

2009

Executive Briefing

Rotman - TELUS

Joint Study on Canadian IT Security Practices

Securing Government: A Canadian Perspective

Alan LeFort, TELUS Security Labs

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 Security Labs



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 in Government?
- What issues should I be concerned about?
- How do I compare to top performers in Government and Industry?
- What best practices should we adopt?
- What does “good enough” look like?

Breaches in Government are up, single breach costs down

- Annual Government breach costs reported at \$1,004,799 up from \$321,429 in 2008
- Average number of breaches at 13.4 up from 3.5 in 2008
- Average cost per breach has decreased to \$74,985 in 2009 from \$92,364 in 2008
- 33% of breaches come from inside

Fastest Rising Breaches

1. Unauthorized access to information by employees (33%)
2. Bots within an organization (18%)
3. Financial fraud (4%)
4. Theft of proprietary information (1%)
5. Laptop theft (50%)

What is Government most concerned with?

Top Breach Concerns

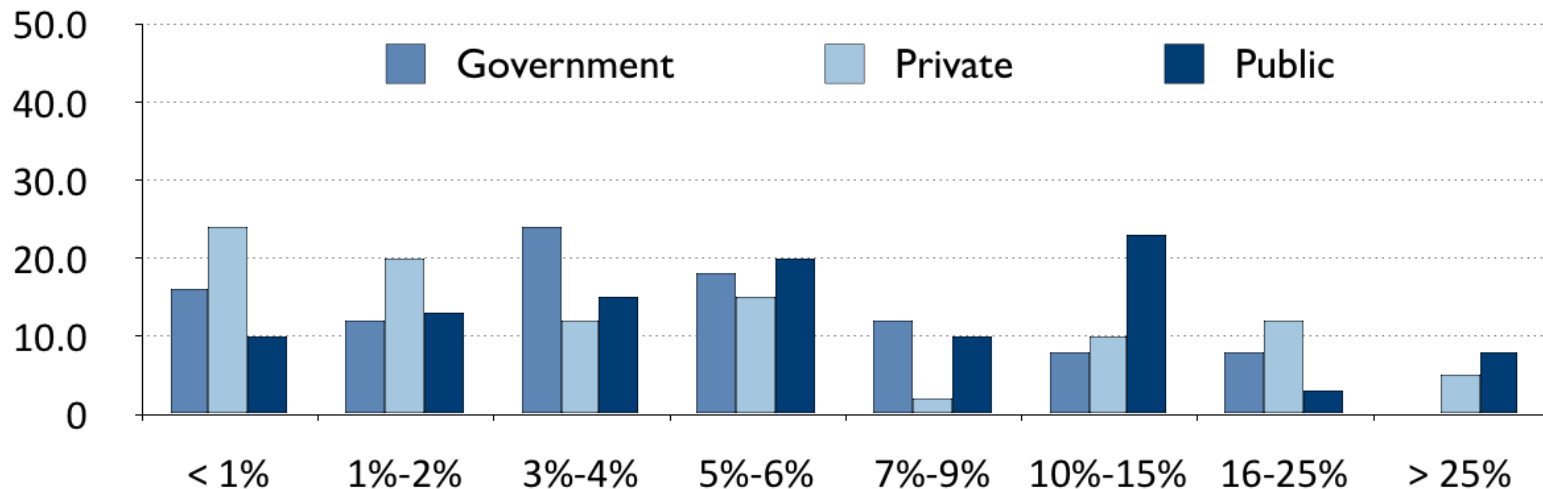
1. Damage to brand, reputation or image
2. Lost time due to disruption
3. Regulatory action
4. Litigation
5. Personal accountability

Top Security Issues

1. Damage to brand or reputation
2. Disaster recovery / business continuity
3. Compliance with Canadian regulation and legislation
4. Managing security of wireless and mobility devices
5. Employees understanding and complying with security policies

Security Budgets are struggling to keep up

- 3-4% of IT spend is the most common Government budget, followed by 5-6%. Below national average(7%)
- 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 in government by 5% in 2009 (versus 10% overall)
- 27% reported an increase in budgets
- 20% reduced reliance on outsourcers and contractors
- 75% reported no changes to headcount



Governance and Education key drivers of security 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)



Outsourcing and cloud security share trust concerns

- 60% willing to outsource in 2009
- Privacy concerns lead to on-shoring policy (41%)
- 59% actually outsourcing in last 12 months, focusing on testing, firewall management and IPS management

Table 50: Concern with security services in the cloud in ranked order (government organizations)

Concern	Ranking
We are concerned about the location of our data	1
We are concerned about connecting business critical systems to security mechanisms outside our full control	2
We are concerned about our ability to audit the environment for compliance with our security needs	3
We are concerned with the level of security in a multi-tenant environment	4
We are concerned about our ability to perform forensic analysis on cloud security systems in the event of a breach	5
We are concerned with the ability to remove/recover our data from the cloud	6
We are concerned that our availability needs cannot be met with a cloud-based service	7

Government Investment is....

Driven by breaches...

- 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”

Best practices of top performers in Government

- 1 Invest right amount of staff and give them sufficient authority *
- 2 Developing flexible programs based on threats
- 3 Focus on education for IT, Developers and employees
- 4 Balance technology spend with staffing

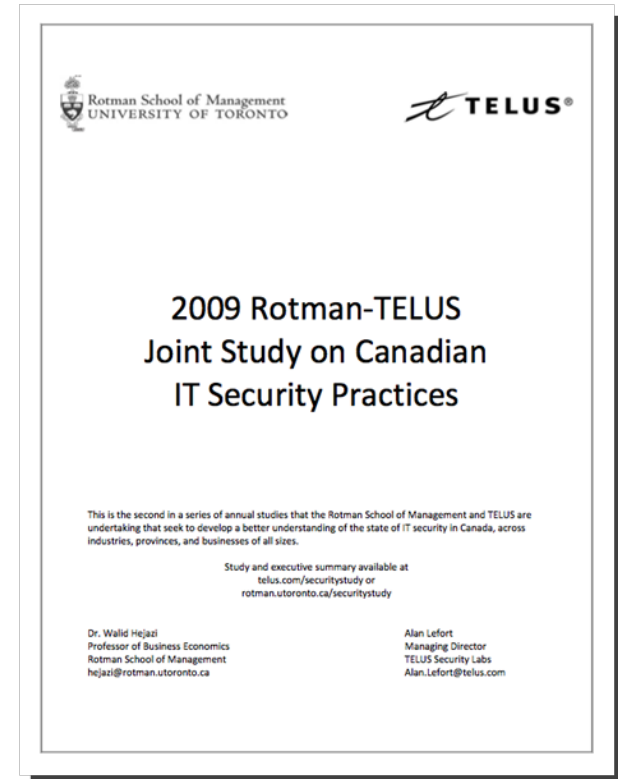
What else does the study cover?

Full study 80 pages long

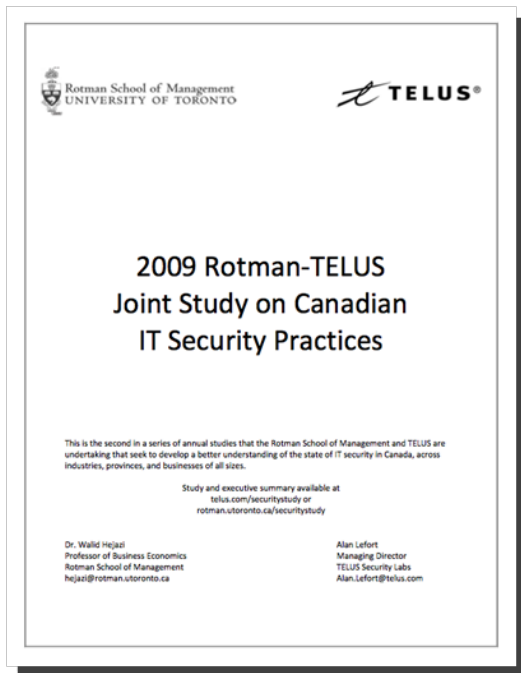
- 50 pages of analysis
- contains full survey results

Covers the following in detail:

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



See TELUS booth for Executive Summary



telus.com/securitystudy

Oil and Gas • Finance and Insurance • Government

Manufacturing • Utilities • Construction • Retail • Health Care

Education • Professional Services • Information Technology

2009 Rotman-TELUS Joint Study on Canadian IT security Practices

Calgary • Edmonton • Montreal • Ottawa • Toronto • Vancouver