

ARMA Vancouver Chapter  
January 14, 2010

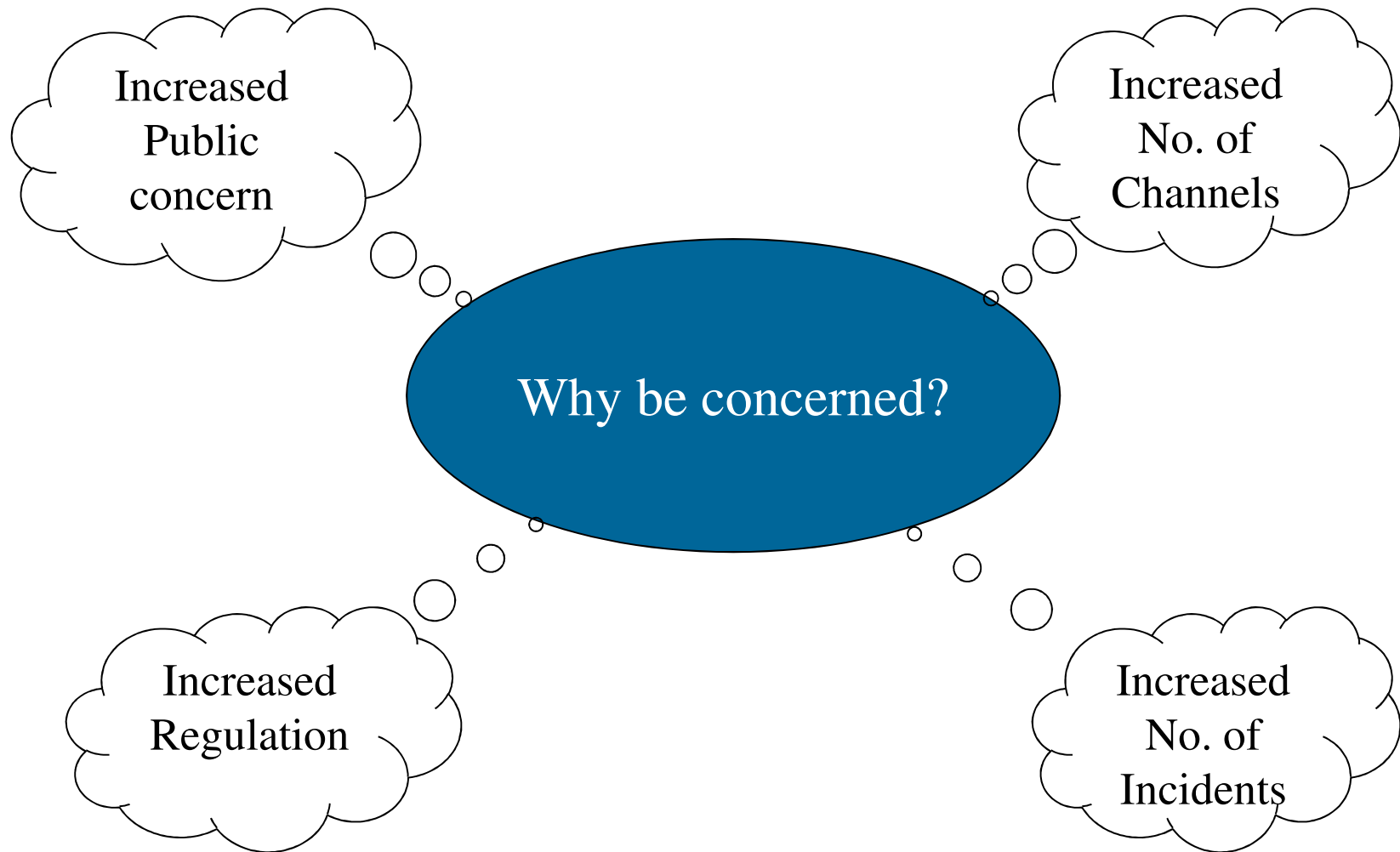
# Data Loss and Leakage

Causes, Costs and Avoiding  
Catastrophes

Dr. Victoria Lemieux

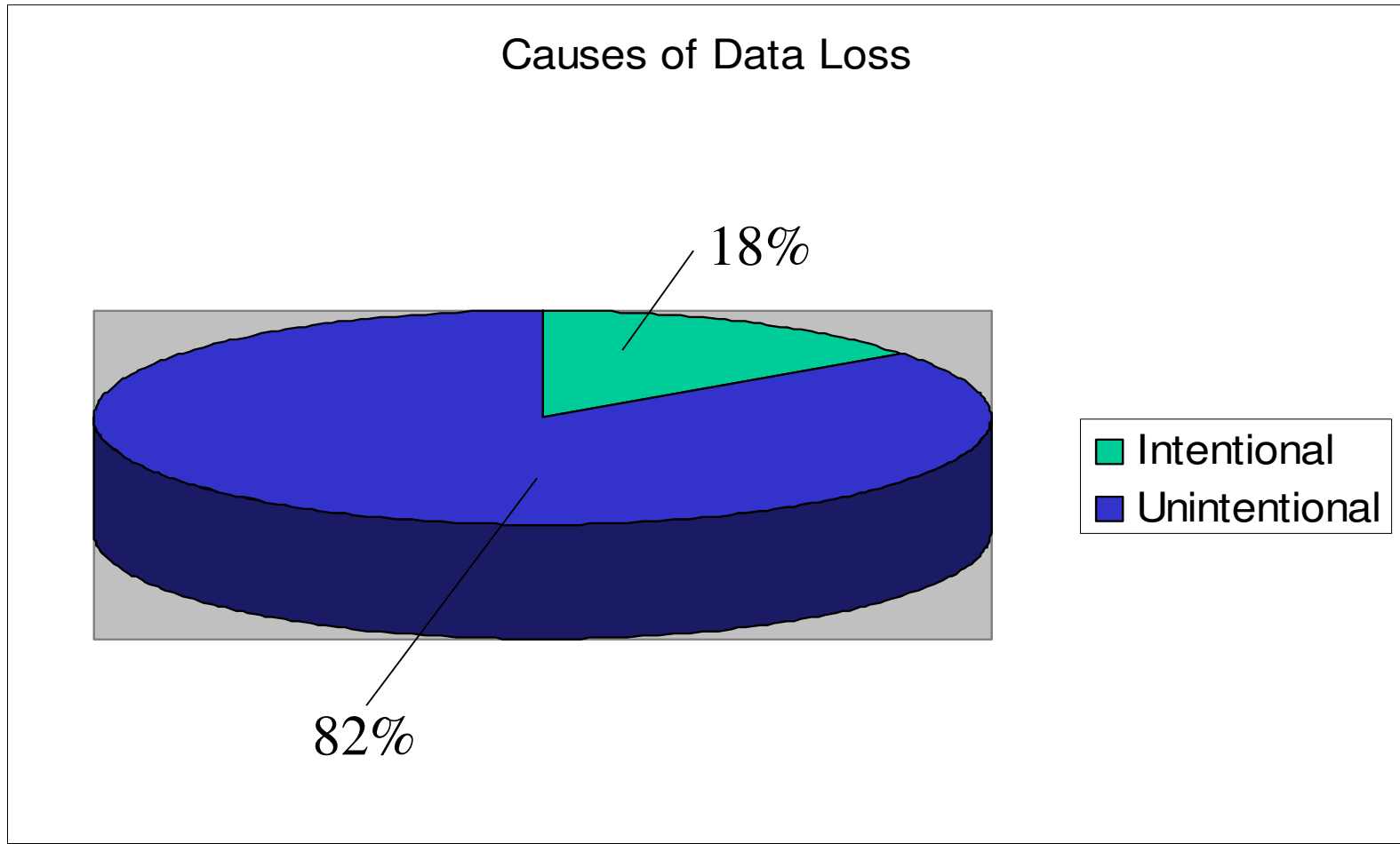
# I. Introduction

# Data Loss and Leakage



## II. Causes

# Recent Research



Presentation by Victoria L. Lemieux

# Scenario 1

*An employee of Bank 1 takes home a laptop. During a domestic burglary, the laptop is stolen. The laptop is unencrypted and contains details of 11 million customers. An FSA investigation is launched and the Bank is fined £980,000 million pounds for failing to have effective systems and controls for managing its information security risks.*

## Scenario 2:

*Bank 2 receives a number of complaints from customers that money has gone missing from their accounts. On investigating, the Bank finds that the losses can be traced to an employee at the Bank's offshore data processing facility in India who used false records to obtain a job at the bank. The employee misused confidential information to transfer money from customer accounts. Losses to customers in the UK amount to £233,00 before the fraud is stopped.*

# Scenario 3:

*Bank 3 gives an unencrypted backup tape to Archives Storage Inc., a storage firm, for transportation to a storage facility but the tape never makes it there. Bank account information on 4.5 million customers and investors goes missing. Local authorities call the loss “inexplicable and unacceptable” and call the bank’s one year offer of free credit monitoring “grossly inadequate.”*

# Scenario 4:

*Weaknesses in Bank 4's systems and controls allowed fraudsters to use publicly available information including names and dates of birth to impersonate customers and obtain sensitive customer details from its call centres. They were also, in some cases able to ask for confidential customer records such as addresses and bank account details to be altered. The fraudsters then used the information to request the surrender of 74 customers' policies totalling £3.3 million in 2006. The FSA fines Bank £1.26 million for failing to protect sensitive customer information.*

# Scenario 5:

*Bank 5 has a number of old desktops and servers it wishes to dispose of. As these pieces of equipment have been lying around in storage, no one has any recollection of what data is stored on them. A private firm is contracted to collect the old hardware and dispose of it. Several months later, hardware that has been disposed of, turns up in an educational institution where it is discovered that the account details of several thousand of the Bank's customers are still on the hard drive of the computer.*

# Scenario 6:

*Bank 6 has issued VISA cards to several of its customers. It discovers an increased reporting of fraudulent transactions in respect of transaction being processed by a particular payment processor. It notifies the processor and the processor investigates and discovers malicious software has been planted on the company's payment processing network that is recording payment card data as it is being sent to the company. A reported 100 million customers' data is compromised, the payment processor suffers huge reputation loss, is forced to hire teams of forensics specialists to investigate, set up a special website to keep the public, regulators and other updated on the breach and step up plans to deploy an encryption solution*

Presentation by Victoria L. Lemieux

# Underlying Causes and Common Themes

- Inadequate process controls
- Employees lacking in awareness
- Increased channels of loss
- Increased volumes of data
- Third party data processing

# III. Costs

# Balance Sheet Impact: Summing up the Losses

Customer Losses	\$400,000.00
Regulatory Fines	\$600,000.00
Loss of Trade	\$500,000.00
Brand equity	\$600,000.00
Admin costs (e.g., notifications)	\$200,000.00
Legal fees	\$500,000.00
<b>Total</b>	<b>\$2,800,000.00</b>

*Average cost of a data loss incident in the \$CDN\**

\*Figure based on 2008-2009 research by the Ponemon Institute

Presentation by Victoria L. Lemieux

# IV. Avoiding Catastrophes

# Lessons Learned: Avoiding Catastrophes



1. Establish clear governance structure
2. Establish clear data classification scheme
3. Establish clear information use policies and training to users
4. Conduct background checks
5. Conduct risk assessment to identify compliance gaps
6. Identify and implement appropriate tactical and strategic solutions (technical and non-technical) to close gaps and address risks
7. Closely monitor contractors and third party relationships
8. Develop an incident response plan
9. Continue to scan threat horizon
10. Monitor compliance

Presentation by Victoria L. Lemieux