Identity Theft Could Hit Your Business Next:

How to Protect Your Customers' Privacy

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner

Ontario

Infosecurity Canada

June 20, 2006

IPC

Identity Theft

- The fastest growing form of consumer fraud in North America;
- Identity theft is the most frequently cited complaint received by the F.T.C – *40% of total complaints received*;
- 10 million victims of ID theft each year, costing businesses $50 billion, and $5 billion in out-of-pocket expenses from individuals;

— Federal Trade Commission, 2003

IPC

A Sample of Major Privacy Breaches*

Nov 2004: *ChoicePoint* — Identity theft involving 145,000 persons;

Dec 2004: *Bank of America* — 1.2 million records misplaced;

Apr 2005: *TimeWarner* — Lost files on 600,000 employees;

Jun 2005: *Citibank* — Lost files on almost 4 million customers;

Jun 2005: *CardSystems* — Hacker theft of 40 million Visa/MasterCard records;

Feb 2006: *FedEx* — Accidentally exposed 8,500 employee tax forms;

Feb 2006: *OfficeMax* — Hacker accessed 200,000 debit card accounts;

Feb 2006: *Ernst & Young* — Laptop stolen containing 38,000 customer files;

Mar 2006: *Fidelity Investments* — Laptop stolen with 196,000 customer files;

Mar 2006: *Georgia Technology Authority* — Hacker theft of 553,000 pension files.

May 2006: *Department of Veterans Affairs* – Theft of 27 million records.

*****_For a full chronology of data breaches visit Privacy Rights Clearing House at,_ www.privacyrights.org/ar/ChronDataBreaches.htm

IPC

Burglary Leaves Millions at Risk of Identity Theft

- **May 2006**, 27 million U.S. veterans were placed at risk of identity theft after a burglar stole an electronic data file from the home of a Department of Veterans Affairs employee containing **unencrypted** names, birth dates and Social Security numbers; The employee took the information home to work on an ongoing project but without authorization;
- The theft represents the biggest unauthorized disclosure ever of Social Security data, and it could make affected veterans vulnerable to credit card fraud;
- The House Veterans Affairs Committee issued a statement calling on the department to restrict access to sensitive information to essential personnel and to enforce those restrictions;
- The department has sent letters to all of the veterans to notify them that their personal information has been compromised;
- Further, the department will require all employees to complete a computer security training course and conduct an inventory of positions that require access to sensitive data.

IPC

Hummingbird

- **June 2006**, an employee of Toronto software provider Hummingbird Ltd. lost a piece of computer equipment that contained the names and social security numbers of 1.3 million American students who borrowed funds from a Texas based non-profit company that administers education loans;
- The equipment was password-protected and it is believed to be "extremely unlikely" the data will be misused;
- The loan provider said customers whose information was lost are being notified over the coming weeks and given advice on how to guard against identity theft;
- Even though this information cannot be easily accessed and used, Hummingbird will nevertheless issue a release as a precautionary measure because the piece of equipment cannot be located and therefore security guarantees cannot be made.

IPC

Identity Theft: *Case In Point*

- **ChoicePoint — *January, 2006,*** charged with violating consumers' privacy rights and federal laws by compromising personal financial records of more than 163,000 consumers by not having reasonable procedures to screen prospective subscribers, and turning over consumers' sensitive personal information to subscribers whose applications raised obvious "red flags."

- The settlement requires ChoicePoint to pay $15 million in fines and to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes in addition to establishing and maintaining a comprehensive information security program with independent third-party audits every other year until 2026.

  Full Report: www.ftc.gov/opa/2006/01/choicepoint.htm

IPC

Don’t Blame the Victim

- Violations of privacy can be viewed as an external cost – a negative externality;
- ***Businesses however, not consumers, create privacy externalities through their misuse or lack of sufficient protection of their customers’ personal information;***
- It would be far more costly for individuals to prevent, or attempt to remedy, the abuses of their personal information – if possible at all;
- **We place the responsibility for protecting customer’s PII squarely upon business.**

IPC

Poor Information Management Practices at Fault

- Businesses that collect personal information from customers and retain it in their databases must separate the personal identifiers from the transactional data;
- The Gartner Group has estimated that internal employees commit 70% of information intrusions, and more than 95% of intrusions that result in significant financial losses;
- Personal identifiers cannot be left in plain view in databases when linked to transactional data contained in databases;
- Personal identifiers may be separated from transactional data in a variety of ways including encryption, severing, masking, etc.

— IPC Publication. *Identity Theft Revisited: Security is Not Enough*, www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf

IPC

The Current Privacy Storm
United States

- To date, **thirty-four states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – **twelve** other states have such legislation pending;

- Although the new laws are similar to California's SB1386, ***varying state requirements will likely put pressure on Congress to pass a federal bill.***

IPC

Data-Breach Notification

States Differ on When to Sound the Alarm

State laws conflict, define breaches differently, and prescribe different thresholds for notification;

Three General Areas:

1. Threshold Notification:

Discretion is allowed regarding whether or not to provide notice, on a harms/severity-of-the-breach basis;

2. California Model:

Notification is required as soon as personal information is breached, unless the data are encrypted;

3. Consumer Reporting Agency Notification:

Some state legislation requires notification to nationwide consumer reporting agencies.

IPC

Pending Federal Data-Breach Notification Bills

- **H.R. 3997 - *Financial Data Protection Act*:**

  Notification to consumers if "information is reasonably likely to have been or to be misused in a manner causing harm or inconvenience" to commit identity theft or make fraudulent transactions;

- **H. R. 4127- *Data Accountability and Trust Act*:**

  Notification required unless "no reasonable risk of identity theft, fraud, or other unlawful conduct;"

- **S.1789 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if there is "no significant risk" that it has or will result in harm;

- **S.1332 - *Personal Data Privacy and Security Act*:**

  Notification of breach not required if "de minimis" risk of harm;

- **S.1408 - *Identity Theft Protection Act*:**

  Notice required if breach creates a "reasonable risk of identity theft", taking into account whether data is in the possession of a third party "likely to commit identity theft;"

- **S.1326 - *Notification of Risk to Personal Data Act:***

  Notification if breach results in "significant risk of identity theft."

** The above pending bills are designed to pre-empt state laws.*

IPC

Debate Over Notification

- Consensus is elusive on when companies should be required to notify consumers that their information has been exposed during a breach;
- Kirk M. Herath, Chief Privacy Officer and Associate General Counsel for Nationwide Insurance Companies said the notification standard should be set to reflect when there is "a clear risk of danger to the consumer;"
- Kirk J. Nahra, a partner at Wiley Rein &Fielding LLP, adds that there is little to be gained by "over-notification" of consumers;
- However, many disagree arguing that companies should not control under what circumstances and when consumers should be notified of a breach or potential harm.

— Jaikumar Vijayan, *Breach notification laws: When should companies tell?,* ComputerWorld, March 2, 2006.

IPC

What Consumers Think

- 82% of consumers believe that it is **always** necessary for an organization to report a breach even if there is no imminent threat;
- Early notification of breached personal information may significantly lower misuse rates, according to ID Analytics' National Data Breach Analysis;
- There was strong evidence that once a privacy breach was made public (notice of breach), the misuse of the stolen data dropped significantly;
- This suggests that breach notification could serve as a deterrent.

IPC

Data Protection Vs. Data Breach: *Do The Math*

- Data protection, such as encryption, is far less expensive than cleaning up after a breach;
- Research indicated that it would cost about **$6** per customer account to encrypt data, compared to an estimated **$90** per account after the data are exposed during a breach;

— Avivah Litan, Gartner Analyst

- ***The math is simple:*** For a company with 10,000 customer accounts, it can either mean **$60,000** in preventive measures **or** up to **$900,000** in data breach containment costs.
- ***An ounce of prevention or a pound of cure?***

IPC

Privacy Breach Protocol
Alert Your Incident Response Team

- **Containment:** *Identify the scope of the potential breach and take steps to contain it;*
- **Notification:** *Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly;*
- **Investigation:** *Conduct an internal investigation into the matter, linked to the IPC's investigation and with law enforcement if so required;*
- **Remediation:** *Address the situation on a systemic basis where program or institution-wide procedures warrant review.*

IPC

Make Privacy a Corporate Priority

- An effective privacy program needs to be integrated into the corporate culture;
- It is essential that privacy protection become a corporate priority throughout ***all*** levels of the organization;
- Senior Management and Board of Directors' commitment is critical.

IPC

Conclusion

- Poor information management practices are usually at fault;
- Protecting your customers personal information is ***your business's*** responsibility;
- When faced with a breach, lead with openness and transparency: Contain the damage, then notify affected parties;
- Privacy enhances consumer confidence and trust;
- Use privacy as a tool to gain a competitive advantage;
- Think strategically about privacy – ***it makes good sense – good business sense.***

IPC