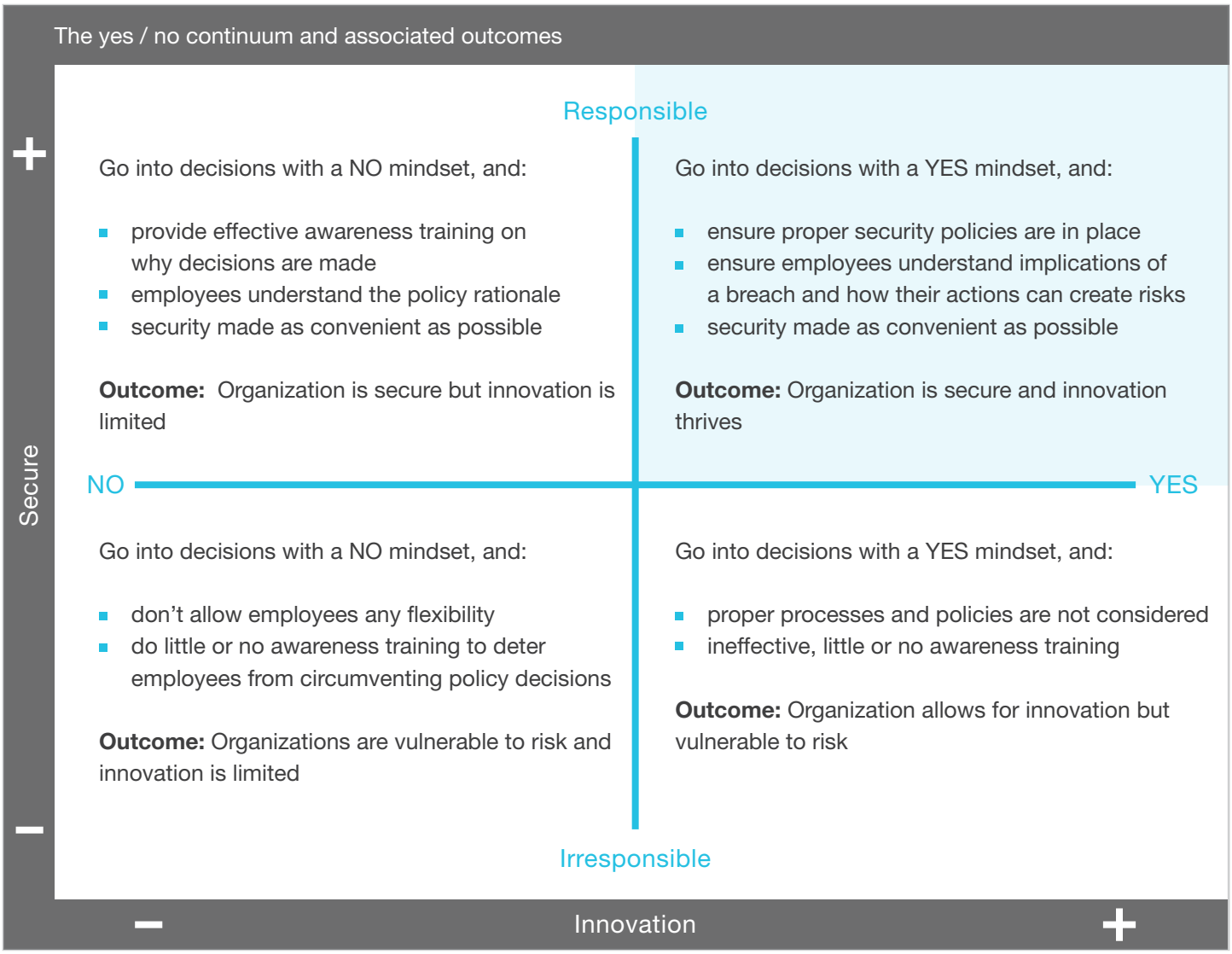



Diagram 3

> "We aren't in control of mobile devices being used by our employees. If you don't put in certain logical controls, they're just going to do it anyway. The pervasiveness of the digital connected community is so entrenched now that IT organizations are going to have a real hard time grappling with how to control their information."

participants also felt that simply allowing employees free reign over new technologies is not a sensible approach. IT managers must stay ahead of possible trends and work to create a plan that allows employees to leverage new technologies responsibly and within security guidelines. Those plans must complement the existing security program and be convenient, clearly articulated and have support from every level of management and the business units.

The advantages of being a "yes" organization definitely resonated with participants. Many participants expressed that they feel more secure after having allowed these new technologies: "At least we know what our people are doing – they aren't doing it in ways that we can't monitor."

## Breaches make security an easier sell internally

Not surprisingly, all of the participants reported that it's easier to sell security internally during breach disclosures – both when the breach occurs within the organization and in other organizations, especially in the same sector. As several security managers stated, "there is nothing more effective at demonstrating the urgency of enhancing the security posture of an organization than a breach at a competitor, especially if the breach takes place in Canada. These events bring home the risks – it makes them real." Another manager said, "it is difficult to relate to averages, especially when they are based on U.S. data." Breach incidents at similar organizations make it very difficult for security leadership to ignore their own security posture.

> "Other organizations having experienced very public breaches allows us to have a very different kind of conversation with the board and with the executive team."

The discussion of selling security internally in the face of a domestic breach led to reflections on today's threat landscape being characterized by advanced, targeted and sophisticated threats. Participants expressed concern about the level of cooperation between hactivists, intellectual property thieves and threat profiteers. Consumerization of IT, supply chain weakness, a heterogeneous network perimeter and outsourcing are also adding new layers of complexity to the threat landscape and increasing the risk and impact of breaches.

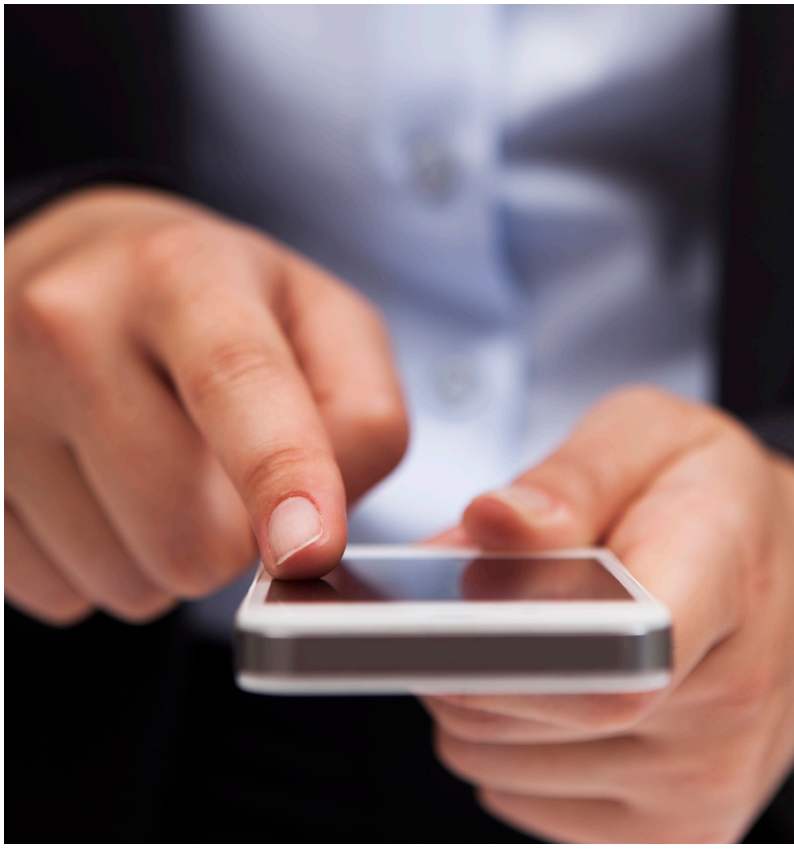
> "We are seeing a level of cooperation in the last twelve months between hactivists, intellectual property thieves and those who profit from threats. Threats are becoming more sophisticated."

### Managing the process of an employee leaving the company is critical to protecting information

Security leaders take the potential security risks associated with employee termination quite seriously, especially when layoffs occur on a large scale. Defined process and technology solutions, including device wipe, are critical. We heard several stories about situations where personal devices were not wiped before the separation event. The ex-employee disabled the radio on the device, making a virtual wipe impossible. One participant recounted a scenario where a company did not execute the remote wipe for several weeks, which was deemed illegal at the time, resulting in legal action against the company.

> "Offshoring and outsourcing poke more and more holes in my perimeter. The second biggest thing keeping me awake at night is the erosion of traditional perimeters."

In a similar vein, end-of-life protocols for corporate and employee-owned devices remain a source of controversy for security leaders. Through our discussions, we uncovered that some participants believe that a virtual wipe or manual wipe is sufficient to minimize the risk of data loss. Others believe that physical destruction is the only way to ensure optimum risk mitigation. Consensus is also lacking on the effectiveness of outsourcing this process as a result of the viability, authenticity and accountability of providers in a crowded, competitive market. Regardless of the individual viewpoint, having a defined process for dealing with technology, either as a result of employee termination or life cycle completion, is critical to mitigate data loss that could lead to a potential breach.



# 2.2 How will a breach affect my brand?

In today's information-based economy, organizations require customers to share sensitive information to facilitate transactions and to confirm identities. Increasingly however, organizations are leveraging this data to drive more effective business strategies and revenues. The damage resulting from a customer data breach leaves a long-lasting impact on brand value as well as customer confidence. In recent years, for example, companies such as Sony, Visa, Honda and MasterCard have been victims of breaches involving customer data. They have had to respond to massive class action suits involving millions of their customers, and the costs have been substantial.

> "What's keeping me awake at night? Any breach that could impact confidential information from our loyalty program getting into the wrong hands."

Breaches come in different forms. We are all too familiar with the impact that a denial of service attack can have on critical infrastructure. In the private sector, corporations are susceptible to large targeted attacks and hacktivism. Being able to thwart these attempts enables the business to deliver on the brand promise – assuring a high degree of service availability and secure interactions. In these organizations, security has significant business value because it protects brand value directly.

The security executives that we interviewed all agreed that keeping their company from 'showing up on the front page of the newspaper' was their number one objective and an incentive for obtaining approval for security initiatives.

### Varying perceptions on direct financial costs of a breach

Many of our roundtable participants were all too aware of the effects of a breach on stock value, jobs, lawsuits and penalties, but confirmed that none of these can compare to the cost of lost consumer confidence. One participant organization has reported that the cost of losing an HR record is approximately $60. To put this into context, a breach of 100,000 records would cost that organization six million dollars.

While quantitative information is not readily available for consumer confidence, research participants agreed that the damage to a brand as a result of breach is of paramount importance. And the effects of a security breach are not restricted to the organization that has been breached. The market value of organizations within the supply chain or same industry can be affected as well.

> “Our number one threat concern: loss of trust in our ability to protect customer data.”

There were some security managers that minimized the impact of the direct financial costs. As the CIO of a major Canadian retailer put it, “we are not concerned about paying the fines associated with a data breach. That is just a political statement. Rather we are worried about all of our customers and stakeholders knowing that a breach occurred. That would really hurt our brand, and that’s exactly what I am protecting this company from.”

### New technologies create new brand vulnerabilities

Employees want to work for organizations that are seen as progressive, with strong corporate strategy and brand presence. They are looking to join dynamic cultures where they have access to social networks and freedom to pick their device of choice for optimum productivity. Although seen as differentiators for employees, these ‘necessary evils,’ as they were referenced by one of the participants, must be controlled and monitored for brand infractions.

With the influx of social networking, chats and blogs in the workplace, disgruntled employees or naïve insiders can compromise a corporate brand easily.

> “Employees are our single greatest threat – it’s not malicious, it’s just not knowing.”

All it takes is disclosing confidential details (or pictures) of their organization innocently on Facebook, LinkedIn or other personal sites. One organization with a low external security profile has had to implement a surveillance function to monitor social networks for brand transgressions and release of unauthorized corporate information. The major threat to its brand is internal. Other more advanced companies have teams and sophisticated means to control the presence and representation of the brand online.

> “Being a custodian of customer data is a driver for security.”

### Breaches also have internal impacts

A major breach – a loss of trust by definition – is not limited to external impact. Breach impacts can filter to employee engagement and satisfaction. It also reverberates within the walls of an organization, not just at the time of the breach, but also during the time it will take to recover. With social media, word of breaches spreads quickly, which can also affect HR’s ability to hire and retain top talent. Rising stars within their industries want to be associated with companies that they perceive to be leaders, who invest in brand integrity, new technologies, progressive work styles and customer experience. A breach negates this perception, creating greater challenges for HR to sell confidence in the organization.


"According to participants, complying with government and industry regulations is the minimum level of security required. However, it does not constitute the necessary level of security required in a landscape characterized by targeted, advanced threats."

### Is being compliant being secure?

Sophisticated organizations that acknowledge the importance of brand integrity as an offshoot of security recognize the difference between being compliant and being secure. And as one interviewee noted, "being compliant is not necessarily being secure." According to participants, complying with government and industry regulations is the minimum level of security required. However, it does not constitute the necessary level of security required in a landscape characterized by targeted, advanced threats. Not surprisingly, participants that strongly correlated security events and brand impacts were further ahead in terms of security planning beyond compliance.

# 2.3 What are my employees doing with corporate data?

With the growth of BYOD, social technologies and the increasing accessibility of public cloud solutions, Canadian security leaders are concerned with what their employees are doing with corporate data. The evolution from a highly controlled environment to a less-controlled, more heterogeneous environment is an important factor when considering these new technologies. Previously, when some security leaders were concerned about employees saving data on USB keys for example, they had the ability to take action, either through policy or through more extreme measures, including disabling USB ports on computers.

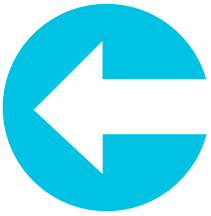
But as we discussed earlier, employees feel entitled to use any technology that they consider will make them more productive, efficient and quick. Security is a secondary consideration, especially if it makes accessing those technologies cumbersome or inconvenient. And this is precisely the catch-22 of enabling device freedom, permitting the use of social media and public cloud solutions. Employees want it, they feel empowered by it and productivity benefits. But for security leaders, gaining and maintaining visibility and control becomes more complex.

> "We need to have the controls and tools in place to protect [corporate data on mobile devices]. Conversely, if we weren't set up with the right foundational tools like mobile device management then it would be a red herring for us."

### Grappling with BYOD and social technologies

A research participant suggested that the BYOD trend, while essentially unavoidable, exposes organizations to significant risks. He argued that until organizations do "data classification" and are well prepared for the new risks that come with the introduction of employee owned, and not always fully supported, devices, then the risks are too high. He advised against allowing the introduction of these devices – but understands why there is an "urgency" around keeping up with these new trends.

> "We can influence our employees and make them aware, but we can't control their actions."



Regardless of these views, BYOD and social technologies are integrated into the fabric of how employees live and work. The majority of our research participants conceded to this reality. These participants were very clear in stating that if organizations block access to social networking sites, or prevent employees from bringing their own devices to work, employees are going to do it regardless. As such, these new trends should be embraced and be viewed as business enablers, however policies must in place to ensure responsible use. Policies must prevent unauthorized sharing, posting or use of corporate information in personal blogs, chats and sites. Employees must also be made aware that inappropriate personal information being shared on these public sites may be highly detrimental to corporate reputation and brand.

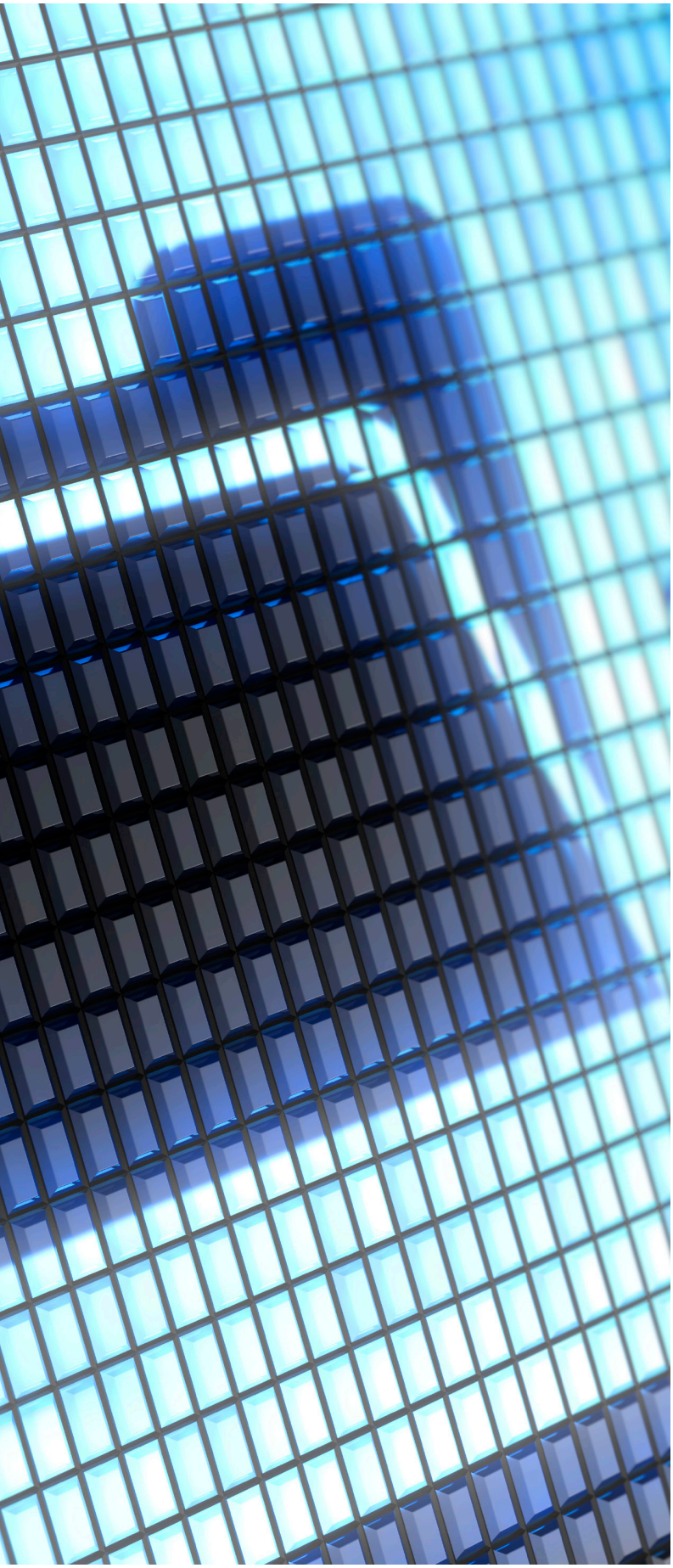
There is also debate about whether devices that are not supported at work are actually increasing the risks associated with security policy non-compliance. This is entirely consistent with other parts of this study and our earlier work: security must be convenient and employees must understand why security policies are in place. In one of the roundtable sessions, a participant advised on how his organization holds a yearly 'security awareness day' to promote policy compliance and understanding of the potential security risks. They also have screen banners reminding employees that they are under surveillance and highlighting their responsibilities when it comes to the protection of the organization's information.

## The cloud conundrum

Today, public clouds represent a common approach for employees to access data when they aren't in the office. For Canadian organizations this creates multiple risks and liabilities, including the fact that corporate data could be leaving a Canadian jurisdiction and being stored in a foreign country. While the desire for cloud is definitely present as a driver of cost reduction, increased efficiency and a redirection of focus to core competencies, wariness still abounds.

## Specifically, security leaders' cloud concerns include:

- **A lack of visibility into and control over data at rest and in transit** – when trusting a service provider with sensitive information, there is uncertainty regarding the provider's ability to protect data. IT security managers need to ensure that service providers have the controls in place to secure the data both in transit and at rest effectively. Considerations brought up by participants include controls already in place, regulatory adherence and data protection measures. IT security professionals also need to understand these considerations in order to effectively select their cloud services provider.
- **Securing stored sensitive data** – similar themes affect the security assurance of data in the cloud. Most respondents felt that service providers must have the appropriate controls and skills to enable secure storage of cloud data. For most, it once again becomes a balance of risk appetite versus the clear business advantages of storing data in the cloud. Many respondents also felt that they needed to make decisions regarding how far they want to go in terms of the level of sensitivity of data they are willing to risk.
- **Legal issues and international privacy law** – by their very nature, cloud services do not require data to remain within the confines of an organization's infrastructure let alone national borders. Organizations need to understand the implications of where the data resides and the laws that govern data within the location of where the data sits. Security managers need to maintain a good understanding of increasing privacy risks, how the flow of data and where it resides affects contractual obligations and how personal information flows between borders.
- **A lack of access to controls** – many of the concerns reported by respondents revolved around the fear of access to sensitive resources or private and proprietary information. As in the case of secure storage of sensitive data, respondents have expressed a need to ensure that effective access controls are in place via the cloud service provider.

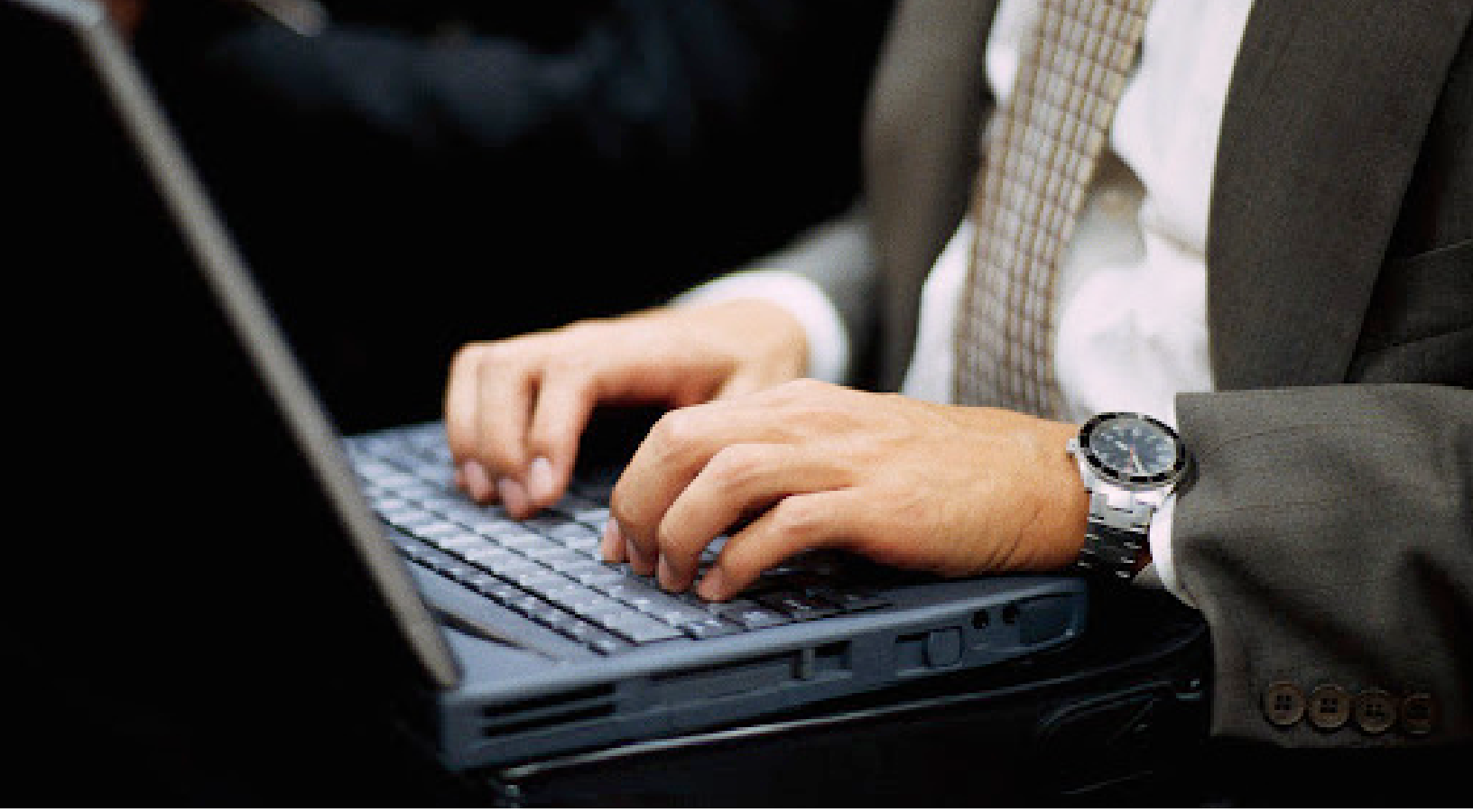


While many organizations are planning for cloud adoption within the next 12 to 18 months, both business and security leaders feel uneasy about tools that remove potentially sensitive corporate data from residing on premise. However, enterprise-focused cloud services from reputable providers are now available in the market for public, private and hybrid cloud implementations. A handful of these services eliminate jurisdictional data issues by offering Canada-based data storage in state-of-the-art data centres, which offer enterprise-level security at the physical, infrastructure and information levels.

## 2.4 How do I retain my security resources?

An organization's ability to remain effective in securing its infrastructure, in part, hinges on the level of talent that it is able to recruit and maintain. In this era of complex, targeted attacks, the skill level required to secure a corporate environment is very high and expensive. Some organizations invest greatly in training resources, enabling them with new technologies and skills. In some cases, it is becoming commonplace to hire specialized personnel that are trained in detecting anomalies and threats within the organization's environment (i.e. digital forensics). Some organizations prefer to outsource this and other types of security work given the scarcity and high cost of the required skill sets. Outsourcing can also help minimize training, retention and employee churn costs.

Attracting and retaining top talent remains a significant challenge for Canadian organizations, particularly in the government sector. Several government organizations reported that employees take positions in government to gain a thorough and deep understanding of risk and optimal security strategies but then move into the private sector when seemingly better and more profitable opportunities arise. We found evidence of salary differentials in both our 2009 and 2011 studies to support this talent challenge. In 2009, we reported that 35 per cent of security professionals working in government



earned more than $100,000 per year, compared to 47 per cent in private organizations and 57 per cent in public organizations. In 2011, we documented a similar salary variance. CIOs in government earned $150,000 per year, while C-level security professionals in private organizations earned $200,000+.

The ability of organizations to embrace innovation and use security as a business enabler creates an environment where security professionals can succeed. This involves proper security education and awareness, as well as clear lines of communication with and support from C-level executives. As more organizations move the security function closer to the business or have security leaders reporting into C-level executives, the better the outcomes of the security program, including the satisfaction and engagement levels of the security team.

Participants suggested several excellent ideas to overcome the talent retention challenge including:

- Providing training and certifications
- Encouraging employees to participate in communities to gain additional insights from other organizations
- Create access to tools that enable benchmarking of the security posture against 'like' organizations, including sophistication of security skills and resources

Organizations that have programs to recruit personnel from internal IT departments or from academic institutions are having some successes. However, HR must be proactive in identifying the tipping point for these recruits (when they gain sufficient knowledge to become marketable) and in initiating aggressive and comprehensive retention programs to make staying a more attractive option than moving to another organization. This is not only important to preserve HR investments, but critical to ensuring that the organization is not left exposed in the absence of its security leaders.

# Conclusion and Recommendations

In 2008, when TELUS and Rotman partnered to study the state of IT security in Canada, there were no studies publically available. As such, Canadian IT security managers were forced to assume implicitly that the risk landscape in Canada was the same as that in other countries. During the subsequent four years, TELUS and Rotman have published an annual quantitative study, which has enhanced clarity around IT security in Canada. As a result Canadian IT security managers are better placed to make security decisions, and IT systems are more secure.

This year's qualitative study takes our analysis one step further. Using a qualitative approach, we have been able to provide clarity not just on the numbers, but also on the thinking of security managers. Our discussions with IT security professionals allowed us to validate many previous insights and provide a richer context for those insights. We also gained a better understanding of top-of-mind issues, which would have been more challenging to tease out of a quantitative study. As such, this year's qualitative study complements earlier quantitative studies, further clarifying the state of IT security in Canada.

## Data and Deep Insights

Whether in Vancouver, Calgary, Toronto, Ottawa or Montreal, security leaders across verticals and the public and private sector who participated in this year's study have four top-of-mind issues that keep them up at night:

1. Has my organization been breached, and I don't know about it?

2. How will a breach affect my brand?

3. What are my employees doing with corporate data?

4. How do I retain my security resources?

By delving into these four concerns in a qualitative fashion this year, we have provided Canadian security leaders with a comprehensive framework that includes both data (from our previous four years of quantitative studies) and deep insights. Leveraging this framework, Canadian organizations can compare their security postures as well as learn from their peers.

Beyond provoking thought with the insights of our security leader participants, we also wanted to help Canadian organizations take action. We spent a lot of time talking with security leaders about new technologies and innovation and their impact on security. It was through these discussions that the yes/no continuum, which we profile in the introduction of the report, came to light. Many organizations expressed the aspiration of becoming a "yes" organization – being able to enable innovation responsibly by supporting it with proactive, strategic security.

To that end, the research team developed a list of five comprehensive recommendations to help organizations position security as an enabler of innovation. With this advice and guidance, it is our hope that we can help to move Canadian organizations along the “yes” continuum, transforming a potentially false sense of security that comes with saying “no” into awareness and proactive action to mitigate information security risks.

## Recommendation 1: Don’t assume that you haven’t been breached.

Simply because your organization has not detected a security breach, does not mean that you have not been breached at any point in time or that the breach is no longer being perpetrated. It is critical to have the infrastructure in place to review events that occurred in the past within your organization’s environment. Auditing data from Log Management solutions is key to being able to review events historically. This can still be difficult as looking for a breach that may or may not have occurred in the past can be equated to searching for a needle in a haystack.

Given the advent of sophisticated, targeted threats in today’s environments, a formal threat analytics program can help your organization invest in the right skills and technologies to help to identify threats. Next generation application-aware firewalls and intrusion detection and prevention systems enable threat detection. In addition, establishing a program that allows for the analysis of the data being generated by security infrastructure is also key to helping to ensure that breaches are detected. These skills are hard to come by, but investing in developing them internally or outsourcing those capabilities can help to promote a proactive threat analytics program.

When thinking about threat detection and analysis, it’s important for organizations to understand that threats are both external and internal. Most organizations focus on stopping threats from the outside, but it’s a misplaced emphasis. When looking to detect breaches, organizations must place equal emphasis on what is considered to be the biggest risk to security - the threat within. The vast majority of risks to an organization

reside within the organization itself. This can happen as a result of both malicious and careless actions on the part of employees, such as sharing passwords, accessing corporate resources by logging on to public computers that may have key loggers installed, downloading files that have malware or using web sites that are infected. Security managers need to appreciate this risk and dedicate time and resources to mitigating it by establishing security awareness programs aimed at educating the employee who is viewed often as the weakest link in an organization's security.

## Recommendation 2: Security diligence must be ongoing.

Security is not a onetime effort. It needs to be embedded in all business processes, as it is a business enabler if done correctly. Security diligence must be seen as a mode of operation for everyday life. Given the significant pace of technological innovation that affects the security of information systems, IT security managers have to keep up with how these innovations impact the risk profile of the organization and respond appropriately. A simple wait and see approach will not serve the organization's security posture well. In essence, security needs to be part of life. IT programs and projects (including cloud, BYOD, social networking and the introduction of other new applications and tools) must have security built in to every aspect of the initiative.

Collaboration with business leaders is a key tenant of security diligence. Security leaders must engage the business to implement sustainable governance and oversight processes to assess periodic violations of policy. Any component – design, architecture, IT security infrastructure implementation, security policies, procedures and employee training – can be a potential point of failure. Organizations must ensure that all consensual policies are enforced. This extends beyond the organization itself as well, as security breaches can also result from supply chain exposure. Security managers need to be diligent with respect to all possibilities, including ensuring that vendors and partners have policies in place that mitigate security threats within the products and services that are being provided. It is important to demand that partners provide proof of compliance to regulatory and security requirements to prove the safety of their products.

End-of-life protocols represent one example of ongoing security diligence that came up as a recurring theme throughout our discussions with security leaders. How an organization deals with the safe destruction or disposal of old devices is a critical element of any security program because these policies can impact an organization's risk profile. Organizations must ensure that data is destroyed securely and at levels that coincide with the organization's risk appetite. Understanding the effectiveness and relative merits of a virtual wipe versus physical destruction underscores this issue. Furthermore, ensuring that reliable service providers execute these services helps to mitigate the risk associated with potential leaks of information that may reside on recycled or discarded devices.

## Recommendation 3: Compliance is not the same as security.

Meeting minimum required standards should be viewed as exactly that, the minimum required. Organizations need to understand the risks that they face and deploy the appropriate strategies in light of those assessed risks. While an organization can never be fully secure, it needs to find the right balance between risk and preparedness.

> "We see BYOD as an opportunity for our organization. We have to embrace it as we can't be close to our customers without being like them."

This can be achieved by developing a security program that reflects business activities and operational models by using internal skills, if they are available, or by hiring external security expertise. The program must allow for the creation of a security practice that accounts for the organization's requirements and its risk appetite, striking the right balance between security, risk and cost. It is also important to assess the security posture periodically against industry peers and establish a partnership with the business that enables security to integrate into projects at the start of the lifecycle and carry through to implementation and management.

## Recommendation 4: Organizations should work to be "yes" organizations.

When employees request the use of new (or popular) technologies, IT security's first instinct should be to say yes. This is not to say that IT security managers should simply say yes blindly and deploy new IT strategies without due diligence. Rather, security managers need to understand that simply saying no will not work. Employees will very likely "do it anyway" in a way that is not monitored, exposing the organization to increased risk. Security managers need to work with the employees on how innovation can be used in the most secure way possible. This makes employees more efficient, the firm more innovative and gives IT more control and visibility into the environment. As evidenced in our panel discussions as well as prior TELUS-Rotman studies, "yes" organizations are less likely to experience internal breaches. Employees are less likely to circumvent security policies, but there must be a plan.

- **If you have a security policy that works, use it!** The advent of enabling innovation or wanting to be a "yes" organization does not equate to disregarding existing security policies and internal compliance requirements. Base decisions on the organization's existing policies for securing infrastructure. In essence, do your research and make sure security risks are covered, minimized or mitigated.
- **Obtain user buy in.** Simply saying "no" isn't going to cut it. Provide an explanation of the plan of action for the introduction of new technologies. Be up front regarding the steps taken to enable user access to technologies while demonstrating the need for due process and security.
- **Educate.** Ensure that your security program includes formal education on how to use these technologies safely and responsibly.

From speaking with security professionals across the country, the above steps can help to mitigate security threats associated with the introduction of new technologies and allow organizations to be innovative in increasing productivity and employee satisfaction. In addition, convenience is the key to end user buy in. If following the security procedures inhibits employee efficiency, they will be inclined to circumvent the policy, and in the process, make the organization more vulnerable. Examples can be seen with the advent of policies allowing the use of tools such as smartphones and tablets. Saying no to BYOD? Organizations may take that stance if they wish, but they should be wary of rogue devices being used on the network. Say yes and restrict the devices? Be aware that users may chose to ignore security policies that restrict the native use of the device, potentially putting the organization at risk. To the extent possible, organizations need to make security convenient. Some IT security managers have been working to make the recommended secure approach also the most convenient, limiting (or eliminating) this source of potential exposure.

## Recommendation 5: Awareness training is key.

There are three pillars to security: people, processes and technology. Security is only as good as its weakest link, which often comes down to people. As a result, awareness training must be consistent and relevant to new innovations and threats. Particularly in "no" organizations, it is common for employees to implement new strategies or deploy new devices without seeking permission as discussed in recommendation 4. Ensuring

that employees understand the associated risks is critical to mitigating this threat and reducing the likelihood of exposing the organization to internal breaches and external breaches. Many participants in our discussions emphasized the importance of education in maximizing employee security awareness. However, we recommend trying to avoid awareness fatigue. Sending out emails, which highlight new risks facing the organization, or reminding employees to change old passwords is perhaps necessary, but is in no way sufficient to ensure that employees are aware. Often employees dismiss or delete these emails without reading them. IT security managers need to figure out how to reach employees most effectively. Many organizations have deployed computer-based training strategies that introduce policies covering the use of the Internet, social networking, end of life protocols, social engineering threats and password management.

## Sources


1. Finance Department and Treasury Board: *http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html*;
   TJ Maxx: *http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever*;
   Operation Shady Rat: *http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf*

2. Chinese Hackers Suspected in Long-Term Nortel Breach. Siobhan Gorman. Wall Street Journal (online), New York, NY, February 14, 2012.

3. Foreign Hackers Attack Canadian Government. Greg Weston. CBC (online), posted February 16, 2011, 8:59pm ET.

# About the Authors

## DR. WALID HEJAZI

Walid Hejazi is an Associate Professor of Business Economics, and Academic Director, at the Rotman School of Management where he regularly teaches Canada's current and future business leaders in the MBA, EMBA, and custom Executive programs. He is also the Rotman lead on the annual TELUS-Rotman IT Security Study. He has published extensively in many 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 develop and deploy new strategies and initiatives.

Walid has consulted for several branches of the Canadian and foreign governments on themes related to international trade, foreign investment, and global competitiveness. He has appeared several times before parliamentary committees on these topics, and is a regular commentator in the media on important business and economic issues.

## HERNAN BARROS

Hernan Barros is currently the director of product management for TELUS Security Solutions.

Hernan's vision is to make TELUS Security Solutions the most recommended provider of Managed and Integrated Security solutions in Canada. His passion for growth and innovation has contributed to the successful market delivery of 30 per cent year over year growth within the TELUS Security Solutions portfolio since 2007.

Hernan surrounds himself with a solid team of individuals that consistently deliver strong results. His vision, together with his open and transparent leadership style, inspires his team to successfully deliver innovative product solutions. With 11 years as a security professional behind him, Hernan's experience has helped develop TELUS Security Solutions to be one of Canada's leading security providers. He has presented on numerous occasions and has contributed in previous years to the TELUS-Rotman IT Security Study. Hernan is also a proud family man who lives in Aurora with his wife and two young children.

## Contributors

We had an inspiring group of security leaders share their insights and expertise with us. Here is a list of the contributors, excluding those who requested to remain anonymous:

Anthony Bertuzzi, TELUS Communications Inc.
Bob Long, Trimac Transportation
Francis Castonguay, Canadian Forces
Gord Halfnights, Raymond James
Irene Vieira, TELUS Communications Inc.
Jay Mehta, ING Direct Canada
Jonathan Raymond, TELUS Communications Inc.
Kenneth Haertling, TELUS Communications Inc.
Kevin Pasveer, Canadian Pacific
Lorraine Tait, TELUS Communications Inc.
Michael Argast, TELUS Communications Inc.
Noel Lachance, Office of the Privacy Commissioner of Canada
Nunzio Fortugno, Athabasca Oil Corporation
Peter Bier, Osler, Hoskin & Harcourt LLP
Ryan Wilson, TELUS Communications Inc.
Stuart Irvine, MPAC
Sunil Chand, TELUS Communications Inc.
Tony D'Alessandro, The Co-operators Group
Warren Harvey, TELUS Communications Inc.
Yogen Appalraju, TELUS Communications Inc.
Yves Rousseau, Uni-Select

## Additional Materials and Resources

An electronic copy of the executive briefing is available at:

*www.telus.com/securitystudy* or
*rotman.utoronto.ca/securitystudy*

Regular updates will be available at

*www.telus.com/securitystudy*
*www.telustalksbusiness.com*

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


### DR. WALID HEJAZI
Professor of Business Economics
Rotman School of Management
hejazi@rotman.utoronto.ca

### HERNAN BARROS
Director of Product Management,
TELUS Security Solutions
hernan.barros@telus.com


## About TELUS Security Solutions

TELUS Security Solutions offers customers the most comprehensive security portfolio including consulting and managed services, technology solutions, plus partnerships with 16 of the top 20 global security vendors. In addition, TELUS Security Labs is a leading provider of security research to more than 50 of the world's top security product vendors. Whether your priority is handling targeted threats with real-time context, securing your mobile enterprise or removing your security management challenge, TELUS Security Solutions can help you gain visibility, understanding and control.

For more information about TELUS Security Solutions, please visit *telus.com/BusinessSecurity*.

## About Rotman School of Management

The Rotman School of Management at the University of Toronto is redesigning business education for the 21st century with a curriculum based on Integrative Thinking. Located in the world's most diverse city, the Rotman School fosters a new way to think that enables the design of creative business solutions. The School is currently raising $200 million to ensure Canada has the world-class business school it deserves.

For more information, visit *rotman.utoronto.ca*.

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