Technology Security - Mandatory and Unachievable (but Approachable)

Scott Bradner
University Technology Security Officer
Harvard University

5 November, 2008

1

Agenda

- the real (ugly) world
- what
- how
- he is us
- why
- rules
- your role

2

The Real (ugly) World

- 554 breaches so far in 2008
  30,422,125 people's data exposed
- $56 B cost of ID theft in 2005
  (random guess by a)
- top of the curve - TJX
  94 M credit cards - $250M cost (as of mid 2008)
- but it's not just identity theft
  personal privacy, business secrets, etc

3

What is at Risk?

- ID theft data (act as you)
  e.g., SSN, credit card, bank account # etc
- blackmail/economic/job threat
  e.g., medical records, social interactions
- considered private
  e.g., salary and personnel information, business plans

4

A Definition

- confidential information

  Information about a person or an entity that, if disclosed, could reasonably be expected to place either the person or the entity at risk of criminal or civil liability, or be damaging to financial standing, employability, or reputation.

5

How

- hacking (to the cops, not a good thing)
- put world on laptop, lose same
- insider needs money
- forget to read protect a file on a web site
  or assume no one will find it
  or donate computer with uncleaned disk
- B&E
- social engineering

6

He is Us

- jan/feb 2008
  - laptop - 22%
  - hacker - 16%
  - non-laptop - 26%
  - exposed - 28%
  - employee - 10%

- 66% data victim did not know was on system (Verizon report)
- 22% of 2008 breaches from education

7

All your computer are belong to us

- factoids
  - Microsoft researcher: average time until an unpatched Windows XP box is owned - less that 15 min
  - Windows XP - 40 M lines of code
    - Vista adds another 10 M
  - mom is not a computer security expert
  - people have a job to do - security can get in the way

8

Why?

- was fun, now money
  - spam, ID Theft etc
    - hack to get at data, phishing
    - e.g., Jeremy Jaynes - $.5M/mo
  - botnets - 100s of thousands of zombie machines - used to forward spam & DoS attacks (for a fee)

9

Rules

- philosophy
  - Europe - your data belongs to you
  - US - your data belongs to whoever has it
- no meaningful US government rules on general data protection
  - some specific rules for student, health & human subject data
- regulations for new Mass ID theft law
- MIT rules

10

Mass Rules

- law: "duty to protect" "personal information"
- personal information: SSN, credit & bank account #s, etc
- new regulations explain what the "duty" involves
  - lots of rules
- not just bits
  - paper as well as electronic data

11

FERPA

- Family Educational Rights and Privacy Act
- federal law
- give students control over their records
- if not directory info then confidential
  - student can block inclusion in directory
    - blocked student does not exist - problem for phone-based help desks

12

MIT Rules

- http://web.mit.edu/ist/topics/policies/

  "MIT maintains certain policies with regard to the use and security of its computer systems, networks, and information resources. All users of these facilities, including technology developers, end users, and resource administrators, are expected to be familiar with these policies and the consequences of violation."

13

Your Role

- be aware
  - of what data you have
  - of how to protect the data
    - know the rules
  - of who you give data to
    - make sure they know its nature
  - proper destruction when it is time

14

More of Your Role

- don't be a voyeur
- don't run in stealth mode
  work with IT to protect & (if needed) recover

15