2013 TELUS-Rotman IT Security Study Executive Summary

A qualitative approach: adding context to four years of data insights

Hernan Barros
Director, Security Solutions, TELUS

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

TELUS®

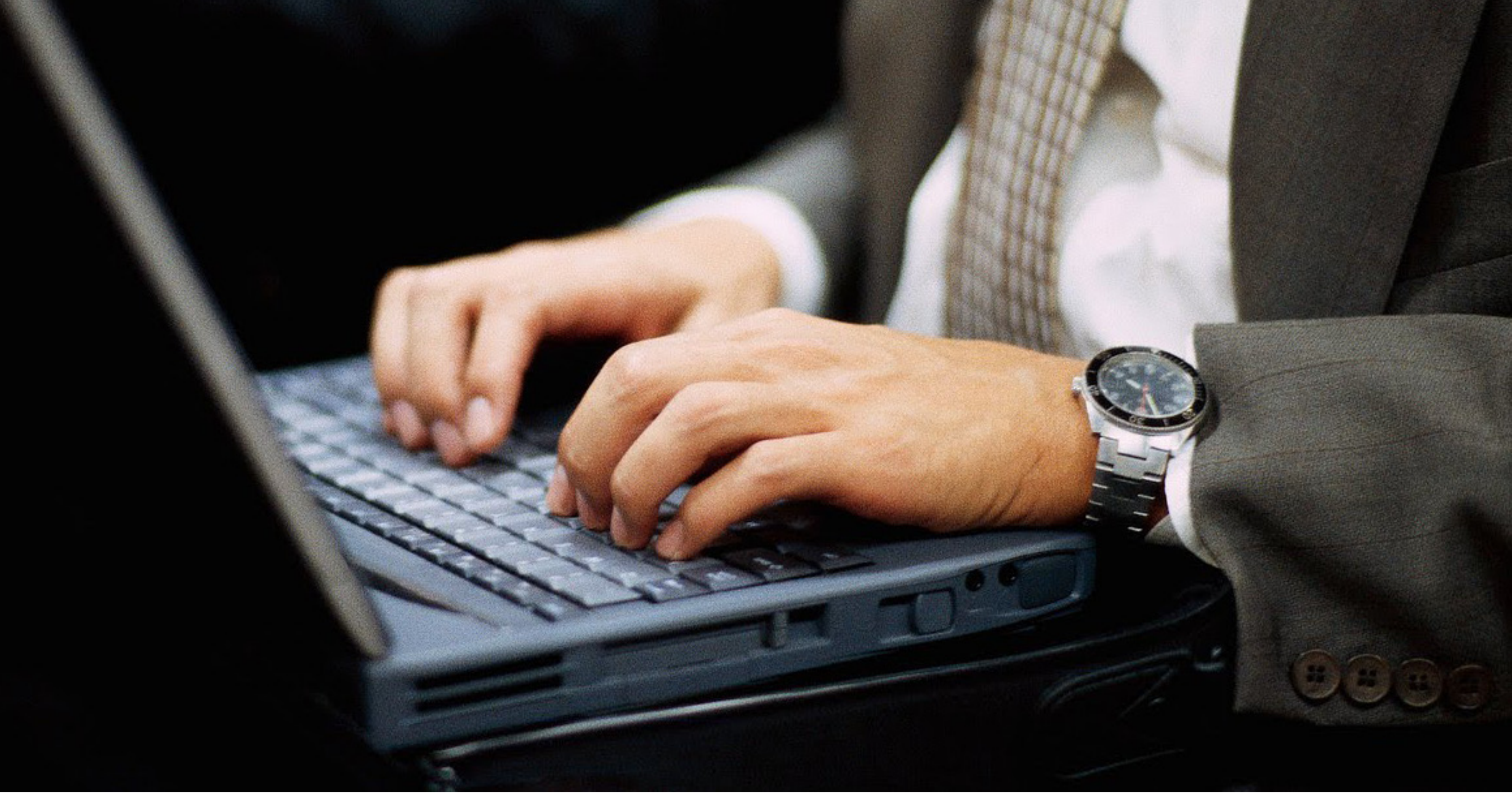
Rotman School of Management
UNIVERSITY OF TORONTO

A qualitative approach: adding context to four years of data insights

When examining how Canadian enterprises are approaching security in an age of intense technology disruption from innovations including mobile, cloud and social networking, an interesting continuum emerges. Some organizations are adamant about avoiding these types of innovations as a result of security concerns. They feel that saying "no" to innovation protects them from the inherent security risk. The organizations that are saying "yes" are at the other end of the continuum. They are emphasizing a balanced approach to security to help ensure the responsible adoption of innovation based on strategy, awareness, education and buy in. And along the continuum are the organizations that are aspiring to "yes," fashioning their security practices and infrastructures to make "yes" a distinct possibility and eventual reality.

Within the context of this continuum, TELUS and the Rotman School of Management at the University of Toronto broadened their approach to clarifying the state of Canadian IT security. After four years of trending Canadian IT security quantitatively, the research team chose to add a qualitative element in 2013 to layer the context on to the numbers. And so, the research team gathered security leaders from across the country, in a diverse array of sectors, at roundtables to discuss security with their peers. An additional dozen security experts were interviewed one on one to glean their insights.

The result is the 2013 TELUS-Rotman IT Security Study — offering professional insights, expert viewpoints and personal perspectives about Canadian enterprise security from the leaders living it every day. The context coming out of this year's report both augments and validates the quantitative data collected since 2008, and offers Canadian security leaders additional dimensions from which they can benchmark their organizations – real life experiences of security leaders and their organizations, actual strategies and progressive thought leadership.



What about IT security keeps you up at night?

The research team began every discussion with this question. It was a provocative inquiry, which resulted in four dominant themes emerging that shaped this year's contextual findings. These include:

- 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?

In exploring these themes, several key insights emerged including:

- For most security leaders, there is a pervasive sense of vulnerability about the inevitability of a breach event coupled with a lack of confidence in the ability to detect the event accurately to stem the tide of any potential damage.
- People represent the weakest link in the IT security chain, and organizations must understand how to protect IT systems from the threat with well-designed, strategically planned security awareness programs.
- Security must be convenient otherwise employees will circumvent it, rendering controls more of a risk to security than an enabler.
- "Yes" organizations, where security works in collaboration with employees to ensure the responsible adoption of innovation, are often times more secure than "no" organizations because they avoid the false sense of security that can come from a sole focus on rigid IT controls, which is common in "no" organizations.
- Brand impacts resulting from a security breach are more of a concern for some organizations than the associated direct costs.
- Security leaders are concerned about cloud adoption from a security perspective, but are planning on adoption in the next 12 – 18 months; enterprise-grade cloud services from reliable providers can help to address some of the wariness regarding security.
- Canadian organizations continue to devise ways to deal with IT security resource retention including high touch internal training; outsourcing; embracing innovation and positioning security as an enabler to promote a dynamic environment for security professional growth; and instituting aggressive retention programs in collaboration with HR.

Taking action: five recommendations to enable the move along the continuum to “yes”

In addition to providing a solid understanding of the context shaping security in 2013, the research team wanted to help organizations take action. The five recommendations are not meant to be all encompassing, as the exact scope of security is specific to every organization’s experience. However, they are targeted in response to the insights shared by security leaders about the trends and challenges they face in trying to achieve a balanced level of security. As well, they can help enterprises move more confidently along the continuum to “yes,” replacing a potentially false sense of security with a genuine sense that enables innovation adoption while mitigating security risks.

1. **Don’t assume you haven’t been breached** – make the resource, strategy and technology investments to detect breaches historically, implement a formal threat analytics program and initiate an employee security awareness program.

2. **Security diligence must be ongoing** – to ensure that security is a true business enabler, it must be embedded into all business processes, which requires ongoing collaboration with business leaders.

3. **Compliance is not the same as security** – compliance is the minimum security required, and the goal should be to work to find the right balance between risk and preparedness based on the business activities and operational models of the organization.

4. **Organizations should work to be “yes” organizations** – security leaders need to work with employees to uncover how innovation can be used in the most secure way possible, with that security being the most convenient possible.

5. **Awareness training is key** – security awareness training must be ongoing, and content must reflect the latest innovations and threats so that employees gain an understanding of the “why” behind security policies and procedures.

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.

To download the full report, visit **telus.com/securitystudy**