

# Study introduces a "security responsible" approach to technology innovation

April 30 2014, by Ken McGuffin

---

ELUS and the Rotman School of Management at The University of Toronto today released the 2014 TELUS-Rotman Security Study. Now in its sixth year, the annual survey tracks industry trends and documents the state of IT security in Canada. The 2014 report focuses on how enterprises can stay secure while making progressive innovation decisions by taking a "security responsible" approach.

Returning to a quantitative approach for this year's study, the research team surveyed more than 400 Canadian security professionals to get the pulse on trends it has been following since 2008. This year's study also includes global perspectives on the data, trends and analysis from key security thought leaders from companies including Salesforce.com, British Telecom and Cylance Inc.

"As we examined and analyzed the data, four key security best practices came into view: a strong focus on risk management, retaining the right skills and expertise within an organization, effective policies and governance, and employee education," said Dr. Walid Hejazi, professor of Business Economics, Rotman School of Management. "As our thinking crystalized, the concept of 'security responsible' emerged as the central theme of the research."

To quantify the concept of security responsible, the research team assigned a proprietary rating scale of zero to seven (with zero being the least and seven being the most responsible). Regardless of whether enterprises say 'yes' or 'no' to innovation, those that rate higher on the

security responsible scale experience more security success in terms of:

- Greater satisfaction with their security postures (mean rating of 3.8 vs. 3.2 out of 5)
- Fewer breaches (9.5 vs. 14.9 breaches, averaged during previous 12 months)
- Better risk management capability (mean rating of 3.6 vs. 1.5 out of 5)

However, the greatest business benefits are realized by organizations that say 'yes' to innovation in a security responsible manner; creating an environment where security and innovation both thrive.

"Canadian companies that embrace business-enabling innovations and are 'security responsible' enjoy the best of both worlds," said Hernan Barros, Director, Security Services, TELUS Security Solutions. "By taking a security responsible approach, an organization can realize productivity gains and cost savings through innovations like 'bring your own device,' social networking and cloud computing while maintaining a high level of security success."

Additionally, the report explores how security responsible organizations are more successful in the areas of employee retention, [mobile security](#) and dealing with advanced threats. The findings include:

- Employee retention: organizations that adopt business-enabling innovations with a security responsible approach are more than three times more likely to have no difficulty retaining security staff;
- Mobile security: while only 37 per cent of Canadian organizations take a security responsible approach to mobile security, those that do report higher satisfaction with their security postures.

- Advanced threats: a security responsible approach to advanced threats (rigorous threat monitoring procedures) drives down breach numbers and improves satisfaction (70 per cent for those with rigorous monitoring versus 39.5 per cent for those who don't actively monitor).

"The focus on 'security responsible' is really a call to action for Canadian enterprises," continued Mr. Barros. "The data shows us that executing on security in a responsible way delivers tangible benefits in terms of security satisfaction, lower breach numbers and improved risk management – all of which are key measures of security success. It is possible for every organization to take action on these findings by evaluating how security responsible they are and identifying where they can improve."

The report includes four key recommendations to help Canadian enterprises become more security responsible:

- Focus on risk: compliance is essential but is also the bare minimum; being risk-focused means continuously assessing the environment and understanding how a security breach could impact brand and revenue.
- Retain the right skills: the best and brightest security professionals have high standards when it comes to what constitutes good security practices and will move on quickly from organizations that aren't security responsible enough.
- Focus on policy diligence: proven standards and procedures offer the governance needed for technology decisions, including the adoption of business-enabling innovations.
- Educate employees: employees play a crucial role in [risk management](#), so it's important that they understand [security](#) policies, the rationale behind them and the pros/cons of compliance.

**More information:** The detailed breakdown and analysis of the data and recommendations are available online: [www.telus.com/securitystudy](http://www.telus.com/securitystudy)

.

Provided by University of Toronto

Citation: Study introduces a "security responsible" approach to technology innovation (2014, April 30) retrieved 19 April 2024 from <https://phys.org/news/2014-04-responsible-approach-technology.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.