Smashing the Stats for Fun and Profit

2009 SECTOR Briefing

Rotman - TELUS

Joint Study on Canadian IT Security Practices

Ben Sapiro, TELUS Security Labs

October 6, 2009

Oil and Gas • Finance and Insurance • Government
Manufacturing • Utilities • Construction • Retail • Health Care
Education • Professional Services • Information Technology

Calgary • Edmonton • Montreal • Ottawa • Toronto • Vancouver

TELUS
the future is friendly

Rotman School of Management
UNIVERSITY OF TORONTO

Why a Rotman-TELUS Study?

Why Canada?

- Canada is different than the US and needs to make decisions based on its OWN experiences

Why Rotman?

- Security is a business issue. Rotman is a business thought leader

Why TELUS?

- We are committed to security research through TELUS Security Labs

Why this study matters…

The study answers key questions like:

- What's happening to my peers?
- What issues should I be concerned about?
- How do I compare to top performers?
- What best practices should we adopt?
- What does "good enough" look like?

Three Things to Takeaway from Today

- Detection alone is not security
- Align with compliance to get support, not for end-of-job
- Budgeting processes are not optimal for an evolving security landscape

TELUS
the future is friendly

Rotman School of Management
UNIVERSITY OF TORONTO

Breaches are up, single breach costs down

- Annual breach costs reported at $834,149 up from $423,469 in 2008
- Average number of breaches at 11.3 up from 3.0 in 2008
- Average cost per breach has decreased significantly

Fastest Rising Breaches

1. Unauthorized access to information by Employees
2. Bots within an organization
3. Financial fraud
4. Theft of proprietary information
5. Laptop or mobile device theft

TELUS
the future is friendly

Rotman School of Management
UNIVERSITY OF TORONTO

What are organizations concerned with?

Top Breach Concerns

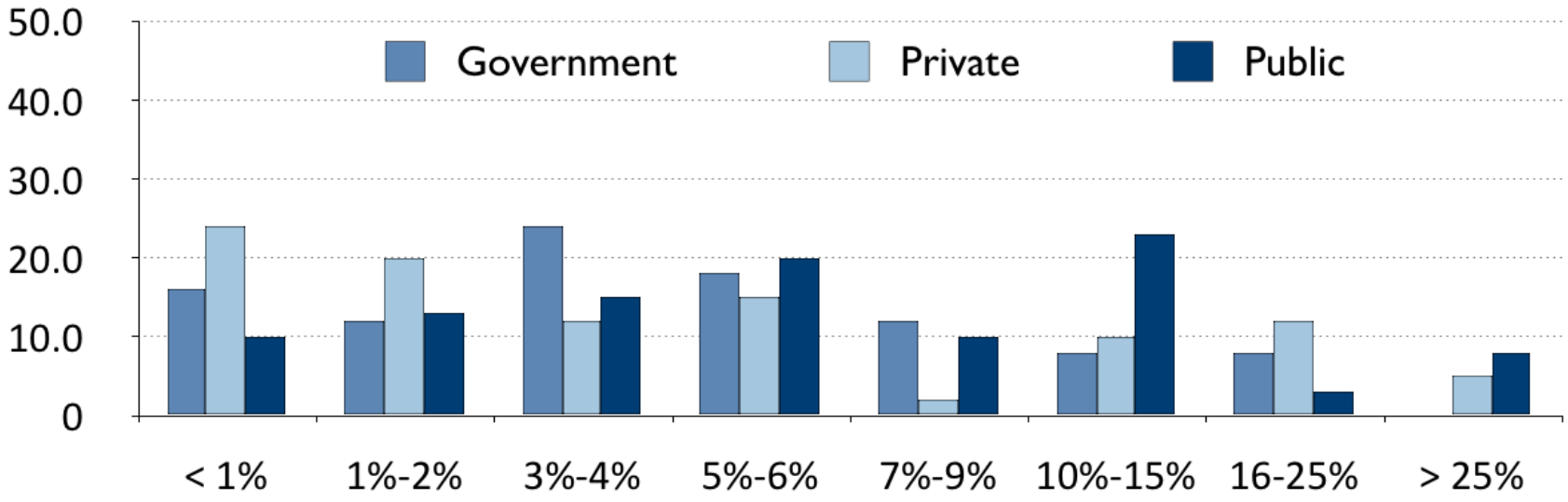
1. Damage to brand or reputation
2. Lost time to disruption
3. Lost customers
4. Regulatory actions
5. Litigation

Top Security Issues

1. Disclosure or loss of confidential data
2. Compliance with Canadian regulations and legislation
3. Business continuity and disaster recovery
4. Loss of strategic and corporate information
5. Employees understanding and complying with security policies

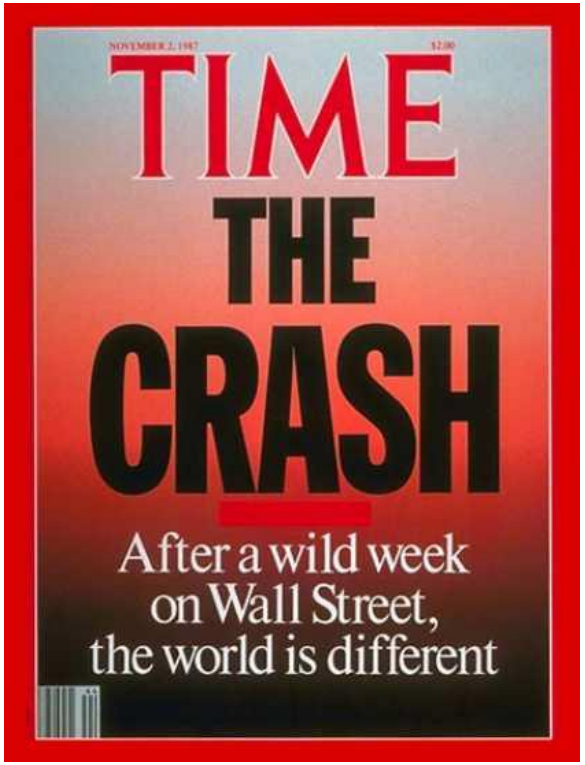
Security Budgets are struggling to keep up

- 7% of IT spend is the average
- Top performers had budgets of 15% of IT spend or more (5% in 2008)
- Budget effectiveness is highly sensitive to changes in threats



Impact of the Financial Crisis

- Budgets cut on average by 10% in 2009
- 25% reported an increase
- 20% reduced reliance on outsourcers and contractors
- 75% reported no changes to headcount



Governance and Education drive performance

- Using business-level security metrics increased the perceived value of security by 47%
- Awareness programs for staff and third parties drive better security performance (about a 50% increase)
- High performers twice as likely to Measure IT staff performance on security goals (accountability)

TELUS
the future is friendly

Rotman School of Management
UNIVERSITY OF TORONTO

Technology Investment is....

Driven by Malware...

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

"70% of organizations report malware related breaches"

not by insider threats...

- Data leakage prevention (23rd in sat)
- Log management (22nd in sat)
- Security Information & Event Management (20th in sat)
- Wireless Intrusion Prevention (19th in sat)
- Network Admission Control (18th in sat)

"Technologies which automate detection but not response have lower satisfaction"

Application Security

- Most orgs focus on detective approaches and investing in defending rather fixing
- Public companies are spending more time on secure development
- Internal development teams are least likely to bother with secure development
- Compliance centric organizations are significantly less likely to do secure development
- Preventative secure development leads to greater satisfaction with security programs

Security Testing is more than Hackers

- Who tests matters most - skills are important, but access to senior management wins (use the External Auditors)
- Tools are no replacement for experience
  - 76% of respondents don't have formal experience with development
  - Tools are falling out of favour
- Tools are a key part of a complete application security program, but they’re not the entire program

Align Budget Requests with Business Drivers

- Compliance and negative drivers are more successful
- Alignment with business enabled (for example - require security education for remote access)

Top Funding Justifications

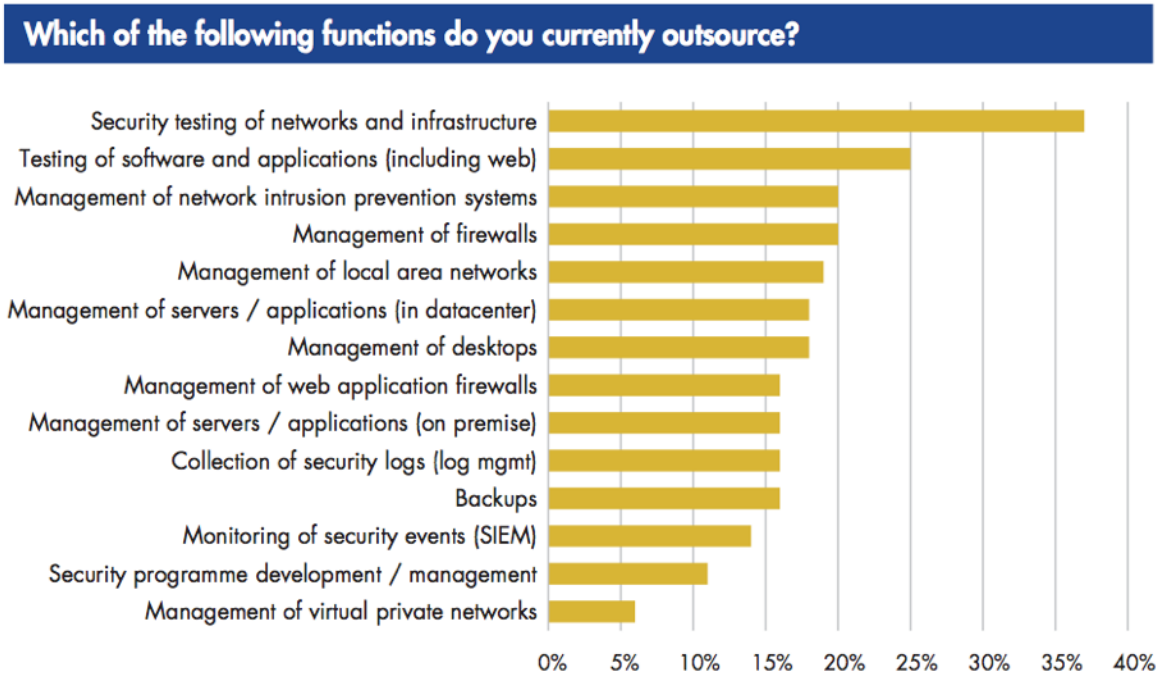
1. Compliance
2. Security Breaches
3. Risk from employees
4. Risk Management (losses)
5. Media/Reputation
6. Client/customer demand
7. Breaches at competitors & third parties
8. Security as a competitive advantage

Compensation of Security Professionals

- Certifications are less important, formal education is worth more
- CISA and CISM command a modest premium, so does business continuity - CISSP does not
- Twice as many lower paying organizations experienced high level of turnovers
- Publicly traded companies are most likely to pay more

Outsourcing and Cloud security share trust concerns

- 60% willing to outsource in 2009
- Privacy concerns lead to on-shoring
- Location of data greatest concern



Best practices of top performers

1. Manage the complete breach life cycle
2. Developing flexible programs based on threats
3. Focus on education for IT, Developers and employees
4. Balance technology spend with staffing

Three Things to Takeaway from Today

- Detection alone is not security
- Align with compliance to get support, not for end-of-job
- Budgeting processes are not optimal for an evolving security landscape

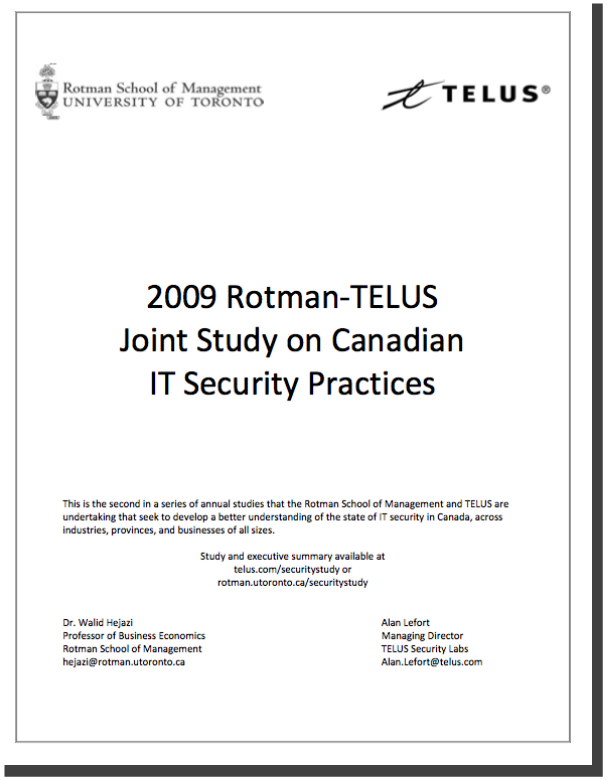
What else does the study cover?

Full study 80 pages long

- 50 pages of analysis
- contains full survey results

Covers the following in detail:

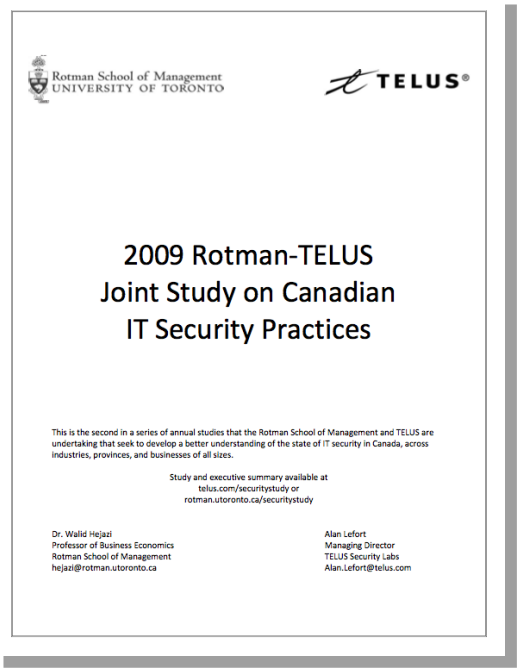
- demographics
- organizational structure
- governance, risk and compliance
- application security
- breaches
- outsourcing and cloud security
- technology initiatives



TELUS
the future is friendly®

Rotman School of Management
UNIVERSITY OF TORONTO

See TELUS booth for Executive Summary


Rotman School of Management
UNIVERSITY OF TORONTO

TELUS®

2009 Rotman-TELUS
Joint Study on Canadian
IT Security Practices

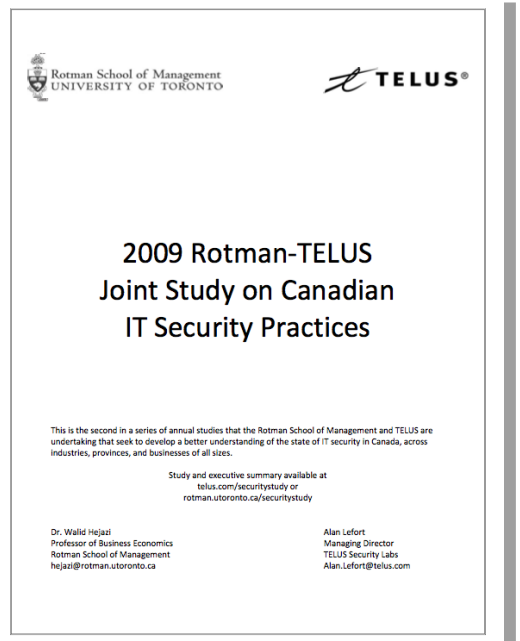
This is the second in a series of annual studies that the Rotman School of Management and TELUS are undertaking that seek to develop a better understanding of the state of IT security in Canada, across industries, provinces, and businesses of all sizes.

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

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

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

telus.com/securitystudy


Rotman School of Management
UNIVERSITY OF TORONTO

TELUS®

2009 Rotman-TELUS
Joint Study on Canadian
IT Security Practices

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

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

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

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

ben.sapiro@telus.com