www.pwc.com

Detecting and Deterring Fraud

Aboriginal Financial Officers Association of Saskatchewan

September 30, 2015

pwc

Agenda

1. Introduction
2. Impact of Fraud
   - *PwC 2014 Global Economic Crime Survey*
3. Fraud Environment
   - *Common Themes and Red Flags*
4. Fraud Trends
   - *Cyber Crime, Theft of Assets, Employee Expense Fraud, Procurement Fraud*
5. Fraud Prevention
   - *Anti-Fraud Regime Framework*
   - *Compliance Sensitive Accounts*
   - *Corporate Intelligence and Due Diligence*
6. Conclusion

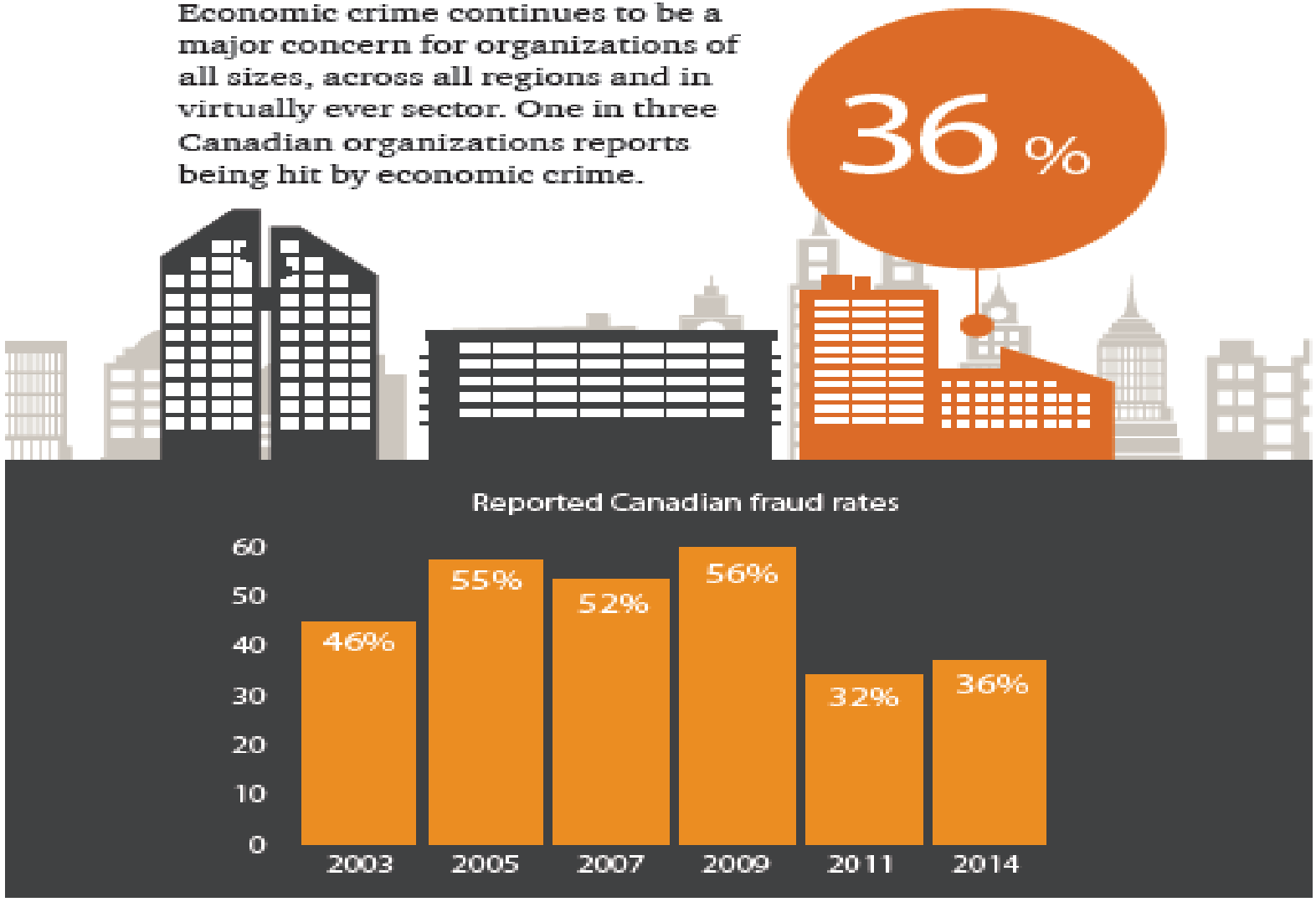
1. Introduction

2. Impact of Fraud

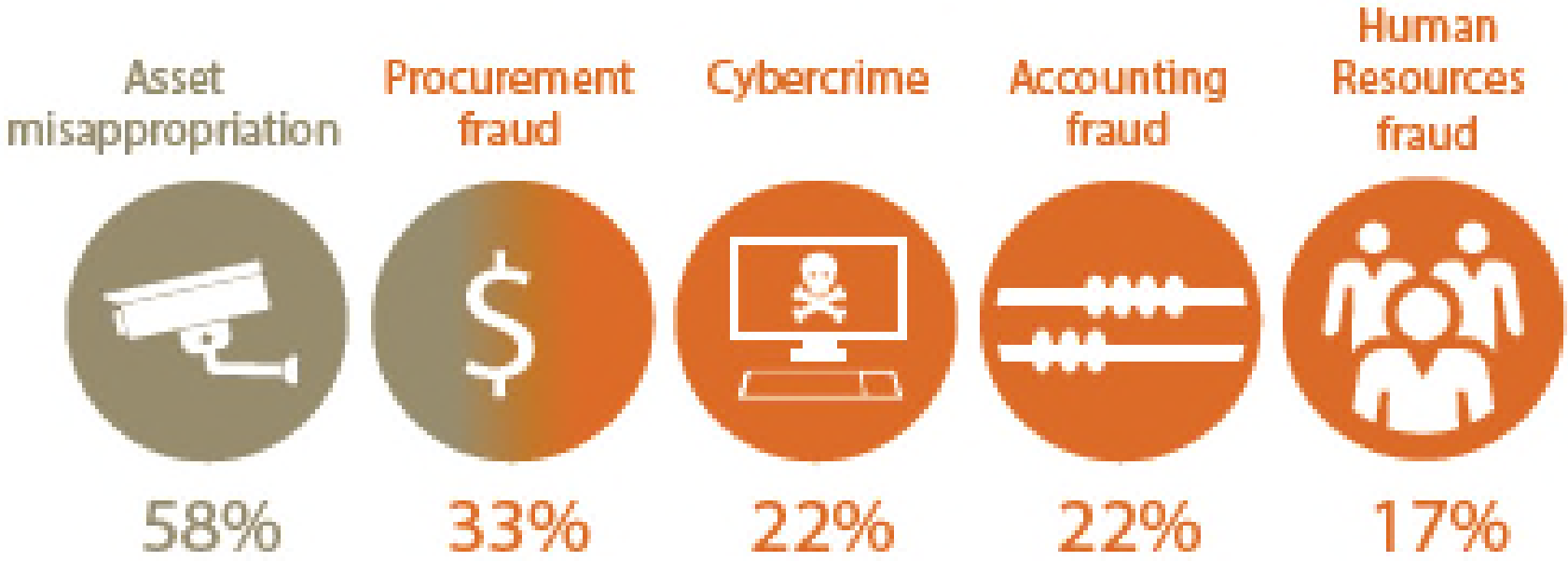
PwC 2014 Global Economic Crime Survey

The Big Picture

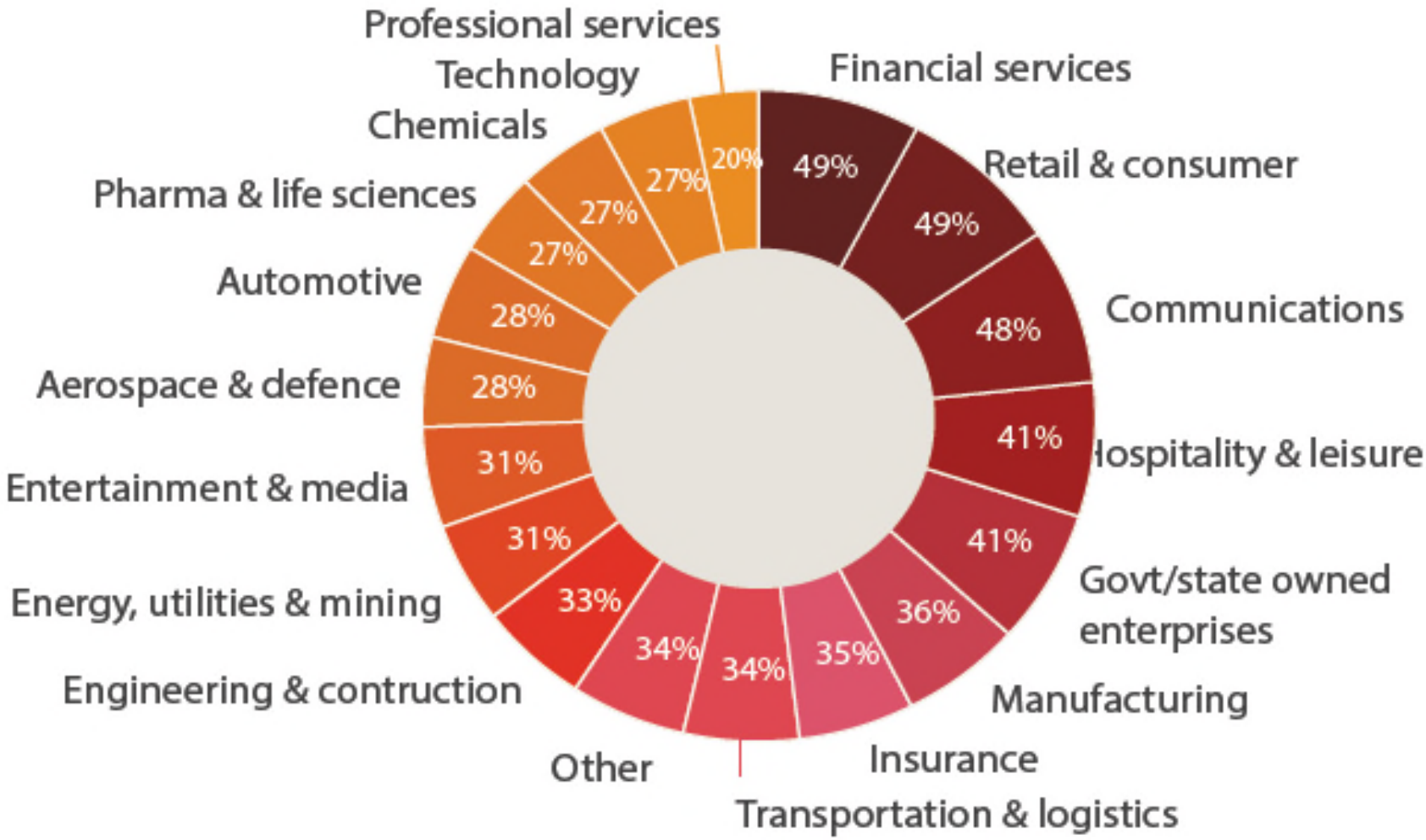
Economic crime continues to be a major concern for organizations of all sizes, across all regions and in virtually ever sector. One in three Canadian organizations reports being hit by economic crime.



Most commonly reported types of economic crime



Crime by industry



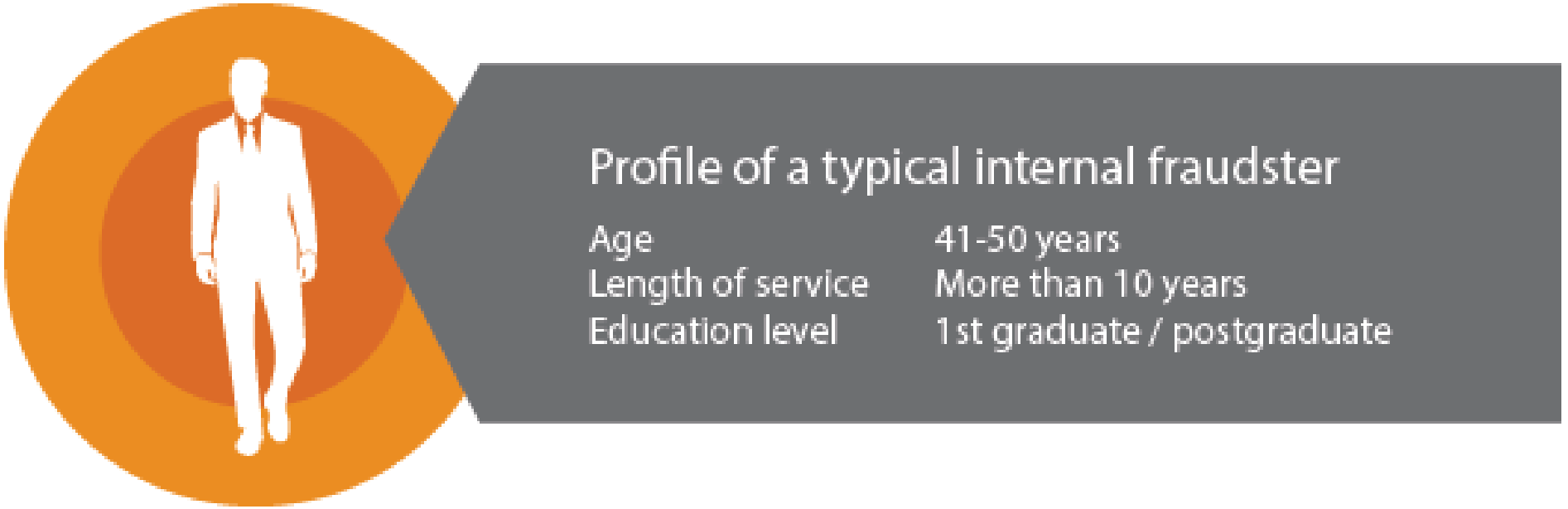
Cost of Economic Fraud

Fallout from fraud is not simply the direct costs. Can also impact:

- Staff morale/motivation
- Reputation/brand image
- Business relationships with customers, suppliers, stakeholders, etc.
- Relationship with funding sources and lenders
- Programs and resources
- Reallocation of staff time

Typical Internal Fraudster

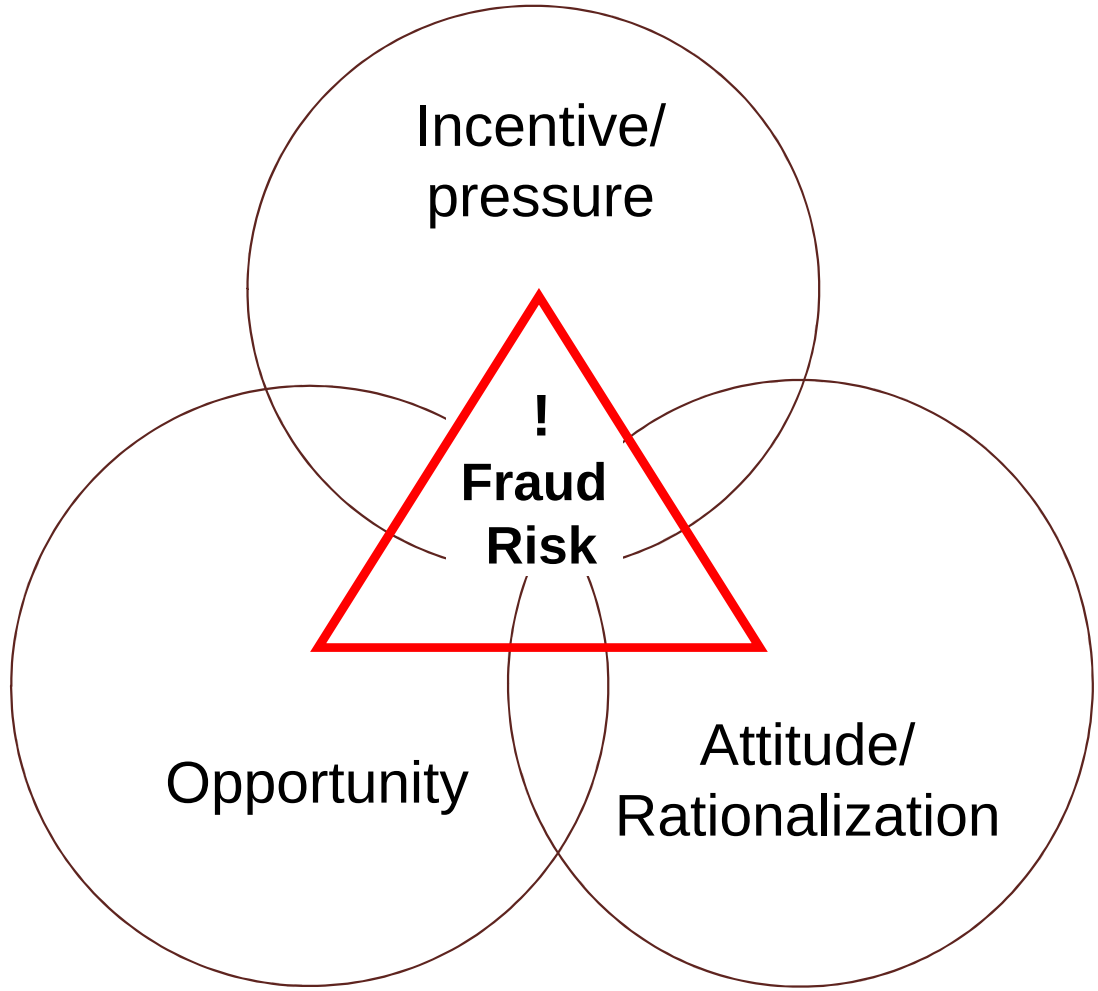
61% of the economic crimes reported were perpetrated by an employee.



Rule of Thumb

The Perfect Storm

Three conditions commonly found when a fraud occurs:



3. Fraud Environment

Common Themes

Red Flags

Typical Environment in Which Fraud Occurs

- Poor tone from the top
- Trust is placed in employees
- Employees have detailed knowledge of the accounting systems and its weaknesses
- Management domination subverts normal internal controls
- Expected moral behaviour is not communicated to employees
- Unduly liberal accounting practices
- Ineffective or nonexistent internal auditing staff
- Lack of or ineffective internal controls combined with liquid assets
- Poor accounting records
- Incomplete and out of date procedural documentation

Red Flags of Fraud

- Round dollar invoices
- Insufficient description of service on invoices
- Management/control override
- Lack of segregation of duties
- Inadequate processes for approving payment
- Inadequate matching procedures for payment approval
- Cash payments
- No vendor on boarding due diligence process

4. Fraud Trends

Cyber Crime

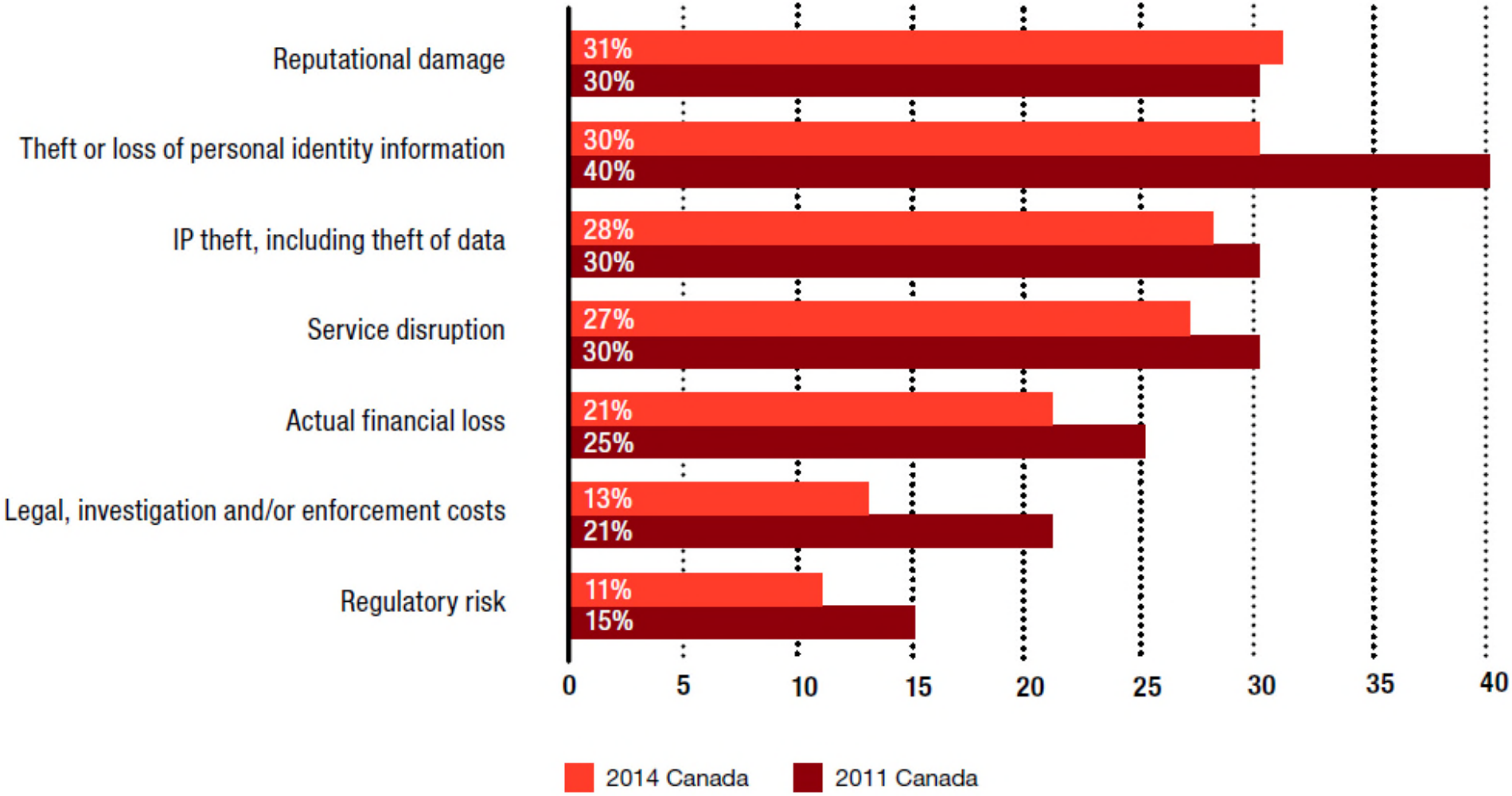
Theft of Cash /Other Assets

Employee Expense Fraud

Procurement Fraud

Cyber Crime in our Networked World

What do organizations care about? (PwC GECS 2014)



Theft of Cash / Other Assets

- Asset misappropriation is the most common type of fraud reported by companies
- This could include theft of cash or any other company assets
- Theft of inventory (e.g., supplies)
- Theft of confidential information
- Theft of cheque stock or cheque tampering to obtain money

Theft of Cash / Other Assets (continued)

- Some Red Flags
  - Payments to unknown employees and casual staff
  - Payments to unknown vendors and suppliers
  - Approval after payment has been made
  - Management override
  - Lack of segregation of job duties and approvals
  - Lack of a well-conceived and designed approval procedures for payments including matching process for payments
  - Lack of effective anti-fraud risk management plan

Employee Expense Fraud

- There is a significant amount of abuse in this area
- Some red flags:
  - Falsified receipts and invoices
  - Expenses without supporting receipts
  - Re-use of receipts
  - Lack of approval or inappropriate level of approval on expenses being claimed
  - False claims (meals, mileage, etc.)
  - Unauthorized claims or payments

Procurement Fraud

- Be alert for purchases that violate procurement policies
- Remember these questions and considerations:
  - Were proper procurement processes followed?
  - Competitive tendering when appropriate
  - Were proper approvals obtained?
  - Do invoices have appropriate signatures before being paid?
  - Remember value-for-money / quality of goods and services
  - Disclosure of conflicts of interest
  - Be alert for fictitious vendors and/or invoices

5. Fraud Prevention

Anti-Fraud Regime Framework

Compliance Sensitive Accounts

Corporate Intelligence and Due Diligence

The Anti-Fraud Regime Framework

Eight Components of an Anti-Fraud Regime

- Governance – Oversight by the Audit Committee and the Board
- Fraud Risk Assessment
- Code of Business Conduct and Ethics
- Incident Reporting Mechanisms – internal and external
- Investigative Protocol
- Remediation Protocol
- Hiring and Promotion Policies and Procedures
- Management Evaluation and Testing

Components of an Effective Anti-Fraud Regime

- An effective anti-fraud regime includes all eight components;
- All components are equally important and inter-related
- Identify areas of heightened risk through fraud assessment and analysis
- Ensure policies, procedures, processes and practices are in place to prevent, detect and react to fraud
- Effective anti-fraud regimes require ongoing assessment, analysis, training including fraud risk assessments and annual fraud audits
- Effective anti-fraud regimes require support at all levels of your organization starting at the top

Compliance Sensitive Accounts

- Inter-company Transfers
- Gifts
- Donations
- Charities
- Sponsorships
- Entertainment
- Training
- Marketing/Consulting Fees
- Legal Fees
- Audit/Tax Fees
- Commissions
- Travel
- Customs/Duties
- Visas/Permits/Licences
- Security
- Other/Miscellaneous Accounts

Corporate Intelligence and Due Diligence

- In today's environment, it is important for organizations to obtain relevant and timely information to make **informed business decisions**
- A significant problem faced by many companies today is the sheer volume of information available
- Corporate Intelligence is the **gathering and analysis of facts** presented to decision-makers in a **clear and concise** manner, and is a key component of an anti-fraud and anti-bribery & corruption regime

Failure to know the background of an individual or entity with whom you are dealing can be very costly.

Corporate Intelligence and Due Diligence

The reasons to consider background research and due diligence include:

- Do you truly know who you are dealing with?
- Are there issues or information that you are not aware of that would influence your decision to become involved with these individuals or organizations?
- Does the information available to you make sense, does it pass the “Smell Test”

Areas of vulnerability that can be addressed include:

- Employee hiring and promotion
- Investment partners
- Vendors and service providers
- Changes to a relationship or circumstances
- New information relating to an existing relationship

Corporate Intelligence

Background checks use a wide range of private and public databases to determine what information is available in the public domain, including but not limited to:

BCS checks often include a combination of the following for <u>individuals</u>:

- Criminal records
- Bankruptcy and credit history
- Personal certification and educational/professional verification
- Driving records/vehicle registration
- Litigation and court record searches
- Directorship and business affiliation
- Personal property

6. Conclusion

Key Points

Key Points to Remember

- Fraud is prevalent in Canada
- Increasing requirements and public pressure on all organizations
- Deterrence, detection and prevention of fraud is an ongoing process
- The key to success is transparency and consultation

Key Points to Remember (continued)

- Impact of economic crime on **reputation** and **staff morale** can be more important that the direct financial loss
- It is not a matter of **IF** an organization will be the victim of an act of fraud, but **WHEN**
- **Be alert for red flags and communicate concerns**

Questions?

H.Ray Haywood
Director, Forensic Services
(403) 509-7367
h.ray.haywood@ca.pwc.com