


Protecting Your Electronic Research Data

IRBMED Educational Symposium
University of Michigan
May 8, 2007


1



Outline

- ◆ Privacy & Security Explained
- ◆ Top Security Risks
- ◆ Defense in Depth
- ◆ Case Studies
- ◆ Handling Incidents
- ◆ Where to Get Help


2



Privacy vs. Security

- ◆ **Privacy:** Ensuring that we use and share data appropriately
- ◆ **Security:** Protecting the confidentiality, integrity, and availability of data


3



Security Basics

- ◆ **Goals:** Confidentiality, Integrity, and Availability
- ◆ **Motivations:** ethics, law (HIPAA, Common Rule, intellectual property), practical concerns
- ◆ **Risks:** Damage to subjects, enforcement action, lawsuits, adverse publicity


4



Cost vs. Benefit

- ◆ Balance security measures against cost and inconvenience
- ◆ Cost/benefit analysis: the more damaging it would be if something happens, the stronger the measures that may be appropriate
 - ◆ Sensitivity
 - ◆ Criticality

5



Common Risks: attrition.org

- ◆ **attrition.org** database:

Chrysler Financial (2008-04-23)
(Data lapse lost in transit contained personal information)

Southern Connecticut State University (2008-04-23)
(11,000 students and alumni e-mails on website)

University of Texas Health Science Center (2008-04-23)
(Social Security numbers available on about 2,000 billing envelopes)

Collegis/axim (2008-04-22)
(List of hard drive expenses 200,000 customers during office relocation)

University of Massachusetts (2008-04-22)
(Electronic health system accessing thousands of medical records)

Roots Dental Plan (2008-04-22)
(Account details of 34,000 stolen from courier)

LendingTree (2008-04-22)
(Social Security numbers, names, addresses, and other personal information inappropriately accessed)

Bank of Ireland (2008-04-22)
(Account information, addresses, and medical information of 10,000 on stolen laptops)

Central Collection Bureau (2008-04-19)
(Social Security numbers and names of 700,000 on stolen server)

University of Miami (2008-04-17)
(E-mails files containing names, addresses, Social Security and credit card numbers of 47,000 patients)

Connecticut State University System / Buffalo State / Northwest Missouri State University (2008-04-17)
(Stolen laptop contains names and Social Security numbers of 20,000 students)

6

M University of Michigan Health System **Common Risks: attrition.org**

◆ **Most common categories:**

Category	Frequency (Approximate)
Lost/Stolen Laptop	210
Hack	160
Web	110
Lost/Stolen Media	90
Lost/Stolen Computer	70
Fraud SE	60
Disposal	50
Lost/Stolen Document	40
Postal Mail	30
Lost/Stolen Disk Drive	20
Unknown	10
Email	5
Other	5

7

M University of Michigan Health System **Common Risks: attrition.org**

Evaluating the attrition.org reports:

- ◆ Taken from media reports
- ◆ Undercounts types of incidents that are easier to conceal
- ◆ BUT a good indication of the types of incidents that get media attention (= adverse publicity)

8

M University of Michigan Health System **Defense in Depth**

A model for thinking about controls on data:

- ◆ Overlapping layers of protection
- ◆ Some may be sufficient in and of themselves
- ◆ BUT require at least two for “acceptable practice” level of assurance

9

M University of Michigan Health System **Defense in Depth**

Categories:

- ◆ Content Controls
- ◆ Physical Access
- ◆ Remote Access
- ◆ Passwords & Authentication
- ◆ Encryption

10

M University of Michigan Health System **Defense in Depth: CONTENT CONTROLS**

Don't access/store/move data you don't need:

- ◆ Avoid highly sensitive data – PHI, SSN, financial info – whenever possible
- ◆ When possible, de-identify or use a limited data set
- ◆ If you need sensitive data, consider separating it out
- ◆ Question whether you need everything you're getting (sometimes may need for regulatory reasons)
- ◆ If you don't have it, you can't expose it


11

M University of Michigan Health System **Defense in Depth: CONTENT CONTROLS**

Resources

- ◆ UMHS Policy on use of PHI in Research
<http://www.med.umich.edu/i/policies/umh/01-04-360.htm>
- ◆ UMHS Policy on De-Identification of Data
<http://www.med.umich.edu/i/policies/umh/01-04-340.htm>
- ◆ UMHS Policy on Limited Data Sets
<http://www.med.umich.edu/i/policies/umh/01-04-342.htm>
- ◆ ITSS Resources on Identity Theft
<http://identityweb.umich.edu/>

12




Defense in Depth: PHYSICAL ACCESS

Take measures to prevent theft/loss or damage to physical items containing data:

- ◆ Store laptops and other portable devices securely
- ◆ Lock your office and lab
- ◆ Use care when traveling
 - ◆ Don't transport devices when you don't need to
 - ◆ Don't leave devices unattended in cars, etc.

13




Defense in Depth: PHYSICAL ACCESS

Resources

- ◆ CERT
 - <http://www.us-cert.gov/cas/tips/ST05-017.html>
 - <http://www.us-cert.gov/cas/tips/ST04-017.html>
- ◆ UMHS Policy on Physical Security of ePHI
 - <http://www.med.umich.edu/i/policies/umh/01-04-520.htm>
- ◆ UMHS Policy on Security of Portable Devices
 - <http://www.med.umich.edu/i/policies/umh/01-04-502.htm>

14




Defense in Depth: REMOTE ACCESS

Most computers are connected to a network, which can serve as a means of attack. You will need to secure your machine:

- ◆ Keep anti-virus software up to date
- ◆ Keep system software up to date with security patches, etc.
- ◆ Be careful what you access on the Internet
- ◆ Secure your local network where possible

15




Defense in Depth: REMOTE ACCESS

Resources

- ◆ Your IT service Provider (or MSIS – you will get the help you need)
- ◆ UM ITSS Security Essentials
 - <http://www.safecomputing.umich.edu/tools/SS-3SecEssentialsPC.html>
- ◆ CERT
 - http://www.cert.org/tech_tips/home_networks.html
- ◆ Microsoft
 - <http://www.microsoft.com/protect/computer/default.msp>
 - <http://www.microsoft.com/protect/yourself/default.msp>
- ◆ Apple
 - <http://www.apple.com/support/security/guides/>

16




Defense in Depth: PASSWORDS & AUTHENTICATION

Good passwords are “necessary but not sufficient”:

- ◆ Passwords alone are not enough, because they can sometimes be bypassed by other methods, but they can be the only thing that protects your data
- ◆ “Strong” passwords address the cracking strategy, which is very useful if you block other access routes
- ◆ Pick strong passwords; don't share them; don't write them where they may be found

17



Defense in Depth: PASSWORDS & AUTHENTICATION

A strong password is good against:

- ◆ People who don't know you:
 - ◆ Dictionary attacks (in any language)
 - ◆ Brute force attacks (length and complexity)
- ◆ People who do know you:
 - ◆ Social hacking (innocent questions)
 - ◆ General knowledge (facts about you)
 - ◆ Information “on the record” (address etc.)

18

University of Michigan Health System **Defense in Depth: PASSWORDS & AUTHENTICATION**

At 15 million password guesses per second...

length: 4, complexity: a-z	==> less than 1 second
length: 4, complexity: a-zA-Z0-9 + symbols	==> 4.8 seconds
length: 5, complexity: a-zA-Z	==> 25 seconds
length: 6, complexity: a-zA-Z0-9	==> 1 hour
length: 6, complexity: a-zA-Z0-9 + symbols	==> 11 hours
length: 7, complexity: a-zA-Z0-9 + symbols	==> 6 weeks
length: 8, complexity: a-zA-Z0-9	==> 5 months
length: 8, complexity: a-zA-Z0-9 + symbols	==> 10 years
length: 9, complexity: a-zA-Z0-9 + symbols	==> 1000 years
length: 10, complexity: a-zA-Z0-9	==> 1700 years
length: 10, complexity: a-zA-Z0-9 + symbols	==> 91800 years

19

University of Michigan Health System **Defense in Depth: PASSWORDS & AUTHENTICATION**

Don't compromise a password by:

- ◆ Sharing it
- ◆ Using it on multiple systems, especially where some are less secure
- ◆ Writing it down somewhere easy to find
- ◆ Transporting it with your laptop/USB key/DVD-R

20

University of Michigan Health System **Defense in Depth: PASSWORDS & AUTHENTICATION**

Resources

- ◆ UM ITCS Password Guidelines
<http://www.itd.umich.edu/itcsdocs/r1162/>
- ◆ Microsoft Password Guidelines
<http://www.microsoft.com/protect/yourself/password/create.aspx>
- ◆ Microsoft Password Strength Check
<http://www.microsoft.com/protect/yourself/password/checker.aspx>
- ◆ UM ITCS "Password Safe" Information
<http://www.safecomputing.umich.edu/tools/SS-ManagePWs.html>

21

University of Michigan Health System **Defense in Depth: ENCRYPTION**

Encoding data so others cannot read it without a key works well, but can be inconvenient:

- ◆ Best when built into the infrastructure (e.g. encrypted web traffic, which is easy and transparent to user)
- ◆ Strongly recommended when sensitive data has to leave a "secured" environment -- laptops, USB drives, sending data outside UMHS
- ◆ Can carry a risk of data loss
- ◆ Only as secure as the password used

22

University of Michigan Health System **Defense in Depth: ENCRYPTION**

Resources

- ◆ Encryption from your UM/UMHS IT provider?
- ◆ MCIT Core Image laptop encryption, 3rd Qtr 2008
- ◆ UM ITSS Encryption Documents
http://safecomputing.umich.edu/tools/security_shorts.html
- ◆ UMHS Policy on Security of Portable Devices etc.
<http://www.med.umich.edu/i/policies/umh/01-04-502.htm>

23

University of Michigan Health System **Defense in Depth: ENCRYPTION**

Resources, continued

- ◆ Other local file encryption options:
 - ◆ Mac OS X Disk Utility / File Vault
 - ◆ Microsoft Word, Excel with strong encryption and a strong password
 - ◆ AxCrypt
 - ◆ TrueCrypt

24



Case Study 1: Portable Devices

- ◆ Research database carried on laptop and USB drive
- ◆ Appropriate methods:
 - ◆ Content Control
 - ◆ Physical Access (note also: don't carry them together if one is intended as a backup)
 - ◆ Passwords
 - ◆ Encryption

25



Case Study 2: Transmitting Data

- ◆ Sending data outside UMHS (e.g. for multi-center study)
- ◆ Appropriate methods:
 - ◆ Content Control
 - ◆ Remote Access
 - ◆ Passwords
 - ◆ Encryption

26



Case Study 3: Private Servers

- ◆ Keeping data or systems needed for research on locally-maintained servers
- ◆ Appropriate methods:
 - ◆ Content Control
 - ◆ Physical Access
 - ◆ Remote Access
 - ◆ Passwords
 - ◆ Encryption(?)

27



Handling Security Incidents: When is an incident Serious?

- ◆ PHI, identifiable human subjects, SSNs, credit info
 - ◆ Includes de-identified data and key on same machine
- ◆ Could affect other systems
- ◆ Could involve significant legal issues
- ◆ Affects more than one provider's systems
- ◆ Active threat (the incident is still ongoing)
- ◆ Likely to raise public interest
- ◆ Affects organizations outside UMHS

28



Handling Security Incidents: What should we do?

- ◆ **Serious Incident:**
 - ◆ **Get IT Security assistance:**
 - ◆ Local IT provider (e.g. MSIS, 763-7770)
 - ◆ MCIT (936-8000)
 - ◆ Campus IT Security (ITSS, 647-5794)
 - ◆ If your provider can't be IMMEDIATELY reached, call MCIT (936-8000)
 - ◆ **Report it to UMHS Compliance (615-4759)**

29



Handling Security Incidents: What should we do?

- ◆ **"Normal" Incident:**
 - ◆ Get IT Security assistance:
 - ◆ Local IT provider (e.g. MSIS, 763-7770)
 - ◆ MCIT (936-8000)
 - ◆ Campus IT Security (ITSS, 647-5794)
 - ◆ IT Provider must report to UMHS Compliance (615-4759)

30



Where to go for help

- ◆ Help on Incidents: Compliance Office, (615-4759).
- ◆ Security Advice: IRBMED
- ◆ Compliance Website:
(www.med.umich.edu/u/compliance)
- ◆ Questions: Compliance Office (615-4759)