

# Lessons from the Rotman TELUS Joint Study of IT Security Practices

Roger Tremblay  
Principal Consultant - TELUS Security Solutions

October 18<sup>th</sup>, 2011



# Agenda

1. The Rotman-TELUS Joint Study of IT Security Practices
2. Key Findings
3. Survey results as they relate to Government of Canada
4. Threats and Challenges faced by Canadian public sector organizations

# Agenda

1. **The Rotman-TELUS Joint Study of IT Security Practices**
2. Key Findings
3. Survey results as they relate to Government of Canada
4. Threats and Challenges faced by Canadian public sector organizations

# 2010

## Rotman - TELUS

### Joint Study on Canadian IT Security Practices

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

# 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

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

# 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?

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

# Regular releases and posts on Security

- Ongoing monthly updates focusing on single topics over subsequent year
  - *Mobile Security*
  - *Managing the risks of Social Networks*
  - *Financial Industry in Canada*
  - *Maintaining Threat Awareness*
  
- Through the summer, weekly blog posts on Security
  - [www.telustalksbusiness.com](http://www.telustalksbusiness.com)

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

# Questions that shaped our 2010 Study

1. Would budgets return to 2008 levels (i.e. pre financial crisis)
2. Would breach costs continue to rise or come down, and why?
3. How would the challenges experienced in 2009 shape security plans for 2010?
4. What impact would the prevalence of new technology trends like enterprise mobile computing, social networking, virtualization and cloud computing have on security?

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

# Questions that shaped our 2011 Study

1. Breaches in the age of global hacks: numbers, types of incidents, and insider/outsider sources
2. Top concerns from senior management (Compliance vs. Risks vs. Costs)
3. Satisfaction with technologies – are they delivering the value proposition?
4. Insights into the introduction of mobile devices into the workplace
5. The relative value in security for people, processes and technology

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)

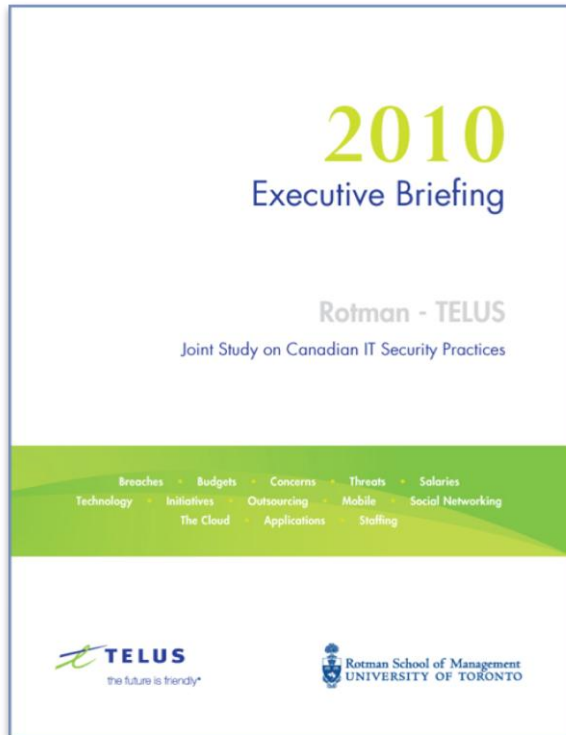
IPS • SIEM • Vulnerability Scanning • Data Leakage Prevention

Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# Available online



[telus.com/securitystudy](http://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

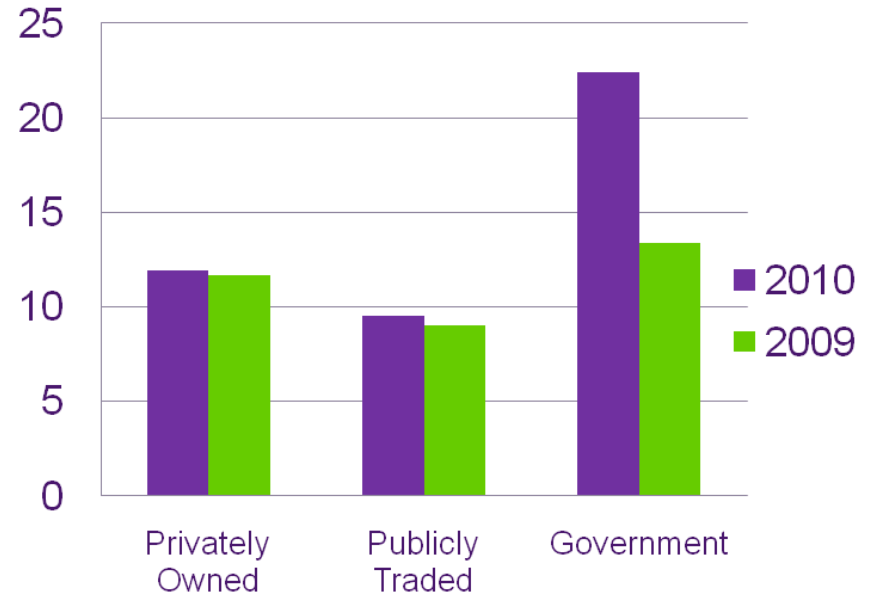
# Agenda

1. The Rotman-TELUS IT Security Study
2. **Key Findings**
3. Rotman-TELUS Survey results as they relate to Government of Canada
4. Threats and Challenges faced by Canadian public sector organizations

# The threat landscape continues to evolve

- Breaches up, costs down
  - Canadian security breaches rose 29%
  - Breach costs decreased by 78% to an average of \$179,508

**Breach Increases  
2009-2010  
(Avg # in last 12 Mo)**



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

# Attacks are more focused

## Top Breach Types

1. Malware and spam
2. Device theft
3. Phishing
4. Unauthorized access to information by employees
5. Bots within the organization / Denial of Service attacks

- Getting better at keeping out malware and common attacks (21% drop)
- Attackers are apparently becoming more focused and sophisticated

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

# Insiders continue to be a problem

- 1 in 3 breaches originates internally
- Policy violations twice as likely by Executives and Management
- Third parties, contractors and administrative staff more likely to comply with policy
- Security performance improves when security is outsourced

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

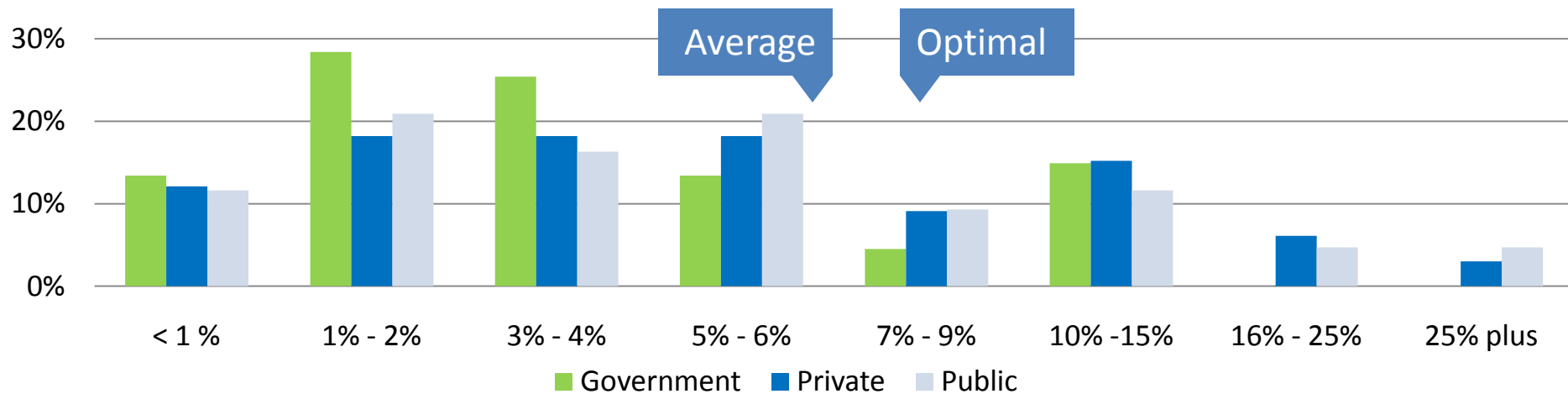
Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# 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 has increased



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

# Secure development practices are lagging

- No significant increase in the number of companies using secure development practices
- 1 in 4 respondents just assume secure development will happen
- 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
  - Twice as likely to adopt preventative practices
  - ~90% test their system security

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

# Investments 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)

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)

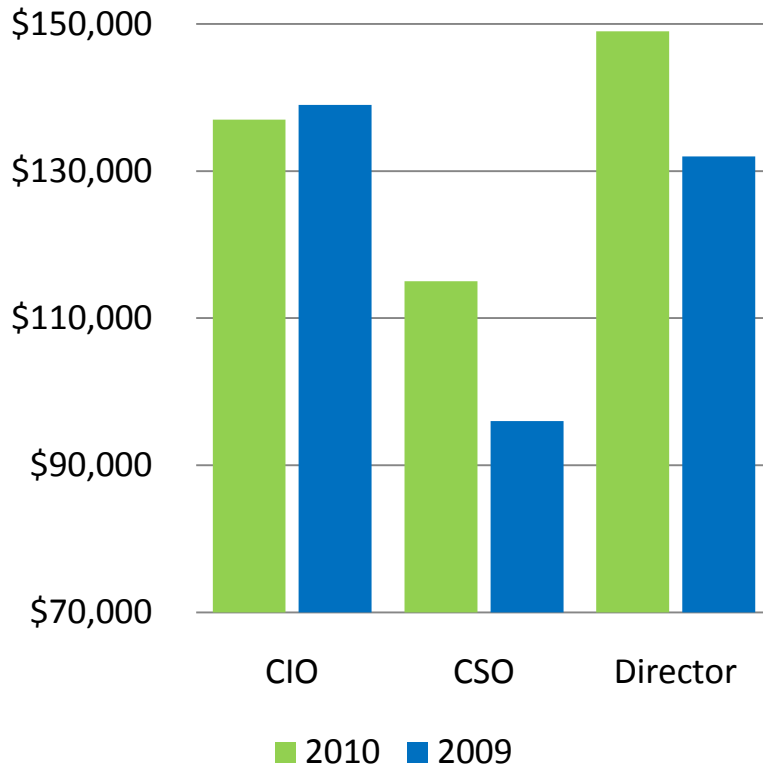
IPS • SIEM • Vulnerability Scanning • Data Leakage Prevention

Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# Security leadership in demand



- High calibre professionals required to balance risks with business requirements
- Ability to communicate with business is key
- Only half of respondents have 10+ years of experience
- Most top earners had 6+ years in IT security

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

# Data loss and compliance top of mind

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

## Ranked Concerns (Gov.)

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

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

# Complexity undermines initiatives

- Complex technologies are still 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

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

# Agenda

1. The Rotman-TELUS IT Security Study
2. Key findings
3. **Rotman-TELUS Survey results as they relate to Government of Canada**
4. Threats and Challenges faced by Canadian public sector organizations

# 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

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

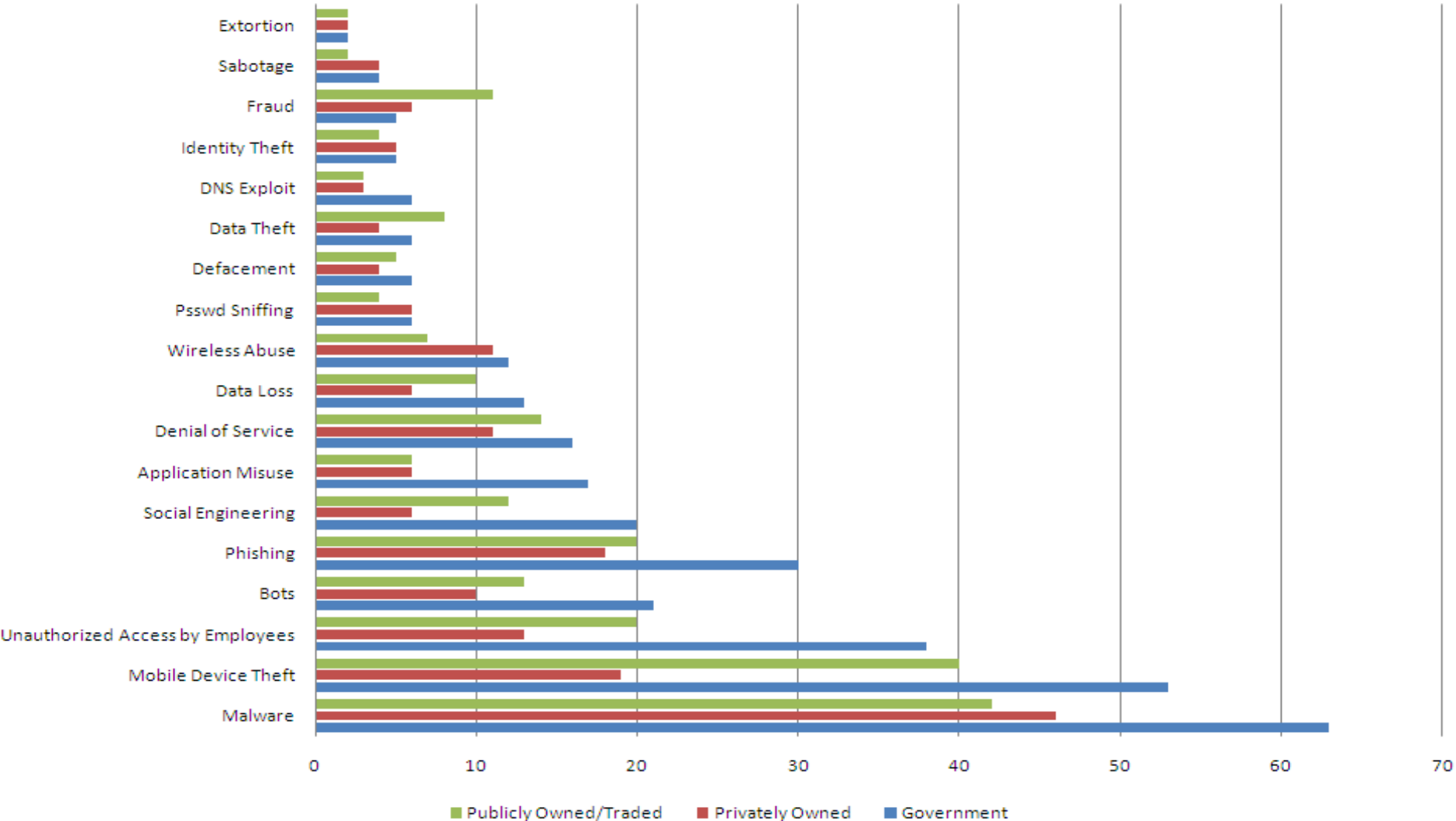
Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# Security Breaches - Government

Breach Type per Legal Ownership



# Security Concerns

## Ranked Concerns (Gov.)

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

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

# 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 security guidelines

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

# Top performers

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

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

# Agenda

1. The Rotman-TELUS Joint Study of IT Security Practices
2. Key Findings
3. Survey results as they relate to Government of Canada
4. **Threats and Challenges faced by Canadian public sector organizations**

# Threats and Challenges

- Given the rise in reported breaches and targeted threats, organizations need to acquire new capabilities to:
  - Increase focus on education and awareness
  - Manage the complete breach or incident lifecycle (including preventing measures)
  - Develop strong core capabilities and the ability to adjust rapidly

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

# Cloud computing concerns

## 2009 Concerns

1. Data location
2. Outside the business
3. Multi-tenancy
4. Ability to audit
5. Remove data from the cloud
6. Difficult to perform forensics
7. Availability

## 2010 Concerns

1. Malicious control of the hypervisor
2. Keeping VM images patched
3. Shared resource dependencies
4. Monitoring inter-VM communications
5. No visibility into host system security

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

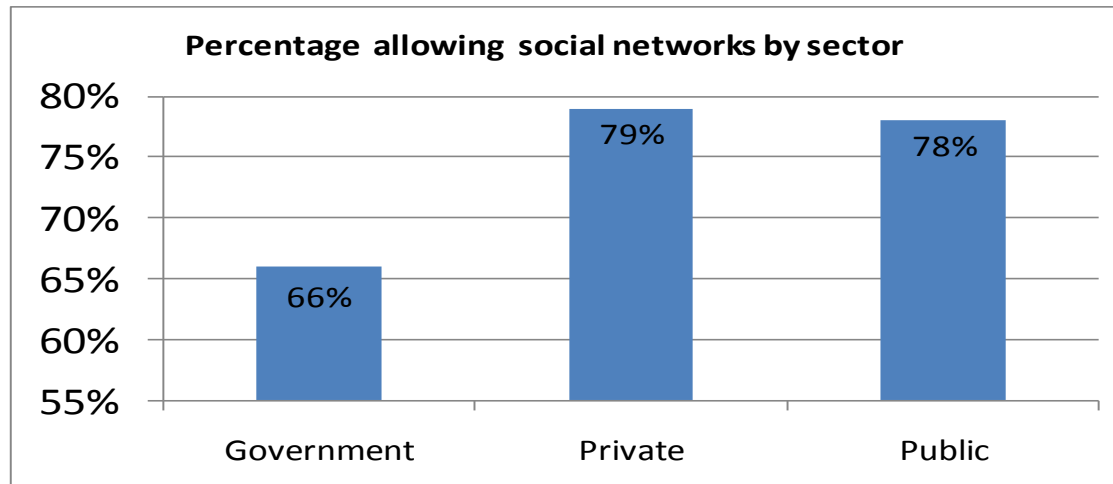
Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# Social Networking and Security

- Two government organizations in three allow access to social networking sites in the workplace
- Organizations that block quote security as the primary reason followed by productivity concerns and brand management



# Response to concerns and perceptions

- Blocking access to social networks may have benefits; however, it does not reduce the occurrence of breaches and may even distract organizations from the important task of risk management.
- Using the issue of social networks as a mean to educate users on security can improve an organization's security significantly.

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

# Recommendations

- Clear rationales and education are essential to user understanding
- Block selectively, not all social networks activities carry equal risks
- Cover all access points, limiting user's abilities to circumvent the control
- Maintain the existing security posture, look to integrate blocking into broader security initiatives

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

# Mobile Devices in Complex Environments

- Increasing use of personal mobile devices
- Provisioning of IT equipment may not remain straightforward

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

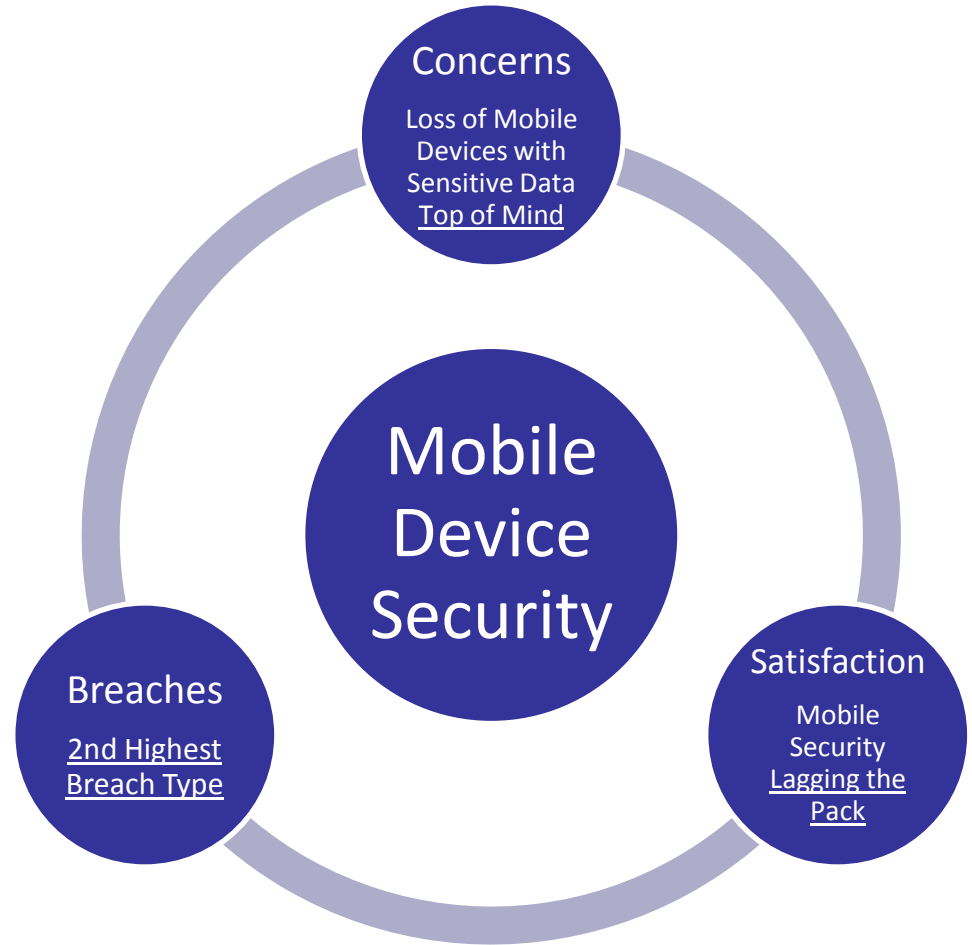
Breaches • Budgets • Concerns • Threats • Salaries

Technology • Initiatives • Outsourcing • Mobile • Social Networking

The Cloud • Applications • Staffing

# Mobile Security Industry has work to do

- Mobile breaches 2nd highest breach category
- Loss of mobile devices with sensitive information top concern for all organizational types
- Satisfaction with Mobile Security lags most technologies



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

# Response to Concerns and Perceptions

- Establish a mobile security strategy, governance and policy
- Use a risk management approach to mobility
  - Maximize protection of corporate data
  - Increase control of the device
- Minimize impact to the end user

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

# Recommendations

- **Strong governance and security posture**
  - Assessing the overall risks and readiness for adoption
  - Clearly communicating the policies that govern use
- **Education and communication are essential**
  - User awareness and engagement to mitigate risks
- **Technical enforcement and monitoring**
  - Available technologies have varying levels of maturity: few with end to end capabilities, trade-offs or multiple solutions may be required.

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

# 2011 Study

---

To receive the 2011 Rotman-TELUS Study as soon as it is published, email us at [pssecurity@telus.com](mailto:pssecurity@telus.com) and we will send it to you later this fall.

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

# Thank You!

Roger Tremblay – TELUS Security Solutions

[roger.tremblay@telus.com](mailto:roger.tremblay@telus.com)

613-683-1619

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