"Identity Theft - Fraud at its Worst: *The Implications of Information Insecurity"*

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

Association of Certified Fraud Examiners
Arizona Chapter
February 13, 2007

IPC

Presentation Outline

1. *Privacy “101”*
2. *Identity Theft and Fraud*
3. *Organized Crime Online*
4. *Phishing and Pharming*
5. *IBM Survey on Cybercrime*
6. *Breach Notification*
7. *Conclusion*

IPC

Privacy "101"

IPC

IPC: Three Statutes

The role of the Information and Privacy Commissioner of Ontario (IPC) is set out in three statutes:

- ***Freedom of Information and Protection of Privacy Act* (FIPPA);**
- ***Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA);**
- ***Personal Health Information Protection Act* (PHIPA).**

Responsibilities

Under its statutory mandate, the Commissioner is responsible for:

- investigating privacy complaints;
- resolving appeals from refusals to provide access to information;
- ensuring that organizations comply with the access and privacy provisions of the *Acts*;
- educating the public about Ontario's access and privacy laws; and
- conducting research on access and privacy issues, and providing advice and comment on proposed government legislation and programs.

Commissioner's Powers

The Commissioner is appointed by the Ontario legislature and is independent from the government;

The Commissioner has the power to:

- Offer comment on the privacy protection implications of proposed programs of institutions;
- In appropriate circumstances, authorize the collection of personal information otherwise than directly from the individual;
- Engage in or commission research into matters affecting the carrying out of the purposes of the *Acts*;
- Conduct public education programs and provide information concerning this Act and the Commissioner's role and activities;
- Receive representations from the public concerning the operation of the *Acts;*
- Order the disclosure of government-held information.

IPC

Understanding the Difference: *Privacy and Security in IT*

- While security and privacy share some important common qualities and features, **security is *not* privacy;**
- Privacy relates to a broader set of protections involving the protection of the individual – ***personal control****;*
- Security involves organizational control, attempting to protect company data, processes and systems, usually from external attacks;
- IT security professionals often make the mistake of believing that if data can be kept confidential and preserved from corruption, then privacy is guaranteed; ***it is not***.

Information Privacy Defined

- **Information Privacy: Data Protection**
  - Freedom of choice; personal control; informational self-determination;
  - Control over the collection, use and disclosure of any recorded information about an identifiable individual;
  - Privacy principles embodied in "Fair Information Practices."

IPC

Privacy Laws
Canada, United States and Europe

Canada:
Public sector privacy laws: federal, provincial and municipal;
Private sector privacy laws: (Federal) *Personal Information Protection and Electronic Documents Act (PIPEDA)*;
Provincial: Quebec, British Columbia, Alberta, Ontario;

United States:
Federal public sector *Privacy Act;*
Sectoral privacy laws;
Safe Harbor Agreement;

Europe:
Both private and public sector privacy laws;
- European Directive on Data Protection.

IPC

Identity Theft and Fraud

IPC

Identity Theft

- The fastest growing form of consumer fraud in North America;
- In the United States, identity theft is the most frequently cited complaint received by the F.T.C – *40% of total complaints received*;
- The F.T.C. reported 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

Identity Theft vs. Identity Fraud

- **Identity Theft** involves the theft of financial or other personal information with the intent of establishing another person's identity as their own;
- **Identity Fraud** – far more common - involves financial or other personal information being stolen and used to make purchases or gain access to the victim’s financial accounts, under their name.

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

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;
Jun 2005: *Citibank* — Lost files on almost 4 million customers;
Jun 2005: *CardSystems* — Hacker theft of 40 million Visa/MasterCard records;
May 2006: ***Department of Veterans Affairs*** **– Theft of 27 million records;**
May 2006: *Red Cross* – Insider access to 1 million Social Security numbers;
Jun 2006: *AIG Insurance* – Stolen computer containing 930,000 records;
Oct 2006: *Chicago Voter Database* – Hacker theft of 1.35 million records;
Nov 2006: *Boeing* – Stolen laptop containing 382,000 records;
Dec 2006: *TJX Cos.* – Hacker theft of 20 to 40 million credit/debit accounts;
Jan 2007: *CIBC Bank*– Lost computer files on 470,000 customers.

Since January 2004, more than 100 million records containing sensitive personal information have been compromised in reported security breaches.

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

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

CIBC – Privacy Breach II

Globe and Mail, *CIBC loses info on 470,000 Canadians*, Thursday, January 18, 2007.

- A backup computer file containing application data for 470,000 investors was lost by CIBC's mutual fund subsidiary Talvest Mutual Funds, in transit on the way to Toronto;
- The files contained names, addresses, signatures, dates of birth, social insurance numbers, bank account numbers and beneficiary information;
- This is the second incident involving a CIBC privacy breach. In 2004, the bank sent errant faxes to a junkyard operator in West Virginia for three years, mistakenly divulging private customer information.

TJX

- **January 2007,** U.S. retailer **TJX Cos.** whose chains include **T.J. Maxx, Winners** and **HomeSense**, reported that a hacker had penetrated its network, stealing consumer credit and debit card information;
- Estimates of the number of persons affected range from **20 to 40 million** cardholders worldwide with the number of persons affected in Canada estimated at two million;
- TJX will not be notifying customers, instead opting to cooperate with financial institutions in notifying those affected;
- In Canada, a class action lawsuit has been launched against Winners and HomeSense by the law firm Merchant Law Group, filing the suit in six provinces;

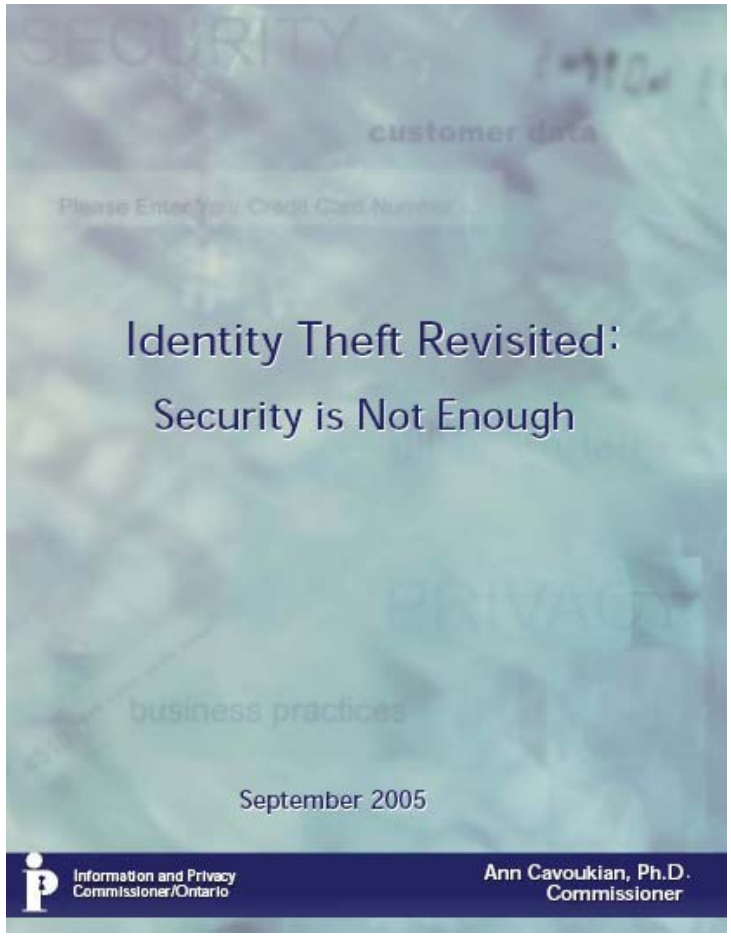
TJX (Cont'd)

- In the United States, two class action lawsuits have been launched against TJX Cos., the parent company of T.J. Maxx:
  - The first lawsuit has been filed by a woman who accuses TJX of negligence for failing to maintain the security of her customer data and for not notifying her of the breach for more than a month;
  - The second lawsuit comes from AmeriFirst Bank which is seeking to recover the costs of replacing compromised credit cards and fraudulent purchases;
- The Massachusetts Credit Union League is also asking TJX to reimburse credit unions for the costs of reissuing credit cards;
- Meanwhile, Massachusetts Congressman Ed Markey has asked the Federal Trade Commission to investigate the security breach;
- Canadian Privacy Commissioners, Jennifer Stoddart and Frank Work, have already launched an investigation into the matter.

Businesses Take Note

The Responsibility Is Yours

- **IPC Publication:**
- 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

Poor Information Management Practices Largely 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

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 names, birth dates and Social Security numbers;
- The employee took the unencrypted personal information of 27 million veterans home to work on an ongoing project but without any authorization;
- The theft represents the biggest unauthorized disclosure ever of Social Security data, and could make affected veterans vulnerable to credit card fraud or identity theft;
- Democrats on 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 sent letters to all of the veterans to notify them that their personal information had been compromised;
- Further, the department now requires all employees to complete a computer security training course and has conducted an inventory of positions that require access to sensitive data.

IPC

Boeing

- **December 2006,** A laptop containing the personal information on 382,000 current and retired workers of Boeing was stolen from an employee's car;
- The information included Social Security numbers, home addresses, telephone numbers, birth dates, and salary information;
- Although the laptop was password protected, the data on it were not encrypted;
- Boeing has begun notifying the affected people and is strongly suggesting that they sign up for a credit monitoring service, which the company will pay for.

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;

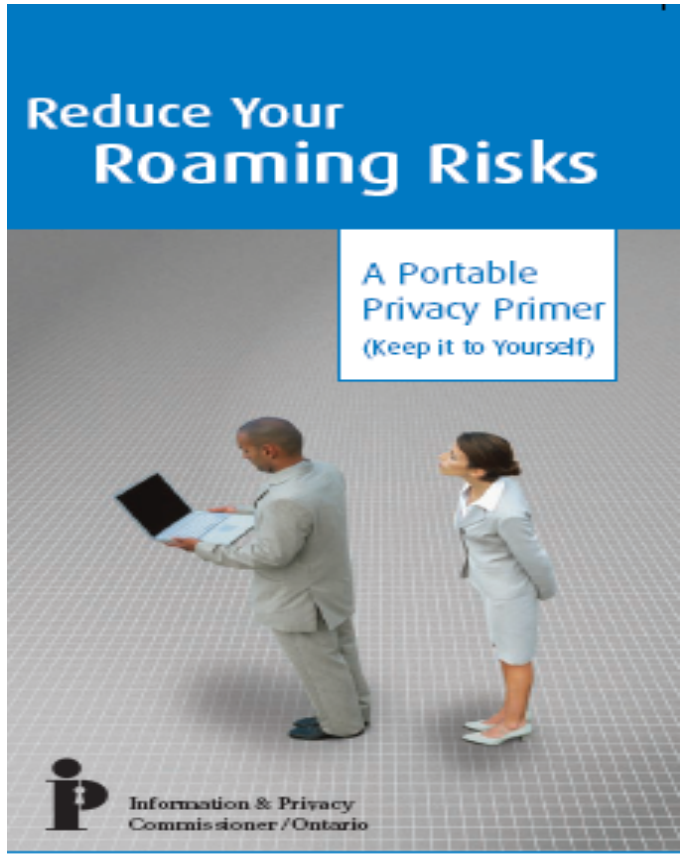
— www.privacyrights.org

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

“Pre-Texting” and Hewlett-Packard

- Computer giant Hewlett-Packard became the center of a major scandal when it was revealed that it used “pre-texting” to investigate information leaks on its board of directors;
- **December 2006**, the company settled a civil case with the California Attorney General's Office for $14.5 million in fines, intended to create a “Privacy and Piracy Fund” to finance investigations of consumer privacy violations;
- In addition, HP agreed to implement a series of legal and ethical measures to ensure that any future internal investigations are conducted according to California law;
- **December 8, 2006**, the U.S. Senate passed the *TRAPP Act*, (Telephone Records and Privacy Protection – S. 2178), that will make it a federal crime to obtain a person's telephone records without permission (pre-texting).

Organized Crime Online

IPC

Organized Crime

- Organized crime and criminal groups in Canada are increasingly involved in online fraud and identity theft;
- They are attracted by the fact that increasing amounts of personal and financial data are being collected, stored and transmitted electronically, which when stolen can be sold to the highest bidder;
- A major difficulty for police services in apprehending identity thieves is the fact that the Internet allows criminal groups to operate from anywhere in the world.

— Criminal Intelligence Service Canada,
The Organized Crime Marketplace in Canada, 2005, www.cisc.gc.ca

Organized Phishers and Pharmers

- Two prolific methods used by criminal gangs to commit identity theft are “phishing” and “pharming;”
- “Phishing” occurs when criminals posing as legitimate institutions send unsolicited e-mails and ask unsuspecting victims to provide sensitive financial information, such as account numbers, date of birth, passwords, etc;
- When “pharming,” hackers exploit vulnerabilities in an organization’s domain name system (DNS) server software and then illicitly redirect Internet traffic to targeted websites;
- Pharming poses an ongoing threat as it can target a financial institution’s entire customer base through a trojan program which embeds itself and waits for unsuspecting victims who log on to perform financial transactions.

— Criminal Intelligence Service Canada,
The Organized Crime Marketplace in Canada, 2005, www.cisc.gc.ca

Carder Networks

- Another less commonly recognized term, but nonetheless a serious threat, is known as “carder networks;”
- Blank credit cards and algorithms to encode a credit card’s magnetic strip can be purchased for illegal use;
- The Canadian Banking Association reported that the banking industry in Canada spends more than $100 million annually to prevent, detect and deter fraud against banks, including activity related to identity theft.

— Criminal Intelligence Service Canada,

The Organized Crime Marketplace in Canada, 2005, www.cisc.gc.ca

Cashing Out Scam

- A recent trend has developed where online poker rooms are used to cash out stolen credit card accounts and other payment mechanisms;
- The fraudster opens an account in an online poker room, funds it with the stolen credit card account, then plays a few hands in an online poker room and intentionally loses all the funds to a collaborator;
- Money changes hands as the collaborator shares the profit with the supplier of the stolen credit card account.

— RSA White Paper, *Phishing Special Report: What We Can Expect for 2007.*
www.rsasecurity.com

MyDoom
Organized Crime Virus

- The MyDoom virus was primarily transmitted via e-mail which contained an attachment that, if executed, resent the worm to e-mail addresses found in local files such as a user's address book;
- Appears to have been **"commissioned"** by organized crime e-mail phishers so as to send junk e-mail through infected computers;
- Several security firms published their belief that the worm had originated from the professional underground and its creator was paid to create it;
- Law enforcement agencies (FBI, RCMP and the U.S. Secret Service) investigating the virus also attributed it to online organized crime gangs.

"Whoever is behind it, they are organized and running a thriving business."

— Mikko Hypponen, Antivirus Research Director, F-Secure Corp, August 2004.

IPC

EarthLink Detectives

- **2004,** EarthLink, a large Internet access provider, went hunting on its own for phishers;
- The company tracked down persons who were sending e-mail messages that pretended to be from EarthLink, but were actually fraudulent attempts to steal customers' passwords, credit card numbers and other personal information;
- **Many of the phishing e-mail messages were believed to come from organized crime groups in Russia, Eastern Europe and Asia;**
- These crime groups have largely evaded capture because they often use computer worms, spread from machine to machine, to send the fraudulent e-mail messages -- a technique that makes it almost impossible to trace the source.

— Saul Hansell, *Organized crime may be behind phishing: Fraudulent e-mail scams show more sophistication*, New York Times, March 29, 2004

IPC

Lo-Tech Solutions

Scams and Fraud:

- NEVER give out any personal information in an e-mail, instant message or pop-up window;
- Be wary of clicking on a link or attachment contained in a message;
- Routinely review your financial statements;
- Update your computer and anti-virus security features;
- Report spam that is phishing to spam@uce.gov
- If you have been scammed, file a complaint at www.ftc.gov
- Sign all your checks with a gel-pen **(Uni-Ball Signo 207)** to protect against “check-washing.”

Fake Email or Phishing:

- The e-mail uses a non-specific greeting such as “dear customer;”
- It contains a request for information such as passwords and usernames;
- It has a prominent Web link that you are encouraged to click on.

IPC

Phishing and Pharming

IPC

Social Engineering

- The essence of phishing is **social engineering:** the goal is to persuade email recipients that they have received a legitimate, urgent message;
- Phishers appeal to fear or greed by:
  - Sending an email stating your account will be shut down if you do not provide and verify your sensitive personal information;
  - Sending an email message that promises the recipient a prize in exchange for a handling or shipping fee.

Phishing: *A Mainstream Industry*

No longer the realm of sophisticated fraudsters who build their own tools and use the credentials they've stolen, phishing now has a structured "supply chain" that facilitates trades between "suppliers" (phishers) and "buyers" (typically local criminals who can "cash out" compromised accounts).

— RSA White Paper, *Phishing Special Report: What We Can Expect for 2007*.
www.rsasecurity.com

IPC

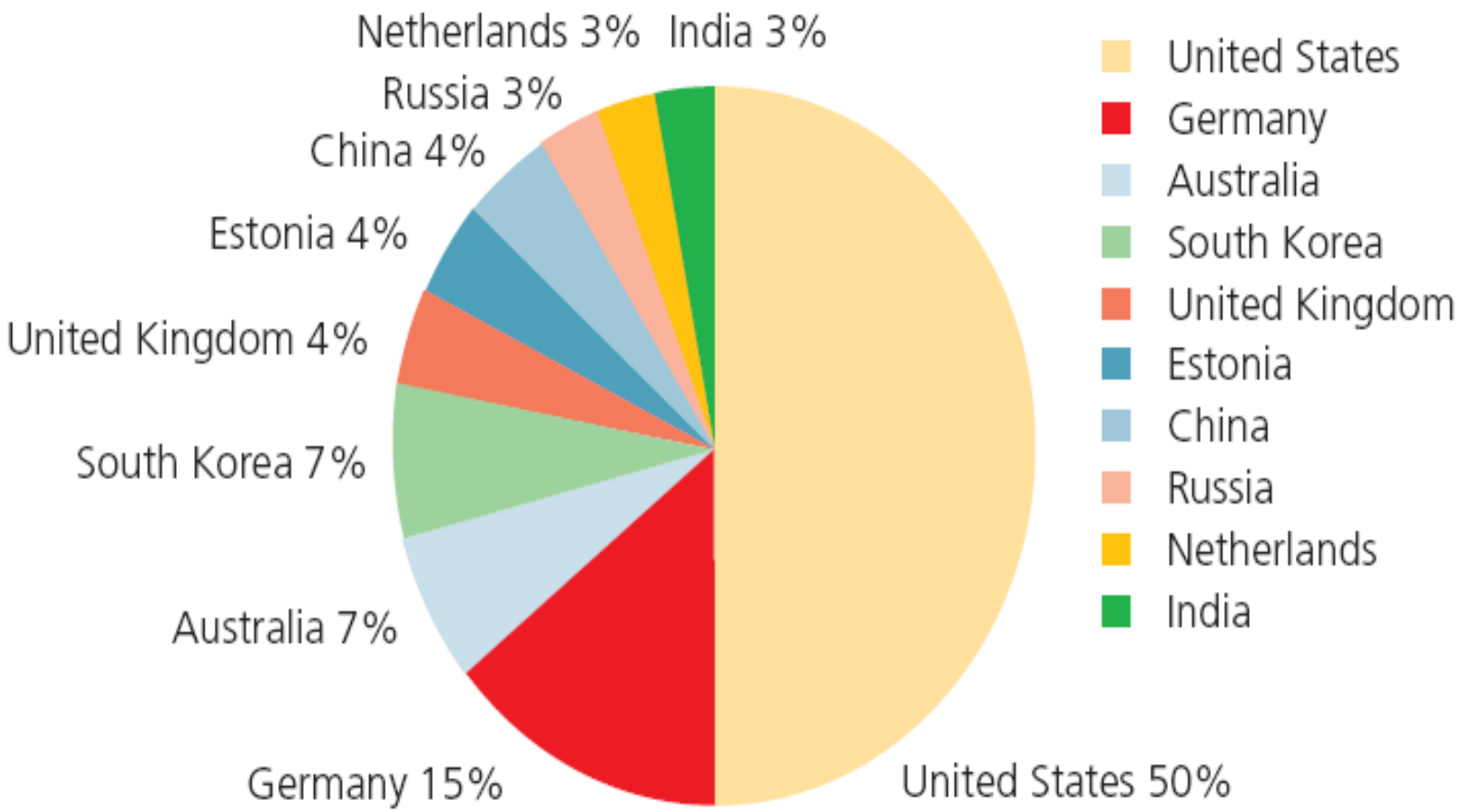
A Growing Industry

Phishing Attacks Per Month

— RSA White Paper, *Phishing Special Report: What We Can Expect for 2007.*
www.rsasecurity.com

IPC

It's Not Always From One of Those "Other" Countries

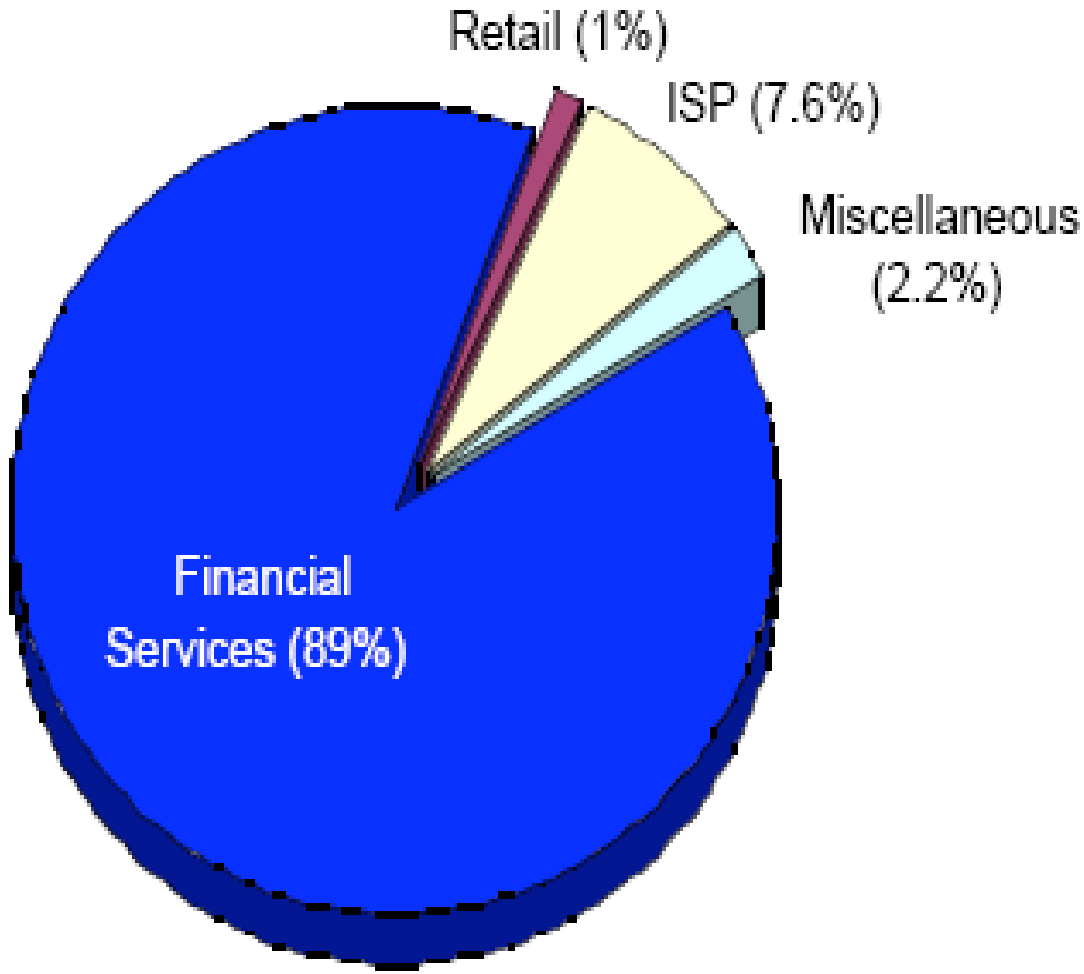


— RSA White Paper, *Phishing Special Report: What We Can Expect for 2007.*
www.rsasecurity.com

IPC

It's Always About the Money…

Financial Services continues to be the most targeted industry sector – 89% of all attacks in the first quarter of 2006.



www.antiphishing.org/reports/apwg_report_apr_06.pdf

IPC

…but it's No Longer About Going After the Big Fish

- Starting in mid-2005, phishers realized that the large financial institutions were taking serious measures to reduce phishing attacks;
- Further, media coverage of phishing attacks on large financial institutions has alerted consumers;
- Thus, large financial institutions no longer account for the majority of phishing attacks. The distribution of phishing attacks on financial institutions during July 2006 was as follows:
  - National banks: 12%
  - Regional banks: 41%
  - Credit Unions: 47%

— RSA White Paper, *Phishing Special Report: What We Can Expect for 2007.* www.rsasecurity.com

Why Does Phishing Work?

- In early 2006, researchers at Harvard and UC Berkeley undertook a survey explaining why phishing works:
- 90% of participants were simply fooled by a well-designed website that looked authentic and mirrored a name brand company's website – the very presence of an icon of a padlock fooled all of the participants who assumed only legitimate businesses would post such symbols;
- Anti-phishing browsing alerts were found to be ineffective – 23% did not even look at the address bar (unique URL) or any of the security indicators;
- 68% of participants ignored the pop-up warnings.

— Rachna Dhamija, *Why Phishing Works*, Harvard-UC Berkley, April, 2006.

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;
- **53%** of consumers hold themselves most responsible for protecting themselves; only **15%** felt it was the job of law enforcement.

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%).

IBM Survey on Cybercrime (Cont'd)
International Comparisons

- Both U.S. and international organizations viewed cybercrime as a greater threat than physical crime - 57% of U.S. and 58% of international businesses;
- Both groups indicated that loss of revenue (63% U.S. vs. 74% international) and loss of current customers (56% U.S. vs. 70% international) would have the highest cost impact;
- Damage to brand/reputation was of much higher concern to international businesses (69%) than U.S. businesses (40%).

Breach Notification

IPC

The Current Privacy Storm
United States

- To date, **thirty-five states** have signed laws that now require consumers to be notified if personal information has been subject to a security breach – of the remaining states, **thirteen** introduced legislation in 2006/2007;
- 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.

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."

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

Conclusion

- Identity theft is becoming an ever-growing problem;
- No longer the realm of sophisticated hackers, phishing is now a mainstream industry;
- Organized crime and criminal groups will continue to be involved in acts of identity theft and fraud since increasing amounts of personal and financial data are stored and transmitted electronically;
- Among the primary causes of identity theft are the poor information management practices of businesses and poor practices governing the use of remote devices;
- Working away from the “bricks and mortar” office also means working outside the traditional security layers, increasing the susceptibility of remote devices (and the information contained) to theft and loss;
- Increased use of encryption and other security measures will be key;
- Heightened awareness, education and increased vigilance will become the new “normal.”

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