Owning the Desktop: Is .edu like .com?

Scott Bradner

Harvard University

University Technology Security Officer

Agenda

- issues (real)
- issues (per vendors)
- extra .edu issues
- throw policy
- technical?

Issues: Software & Vendors

- Bellovin - buggy software a key problem

  e.g., 40 M lines of code in Windows

- slooooow fixes

  patches on a schedule - bugs not follow a schedule

Issues: ID Theft

- ID theft: ability to assume someone's identity
  - not just steal credit card # & exp date
- primary reason we try to protect SSNs
- 246K ID theft reports to FTC in 2004
  - actual count may be as high as 9M ($52B losses)
- can take years to repair

Issues: Crustacean Security

- installing firewalls can install complacency
  - users assume they are protected
- but open to everyone inside the wall
- only real security is host-based
- but firewalls help
  - and are required by many regulations
- firewalls/filters should be put as close to server being protected as possible
  - in addition to perimeter firewalls

Issues: Portable Data

- data migrates to individual user's computers
  - desktops, laptops, handhelds ...
- little encryption on these machines
- stolen or improperly decommissioned machines (& disk drives) can contain important data
  - many examples in news - machine lies to user
- can be issue if machine shared with employee's family

Biggest Issue: People are Human

- people don’t think of consensuses: e.g.,
  - sharing passwords
  - grant process that requires tax returns
  - data on laptops - no encryption, no password-protected screensaver
  - leaving report on desk at night
  - email report to co-worker or vendor
  - hard to know what to protect
  - ...
- corollary: security gets in the way

Foisted Answers

- 1-2 calls from telemarketers per month
  - usually a script kiddie
  - always “best in industry” &/or “protect against ALL malware”
    - control data flow and access
    - ensure patch level
    - protect corporate secrets
    - comply with {SOX, HIPAA, GLB ...}
    - protect against ‘bad’ content in email, surfing etc
- some may be real problems in .edu

Vendor Assumptions

- Ghengis Khan is in charge of network
  the WHOLE network & ALL computers
- all computers controlled by enterprise
- its all Windows
- users do not have admin access
- single control point
- clear understanding of sensitive information
- someone to watch a screen
- many someones to configure system

.edu Reality

- many networks
- many network managers
  with local semi-power
- whole lotta owners
- not just Windows
- agent requirement hard (if possible)
- no clue about sensitive information
- people are expensive
- faculty do not answer to anyone

.edu Risks

- central IT groups generally know what they are doing
- risk areas

  local graduate-student run research labs

  student-owned machines

  researchers (e.g., getting SSNs from subjects)

  data exchange with vendors

  ...

Throwing Policy

- active policy development process
- university-wide mandates
  - local implementations
- on web site -{security|privacy}.harvard.edu
  - policies
  - info on regulations, processes etc
  - contract riders
- internal auditors enforce policy

Some Policies

- passwords
- network/system setup

  checkers, IDS etc
- no Harvard confidential data on portable computers(including vendors)
- human subject data
- credit card security processes & reporting
- ...

What Are We Doing?

- administration computers
  - per school standard disk image
  - includes virus checkers etc
  - central admin adding whole-disk encryption
    - advise other schools to do same
- other computers
  - undergraduate software package
    - includes checker etc
  - state best practices
  - low cost checker software at university store

Biggest Problem

- internal communication

  lots of talks

  mail (e- & paper) to VPs etc

  newspapers

  web site

  on-line training

- but still too few people know policies

  nor do they know where the Personnel Manual is

Example: WWHW

Data Security and Protection: What **YOU** Need To Know

WHAT is Confidential Information?

Personally identifiable information (which is protected by law or contract) and non-personally identifiable information (which is protected by Harvard policies).

Examples include:

- Social Security Numbers
- Health and Employment Information
- Harvard University ID Numbers
- Credit Card and Bank Account Information
- Student Information *other than directory information*
- Harvard plans and summary information about people that could cause institutional risk if disclosed

WHY Protect Confidential Information?

Protecting confidential info is required by:

- Law: HIPAA, FERPA, GLB, Sarbox, US Patriot Act
- Contract: PCI standards

Not protecting information risks:

- Criminal or civil suits
- Financial implications
- Personal or Institutional reputation

HOW Can I Protect Confidential Information?

- BE AWARE of what is confidential. See www.security.harvard.edu.
- DO NOT STORE Social Security or Credit Card Numbers on laptops, floppy disks, flash memory cards or other external devices.
- LOCK AND LIMIT ACCESS to confidential faxes, inboxes and physical files.
- DO NOT SEND confidential information in the body of an e-mail.
- PASSWORD PROTECT computer files that store confidential information.
- LOCK YOUR COMPUTER when it is not in use.
- SHRED confidential information that is no longer needed.
- DO NOT SHARE PASSWORDS or save them on your computer.
- INFORM OTHERS about the responsibility to protect confidential information.

WHO is Responsible for Protecting Confidential Info?

EVERYONE!

This document was prepared by the For additional information visit www.security.harvard.edu; for IT-related questions please e-mail

Can Technology Work?

- can a research .edu use technical protection systems
  - beyond virus checkers etc
  - sure
    - for the business part(s) of the university
    - for places that have a network czar with power
    - for places that have few researchers
- but confidential data seems to have legs and shows up where you least expect it