Grant Thornton

Fraud risks in the new economy

November 26, 2009

Agenda

1) Fraud risks in challenging economic times

2) Information technology fraud

3) Fraud risks: the legal perspective

Fraud risks in challenging economic times

Derek Malcolm, CA•IFA, CFE

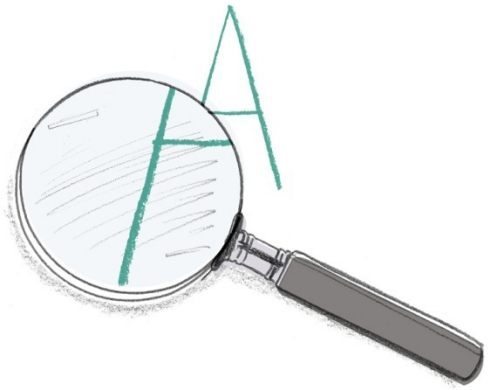
Quotes

Fraud and falsehood dread examination. Truth invites it.

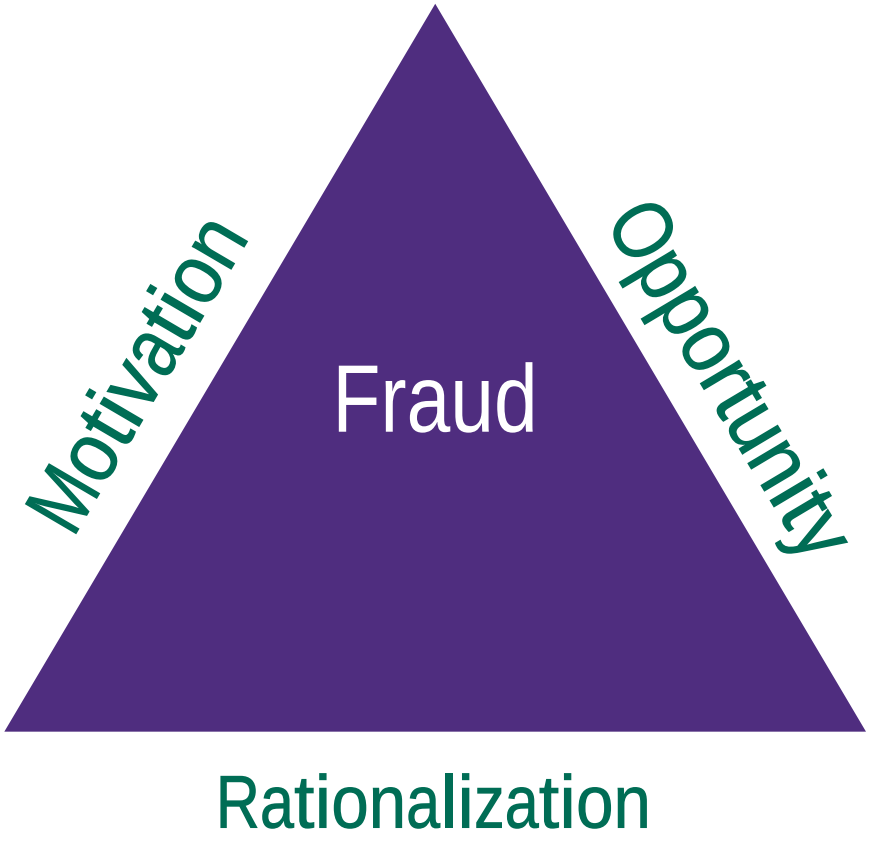
Samuel Johnson (1709-1784)

Fraud and deceit abound these days more than in former times.

Sir Edward Coke - 1602



The fraud triangle



Fraud statistics
Society as a victim

Fraud losses in the US estimated at **$994 BILLION annually**

- 7% of revenues
- *2008 ACFE Report to the Nation*

The personal costs of fraud cannot be measured reliably

- *Canadian Securities Association*

Fraud statistics
Fraud on the shareholder
Financial statement fraud

Costs of financial statement fraud

- Median loss of $2 million per occurrence
  - Losses to shareholders
  - Loss of reputation/ staff
  - Costs to employees
  - Auditor/ director lawsuits
- Domino effect if company fails

Fraud perpetrators

Median loss by individual versus collusive fraud

[Source : 2008 ACFE Report to the Nation]

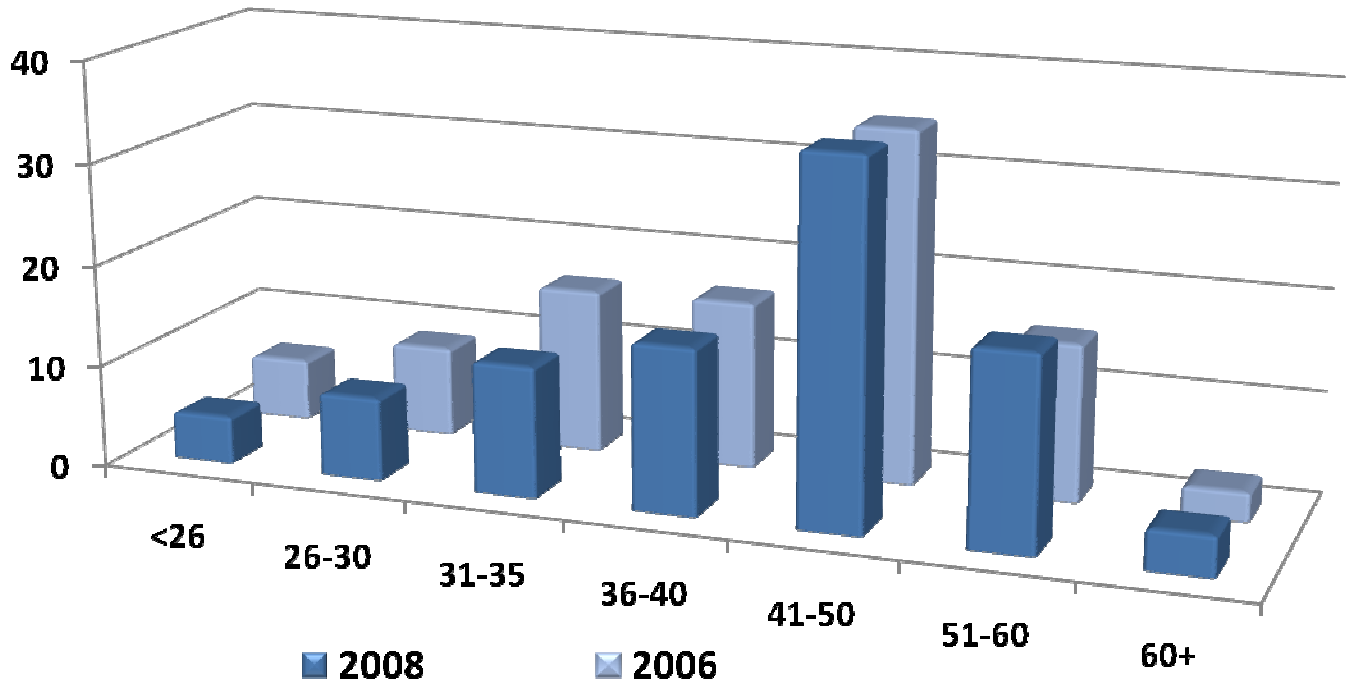
	Single Person	>1 Person (Collusion)
2008	$115,000 (63.9%)	$500,000 (36.1%)
2006	$100,000 (60.3%)	$485,000 (39.7%)

Characteristics of fraudsters

The paradoxical – and tragic – situation of man is that his conscience is weakest when he needs it most.

Erich Fromm

ACFE 2008 Report to the Nation
Perpetrators by age

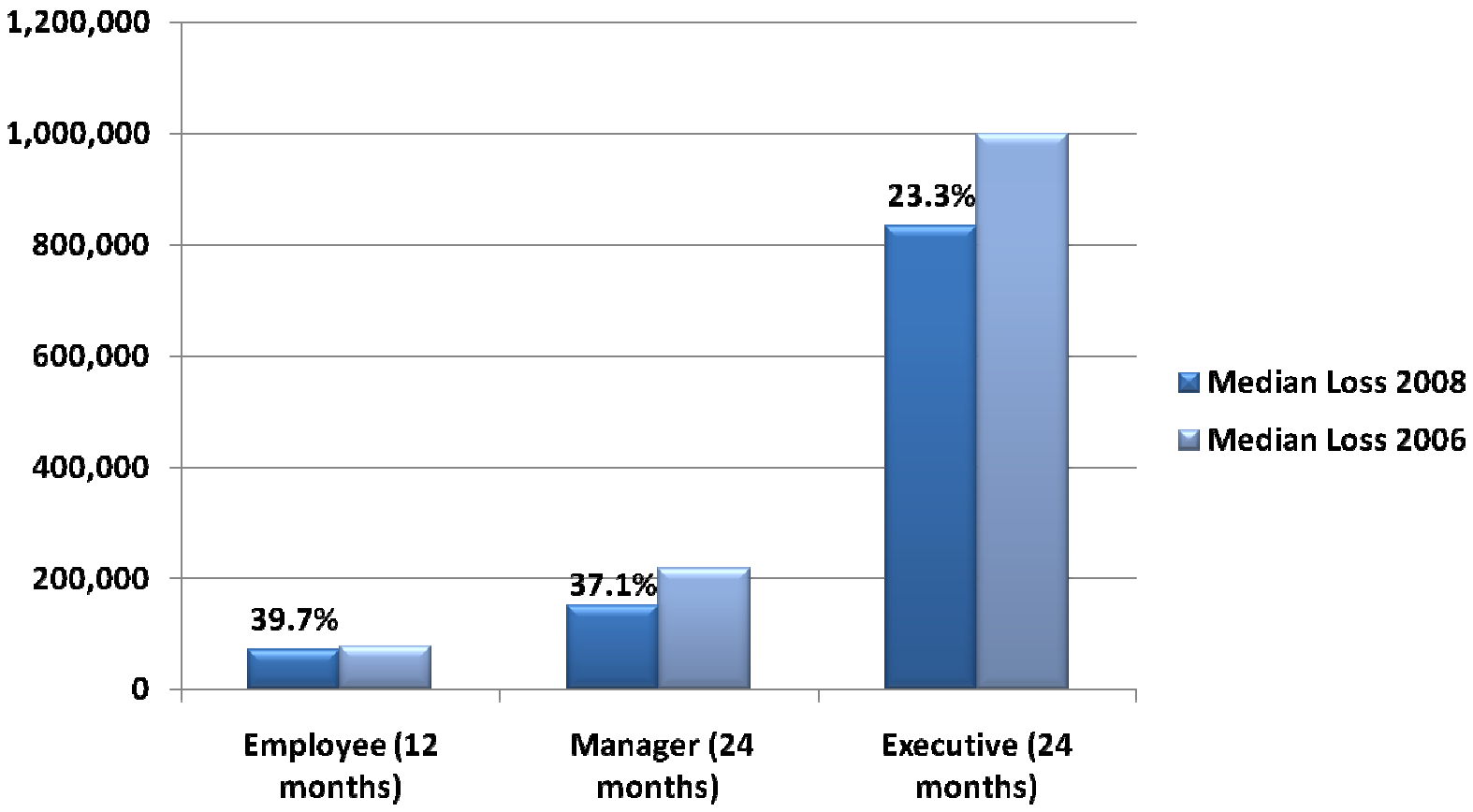


ACFE 2008 Report to the Nation
Tenure

Tenure of Perpetrator	Percentage of Cases	Median Loss
<1 year	7.4%	$50,000
1-5 years	40.5%	$142,000
6-10 years	24.6%	$261,000
>10 years	27.5%	$250,000

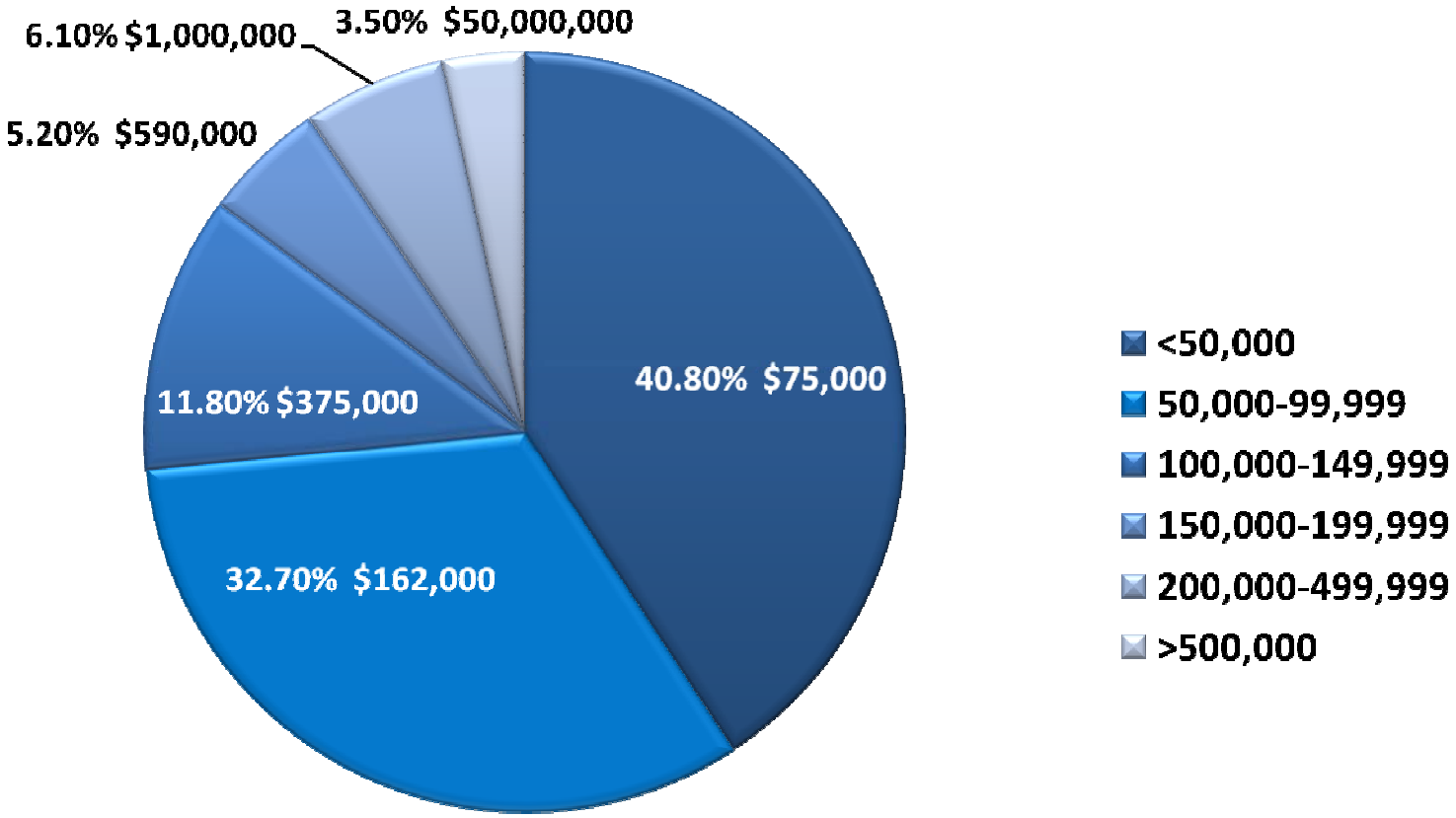
ACFE 2008 Report to the Nation

Position / median loss / frequency and detection period by position

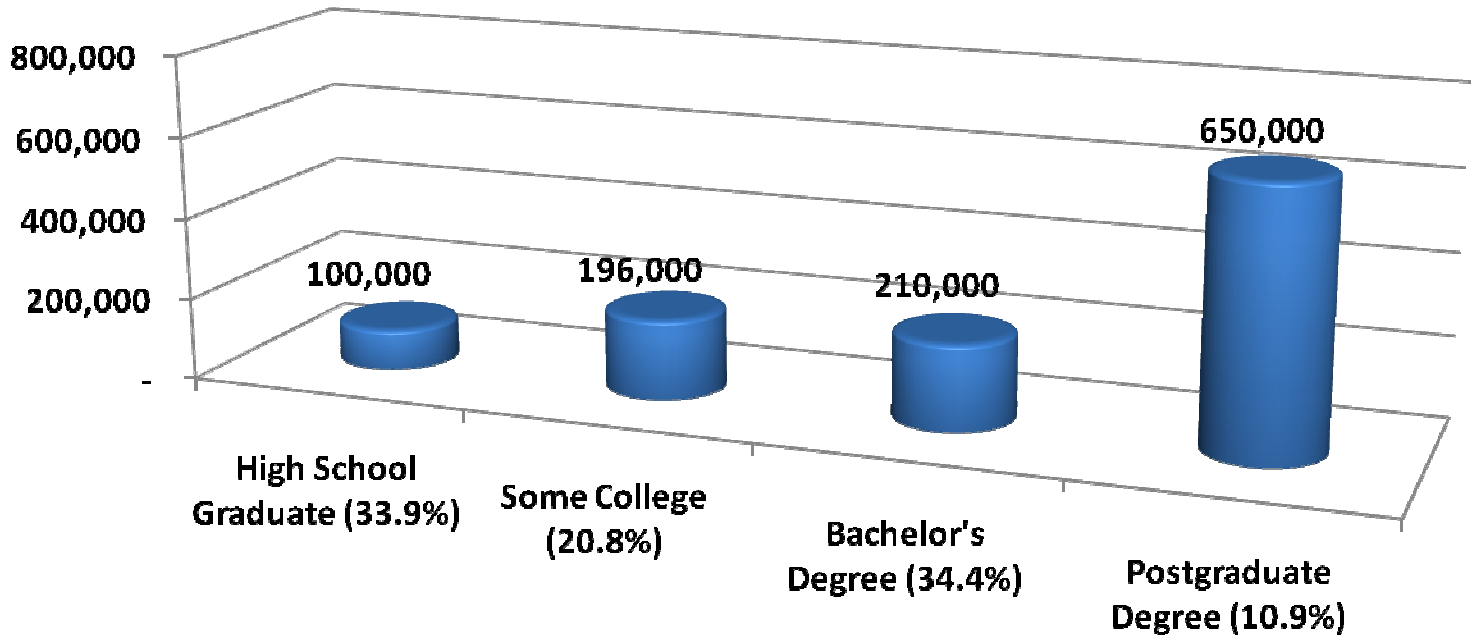


ACFE 2008 Report to the Nation

Median loss and percentage of losses by perpetrator income level

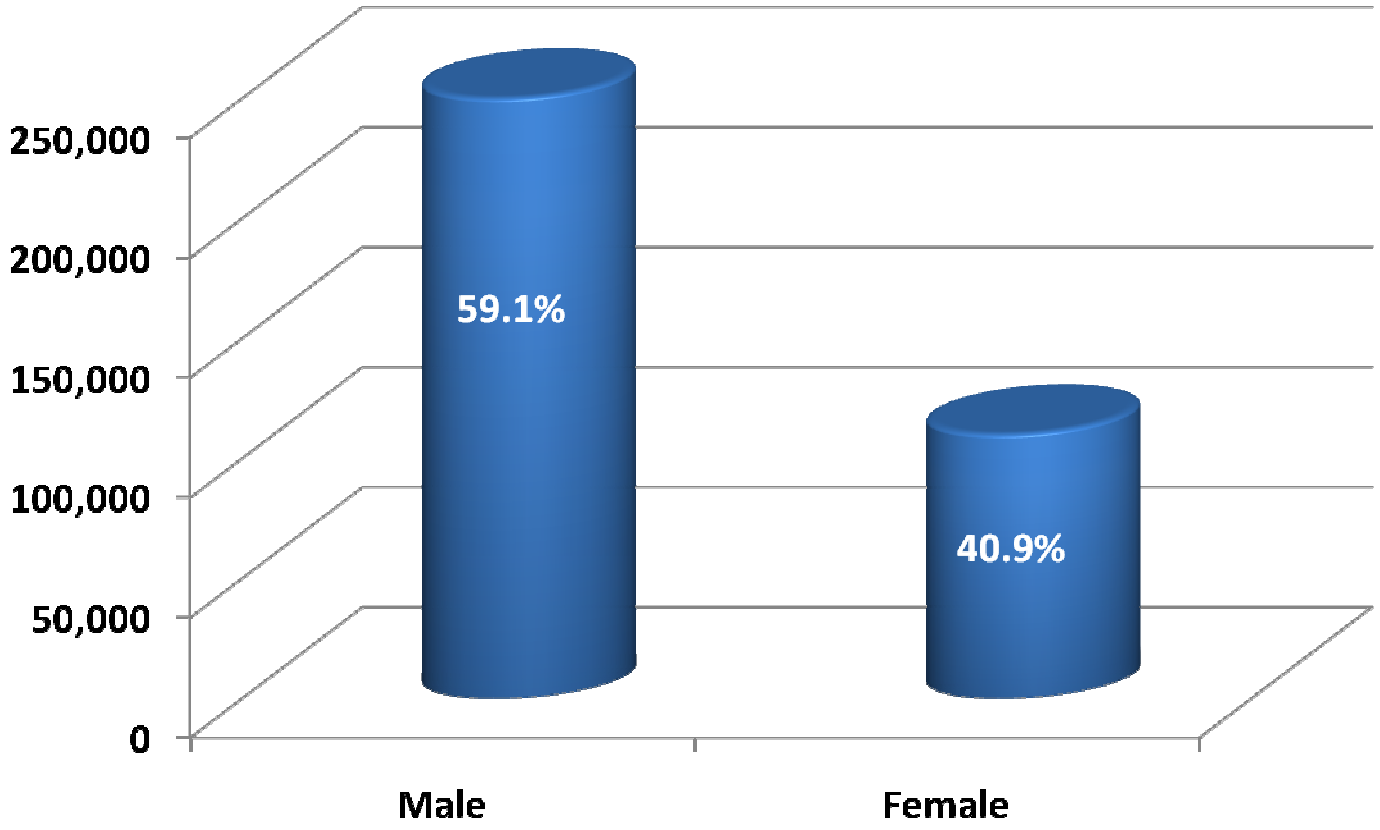


ACFE 2008 Report to the Nation
Median loss by education level



ACFE 2008 Report to the Nation

Median loss and percentage of losses by gender



ACFE 2008 Report to the Nation

Fraud by department

Department	Percentage	Median Loss
Accounting	28.9	$200,000
Executive	17.8	$853,000
Operations	16.1	$80,000
Sales	11.6	$106,000
Finance	3.9	$252,000
Purchasing	2.8	$600,000
Human Resources	0.9	$325,000
Research and Development	0.9	$562,000
Other	17.1	

Major frauds

Surprisingly enough, historical records indicate that most major frauds are perpetrated by senior management in collusion with other employees.

Source: Tone at the Top, Issue 40, August 2008 IIA

Prevention, detection and investigation

Frauds in play during the good times

- **Why?**
  - Hectic pace
  - Controls playing catch up
  - Profit leakage
- **Where?**
  - Pressure Points
  - Occupational fraud
  - Financial statement fraud
- **How will they be seen?**

Fraud Pressure Points

•Degree of Transaction Transparency
•Management training and tone
•Degree of acceptance of management override of controls
•Nature of business and of non standard transactions,
•Degree of interaction to complete a transaction cycle (segregation)
•Degree of technical understanding required (bamboozle factor),
•Amount of control exercised by one person
•Amount of gate keeping/secrecy in organization
•Pay for performance programs

© 2009 Grant Thornton LLP. A Canadian member of Grant Thornton International Ltd. All rights reserved.

Frauds in play during the good times

- **Why?**
- **Where?**
- **How will they be seen?**
  - Breaking the illusion
  - Recognizing the signals

Smoke Signals

•Reconciliations that won't work
•Unusual spreading of invoices over budget lines
•Missing documents
•Explanations for unusual transactions or entries don't make sense
•Additional or unusual charges on invoices
•Unfamiliar vendor invoices
•Disgruntled supplier comments
•Payments to numbered companies
•Fictitious invoices (copier paper example)
•Whistleblower reporting or unusual actions

© 2009 Grant Thornton LLP. A Canadian member of Grant Thornton International Ltd. All rights reserved.

Why fraud will prosper in the new economy

Change is toxic

- Corporate pressures
  - Less employees/resources
  - Profit expectations
- Personal pressures
  - More work/ less pay/entitlement
  - Addictions to cope
- Third party pressures
  - Vendors
  - Customers
  - Banks

Increased motive, opportunity and means

© 2009 Grant Thornton LLP. A Canadian member of Grant Thornton International Ltd. All rights reserved.

I didn’t think it could happen to me!

Steps that can be taken now:

- Don’t just rely on internal controls in place
- Be more skeptical
- Consider a Fraud Risk Assessment
- Prepare investigation protocol in advance
- Increase awareness

© 2009 Grant Thornton LLP. A Canadian member of Grant Thornton International Ltd. All rights reserved.

Top 10 fraud watch

10 Organized Crime
9 Procurement
8 Financial Statement
7 The rise of the Whistleblower
6 Payments and expenses
5 Advance protocols and increasing awareness
4 Details, details, details
3 Seek Legal Counsel
2 Trust but Verify
1 IT access and security (cyber) fraud

© 2009 Grant Thornton LLP. A Canadian member of Grant Thornton International Ltd. All rights reserved.

Information technology fraud

Richard DeBruyne, CISA, CISM, I.S.P., ITCP, PCI-QSA

A definition of cyber-crime

Two parts included in the definition of cyber-crime:

- Traditional crimes that are now being conducted through the use of a computer or other technology;
- Crimes that involve acts against computers and technology directly.

Canada's cyber-crime ranking

- Canada ranked **fourth** in the world for number of perpetrators of internet crime [1;]
- Canada ranked **second** in the world for number of complainants of internet crime [1;]
- Canada ranked **seventh** in the world for identified malicious activity [2;]
- Canada ranked **eighth** in the world for hosting botnet command and control servers [3;]
- Canada ranked **eighth** in the world for countries hosting phishing servers [2;]

1 Source 2007 Internet Crime Report, The US National White Collar Crime Centre, Bureau of Justice Assistance, FBI
2 Source April 2008 Symantec Global Internet Security Threat Report
3 Source September 2007 Symantec Global Internet Security Threat Report

The cloak of cyber-crime

Potentially **unlimited attack source points** with hi-tech diversion and stealth capabilities

Widely available attack tools and automation with exploit availability already at zero days

Attack methods are **low complexity, low cost** and **low risk** for the attacker

High probability of success and large financial gain

Canadian law enforcement

- Almost every crime committed in Canada today has some hi-tech component.
- Cybercrime surpassing drug trafficking as **number one crime in the nation.**
- There are 245 hi-tech law enforcement officers covering all aspects of tech related crime in Canada.
- The average citizen is more likely to be a victim of cybercrime than on the street or in their home.
- Law enforcement is unable to keep up to the growing incidence of cybercrime in Canada.

Source: 1) May 21, 2008 Press Release, Canadian Association of Police Boards (CAPB)

Corporate attackers

Insiders:
- **Disgruntled Employees**
- **Internal Fraud**
- **Internal Surveyors**

Hackers and crackers:
- Challenge/Prestige/Profit
- Access to Knowledge or Insider Information
- Follow the Leader/Game Play

Cyber criminals:
- Corporate Resource Control
- Information Access
- Theft/**Fraud**

Hacktivism groups:
- Corporate Policy/Politics
- Corporate Audience
- Public Embarrassment
- Reputation Assault
- **Fraud**

Cyber terrorists:
- Corporate Access/Power
- Denial/Hijacking of Service
- Destruction
- Kidnapping/Assassination

Cyber spies/espionage:
- Intellectual Capital
- Sabotage
- Market Plans
- Customer Information
- **Fraud**

Information warfare:
- International Political Strike
- Espionage/Reconnaissance
- Critical Infrastructure Surveillance

Corporate attackers

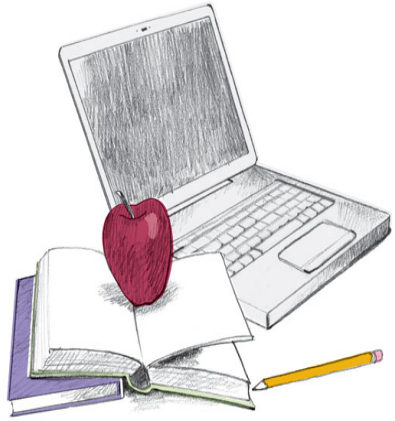
Information Technology fraud

“History has shown that when there is a downturn in the economy, there tends to be an increase in fraudulent activity."

"We expect businesses, particularly small- and medium-sized ones, and consumers to be more vulnerable to scams as they look to minimize expenses in the midst of an economic downturn."

"Last year, the Competition Bureau fielded almost 15,000 complaints about mass marketing fraud, either by mail, telephone or the Internet."

Melanie Aitken
Interim Commissioner of Competition
Competition Bureau

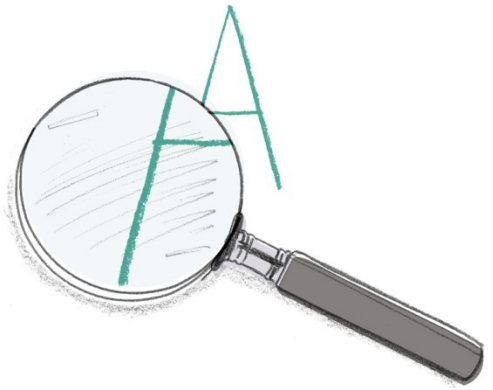


Information Technology fraud

Forty-one percent of small businesses surveyed by Visa Canada said they don't believe data thieves and hackers will target them because of their size.

Of the 885 small business owners surveyed, 24% said they are unaware of where to obtain information about securing their business, and **52% have never sought information about securing their electronic information**.

Gord Jamieson
Head of Payment System Risk
Visa Canada



Information Technology fraud

The Canadian Anti-Fraud Centre reported 7778 cases of identity theft in 2006, resulting in millions of dollars in damages.

The Canadian Council of Better Business Bureaus has estimated that identity theft may cost Canadian consumers, banks, credit card firms, stores and other businesses more than **$2 billion annually.**

Global Centre for Securing Cyberspace (Canada)
http://gcsc.ca/index.php/public/cybercrime

Information Technology fraud

Alarmingly, almost three-quarters (74%) of 601 CIOs surveyed perceive that **threats to corporate security are now coming from inside the organization**.

Nearly 60 percent of U.S. businesses believe that cybercrime is more costly to them than physical crime.

The costs resulting from cybercrime, these businesses report, are primarily from lost revenue, loss of current and prospective customers and loss of employee productivity.

Braun Research Inc.
IBM Survey of 601 Chief Information Officers on the status of cybercrime in their organizations

The cost of information technology fraud

- The true losses are not known because many companies choose not to report them.
- Based on reported crimes, global costs are estimated at more than **$1 trillion dollars** a year in loss of business and damages. [1]
- A single wave of cyber attacks on critical infrastructures could exceed **$700 billion** (US Cyber Consequences Unit). [1]
- The average annual corporate loss resulting from a cybercrime incident rose to **$350,424** in 2007. [2]
- Cumulative financial losses stemming from phishing attacks rose to more than **$3 billion** in 2007. [3]
- **Losses are expected to climb as economy downturns** ``We will never get a definitive answer on how much money Canadians lose to fraud each year" [4]

1 Source Global Centre for Securing Cyberspace (Canada) http://gcsc.ca/index.php/public/cybercrime

2 Source 2007 CSI Computer Crime and Security Survey

3 Source Gartner, Inc. "Phishing Attacks Escalate, Morph and Cause Considerable Damage," by Avivah Litan, December 13, 2007

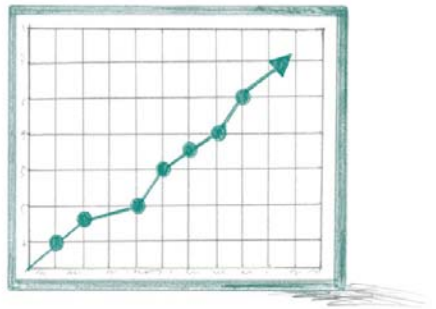
4 Source Cpl. Louis Robertson, a spokesman for PhoneBusters, an RCMP and OPP joint effort

Summary

Companies are increasingly becoming the targets of successful cyber-criminal activity.

Law enforcement is over extended in Canada and is slow to react to financial-based cyber-crime.

Fraud related to Information Technology is on the rise and will continue to escalate into the future.

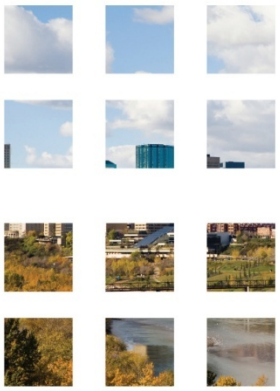


Fraud Risks: The Legal Perspective

November 26, 2009

Steven T. Robertson
Partner, Bennett Jones LLP

Steven L. Major
Partner, Bennett Jones LLP



Bennett Jones LLP

The Lawyers Role

Pursuit of the Rogue: An overview

- Value of Privilege
- Use courts to assist in investigative process (“Disclosure Order”)
- Freeze Assets (“Mareva Injunction”)
- Retain Evidence (“Anton Piller”)
- Cross-Border Efforts
- Dealing with the fall out

Bennett Jones LLP

The Disclosure Order

- What is it?
- Without notice to rogue can trace assets so they may be frozen
- Can be brought in conjunction with a Mareva Injunction
- *Underlying Principle*: A party that has innocently become involved in the rogue's fraud owes a duty to the victim of the fraud to facilitate recovery

Bennett Jones LLP

The Disclosure Order

- Must sue financial institution or other party
- Must demonstrate that recovery will be frustrated without Order
- Undertaking to court regarding damages

Bennett Jones LLP

The Mareva Injunction

- Without notice to rogue can freeze assets
- Must establish a strong *prima facie* case

"The applicant must persuade the court by his material that the defendants are moving or that there is a real risk that he is about to remove his assets from the jurisdiction to avoid the possibility of a judgment, or that the defendants are otherwise dissipating or disposing of its assets, in a manner clearly distinct from his usual or ordinary course of business or living, so as to render the possibility of future tracing of assets remote, if not impossible in the fact or in law."

Bennett Jones LLP

The Mareva Injunction

- Affidavit evidence will attach as exhibits relevant documents to establish the fraud
- Must clearly demonstrate the scheme and address the quantum of the loss
- Must make full, fair and frank disclosure
- Must provide undertaking to court regarding damages

Bennett Jones LLP

The Anton Piller Order

- What is it?
- Made without notice to defendants
- Must establish a strong *prima facie* case
- Damage to the victims, potential or actual, must be very serious
- Must demonstrate that defendants have incriminating evidence in their possession and that there is a real possibility that the evidence will be destroyed
- Contents of an Anton Piller Order
    - procedure
    - safeguards

Bennett Jones LLP

Cross-Border Efforts

- Work in conjunction with international lawyers to collect information, freeze assets and collect
- Forum Advantages

Bennett Jones LLP

Dealing with the Fall Out

- Firing the Rogue
- Cleaning up the mess (lawsuits, victims and Regulators)
- Maintaining your reputation

Bennett Jones LLP

The Lawyers Role

Beyond the Typical Rogue

- Claims involving breach of confidence and theft of trade secrets (forensic reviews required)
- E-discovery
- Theft of Confidential Information (Identity Theft/Privacy Commissioner/Upset Customers)

Bennett Jones LLP