Hackers and the Law
- A Canadian Perspective -

Prepared By: Robert W. Beggs, CISSP CISA
31 May 2006

DIGITAL DEFENCE

DigitalDefence

- Provide Information Security for Canadian small and medium-sized enterprises
- Specialize in pen testing, incident response, incident management
- Professional services – policy development, partner assessments, physical security, penetration testing, incident management and forensics
- Training – penetration testing, hands-on forensics, CISSP (also teach at Ryerson, UOIT)
- Managed services – network forensics

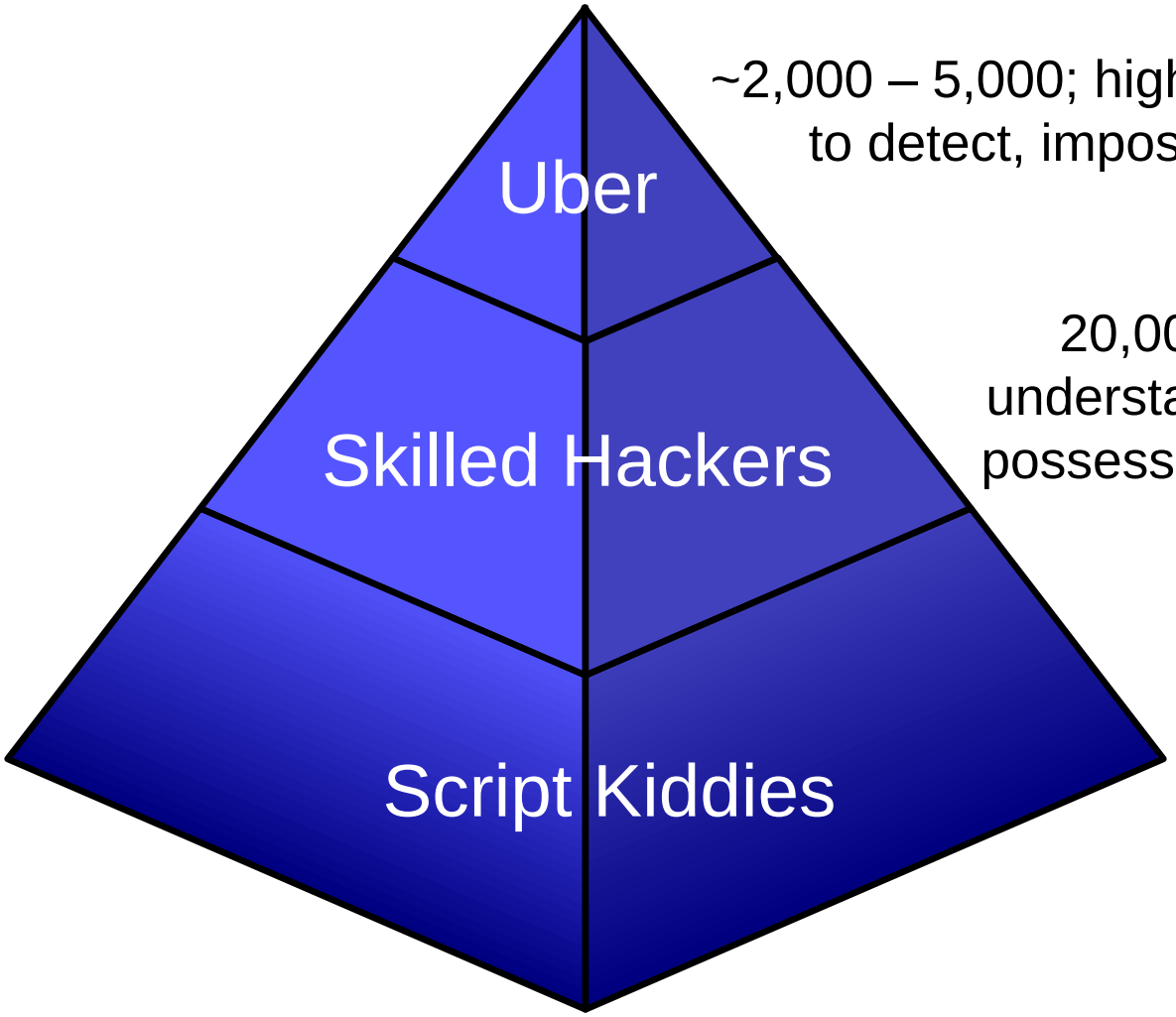
The Material Presented Tonight

- There is a “lack” of critically-assessed (“real”) data on:
  - What is the incidence rate of attacks?
  - Who is doing the attacks? (Insiders, Outsiders?)
  - What types of networks are being targeted?
  - How are the attacks being done?
- DigitalDefence will be releasing a research whitepaper evaluating all available information in June 2006

Why Tonight's Presentation

- Law enforcement is:
  - Overworked
  - Undertrained
  - Working without a reasonable budget
- Once you contact law enforcement, the security incident is public knowledge
- You must be able to support the investigation
- Overall, you are your own policeman!
- How well do you know the law?

Classifying “Hackers” - Skills

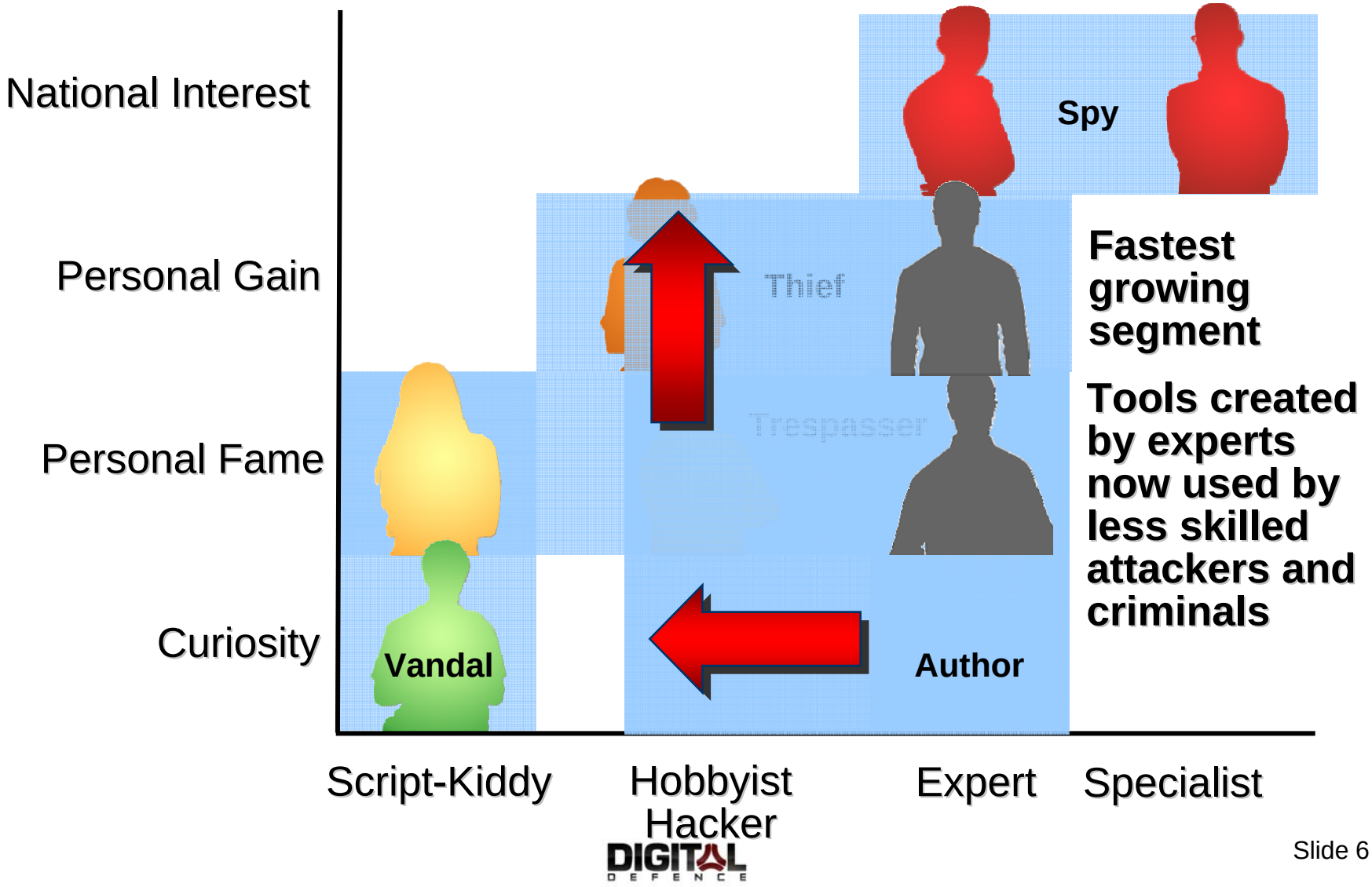


~2,000 – 5,000; highly skilled; difficult to detect, impossible to catch

20,000 – 50,000 in action; understand what they are doing; possess basic to advanced skills

At any time, 5 – 20 million script kiddies in action (numbers game)

Classifying Hackers - Motivation

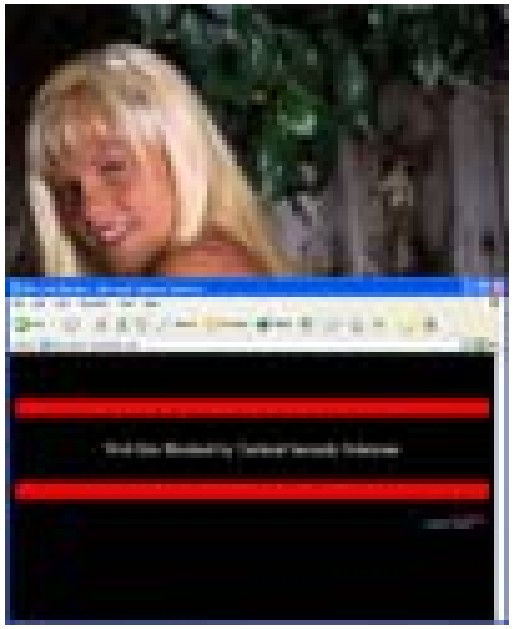


Canadian Computer Crime

Applicable Canadian Criminal Law

- s. 163.1 –child pornography offences
- s. 164.1 – notice and takedown of Internet sites
- s. 172.1 – luring of a child
- s. 184 – interception of private communications
- s. 342.1 – unauthorized use of computer
- s. 342.2 – hacking devices
- s. 430(1.1) – mischief in relation to data
- s. 487 (2.1) and (2.2) – search and seizure for computers

Child Pornography Offences



- Comprise 80%+ of all reported computer offenses
- Most police tech crime groups receive the majority of their funding from victim's groups – child porn is a funded priority
- If 80% of the funding is to cover child porn investigations, then 80% of the work has to be devoted for that purpose
- Overworked, underfunded …

The Sharpe Ruling - 1

- John Robin Sharpe arrested in 1995 for possession of child porn
- Acquitted in 1999 (“current laws restrict artistic freedom”)
- Basically, child porn was legal in province of BC
- 2002 – Supreme Court of Canada sent it back to BC Supreme Court for retrial
- Found innocent for written material; 4 months house arrest for some visual material
- 2002 – Government introduces new laws; weak

The Sharpe Ruling - 2

- July 2005 – Bill C-2 finally passed
- Defence of "artistic merit" in depictions of pornography is removed
- Persons accused of a crime involving child pornography will now have to demonstrate in court that their actions served a "legitimate purpose" - the administration of justice, science, medicine, education, or art - and did "not pose an undue risk of harm to children“
- Holly Jones case

Child Pornography s. 163.1

163.1 (1) In this section, "child pornography" means

- (*a*) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,
  - (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
  - (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years; or
- (*b*) any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act.

Child Pornography s. 163.1

- Accessing child pornography
- (4.1) Every person who accesses any child pornography is guilty of
  - (*a*) an indictable offence and liable to imprisonment for a term **not exceeding five years**; or
  - (*b*) an offence punishable on summary conviction.

Child Pornography s. 163.1

Defence

- (5) It is not a defence to a charge under subsection (2) in respect of a visual representation that the accused believed that a person shown in the representation that is alleged to constitute child pornography was or was depicted as being eighteen years of age or more unless the accused took all reasonable steps to ascertain the age of that person and took all reasonable steps to ensure that, where the person was eighteen years of age or more, the representation did not depict that person as being under the age of eighteen years.

Case #1

- A man brings his computer to the repair shop to have some viruses and spyware removed
- While there, the technician “notices a lot of JPEG files”
- The technician looks at a few, and sees some obviously naked children, and calls the police
- The police agree that it must be child pornography, and interview the computer’s owner
- Turns out, they’re pictures of his 3 year old at bath time → is he guilty of child pornography?

Case #1

- The computer owner is NOT guilty of child pornography
- In this case, refer to the ***intent*** of the pictures
- However, a couple of pictures of bathing Junior is one thing, but if there are several hundred pictures of bathing Junior, and no pictures of the child clothed, it is possible to make a case for possession of child pornography

Case #2

- A 16 year old boy, and his 15 year old girlfriend, take several intimate photographs
- All photographs are taken with full consent of both individuals
- The split apart, and he posts them on a website, representing himself as his ex-girlfriend
- Is she below the age of consent?
- Does this constitute child pornography?
- Does the website owner have to comply with wishes to take down the photographs?

Canada's Age of Consent

- The age of consent is 18 years where the sexual activity involves exploitative activity, such as prostitution, pornography or where there is a relationship of trust, authority or dependency
- For other sexual activity, the age of consent is 14 years (age of partner does NOT matter)
- "Close in age" or "peer group" exception: a 12 or 13 year old can consent to engage in sexual activity with another person who is less than two years older and with whom there is no relationship of trust, authority or dependency

Case #2

Ex-girlfriend's nude photos lead to child porn charges

Last Updated Fri, 22 Apr 2005 10:50:45 EDT
CBC News

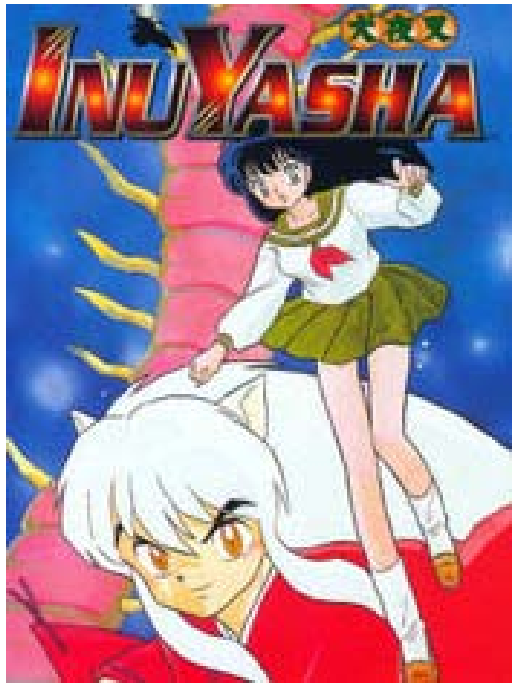
TORONTO - A 16-year-old from Toronto is facing child pornography charges after nude photos of his former girlfriend were posted on a website.

Police can't get the website operator to take down the photos, which were taken with the girl's consent. She was 15 when the photos were taken.

The boy has been charged with possessing and distributing child pornography and with impersonation with intent.

http://www.cbc.ca/story/canada/national/2005/04/22/internet-teen050422.html

Case #3



- An Edmonton area man imports 15 books featuring “manga” artwork
- Manga is Japanese for “comics” or “print cartoons”
- Themes can vary – most are for children, youths, but some feature adult content
- The man in question had previously been convicted of possession of child pornography
- Does the manga “child pornography”?

Case 3

- The court decided manga IS a “visual representation”, and that the cartoon characters represented human beings
- Therefore, charged with possession of child pornography
- 18-month conditional sentence; 100 hours of community service
- Fined $150
- Must under go counseling
- Barred from using the Internet for 18-months
- Must provide a DNA sample and will be placed on the Canadian sex-offender registry for 5-years

To Avoid Confusion in the Future

- Manga refers to cartoons, specifically print cartoons
- Anime refers to animated cartoons
- Hentai – colloquial translation is “perverted”
  - Refers to cartoons that feature sex, degradation
  - Constitutes pornography, child pornography, obscenity depending on what is depicted

Case #4

- While doing a penetration test, you identify a shared drive that is accessible on a network
- The drive contains directories that are accessible to all employees, including one called “lolitas”
- You peek inside, and determine that it contains child pornography
- You inform the customer of your finding, and they tell you to finish off the pen test and that “they’ll deal with it”
- What is your legal responsibility?

Case #4

- You are obligated to inform law enforcement of your findings
- Non-negotiable; otherwise, you are complicit
- Generally, give the business time to organize themselves (what is a “reasonable amount” of time?)
- Once this has passed, you must inform law enforcement
- Include this as a provision in your engagement contract

Case #5

- While do forensic imaging and analysis of a hard drive for something else, you find evidence that the owner of the computer was surfing, extensively, at website that featured child pornography
- What is your legal responsibility?

Case #5

- It’s not as cut and dried …
- Pop-ups from various website can fill a browser cache with links to pornography, child pornography websites – does not mean the person actually visited the site
- You know a computer was accessing child porn (maybe), but do you really know who was using the computer
- May impact ability to bring other matters to trial

Case #6

- Does the punishment fit the crime?
- 5,000 pictures, 5,000 videos of child pornography found on a Montreal man's computer
- Many features his own daughter, starting at the age of 24 months and continuing until she was 4
- The maximum sentence he faced was 15 years in prison
- What is an appropriate sentence?

Case #6

- Original sentence was 15 years
- Reduced to 9 years
- Court cited his young age (32?), his lack of a criminal record (other than the assault of another child when he was 17), and the fact that the assaults were non-violent (no spanking or other physical abuse)

CBCnews

WIRELESS

NEWS
Indepth »
Viewpoint »
BUSINESS
SPORTS
RTS & ENTERTAINMENT
WEATHER

Pedophile's sentence too harsh, judge rules

Last Updated Wed, 31 May 2006 11:22:28 EDT
CBC News

A Quebec judge on Tuesday reduced the sentence of a Montreal man who raped his infant daughter, saying the original ruling was too harsh.

Luring s.172.1

- **172.1** (1) Every person commits an offence who, by means of a computer system within the meaning of subsection 342.1(2), communicates with

  (*a*) a person who is, or who the accused believes is, under the age of eighteen years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155 or 163.1, subsection 212(1) or (4) or section 271, 272 or 273 with respect to that person;

  (*b*) a person who is, or who the accused believes is, under the age of sixteen years, for the purpose of facilitating the commission of an offence under section 280 with respect to that person; or

  (*c*) a person who is, or who the accused believes is, under the age of fourteen years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 281 with respect to that person

Luring (172.1)

Punishment

- (2) Every person who commits an offence under subsection (1) is guilty of
  - (*a*) an indictable offence and liable to imprisonment for a term of **not more than five years**; or
  - (*b*) an offence punishable on summary conviction.
- (4) It is not a defence to a charge under paragraph (1)(*a*), (*b*) or (*c*) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person

Age of Consent / Luring

CBCnews

WIRELESS FR

NEWS
Indepth »
Viewpoint »
BUSINESS
SPORTS
ARTS & ENTERTAINMENT
WEATHER
HEALTH & SCIENCE
CBC ARCHIVES
KIDS
TEENS
PROGRAM GUIDE
E-MAIL NEWSLETTERS
SERVICES

Web luring case raises age-of-consent issue

Last Updated Fri, 11 Mar 2005 09:17:49 EST
CBC News

OTTAWA – Critics are demanding that Canada's age of sexual consent be raised after Ottawa police charged a man from Texas with luring a 14-year-old boy to his hotel room after meeting him on the internet.

Dolita Smith, the president of the Toronto-based Canadians Addressing Sexual Exploitation, said Canada's low age of consent – 14 – is a magnet for internet lurers. The age of consent is 17 in Texas.

"No wonder they come to Canada," she said.

Case #7

- A 32-year old Edmonton man meets a 12-year old girl in a chat room
- He says he's 17; she says she's 13
- Very quickly engage in sexual text chats
- Exchange contact information
- He phones her house, and described an act he wanted to perform
- She hangs up, terrified, and tells her father
- Is the 32-year old man guilty of luring?

Case #7

- NO (decision rendered 31 March 2006)
- Dirty talk does not constitute luring; could represent a fantasy on the part of an individual
- Must convict on the basis of an act that indicates a willingness to follow through with an illegal activity
- Many countries have a legal description of “grooming”; Canada has not yet enacted this

Unauthorized Use of Computer s. 342.1

(1) Every one who, fraudulently and without color of right,

- (a) obtains, directly or indirectly, any computer service
- (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or,
- (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under section 430 in relation to data or a computer system is guilty of an indictable offence and liable to imprisonment for a term **not exceeding ten years**, or is guilty of an offence punishable on summary conviction

Case #8

- A Toronto man is caught driving the wrong way down a one-way street at 5:30 AM, pants around his ankles, and downloading child pornography from wireless access points in the neighborhood
- He is charged with possession of child pornography, and theft of wireless access services
- Why is he charged with under 2 sections of the criminal code?
- Is logging onto someone else's wireless really illegal?

Case #8

- The “theft of services” is a back-up charge: if he manages to wiggle out of the possession of child pornography, his defence of himself will force him to admit to the second charge
- YES, this is an example of theft of services
- The police are not yet rounding up the thousands of people who commit this crime, but only because of limited resources

Possession of Device to Obtain Computer Service s. 342.2

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

- (*a*) is guilty of an indictable offence and liable to imprisonment for a term **not exceeding two years**; or
- (*b*) is guilty of an offence punishable on summary conviction.

Case #9

- A network administrator purchases a packet sniffing software, justifying it to executives as a management tool
- This particular application can be configured to sniff and compile a list of userIDs and passwords
- He places a hub on the network, sets up his sniffer, and soon has the everyone's userID and password
- As a system admin, he could have got this information legitimately
- Is this a violation of Section 342.2?

Case #9

- NO
- By legal definition, a “device” is something tangible, physical – software is not physical
- Act was originally written to catch people using Blue Boxes, or otherwise connecting to the telecomm system
- Is a Blue Box illegal? Depends … it’s all a matter of *intent* (e.g.: lockpicks)

Mischief in Relation to Data s. 430(1.1)

- (1.1) Every one commits mischief who wilfully
  - (*a*) destroys or alters data;
  - (*b*) renders data meaningless, useless or ineffective;
  - (*c*) obstructs, interrupts or interferes with the lawful use of data; or
  - (*d*) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Mischief in Relation to Data s. 430(1.1)

Punishment

- (2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and **liable to imprisonment for life**.

- (3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars
  - (*a*) is guilty of an indictable offence and liable to imprisonment for a **term not exceeding ten years**; or
  - (*b*) is guilty of an offence punishable on summary conviction.

Canada is a “Hacker-Attack Haven”?

Pentagon: Canada is hacker-attack haven

“Toronto -- Justin Davis, a 20-year-old convicted computer hacker from Thunder Bay, says he hasn't met a system yet that he couldn't break into.

"The longest it has taken me to hack a complicated system is 35 minutes."

Globe and Mail, 19 May 1999

DIGITAL DEFENCE

A “Cyberterror Hotbed”

CANADA IS CYBERTERROR HOTBED

U.S. Agency Says 80% of Hacker Attacks Go Through Canada

Source: National Post

Posted on March 25, 2000

An American intelligence agency has determined that up to 80% of foreign attacks on U.S. computers either originate or pass through Canada, according to a report prepared last year for Canada's Department of National Defence.

The report quotes the Defence Intelligence Agency, the U.S. military's counterpart to the CIA, warning that Canada is seen as a "Zone of Vulnerability" and will face growing pressure to do more to combat cyberterrorism.

http://www.e-commercealert.com/article44.html

Russell Sanford (“egodeath”)

- In 1999, hit 60+ computer networks in North America, including US post office and Canadian DND
- 17-year-old high school student penetrated the military's security network in 10 minutes from a computer set up on his mother's kitchen table
- Used unpatched vulnerabilities
- His 15-year old accomplice was caught, and agreed to go undercover on Internet chat lines

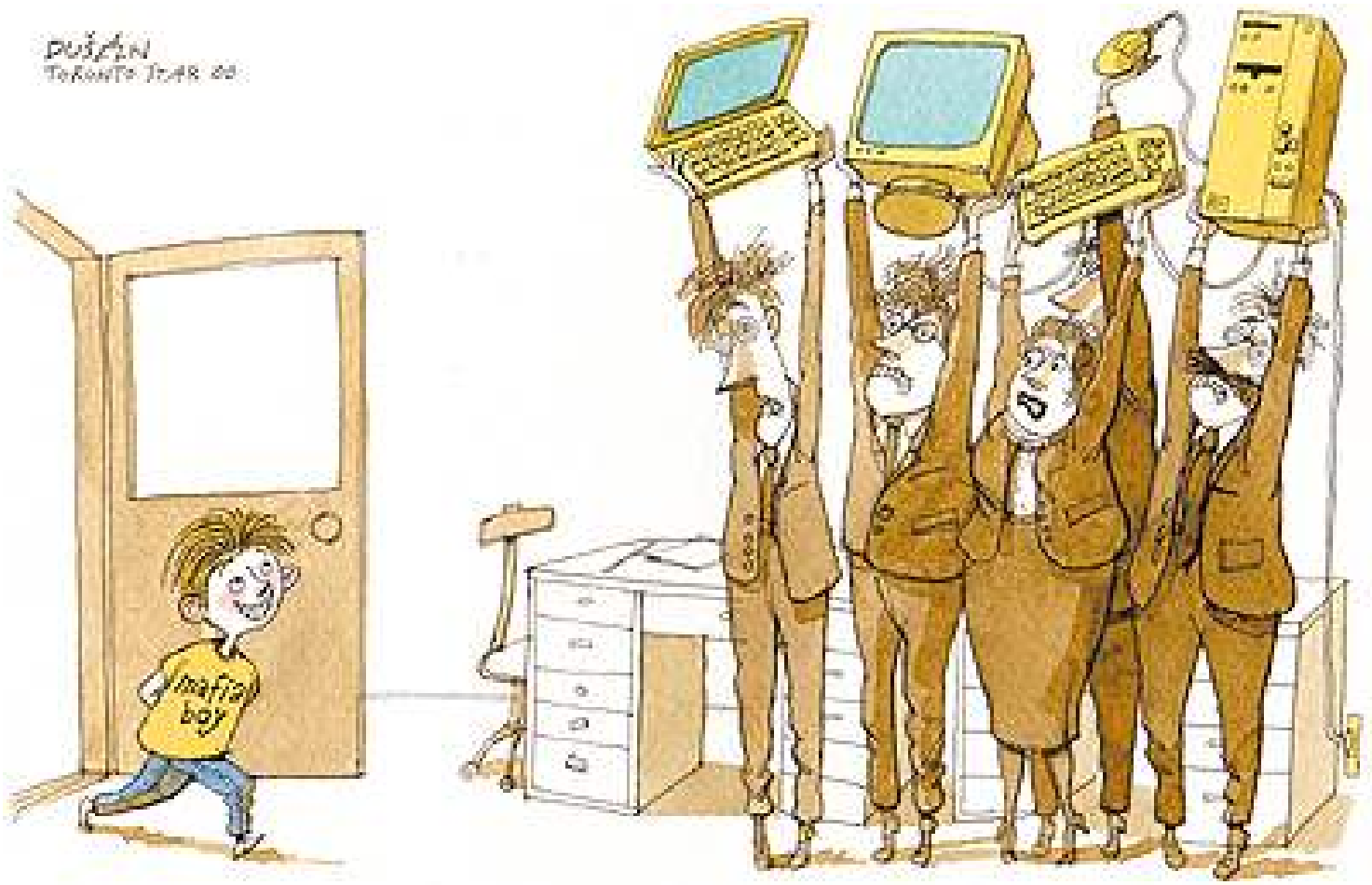
Egodeath's Punishment

- Faced a maximum of 10 years in prison
- Sentenced him to five years' probation on conditions that he keep the peace, stay offline, submit to random polygraph tests and pay $45,000 U.S. in restitution
- Cross-border investigation (FBI, RCMP, DND, + security from 60+ organizations … is $45,000 enough?)
- Caught selling LSD to raise $$ for the fine, sent to prison for 2 years

Mafiaboy

- February 2000 – Several major commercial website come under a Denial of Service attack
- Not sophisticated; script-kiddie stuff
- Damages estimated to be $1.7 – 2 billion dollars
- Start of cross-border media “frenzy”

MafiaBoy



Case #10

- Investigation by RCMP, FBI, US Dept of Justice
- “Mafiaboy” was bragging about the DoS attacks on an IRC channel
- Did a search, found use of that handle at a Montreal ISP, Look Communications
- Seized records, used logs to identify the residence of Mafiaboy
- By use of wiretap, determined it was a 15-year old male
- What was his punishment?

Case #10

- Under Canadian laws in existence at that time, the max penalty was 2 years in jail
- Pleaded guilty to 55 counts of “mischief”
- 8 months in a youth detention centre
- 1 year probation
- Fined $160
- Fair enough ?

Mafiaboy – Final Resolution

Doer, Lord: Passport issue will strain relations

cnews Tech News

› HOMEPAGE

Mafiaboy May 31, 2006

TECH NEWS
Internet
Tech Investor
Tech @ Home
Biz Tech
New Stuff
WHAM! Gaming
COLUMNISTS
Greg Michetti
Greg Gazin
David Canton
CNEWS
CANADA
WORLD

Know the risks when purchasing online

When it comes to security on the Internet, the reliability of credit card transactions is almost always the leading concern. Incidentally, this is with good reason because, in my opinion, the risks are still very important. Full Story

Want free long distance? Use the internet

You want to call anywhere in the world free of charge? This is possible thanks to a software called Skype and high speed Internet access. Full Story

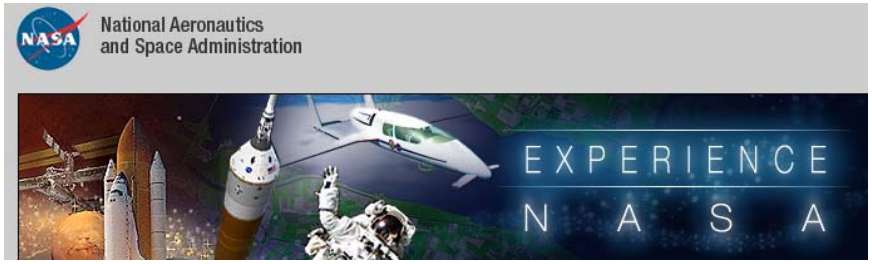
Hacking becoming even easier

In 1999, I heard a lot of criticism from people saying I had no merit for what I achieved, stressing it was easy. I have bad news for them: website hacking is on the way to becoming even easier. Full Story

DIGITAL DEFENCE

Case #11

- 22-year old hacker from Sudbury
- Defaced ~50 websites, including NASA
- NASA home page put out of service; repairs cost $70,000
- Used software for password guessing; not sophisticated application
- What was the punishment?



DIGITAL DEFENCE

Case #11

- Sudbury hacker was sentenced to 6 months in jail
- Fined $6,000

- Compare this to Mafiaboy's punishment – should there be a defined punishment standard for this type of crime?

Case #12

- Canada's "hero hacker" (AKA Citizen Tipster, Omni-Potent)
- 19-year old hacker, lived in parent's basement (!), wrote a Trojan program to find and identify child porn users
- Online up to 16 hours per day, identified 3,000+ users
- Caught an Orange County (USA) Superior Court Judge – diary entries led to photographic evidence on his computer
- Did the Canadian hacker assist in the prosecution?

Case #12

- Judge argued that law enforcement searched his computer, which was the property of the court – accepted, search deemed illegal
- Admitted, and proved, that he molested a boy in 1979 – not accepted into evidence as it was an “old charge”
- The diary and 1,500 photos were uncovered by a Canadian hacker committing an illegal act – constituted an illegal search; not admitted as evidence

Case #13

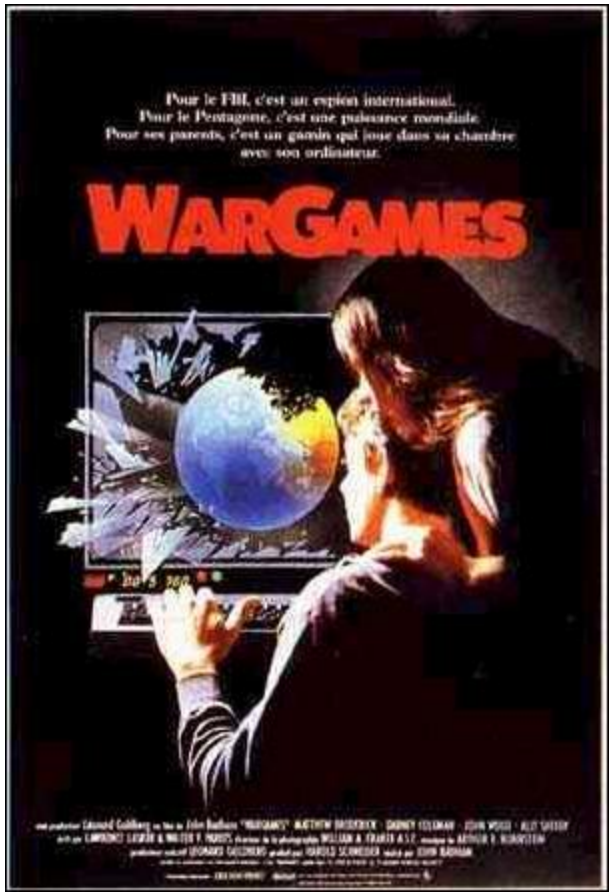
- Hamilton man gains co-workers passwords (shoulder surfing, or copying them from written notes)
- Uses information to access ex-wife's credit information
- Severely damages her credit rating
- What was the he punishment?

Case #13

- For destroying his ex-wife's credit rating, 12 months in jail

Case #14

- 2006 - A Toronto teenager who hacked into a U.S. military computer network in 1999 has finally pleaded guilty
- Gained access to computers at the Charleston Naval Weapons Station in South Carolina and the Coastal Weapons Systems Center in Pensacola, Florida
- Part of a challenge among young hackers to obtain an e-mail address signifying employment in the U.S. armed forces



Case #14

- He was sentenced to two years' probation
- Given an order not to enter the United States until 2008

Cyberactivism – Canadian Style

- March 2000 – The website of the Anglo Society of New Brunswick was attacked, and translated into French
- June 2001 – Hacker spoils ballots during an online vote of NS labour union
- February 2002 – NFLD Tories complain of Liberals “hacking into their computers”
- June 2002 – Hacker links police department web site to porn sites
- March 2003 – Website defaced with anti-Iraq war peace message

Cyberactivism – Canadian Style

- June 2004 – hacker closes down Liberal, Conservative party websites
- 2005 – hacker skews government poll; www.raisetheflag.ca
- 2006 – Electronic sign on GO train modified to read "Stephen Harper Eats Babies"

Insiders - Logic Bombs - 1987

- A disgruntled employee of a London, Ontario, company planted a logic bomb that would have knocked out the computer system. It was detected. The man was prosecuted, but not convicted. Evidence of a previous logic bomb implantation was not admitted because the previous company (in Alberta) had refused to press charges.
- Another Toronto company had a logic bomb triggered the day an employee's termination notice was processed by the computer system. Sgt Green noted that "It wiped out the whole system."

Insiders - Sabotage

- 2005 – During union negations, an employee, represented by the Society of Energy Professionals and working at the Ontario Grid Control Centre in Barrie, threatened to plant a virus in the Network Management System
- The employee has been escorted from the work premises and will remain off the job while Barrie Police conduct a thorough investigation

Insiders – Inappropriate Use

- 2005 – Edmonton police under fire for racist e-mails
- 2005 - Ex-police staff charged over misuse of computer data
- 2001 - … police are under investigation for allegedly using government computers to swap porn and crime-scene pics… the inquiry involves more than 60 police officers from the Ontario Provincial Police (OPP) force
- 1999 – After a 27-year career, David Marshall, the base commander of CFB Esquimalt, was relieved of his command after an investigation into explicit e-mails
- 1998 - Computer sweep at Dofasco Inc. leads to worker suspensions

Insiders - Theft

Bruce McGrath worked in information technology at the head office of the Liquor Control Board of Ontario, in Toronto, for 5+ years

- During that time, he helped design a new system to link the electronic journals at 600 LCBO stores to one central database
- Police claim Mr. McGrath wrote in some extra programming language
- It is alleged that those modifications allowed Mr. McGrath to walk in to any of three LCBO locations, buy a bottle of wine for $16 to $20 on his bank debit card, and ask for $300 in cash back. The debit card reader would electronically approve the transaction. Then, after Mr. McGrath left the store with his wine and his cash, police allege, the computer would automatically cancel the authorization for the cash withdrawal. That way, the $300 was never debited on his account
- Police allege Mr. McGrath stole more than $80,000 this way (Mar, 2003)

Insiders – Theft of Confidential Information

TORONTO STAR
www.thestar.com

Personal data stolen from Bank of Canada

Apr. 7, 2006. 04:30 PM

CANADIAN PRESS

OTTAWA — At least two people got into a Bank of Canada database and obtained the personal information of 14 Canada Savings Bonds clients, RCMP said Friday.

In eight cases, the suspects used the information to redeem the savings bonds, Supt. Dan Killam said. The other six cases saw the information used to apply for credit cards or for other fraudulent purposes.

"Illegal financial activities take money from the pockets of hard-working, law-abiding Canadians," Killam said at a news conference.

"These types of crimes shake the confidence of both consumers and investors."

Police believe the two suspects worked for EDS, a private company that manages the database of thousands of people who buy Bank of Canada savings bonds through payroll deductions.

Insiders - Theft of Intellectual Property

- CIBC is suing Genuity Capital Markets, a new Toronto-based investment management firm established by six former CIBC employees
- The lawsuit centers around CIBC's allegation that these former employees used their BlackBerrys to improperly recruit their colleagues while still working at the bank
- Messages sent BlackBerry to BlackBerry, marked as “private”, are not “private”
- Employee compliance monitoring used to aid a civil suite (May, 2005)

Commercial Attacks – Confidential Information

- February 2003 – attacker at US credit card processing site gains access info of ~110,000 Canadians
- 2003 – IBM “loses” a hard drive containing the personal data of 180,000
- 2004 – Security breach at Equifax
- 2005 – Government of Alberta loses backup tapes containing medical data for 675,000 citizens
- 2005 – Government of PEI loses backup tapes containing medical data for 110 citizens

Commercial Attacks – Confidential Information

- 2005 – Desktop computer stolen from a towing company contains confidential information
- 2005 – Hacker break into US firm EnCase, steal confidential information and credit card info for North American law firms
- 2005 – Equifax hacked (again)
- 2006 – Computer stolen; contained personal information on 11,000 healthcare workers

Commercial Attacks

- 2001 – JDS Uniphase halts trading when a hacker breaks into a public FTP server and steals an earnings report prior to approved release time

- 2002 – Hacker breaks into CryptoLogic, which makes online gambling software; reprograms slot machines and crap tables at 2 websites
  - Every one a winner!
  - 140 gamblers pocket $1.9 million USD
  - Insider

Case #15

- February 2002 – an ethical hacker, frustrated that a company that writes mutual fund analysis software has failed to heed his warning and secure their website, releases information and “proof” to public security newsgroups
- Company denies claims; smears the whitehat
- Company forced to spend thousands for independent penetration testing to regain customer trust
- Is it ethical to publicly relase this information?

Case #15

- The case is still be resolved in the courts
- When a matter resolves itself to ethics, instead of defined law based on a case history, there is rarely a resolution that satisfies everyone

Commercial Attacks

- May 2002 – an insider at Mitel “facilitates” the loss of proprietary data to a location in Vietnam
- Most attacks are not reported
- 2006 – Resolution of the Air Canada / WestJet disput

Case #16

SDAY 07.04.04

PORT BUSINESS

TSX comp.	DJ Ind.	Nasdaq	Dollar	Gold
8,832.71 −25.78	10,570.81 +12.44	2,059.90 −19.22	76.42 +0.25	418.90 +3.50
Technology stocks fall, led by Nortel Networks	Gains by Kodak, International Paper lead index higher	Index falls on Nokia warning, interest rate concerns	Currency rises as expectations subside for June rate cut	Bullion rises as the U.S. dollar falls against the euro

K J HARRISON & PARTNERS INVESTORS

AIRLINES

Air Canada claims WestJet stole data

Alleges that rival illegally accessed its computers to take competitive information

BY PAUL WALDIE AND JOHN PARTRIDGE

Air Canada is accusing competitor WestJet Airlines Ltd. of illegally accessing its computers to steal confidential competitive information, the latest twist in an increasingly bitter rivalry between the two companies.

In a statement of claim filed yesterday in the Ontario Superior Court, Air Canada alleged that one of its former employees who now works for WestJet allowed his employee number and personal identification number or PIN to be used to gain access to Air Canada's employee website a total of 243,630 times between May 15, 2003, and March 19 of this year.

"The ongoing, unlawful exploitation of [Air Canada's] confidential information, has caused [Air Canada] substantial loss, including loss of revenue, profits, and goodwill," alleges the suit, which seeks $5-million in damages.

WestJet officials declined comment last night. "At this time, Westjet has not reviewed Air Canada's statement of claim. As a result, it would be inappropriate for Westjet to provide comment on this matter," the company said in a press release.

The allegations in the lawsuit centre around Jeffrey Lafond, who worked for Canadian Airlines International Ltd. from 1997 to 2000, just before it was taken over by Air Canada.

Mr. Lafond is currently a financial analyst at WestJet.

As part of his separation package from Air Canada, the airline alleges Mr. Lafond received two Air Canada tickets a year, for use on a space available basis, for five years. In order to book flights with the tickets, Mr. Lafond was given access to a special reservation website for the employees and retirees of Air Canada.

The website contains confidential information about the number of passengers booked on all flights at Air Canada and its subsidiary Zip for up to 352 days in the future, the suit claims.

Air Canada alleges that officials at WestJet used Mr. Lafond's access to the website.

The information "would give [Air Canada's] competitors detailed and accurate information on the success of [Air Canada's] routes and market conditions which would not otherwise be available to them," the suit alleges.

Air Canada claims WestJet has accessed the website up to thousands of times each day using Mr. Lafond's access codes. The airline alleges WestJet has used the information to target Air Canada's most profitable flights and adjust schedules accordingly.

Mr. Lafond and Mark Hill, Westjet's vice-president of strategic planning, are named in the suit.

None of the allegations has been proven in court.

■ Rule change affects agents, B...

TECHNOLOGY

SEC probes trading in

HOT MAMMA

Trading in shares of Montreal-based Mamma.com, the self-described "Mother of all search engines," has been hot and heavy. The stock has soared about 250 per cent over the past six weeks.

FOREST PRODUCTS

Court puts Doman on

- Air Canada employee goes to WestJet
- His userID and password are used to access employee travel site
- Having inside route information give WestJet a pricing advantage
- Air Canada files suite, seeking $220 million

Case #16

- The practice was endorsed by WestJet executive management
- Not stopped until discovered by Air Canada
- WestJet to cover $5.5 million in legal fees (2 year battle)
- WestJet to donate $10 million to charities in the names of both airlines
- Win-win solution?

Search and Seizure s. 487(2.1)

- (2.1) A person authorized under this section to search a computer system in a building or place for data may
  - (*a*) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
  - (*b*) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;
  - (*c*) seize the print-out or other output for examination or copying; and
  - (*d*) use or cause to be used any copying equipment at the place to make copies of the data

Anton Pillar Orders

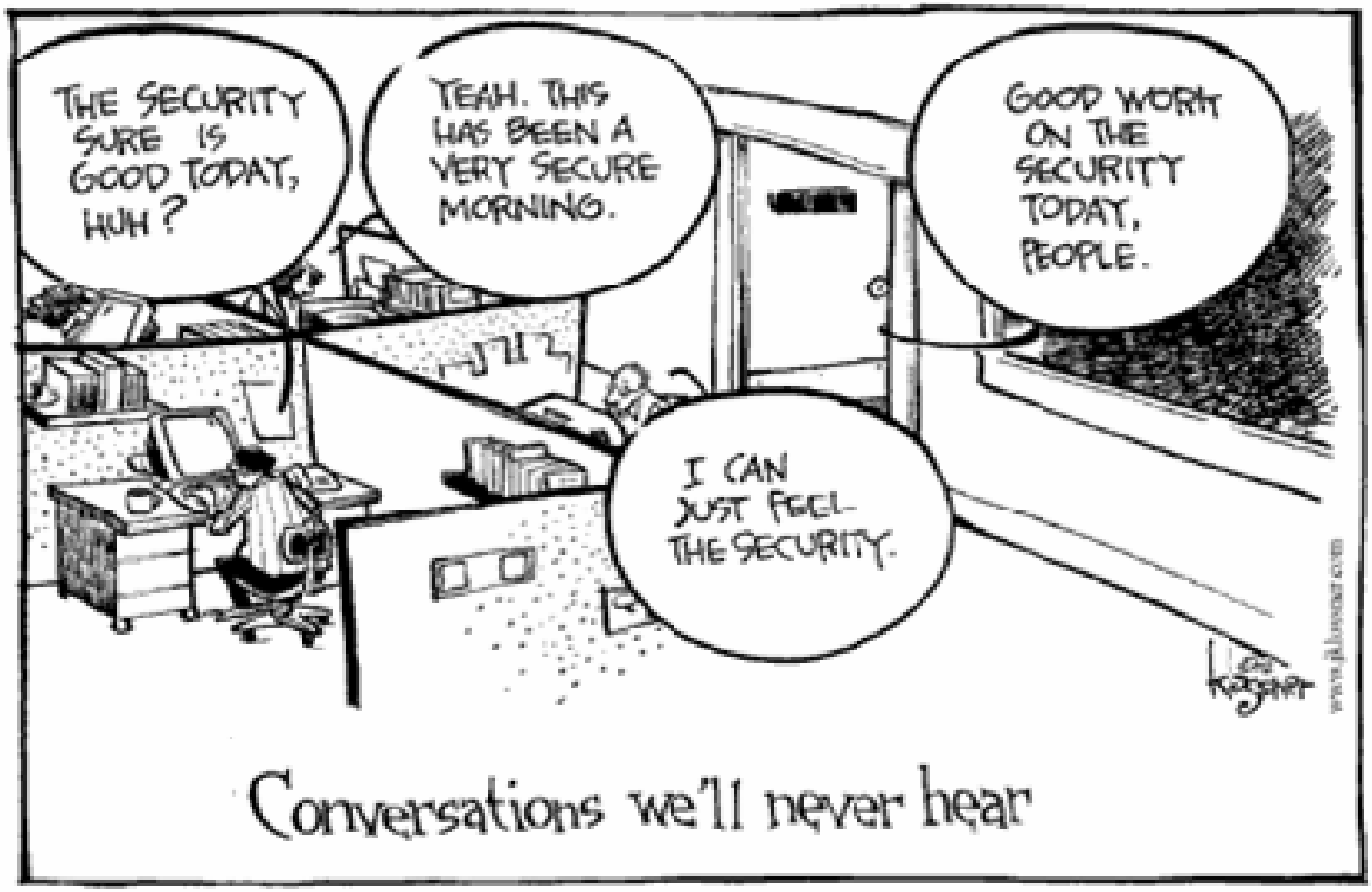
- Civil remedy
- Useful when employees copy sensitive customer information, intellectual property to mobile devices or their home computers
- Provides basis for seizure and search of devices to identify and preserve evidence
- Prevents spoiling of data
- Court order, you must comply – within the bounds of the order as written…

Conclusions

- Reports of hacking in the media are grossly underreported; we estimate that less than 10% are reported
- Nearly all schools, universities have been hacked
- Several Federal and Provincial government departments are known to have been compromised
- Most investigations include participation or assistance from non-law enforcement personnel

Conclusions

- What is a the “hacker profile”?
- For the individuals who have been caught (which slews the sample!) they are:
  - Male
  - Typically between the ages of 15 – 25
  - Not especially skilled
  - Tend to use freely available tools and unsophisticated attacks


THE SECURITY SURE IS GOOD TODAY, HUH?
YEAH. THIS HAS BEEN A VERY SECURE MORNING.
GOOD WORK ON THE SECURITY TODAY, PEOPLE.
I CAN JUST FEEL THE SECURITY.
Conversations we'll never hear

References

- DigitalDefence (www.digitaldefence.ca)

- Canadian Criminal Code, Justice Canada (www.justice.gc.ca)

digital defence

Security. Privacy. Compliance. Trust.

Robert W. Beggs, CISSP CISA
CEO

416.306.5775 (Office)
416.644.8801 (Fax)
647.444.1492 (Mobile)
robert.beggs@digitaldefence.ca

DigitalDefence, Inc.
www.digitaldefence.ca

1st Canadian Place
100 King Street West,
37th Floor
Toronto, Ontario
M5X 1K7