Deceptive Practices:
The Implications of Information Insecurity

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

Gowlings – Information Technology Association of Canada
Privacy Seminar 2007
May 8, 2007

IPC

Presentation Outline

1. *Identity*
2. *Portable Devices*
3. *Health Order 4*
4. *IBM Survey on Cybercrime*
5. *Breach Notification Tool*
6. *Why Privacy is Good for Business*
7. *Conclusion*

IPC

Identity

IPC

What is Your Identity Worth?

- You might think your identity is priceless, but according to a study by Symantec Corp., it's only worth about **$18 U.S,** which includes banking and credit card information, birth date and social security data;
- Thousands of Internet chat rooms and websites openly sell credit card and personal information for the purpose of identity theft -- and are doing plenty of business;
- Many of the sites can be found using an Internet Relay Chat program similar to MSN Messenger or AOL's Instant Messenger software. Simply search for "#cc" and hundreds of websites will pop up;
- Even worse, **54%** of all data lost or stolen is just being carried out the door, compared to hacking which only comprises **13%.**

— Vito Pilieci, *You're worth $18 on identity market: Stolen banking, credit and personal information sells online for paltry sums*, Ottawa Citizen, March 17, 2007.

IPC

Cost of Identity Theft in Canada

- Theft and fraud are costing Canadian retailers **$8 million a day**, or more than **$3 billion a year;**

According to the Retail Council of Canada:

- Credit card fraud in Canada resulted in losses of **$201 million** to major credit card companies in 2005;
- Debit card fraud resulted in losses of **$70.4 million**.

— Mario Toneguzzi, *Theft, fraud cost retailers $8 million a day*, Ottawa Citizen, March 2, 2007.

IPC

Identity Theft: It's Easier Than You Think

- The popular myth of identity theft is that it is committed by renegade hackers using high-tech methods;
- In fact, these crimes continue to depend on a steady and easily accessible supply of personally identifiable information (PII);
- Nearly 90% of the U.S. population can be uniquely identified through the use of only three pieces of information: a person's date-of-birth, sex, and postal code.

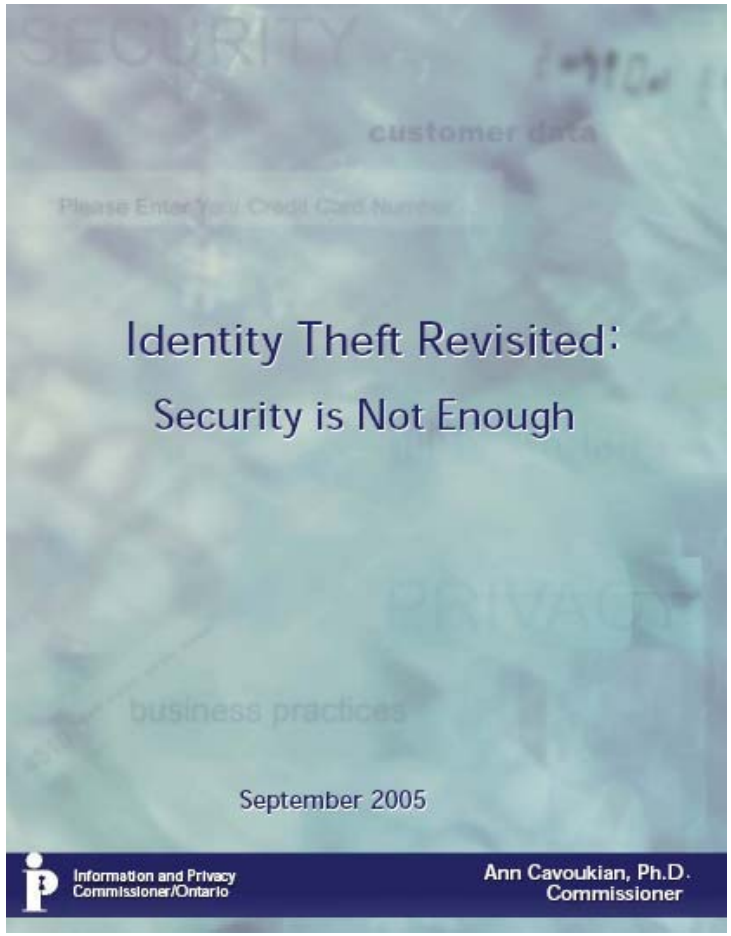
— L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," *Int'l J. Uncertainty, Fuzziness, and Knowledge-Based Systems*, vol. 10, 2002.

IPC

Businesses Take Note

The Responsibility Is Yours

- **IPC Publication, 2006:**
- Organizations that place the burden of dealing with identity theft on their customers run the risk of lost sales and market share through poor reputation, damage to brand image, and the unpredictable costs of litigation;
- This publication outlines how any organization can protect itself and, most importantly, protect its customers.



www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf

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 Largely at Fault

- Businesses that collect personal information from customers and retain it in their databases can dramatically reduce the incidence of identity theft if they 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 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

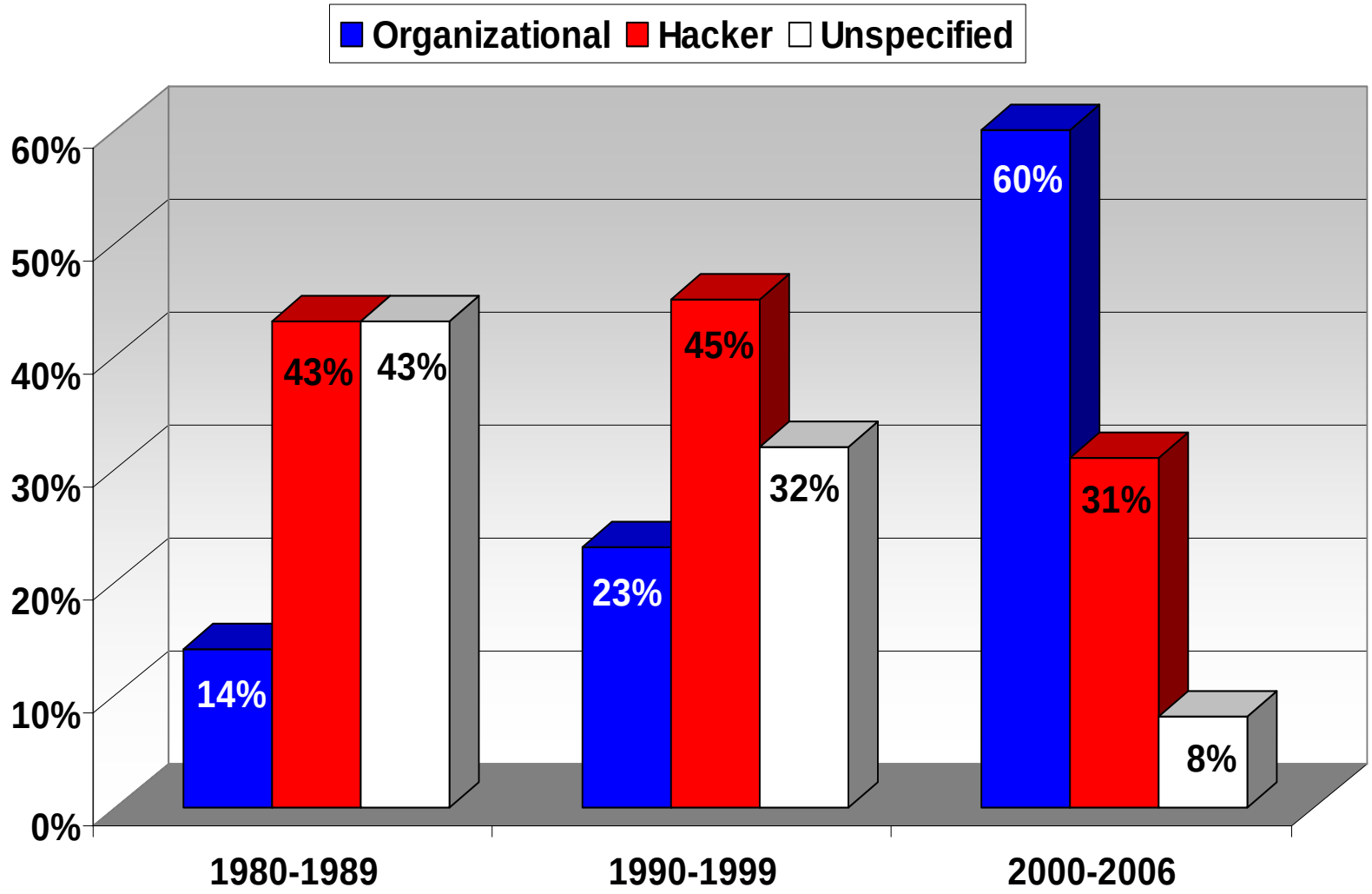
“Corporate Sloppiness is the Real Culprit”

- Researchers at the University of Washington expect to see the **2 billionth** personal record compromised since 1980, by the end of 2007;
- They don’t blame it on hackers or careless individuals, but rather on corporations;
- Hackers have only been responsible for **31%** of confirmed breaches between 1980 and 2006;
- The great majority, **60%**, of incidents of compromised records, were attributed to **organizational mismanagement**;
- Researchers at the university in Seattle estimate that electronic records—those containing Social Security or credit card numbers, academic grades or medical history—are bleeding out of North American organizations at a rate of **6 million a month.**

— Lisa Vas, *Corporate Sloppiness Is the Real Culprit for Data Loss, Not Vilified Hackers*, www.eweek.com, March 28, 2007.

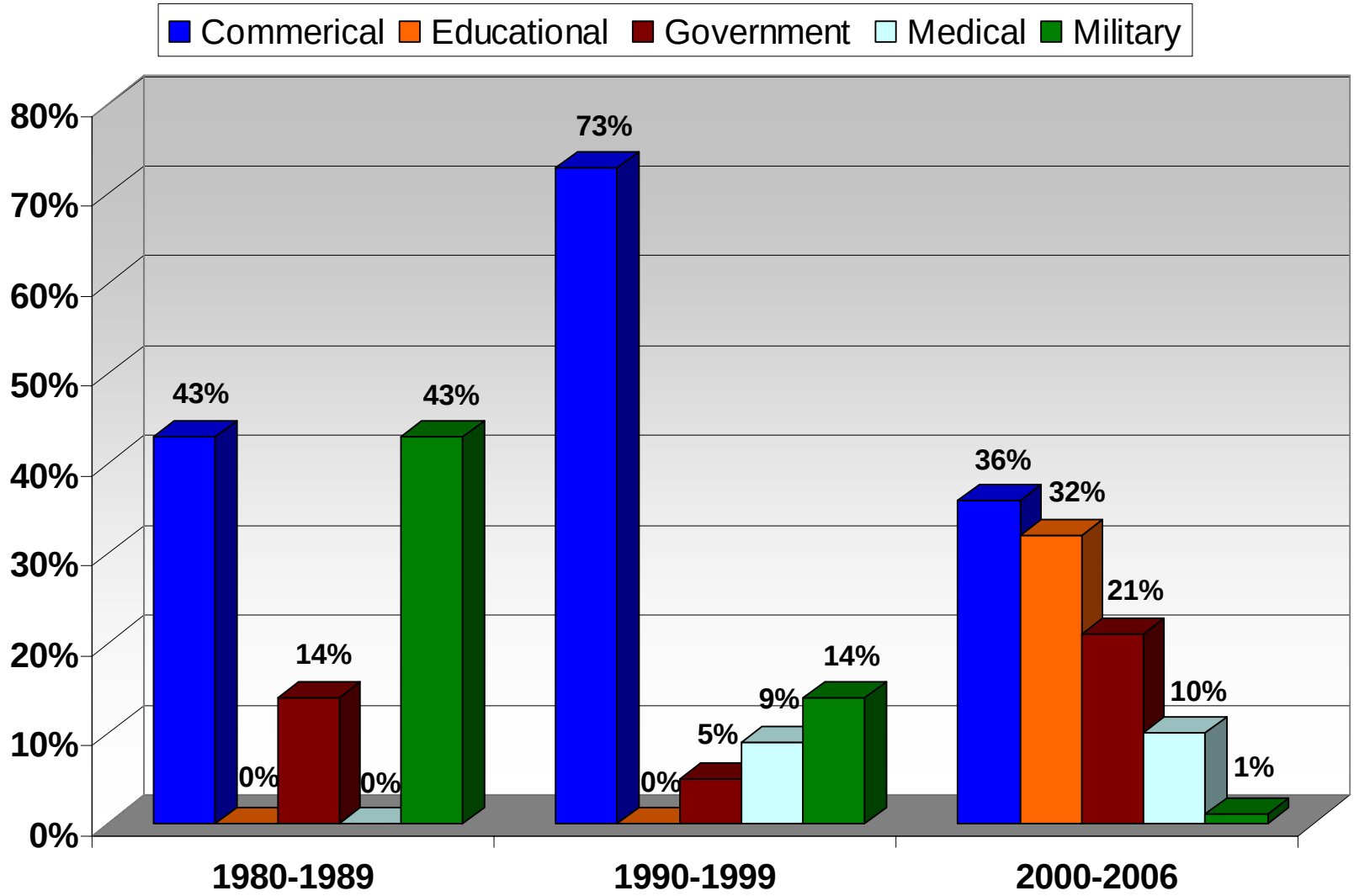
IPC

Hacker vs. Organizational Culpability in Reported Incidents of Compromised Records, 1980-2006



— Journal of Computer-Mediated Communication, *A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records, 1980- 2006*, 2007.

Compromised Records by Sector, 1980-2006



— Journal of Computer-Mediated Communication, *A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records, 1980- 2006*, 2007.

It's What's Inside that Counts

A new study at the University of Washington, Seattle found:

- Internal privacy breaches, such as uploading personally identifiable information accidentally online, missing equipment, lost backup tapes or other administrative errors were responsible for **61%** of breaches;
- **In contrast, only 31% of the incidents were perpetrated by external hackers;**
- With regards to internal errors, human error is the leading cause of privacy breaches at **75%,** while malicious hacking activity by employees was at **20%** of data losses;
- **Further, the primary channels for data loss involve laptops and mobile devices.**

— Jaikumar Vijayan, *Forget hackers; companies responsible for most data breaches*, Computerworld.com, March 14, 2007

U.S. Identity Theft Task Force

Comprehensive Strategic Plan to Combat Identity Theft

April 2007

- Reduce the unnecessary use of Social Security numbers by federal agencies;
- Establish national standards that require private sector entities to safeguard the personal data they possess and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;
- Implement a broad campaign by federal agencies to educate consumers, the private sector and the public sector on methods to deter, detect and defend against identity theft;
- Create a National Identity Theft Law Enforcement Center to allow law enforcement agencies to investigate and prosecute identity thieves more effectively;
- Amending identity theft statutes by adding new crimes to the list of offenses and broadening the statutes that criminalize the theft of electronic data.

"Identity theft is a blight on America's privacy and security landscape. Identity thieves steal consumers' time, money, and security, just as sure as they steal their identifying information, and they cost businesses enormous sums."

— FTC Chairman Deborah Platt Majoras, April 23, 2007.

IPC

Portable Devices

IPC

Portable Devices

- Working away from the “bricks and mortar” office also means working outside the traditional security layers. As a result, appropriate steps need to be taken to safeguard confidential information;
- Between March 2005 and September 2006, there were 65 separate reported incidents in the U.S. of laptops being stolen from both private and public organizations affecting more than **30 million** records containing personally identifiable information;

— www.privacyrights.org

Shoulder Surfing in the U.K.

"Shoulder surfing is apparently something that's embedded deep in the British genetic code, with ***80 percent*** *of the survey respondents admitting to reading over someone's shoulder in public … And being a regular commuter, I can't dispute the finding that* ***56 percent*** *of people admit to trying to read what's on someone's laptop screen."*

— Kevin Taylor, *Who's looking over your shoulder?*,
IT Week, April 30, 2007.

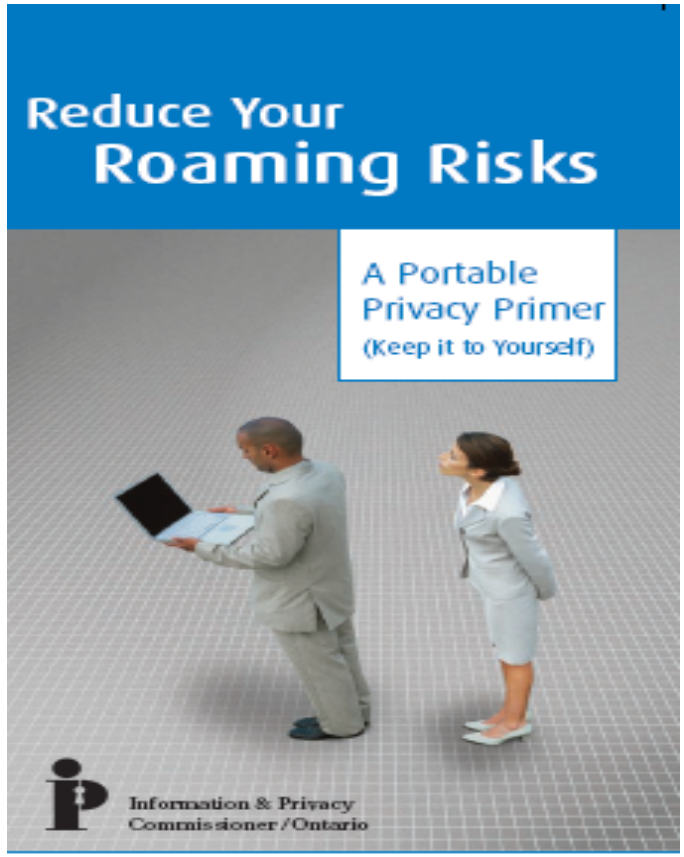
IPC

Reduce Your Roaming Risks
A Portable Privacy Primer

IPC-BMO Publication:

- Working away from the "bricks and mortar" office also means working outside the traditional security layers. As a result, appropriate steps need to be taken to safeguard confidential information;

- This brochure outlines some of the risks associated with "mobile" technology (especially while away from the traditional office) and offers advice on how to reduce these risks.



BMO Financial Group

www.ipc.on.ca/docs/bmo-ipc-priv.pdf

IPC

Health Order 4

(HO-004)

IPC

Health Order 4: *The Incident*

- January 4, a physician at the Hospital for Sick Children (SickKids) took home a laptop computer to analyze some research data;
- However, the physician did not go directly home, parking his car in downtown Toronto and leaving the laptop between the front seats in his mini-van and covering it with a blanket;
- When he returned to his vehicle he discovered that it had been broken into and the laptop was gone. He then immediately filed a vehicle break-in report with the Toronto Parking Authority and the Police;
- The following day, the physician notified his department head and the Chair of the Research Ethics Board;
- January 10, members of the senior management team determined that they would need to contact and notify the affected persons whose information was on the laptop;
- January 15, SickKids notified the IPC of the incident and we immediately commenced an investigation of this incident, pursuant to the *Personal Health Information Protection Act*, PHIPA.

Health Order 4: *The Review*

In my review, I found that SickKids:

- did not take steps to ensure that personal health information (PHI) in its custody or control was protected against theft, loss and unauthorized use or disclosure;
- did not ensure that the records of PHI in its custody were retained, transferred or disposed of in a secure manner;
- did not have information practices in place that comply with the requirements of *PHIPA;*
- did not undertake a comprehensive review of their policies when *PHIPA* came into force on November 1, 2004; and
- is required to notify the individuals whose PHI was contained on the laptop.

Health Order 4: *The Order*

- In HO-004, I Ordered the Hospital for Sick Children to:
- develop policies and procedures to ensure that records of PHI are safeguarded at all times;
- develop a comprehensive corporate policy that prohibits the removal of identifiable PHI in any form from the hospital premises unless it is ***encrypted;***
- implement a hospital-wide endpoint electronic devices policy, applicable to both desktop and portable devices which mandates that any PHI not stored on secure servers ***must either be de-identified or encrypted;***
- develop a privacy breach protocol; and
- provide education and training to staff members on the risks associated with the use of laptop computers, as well as providing detailed instruction on how to secure the information contained on laptop computers.

Health Order 4: *The Message*

"While laptop computers are often stolen for the value of these devices, in some cases, thieves are becoming increasingly interested in the personal information that they contain. There is no way of distinguishing one kind of theft from another. Personal information stored on stolen devices can be used for purposes such as fraud and identity theft – problems that have reached epidemic proportions throughout North America. And with the movement of organized crime into this area, the problem takes on a greater and more sinister complexion."

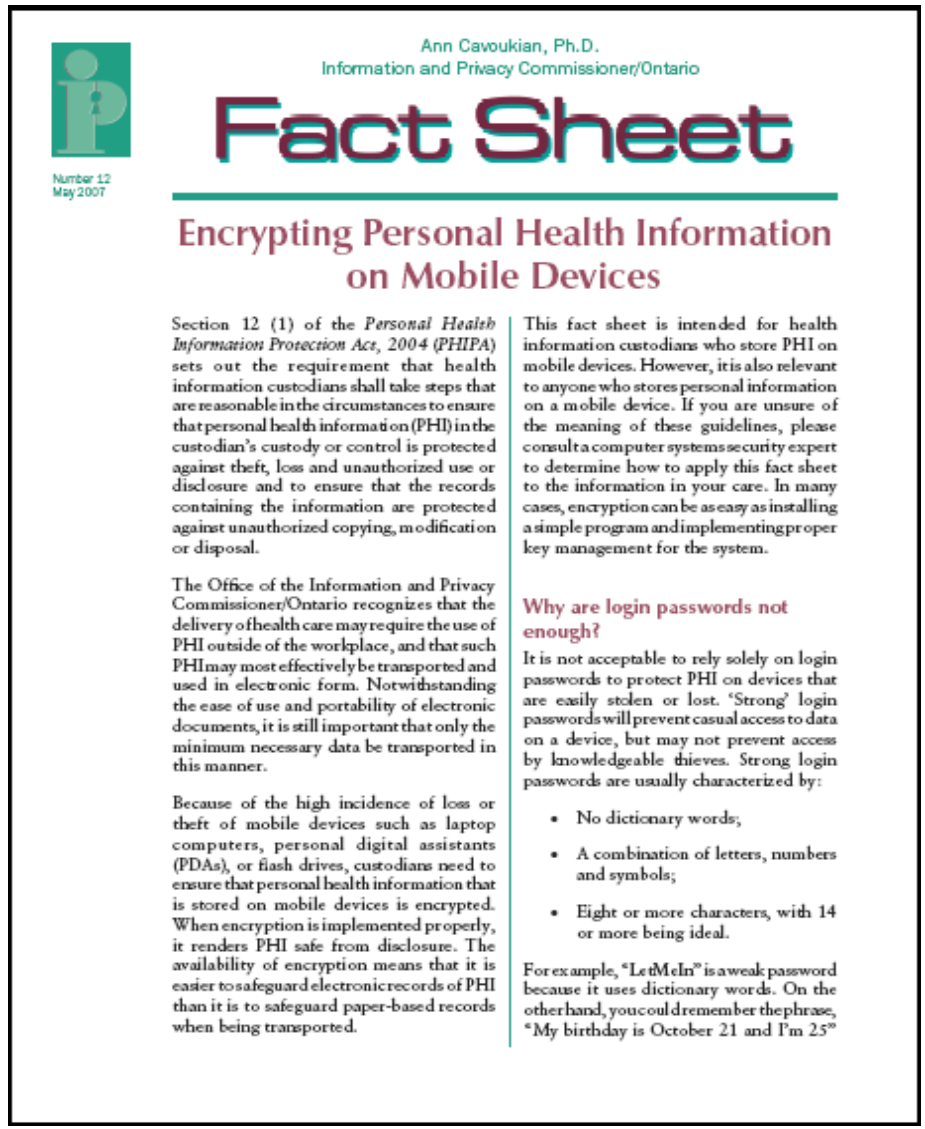
"There is no excuse for unauthorized access to personal health information (PHI) due to the theft or loss of a mobile computing device – any PHI contained therein must be encrypted."

— Information and Privacy Commissioner of Ontario,
Health Order 4 (HO-004), March 2007

IPC

IPC Encryption Fact Sheet

- Why are login passwords not enough?
- What is encryption?
- Are there options?
  - Whole disk (drive) encryption;
  - Virtual disk encryption;
  - Folder or Directory encryption;
  - Device encryption;
  - Enterprise encryption;
  - Encryption standards;
  - Off-site backup;
- Use our easy encryption checklist.



Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Number 12
May 2007

Fact Sheet

Encrypting Personal Health Information on Mobile Devices

Section 12 (1) of the *Personal Health Information Protection Act, 2004* (*PHIPA*) sets out the requirement that health information custodians shall take steps that are reasonable in the circumstances to ensure that personal health information (PHI) in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

The Office of the Information and Privacy Commissioner/Ontario recognizes that the delivery of health care may require the use of PHI outside of the workplace, and that such PHI may most effectively be transported and used in electronic form. Notwithstanding the ease of use and portability of electronic documents, it is still important that only the minimum necessary data be transported in this manner.

Because of the high incidence of loss or theft of mobile devices such as laptop computers, personal digital assistants (PDAs), or flash drives, custodians need to ensure that personal health information that is stored on mobile devices is encrypted. When encryption is implemented properly, it renders PHI safe from disclosure. The availability of encryption means that it is easier to safeguard electronic records of PHI than it is to safeguard paper-based records when being transported.

This fact sheet is intended for health information custodians who store PHI on mobile devices. However, it is also relevant to anyone who stores personal information on a mobile device. If you are unsure of the meaning of these guidelines, please consult a computer systems security expert to determine how to apply this fact sheet to the information in your care. In many cases, encryption can be as easy as installing a simple program and implementing proper key management for the system.

Why are login passwords not enough?

It is not acceptable to rely solely on login passwords to protect PHI on devices that are easily stolen or lost. 'Strong' login passwords will prevent casual access to data on a device, but may not prevent access by knowledgeable thieves. Strong login passwords are usually characterized by:

- No dictionary words;
- A combination of letters, numbers and symbols;
- Eight or more characters, with 14 or more being ideal.

For example, "LetMeIn" is a weak password because it uses dictionary words. On the other hand, you could remember the phrase, "My birthday is October 21 and I'm 25"

www.ipc.on.ca/images/Resources/up-fact_12e.pdf

The Risks of Wireless Technology: Methadone Clinics

- **May 1, 2007**, CBC Radio called about an incident involving a Sudbury methadone clinic which was inadvertently broadcasting video images of patients giving urine samples in the clinic's washroom – *those images could apparently be seen by anyone using basic wireless technology outside of the medical building;*
- My office immediately launched an investigation on the same day – The inadvertent broadcasting was stopped and we told the clinic to shut off the camera and call their service provider;
- The clinic is cooperating fully with my office in discussing options to protect privacy;
- My office is also preparing a Wireless Fact Sheet to underscore the added privacy and security risks associated with wireless technology.

IBM Survey on Cybercrime

IPC

IBM Survey on Cybercrime

A Greater Threat Than Physical Crime

- An IBM survey of companies in the healthcare, financial, retail and manufacturing industries reported that nearly **60%** of businesses believe that cybercrime is more costly to them than physical crime;
- **84%** of executives believe that organized criminal groups possessing technical sophistication are replacing lone hackers;
- **74%** perceive that threats to corporate security are now coming from inside the organization;
- **61%** of executives believe it is the joint responsibility of the federal and local law enforcement agencies to combat cybercrime.

IPC

IBM Survey on Cybercrime (Cont'd)
Safeguarding

83% of organizations believe they have safeguarded themselves and are responding to the increased threat in a number of ways:

- Upgrading virus software (73%);
- Upgrading their firewall (69%);
- Implementing intrusion detection/prevention technologies (66%); and
- Implementing vulnerability/patch management system on network (53%).

Breach Notification Tool

IPC

Debate Over Notification

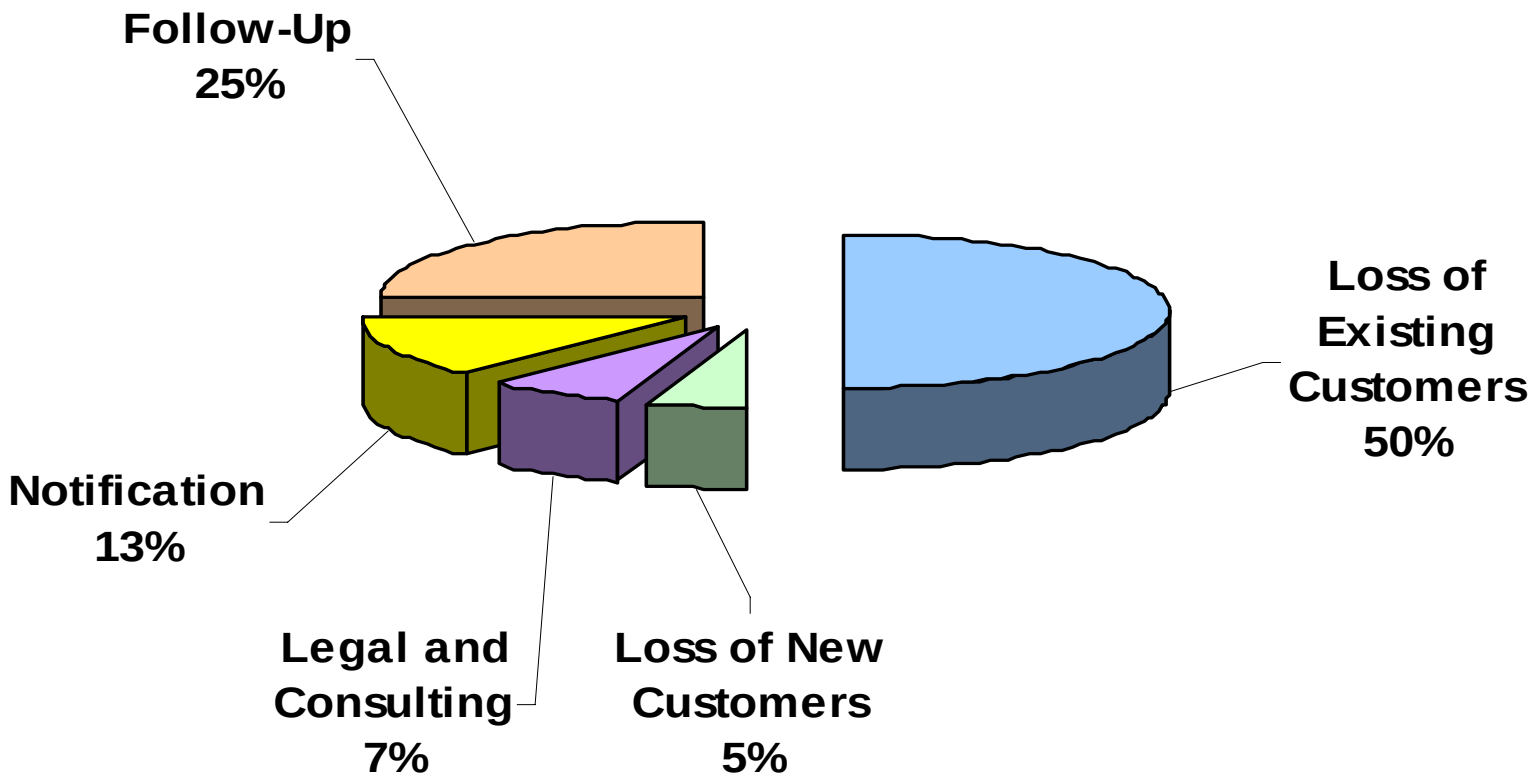
- Consensus is elusive as to when companies should be required to notify consumers that their information has been exposed during a breach;
- Kirk M. Herath, Chief Privacy Officer and Associate General Counsel for Nationwide Insurance Companies said the notification standard should be set to reflect 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, others disagree arguing that companies should not control the circumstances under which consumers should be notified of a breach or potential harm.

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

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. Alternatively, if every incident resulted in a notification, it could create "notification fatigue."

Costs of a Privacy Breach



Consumer data security breaches are leading to customer revolt and an average cost per incident of $14 million -- with costs ranging as high as $50 million.

— Ponemon Institute, *Lost Customer Information: What Does a Data Breach Cost Companies?,* November 2005.

Breach Notification Assessment Tool

- The B.C. and Ontario Privacy Commissioners have jointly produced a Breach Notification Assessment Tool to assist organizations in making key decisions after a privacy breach;
- Organizations that collect personal information should always consider notifying affected individuals when a privacy breach occurs;
- If the breach occurs at a third party that has been contracted to maintain or process personal information, the breach should be reported to the originating entity, which has primary responsibility for notification;
- Our Breach Notification Assessment Tool takes organizations through four decision making steps:

Step 1: Notifying Affected Individuals
Step 2: When and How to Notify
Step 3: What to Include in the Notification
Step 4: Others to Contact

www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf

Why Privacy is Good for Business

IPC

The Bottom Line

Privacy should be viewed as a **business** issue, not a ***compliance*** issue

Consumer Choice and Privacy

- There is a strong competitive advantage for businesses to invest in good data privacy and security practices;
- *"A significant portion of the population is becoming concerned about identity theft, and it is influencing their purchasing decisions."*

— Rena Mears, Deloitte & Touche LLP,
Survey Reports An Increase in ID Theft and Decrease in Consumer Confidence, June 29, 2005

Privacy Concerns are Adversely Affecting E-Commerce

United States: e-commerce sales were only 2.8% of total sales -- $108.3 billion in 2006.

— U.S. Dept. of Commerce Census Bureau, February 2007

Canada: Online sales were just over 1% of total revenues -- $49.9 billion in 2006.

— Statistics Canada, April 2007

IPC

Conclusion

- The majority of data that is lost or stolen is carried out the door;
- Internal privacy breaches make up the majority of privacy breaches with human error as the leading cause;
- Hackers, in reality, are **not** the leading cause of privacy breaches;
- Organizational mismanagement is the leading cause of compromised records;
- Poor information management practices are largely at fault;
- ***Businesses take note: the responsibility is yours;***
- Privacy should be viewed as a business issue, not a compliance issue;
- There is a strong competitive advantage for businesses to invest in good data privacy and security practices.

IPC

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

M4W 1A8

Phone: (416) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca