Data in the Legal Domain through the Information Technology Lens
Definition of Terms

• **Risk** – level of exposure to undesirable outcomes such as data loss, data theft and extortion

• **Protection** – efforts to reduce risk through access control, authentication restriction, backups and other measures

• **Privacy** – the protection of data for the benefit of those who own the data, especially personal or privileged data

• **Security** – the application of protections and the use of other proactive measures, such as monitoring and auditing, to reduce risk and protect data
Conflicting priorities

• We seek to protect our data to reduce our risks
• We respect privacy as a principle

But:

• We have to make use of the data to make it valuable, and that may conflict with protecting it
• In order to be able to apply security principles, we may need to limit or even compromise privacy. The converse may also be true.
The most secure (but not invulnerable) form of computing – offline, isolated
Example: Log Retention

- Logs provide the ability to monitor and audit; they also potentially expose private data, such as in the case of data loss or theft, discovery, subpoenas or lawsuits

- [Duke] Server Log Retention Policy
  - Servers storing HIPAA Data:
    - [...] 
  - Servers storing PCI Data: 12 months (3 months readily available)
  - Servers storing other Sensitive Data: 90 days
  - Servers storing Restricted Data: 30 days
  - Servers storing Public Data: 30 days
Examples of protection/security

- **URLDefense** – urls in email messages are rewritten by vendor – *every click goes through their server* – if phishing or malware is suspected on the other end the user stopped

- **Attachment sandboxing** – every attachment that might be executable is sandboxed in a vendor environment for five minutes before it is released (or not)

- **Login tracking** – if an account is logged in from two locations that cannot both be local to the user (perhaps s/he is using a VPN?), the account is locked until identity is verified

- **More and more services will required multi-factor authentication or VPN/on campus, or both - soon**
“Digital security, which HE ranked second with 50%, versus fifth at 34% for top performers, indicates a higher focus on risk in HE.” ... Too cautious?

2017 CIO Agenda: A Higher Education Perspective
“There is no such thing as absolute privacy in America.” FBI Director James Comey
Source: CNN.Com, March 9, 2017
DATA BREACHES

The loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

Source: USCode House of Representative

In God we trust. All others, we virus scan.
DATA BREACHES

Source: Information Security
Types of data breaches:
- Financial data
- Authentication compromise
- Personal health information (PHI)
- Personal Identifiable Information (PII)
- Organizational data
- Classified information

Source: Federal Communications Commission (FCC)

“If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees”. — Kahlil Gibran
“Wisdom consists in being able to distinguish among dangers and make a choice of the least harmful”. — Niccolo Machiavelli, The Prince
DATA BREACHES – LAW DATA

Why law firms?
Law firms have large stores of personal data
The data is typically not encrypted or secured
Lawyers are not technologists
Less money spent on security and technology
Handling of hardware and software
Authentication and passwords
Employee theft
Hesitancy to reveal a breach

Source: Inside Counsel, 2016

“The man who trades freedom for security does not deserve nor will he ever receive either”. — Benjamin Franklin
DATA BREACHES & the LAW

ABA Model Rules 1.1, 1.6 Amendment: A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.

Source: American Bar Association

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards”. — Gene Spafford
The Computer Fraud and Abuse Act (CFAA) regulates access to a computer without authorization or exceeds authorized access.


The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) regulate the interception of electronic communications and computer tampering.
DATA BREACHES – History of data breaches in the law:

2008: New York law firm hacked – traced to China

2008: law firm data breach (firm was involved with a suit against China) breached traced to China

2009: FBI warned of increased attempts to hack or breach law firms

2010: King & Spalding targeted in breach attempt originating data in China

2010: Gipson, Hoffman, & Pancione targeted after filing a 2.2 billion dollar software piracy claim against China and others

Source: Law360, 2016
2010: Several Canadian law firms were compromised after a China attack

2011: Wiley Rein, LLP faced attacks from China

2012: 80 of top 100 United States law firms were breached

2015: Ziprick & Cramer were victims of ransomware

2015: FBI names law firms as the 7th highest targets for cybercrime

2016: Cravath, Swaine, & Moore LLP and Weil, Gotshal, & Mange LLP attacked (insider trader secrets)

Panamanian law firm Mossack Fonseca breached exposing 2.6 terabytes of data
The numbers are simply staggering. It is estimated over 900,000,000 records of personally identifiable information (PII) have been stolen in the U.S. over the past few years.

The average cost for a breach is $7 million, costing companies an average of $221 per compromised record.

The number of breach records per typical incident in this year range from 5,125 to 101,520 records.

Source: Network World, 2016
DATA BREACHES - PREVENTION:

+ Password.
+ Encrypt your hardware.
+ Use two level authentication.
  + Anti-virus program.
  + Computer updates.
+ Where is your device?.
  + Backup.
  + Verify.
+ Communicating electronically.

“We will bankrupt ourselves in the vain search for absolute security”. — Dwight D. Eisenhower
Case Study: Duke Law Websites

Perks and Perils of Open Source
CASE STUDY: DUKE LAW WEBSITES

Drupal & WordPress Content Management Systems

Keys to security:
• Track security updates
• Install few modules & plugins
  • Only use supported modules
  • Keep up to date
• Limit number of accounts
• Let others do the heavy lifting
  • Single Sign On when possible
  • eCommerce
Other tips for websites and databases

• Encrypted connections via SSL
• VPN connection
• Limit sensitive information
• “Insert only” permissions
• Dedicated servers for different systems
• Silos
collaboration / workflows
organization / lecture capture
Redundancy / replacement
corruption
Miguel A. Bordo
bordo@law.duke.edu

Wayne Miller
wayne.miller@law.duke.edu

Rochelle Newton
newton@law.duke.edu

Michael Wright
wright@law.duke.edu

Playlist:
https://8tracks.com/jupiter8/media-seaall-2017