2010

Hacking the stats for fun and profit

Rotman - TELUS

Joint Study on Canadian IT Security Practices

Ben Sapiro, TELUS Security Labs

VPN • Anti-Virus • Public Key Infrastructure • Encryption
Content Filtering • Patch Management • Identity and Access Management
Network Access Control • Endpoint Security • Firewalls • Log Management
Web Application Firewalls • Two-factor Authentication (tokens, smartcards)
IPS • SIEM • Vulnerability Scanning • Data Leakage Prevention

Breaches • Budgets • Concerns • Threats • Salaries
Technology • Initiatives • Outsourcing • Mobile • Social Networking
The Cloud • Applications • Staffing

Rotman School of Management
UNIVERSITY OF TORONTO

TELUS
the future is friendly

Why a Rotman-TELUS Study?

Why Canada?

- Canada has its own security culture. Decisions should be made using our own experiences

Why Rotman?

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

Why TELUS?

- We continue in our commitment 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 "secure enough" look like?

Study enhancements

Focused questions

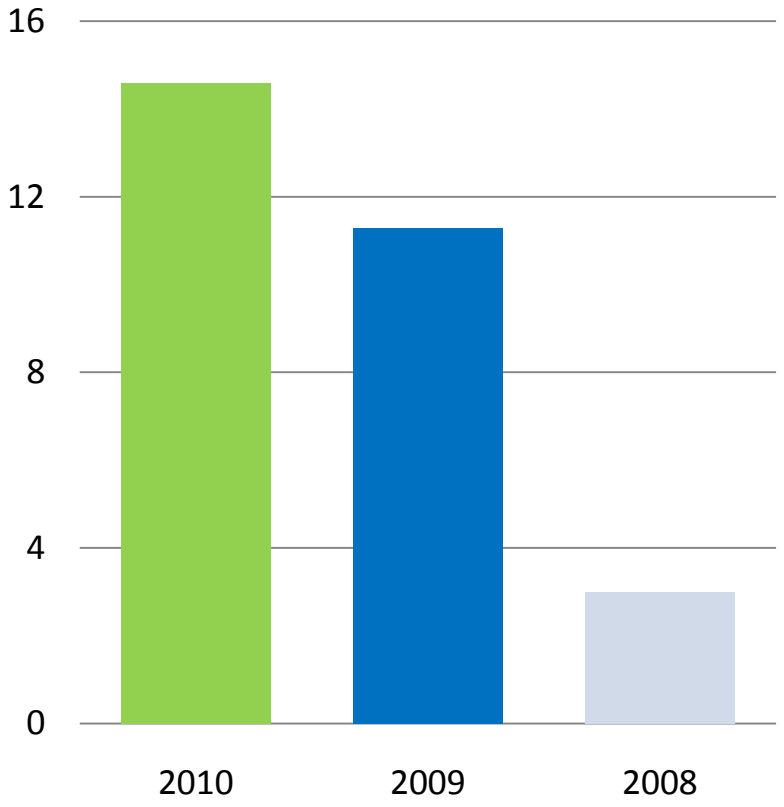
- Explored topics that were likely to change year-on-year
- Consolidated questions to improve response rates

Multiple releases

- Initial summary release in November
- Ongoing monthly updates focusing on single topics in 2011

The threat landscape continues to grow

- Breaches have grown nearly 1/3 from 2009
- Getting better at keeping out malware
- Breaches more focused on data



Insiders continue to be a problem

- 1 in 3 breaches originates internally
- Policy violations twice as likely by Executives and Management, Sales and Marketing only account for 20%
- Third parties, contractors and administrative staff more likely to comply with policy

Data loss and compliance top of mind

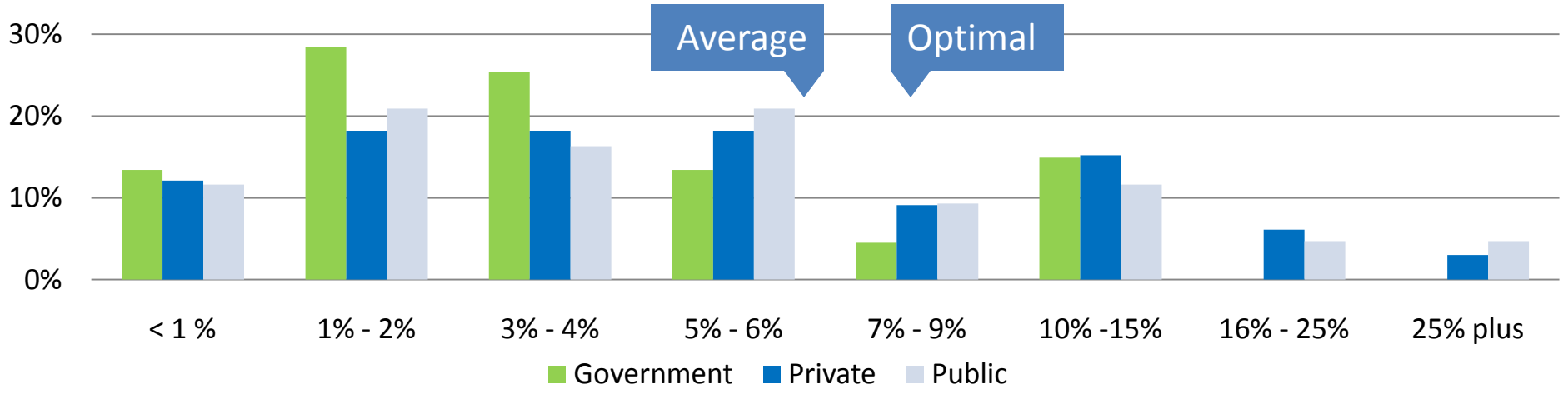
Ranked Concerns

1. Loss of sensitive data
2. Compliance with Regulations
3. Managing security of new technologies
4. User understanding and accountability of access
5. Managing business partner risks

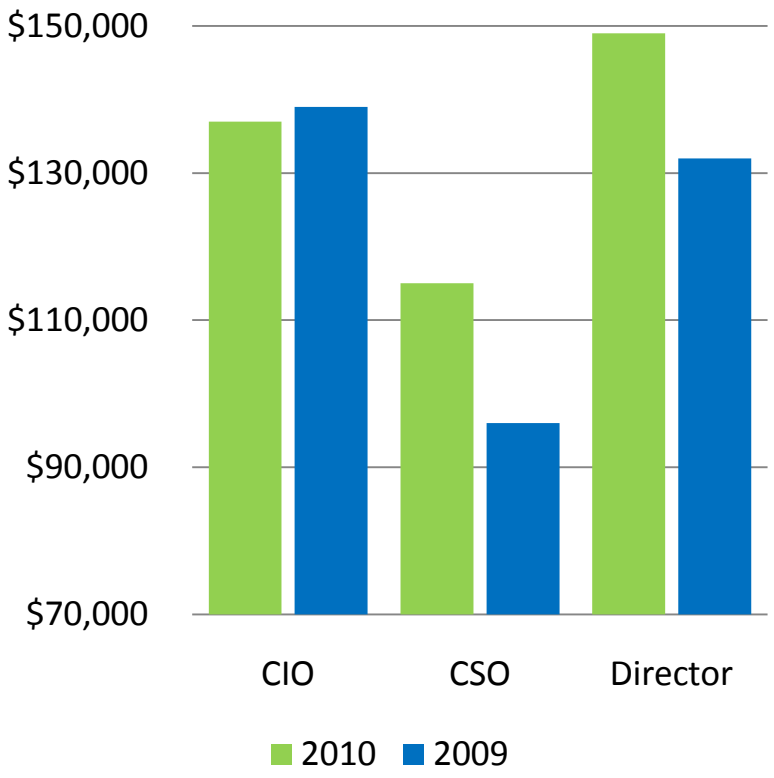
- Contracts are an effective mechanism for managing third party security compliance
- Publicly traded organizations more concerned about new technology, less concerned about user accountability

A pattern of under investment

- Budgets cut on average by 10% in 2009
- Less investment in 2010 with average budgets moving to 6.5% of the IT budget
- Use of outsourcing increased



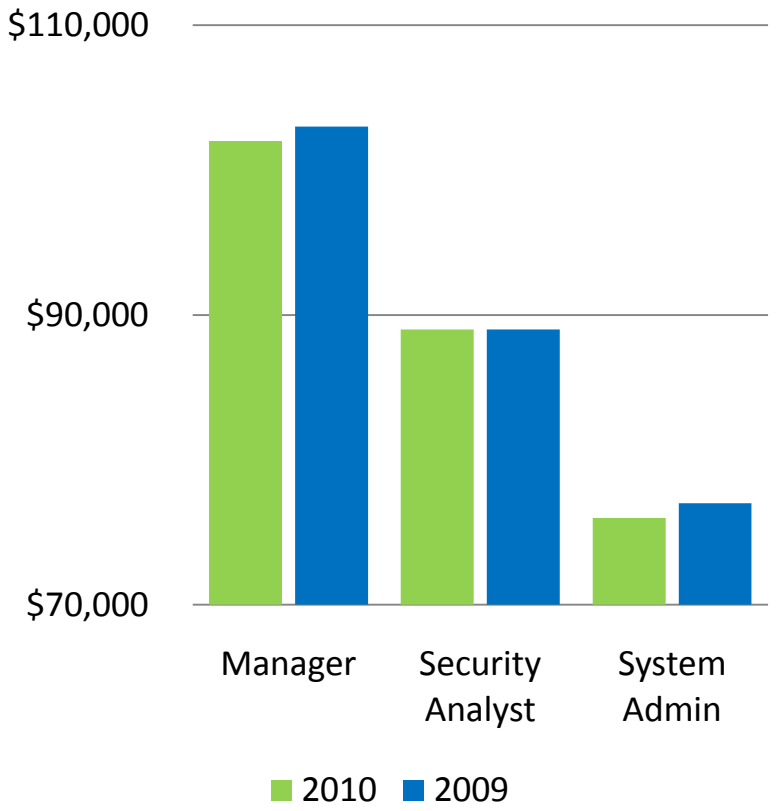
Security leadership in demand



- Managing security risks properly is increasingly by the business
- Majority of respondents have 10+ years of experience
- Most top earners had 6+ years in IT security

Watch for security employee satisfaction

- Managers and below are seeing slight salary reductions
- Individual security professionals are tasked with more
- Team sizes have shrunk



Secure development practices are lagging

- No significant increase in the number of companies using secure development practices
- A concern as respondents are reporting more data centric attacks
- However, those that are already include security into their development practices are increasing their investment

Invest in prevention

Top 5 Initiatives

1. Integration of security into development
2. Business partner security policy compliance
3. Business partner privacy policy compliance
4. Creating a vulnerability management process
5. Developing a security policy

Top 5 Technologies

1. SSL VPN
2. Firewalls
3. IPSEC based VPN
4. Anti-Virus
5. Email Security (anti-spam, anti-malware)

Complexity undermines initiatives

- Complex technologies, such as encryption, are failing to deliver value
- Technology integrators are not addressing requirements management

Lowest ranked technologies

20. Security Information & Event management (SIEM)
21. Data Leakage Prevention
22. Application Security Assessment Tools (web/code)
23. Database Encryption
24. Email Encryption

A note of caution

Increasing breaches coupled with reduced budgets and increased security workloads are laying the ground for further erosion of our security posture

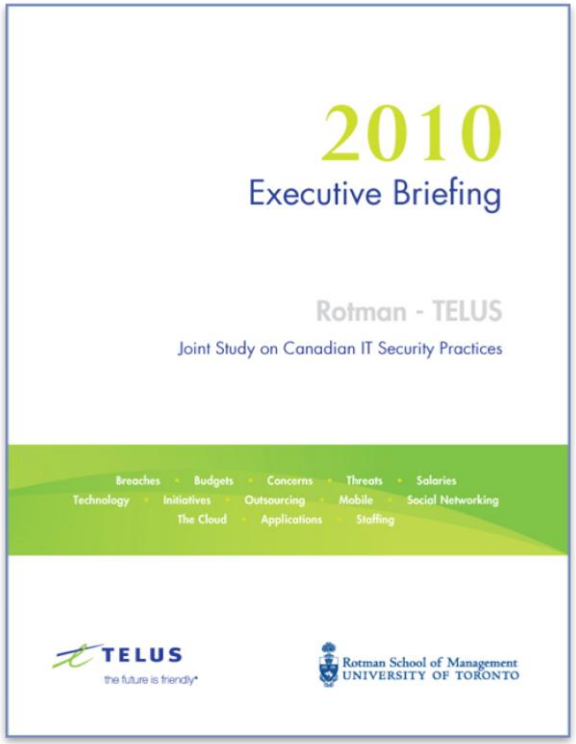
Top performers

- Building capabilities to manage the vulnerability lifecycle from start to finish
- Investing in senior leadership
- Integrating security into their development lifecycle

Rotman School of Management
UNIVERSITY OF TORONTO

TELUS
the future is friendly

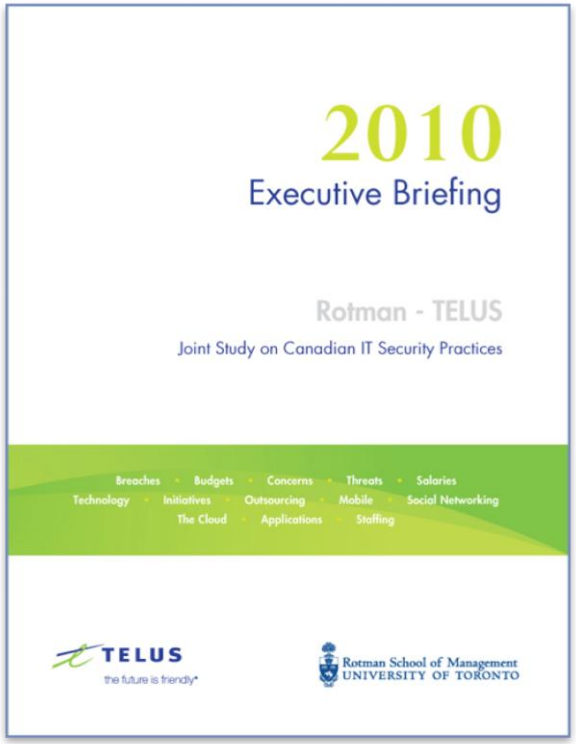
Available November 9th



telus.com/securitystudy

VPN • Anti-Virus • Public Key Infrastructure • Encryption
Content Filtering • Patch Management • Identity and Access Management
Network Access Control • Endpoint Security • Firewalls • Log Management
Web Application Firewalls • Two-factor Authentication (tokens, smartcards)
IPS • SIEM • Vulnerability Scanning • Data Leakage Prevention

Breaches • Budgets • Concerns • Threats • Salaries
Technology • Initiatives • Outsourcing • Mobile • Social Networking
The Cloud • Applications • Staffing



ben.sapiro@telus.com