Cybersecurity Issues Related to Global Records Management and E-Discovery

Wednesday, October 16, 2013

Part 3 in a 4 part series on Cybersecurity

Presented by:

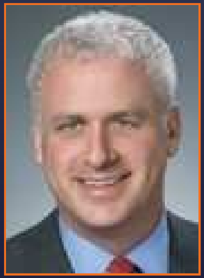
Arthur J. Gallagher & Co.,
Huron Legal and
Pillsbury Winthrop Shaw Pittman

Cybersecurity Issues Related to Global Records Management and E-Discovery

- Presented by:

- Carolyn Southerland, Huron Legal

- Catherine Meyer, Pillsbury Winthrop Shaw Pittman



- David Stanton, Pillsbury Winthrop Shaw Pittman

Today's Agenda

- What is Cyber Security
- Information Governance and Cyber Security
  - Compliance requirements
  - Security issues, risks and solutions
- Cybersecurity in the Context of E-Discovery
- E-Discovery in the Context of a Cyber Event
  - Forensics
  - Discovery challenges
- Questions?

What Is Cyber Security?

Cyber Security Objectives

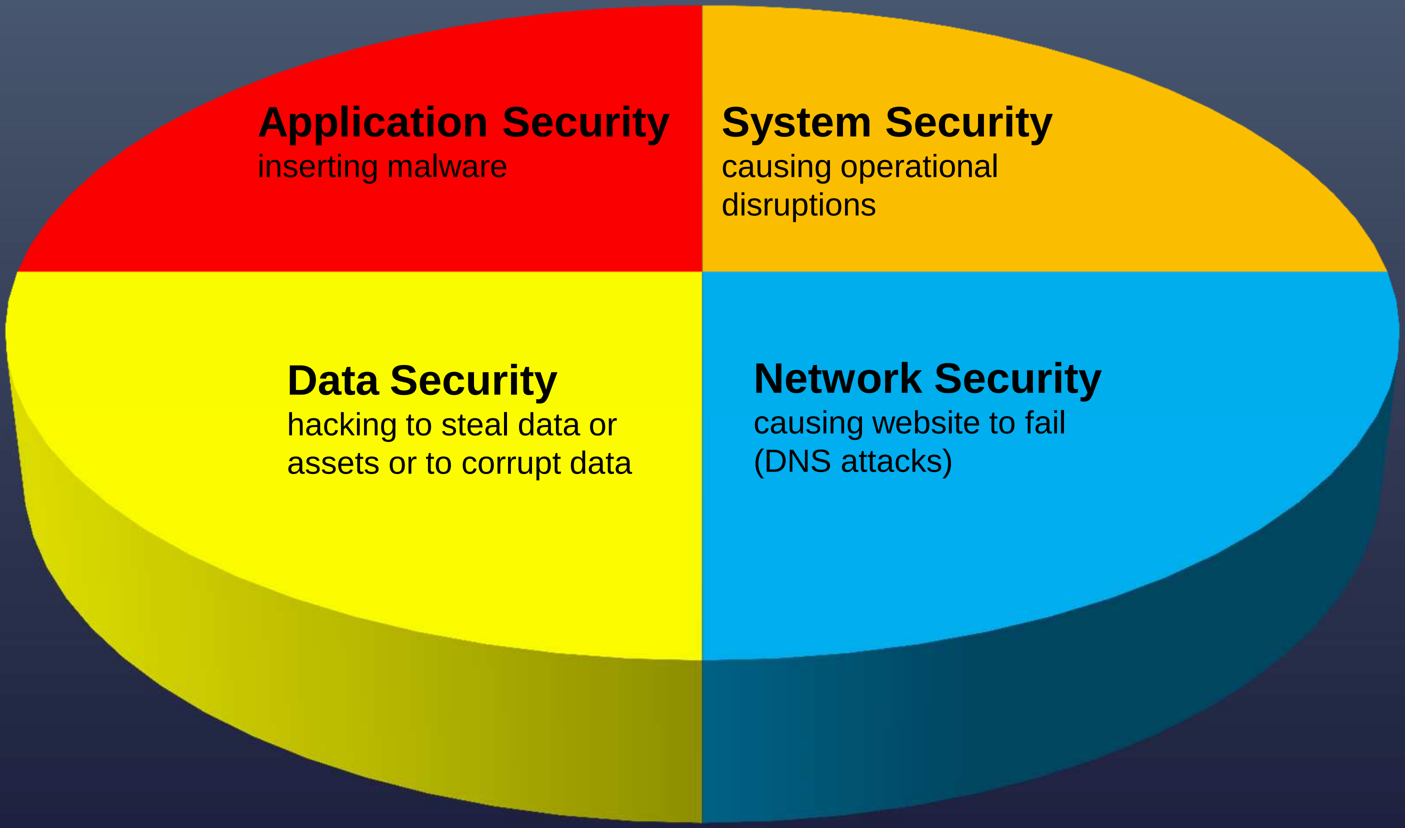
Definition: Cyber security is technology, processes and practices employed “to protect networks, systems, computers, programs and data from attack, damage or unauthorized access.” – *SEC Guidance*

Objectives: Ensure the confidentiality, integrity and availability of information assets

Risks: Costs of inattention, including hard and soft costs, can present an existential threat

Benefits: Cost avoidance, reputation preservation, legal compliance

Cyber Security Attacks



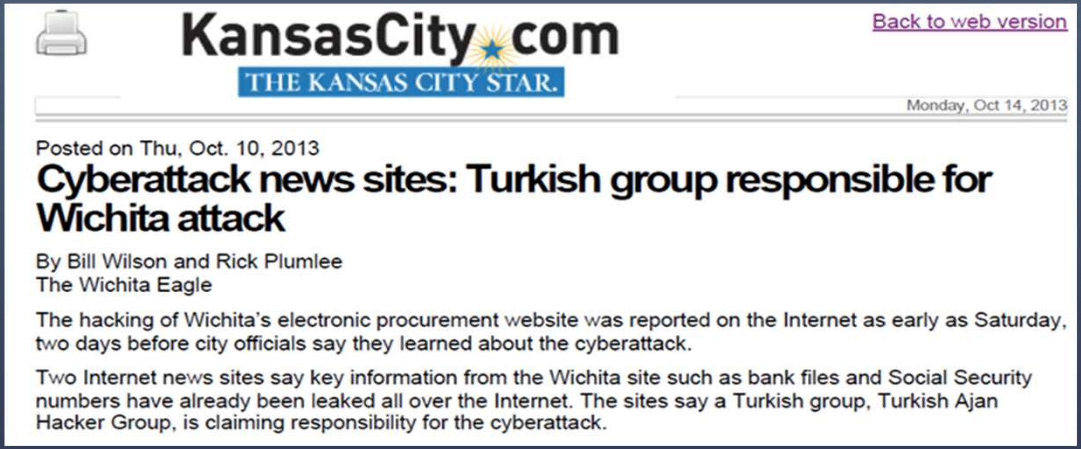
Application Security
inserting malware

System Security
causing operational disruptions

Data Security
hacking to steal data or assets or to corrupt data

Network Security
causing website to fail (DNS attacks)

Why This Stuff Matters



KansasCity.com

THE KANSAS CITY STAR.

Back to web version

Monday, Oct 14, 2013

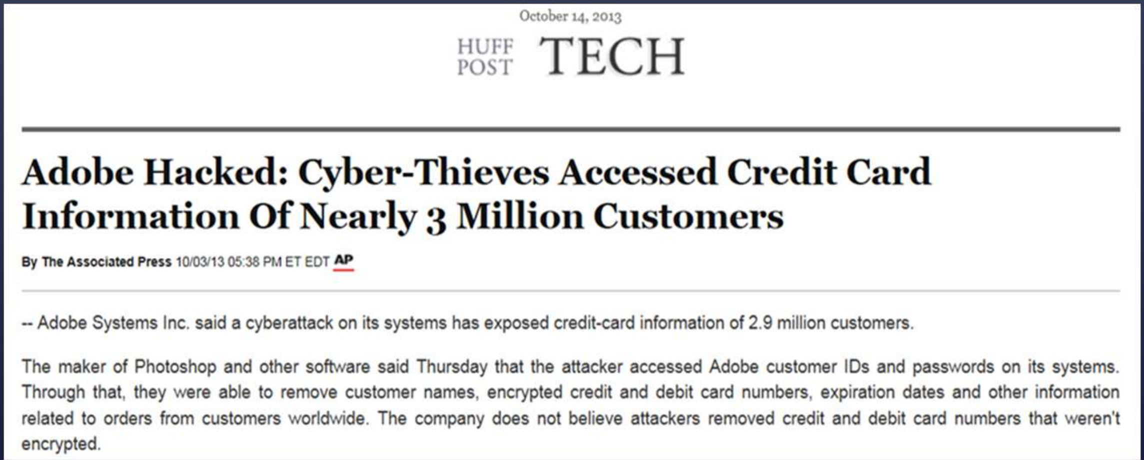
Posted on Thu, Oct. 10, 2013

Cyberattack news sites: Turkish group responsible for Wichita attack

By Bill Wilson and Rick Plumlee
The Wichita Eagle

The hacking of Wichita's electronic procurement website was reported on the Internet as early as Saturday, two days before city officials say they learned about the cyberattack.

Two Internet news sites say key information from the Wichita site such as bank files and Social Security numbers have already been leaked all over the Internet. The sites say a Turkish group, Turkish Ajan Hacker Group, is claiming responsibility for the cyberattack.



October 14, 2013

HUFF POST TECH

Adobe Hacked: Cyber-Thieves Accessed Credit Card Information Of Nearly 3 Million Customers

By The Associated Press 10/03/13 05:38 PM ET EDT AP

-- Adobe Systems Inc. said a cyberattack on its systems has exposed credit-card information of 2.9 million customers.

The maker of Photoshop and other software said Thursday that the attacker accessed Adobe customer IDs and passwords on its systems. Through that, they were able to remove customer names, encrypted credit and debit card numbers, expiration dates and other information related to orders from customers worldwide. The company does not believe attackers removed credit and debit card numbers that weren't encrypted.

Cyber Security Is An Integral Component Of Information Governance

What is Information Governance?

- "Information Governance"
  - The inter-disciplinary framework of policies, procedures and processes designed to optimize business value and to manage costs and risks associated with information.
- IG Processes can include:
  - Retention and Deletion
  - E-Discovery
  - Privacy
  - **Security**
  - Business Continuity / Disaster Recovery
  - Storage Management
  - IT Systems Governance
  - Knowledge Management
  - Document Management
  - Enterprise Search

Key Elements of an Information Governance Program

- People
  - Independent, Inter-Departmental Steering Committee
    - Legal, IT/IS, RIM, Business
  - C-Level Support
  - Geographic Diversity
  - Project Management / Change Management Expertise
- Process
  - Aim toward clearly defined objectives aligned with business strategy of the organization
  - Independence from department silos
- Technology
  - Integration of technical or process improvements with IG objectives.

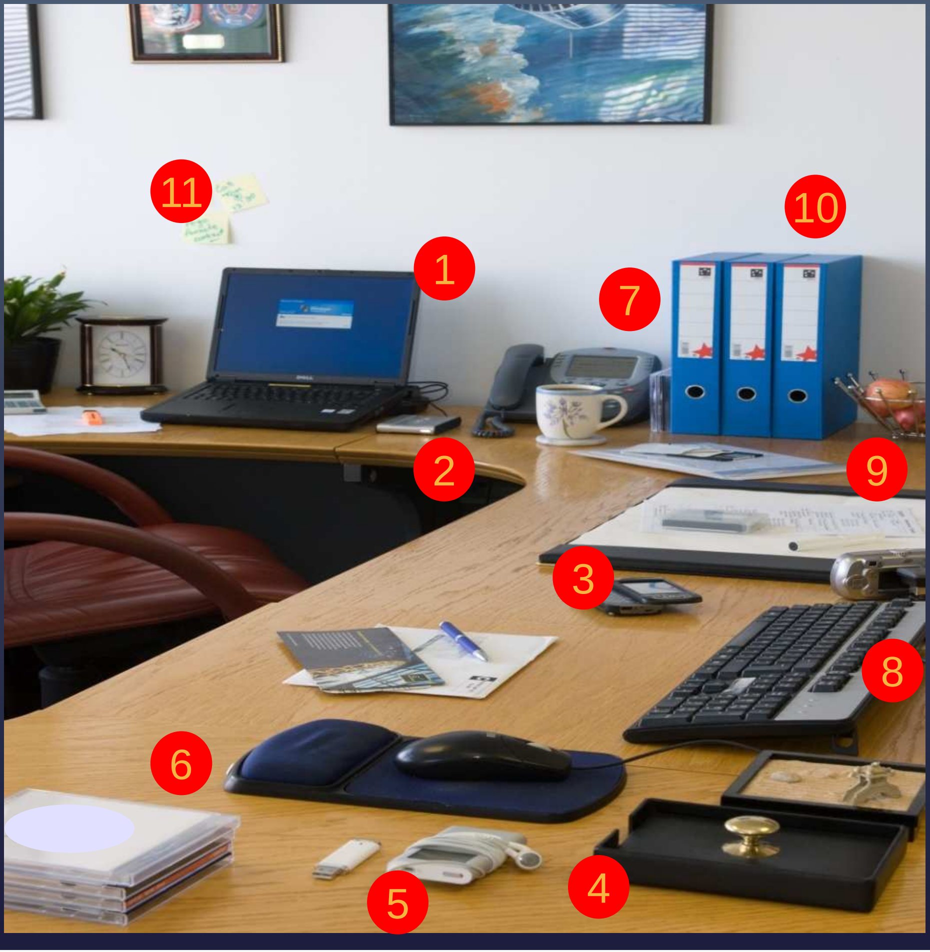
Building the Information Governance Program

- Put a team together / solicit sponsorship / develop ROI
- Gather input and feedback from stakeholders
- Define the strategic objectives of the IG program
- Evaluate existing policies and procedures in light of defined objectives
- Assess existing legal holds and legal hold process
- Target areas of greatest concern
    - Confirm or enhance security measures for confidential/sensitive information
    - Confirm retention of records having permanent value
- Delete what you most readily can
    - Immediate savings
    - Success builds credibility and support
    - Obtain legal guidance and certification as to destruction
    - Consider less expensive alternatives for inactive data

IG Security Assessments and Improvements

- Specify and define business environments and datasets of greatest concern and sensitivity
- Catalogue applications and map information repositories
- Determine policies and practices required by law
  - Consider all jurisdictions
- Design, draft process improvements
- Implementation and training
- Monitor, measure, maintain and update

Security Assessments – Users



1. Laptop computer
2. External HD
3. Smartphone
4. iPod/Tablet
5. USB memory stick
6. DVDs/CDs
7. Telephone/Voicemail
8. Desktop computer
9. Backup tape
10. Paper records
11. Sticky notes

Security Assessments – Enterprise

- Shared Repositories
- CRM Platforms and Other Databases
- Financial Systems
- Applications
- Networks
- Legacy Systems of Acquired Entities
- Third-Party / Cloud Storage

IG and Cybersecurity – Organizational

Effective IG depends upon an organizational approach to information security:

- Enterprise-level decisions about information; balancing of costs and benefits to the organization as a whole
- Involves multiple stakeholders and balances priorities
- Avoids functional and departmental silos
- The goal of IG is to optimize business value and to manage costs and risks associated with information

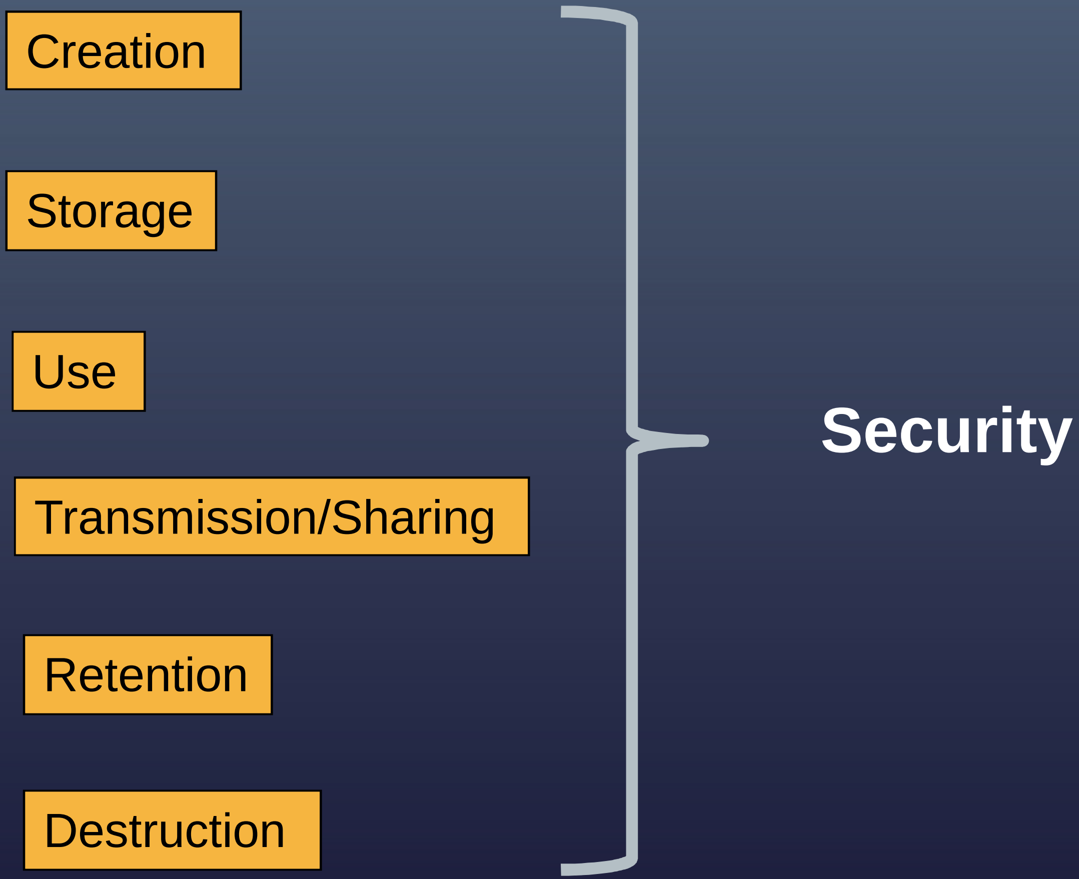
**Security is key to all of these.

IG and Cybersecurity – Functional

IG allows security priorities to be propagated across multiple departments and organizational functions:

- Security – core IG function of protecting confidentiality, integrity and availability of information
- RIM – security issues also addressed during standardization of processes for creating, distributing, storing and destroying ESI
- Privacy – security issues overlap with collection, sharing and destruction of information traceable to an individual
- E-Discovery – security is essential in collecting, processing, reviewing and producing ESI in litigation or investigations

Security Throughout the Information Lifecycle



Creation

Storage

Use

Transmission/Sharing

Retention

Destruction

Security

Security Controls – How Is Data Protected?

- Objectives - Protecting confidentiality, integrity and availability of information.

- Methods - Security Controls
  - Administrative
  - Physical
  - Logical

- Codification - ISO/IEC 27000 series

ISO/IEC 27000 Series on Cybersecurity

- Examples:
  - ISO/IEC 27000 — Information security management systems — Overview and vocabulary [1]
  - ISO/IEC 27001 — Information security management systems — Requirements.
  - ISO/IEC 27002 — Code of practice for information security management
  - ISO/IEC 27003 — Information security management system implementation guidance
  - ISO/IEC 27004 — Information security management — Measurement
  - ISO/IEC 27005 — Information security risk management
  - ISO/IEC 27006 — Requirements for bodies providing audit and certification of security management systems
  - ISO/IEC 27007 — Guidelines for information security management systems auditing
  - ISO/IEC TR 27008 — Guidance for auditors on ISMS controls
  - ISO/IEC 27010 —Information security management for inter-sector and inter-organizational communications
  - ISO/IEC 27011 — Information security management guidelines for telecommunications organizations
  - ISO/IEC 27014 — Information security governance
  - ISO/IEC 27033-1 — Network security overview and concepts
  - ISO/IEC 27033-2 — Guidelines for the design and implementation of network security
  - ISO/IEC 27034 — Guideline for application security

…. several additional guidelines are available under this series

Administrative Security Controls

- Policies and Procedures
- Organizational Structure / Reporting
- Consistency and Proportionality
- Accountability Metrics and Review
- Enforcement and Monitoring

Physical Security Controls

- Access Controls and Permissions
- Personnel and System Surveillance
- Segregation of Systems
- Redundancy and Location
- Separation of Duties

Logical Security Controls

Logical Security Controls

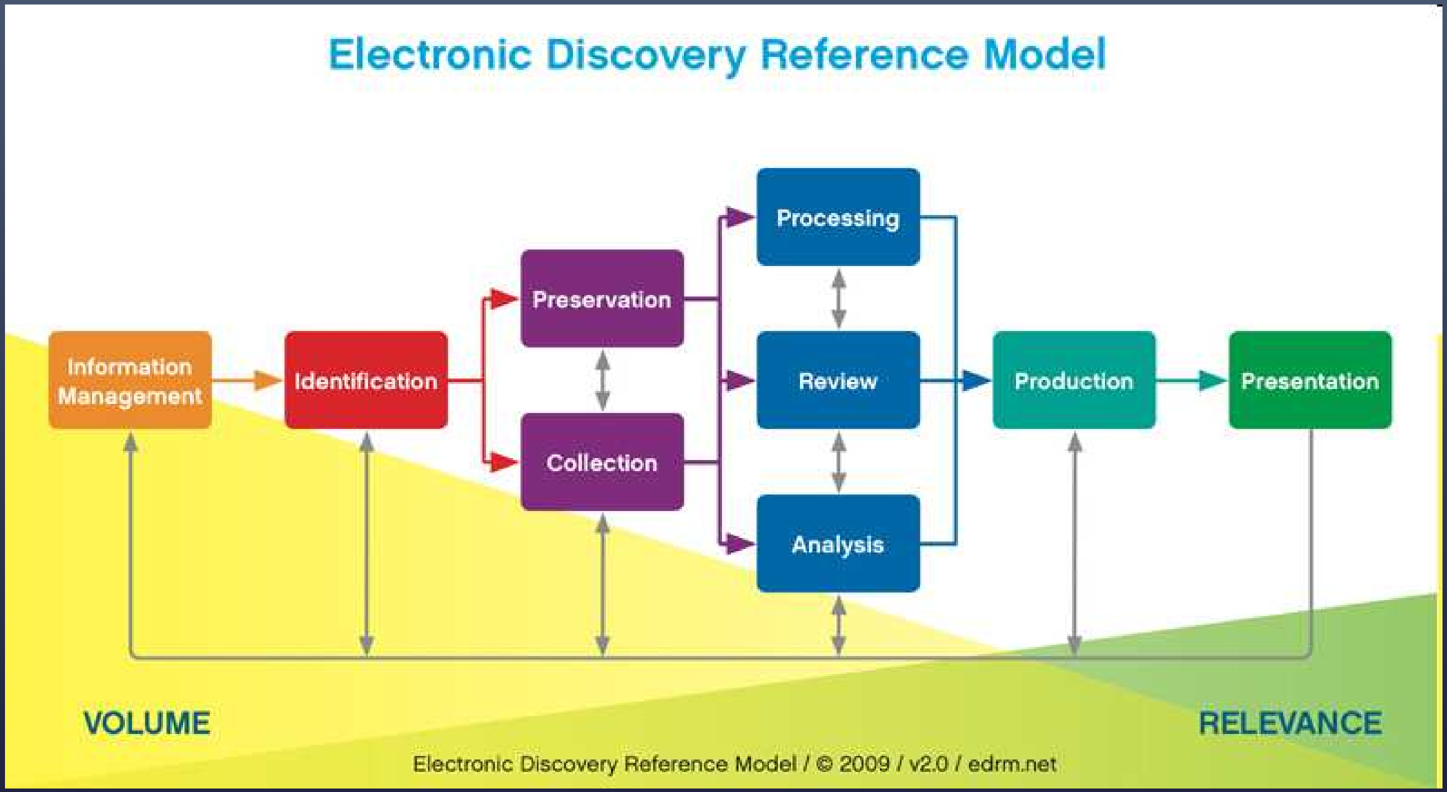
- Tokens
- Passwords
- Two-way authentication
- Biometrics
- Access rights/restrictions
- I/O Monitoring
- Intrusion detection
- “Principle of Least Privilege”

Security Considerations During The E-Discovery Process

E-Discovery Is a Component of Information Governance

- Improving e-discovery practices is one very achievable and practical objective of Information Governance
  - High costs
  - High risks
  - High value of targeted information in lawsuits
- E-discovery in is typically reactive; changing this is key
- The process components of e-discovery are repeatable business processes
- Delegation of e-discovery to trial counsel is inefficient; consider using discovery counsel

E-Discovery and Cybersecurity



Cybersecurity During Collection/Preservation

- Privacy Considerations
  - Personal Devices / BYOD / Comingling
  - Personal and Social Media Accounts
  - HIPPA Issues
  - Global Privacy Regimes
  - Safe Harbor Protections and Cross-Border Transfers
- Security Considerations
  - Qualifications of Forensic Team
  - Access Permissions for Forensics Team
  - Vendor Security Measures and Protections
  - Encryption of Acquired Data

Cybersecurity During Transfers

- Preserving chain of custody
  - Ability to demonstrate authenticity of data is critical even in civil cases
- Delivery and Encryption of Physical Media
- Security of File Transfer Protocol (FTP) site.
- Risks of Peer-to-Peer Sharing and Online Storage
- Secure Email
- Sender/Receiver Roles and Responsibilities
- Transfer Documentation and Tracking
- “Handshake” Validation / Hash Logs

Cybersecurity During Processing/Hosting

- Vendor security
- Global “processing” restrictions / safe harbor compliance
- High value targets
- Concentrated, confidential repositories
- Vendor audits and assessments

"Why do I rob banks? Because that is where the money is!"

Cybersecurity During Review

- Reviewers
  - Reviewer screening and training
  - Policing employees
    - Access permissions
    - Activity Monitoring
  - Restrictions on Downloads / Personal Devices in Review Facility
  - Confidentiality agreements
  - Remote access protocol
- Redactions
  - Ensuring protected information is secured from production
  - Metadata considerations

Cybersecurity During Production

Risks and Benefits During Production

- Agreements and Stipulations
  - Protective Orders
  - Clawbacks
  - Security Agreements
  - Rule 502(d)
- Receiving Party Security
  - Cross-border issues
- Quality Control
  - Redactions
  - Privilege / Privacy
- Anonymization
- Data Tracking and Secure Disposition

N.B. Rule 502(d) does not insulate against inadvertent disclosure of private information

Using the Protective Order to Enhance Security

- Security protocol for receiving parties
- Enforceable requirement to certify secure destruction
- Authentication requirements
- Cross-border issues

E-Discovery During Cyber Events

Preserving the Evidence is KEY

- Assuring data integrity
  - Before and after an event
- Forensic analysis
  - Tracing the event
- Response and restoration

Assuring Data Integrity

- Before the Cyber Event
  - Prepare incident response plan
  - Data Maps
  - Employee training
  - Testing
  - Documentation

- After the Cyber Event
  - Identify intrusion/breach and compromised data
  - Secure and preserve all relevant evidence on all target systems
  - Secure and preserve all relevant logs and ephemeral evidence
  - Document investigation, response and decision-making.
  - Maintain chain-of-custody

Key Cyber Event Evidence Can Be Ephemeral

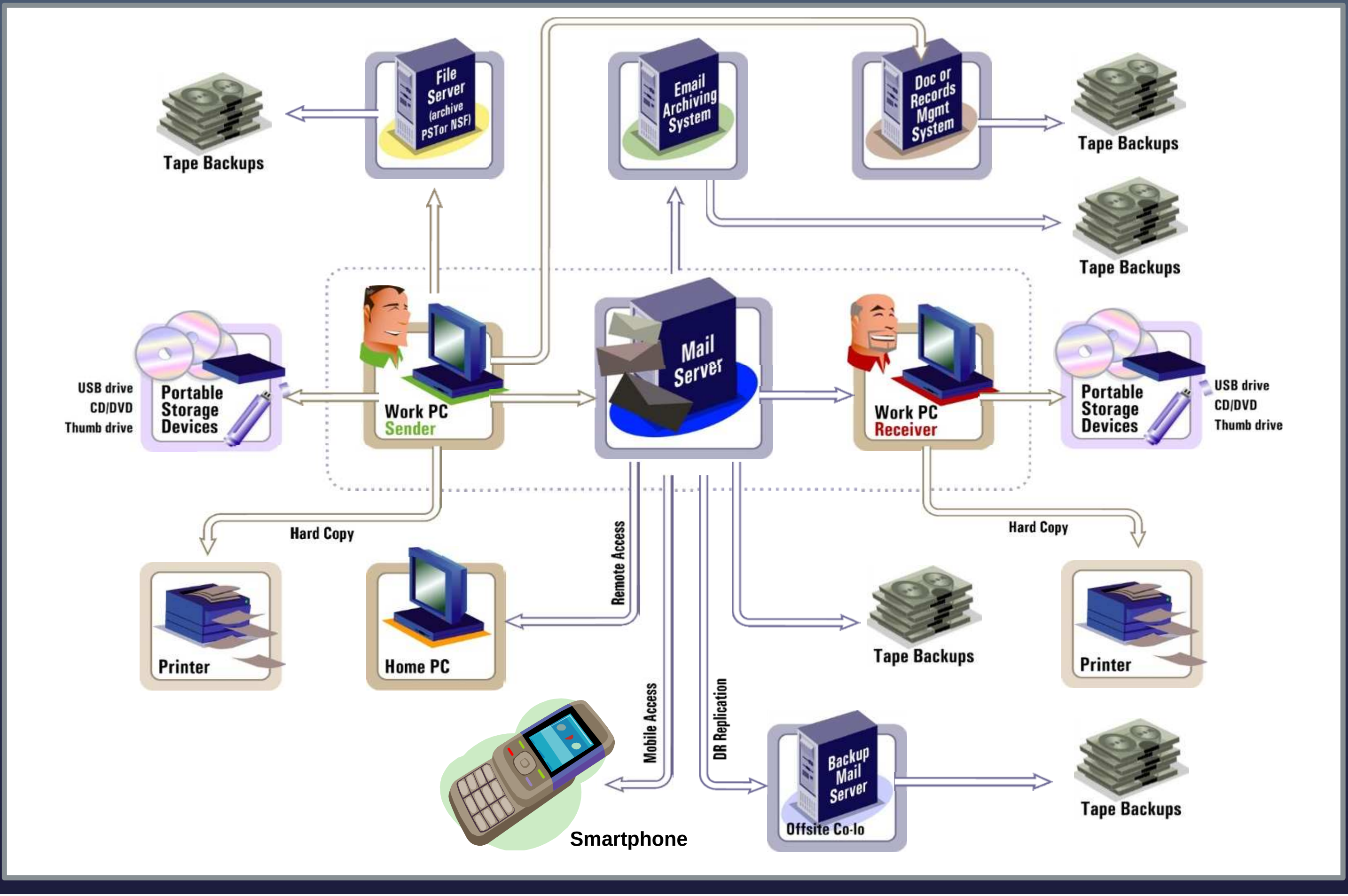
Forensic Analysis – Where is Data at Risk?

“The Hard Drive”

Data lives in:

- PC’s
- Smart Phones
- External Devices
- Servers
- iPods/iPads
- Copy Machines
- Printers
- Cloud Storage

Forensic Analysis – Where is Email At Risk?

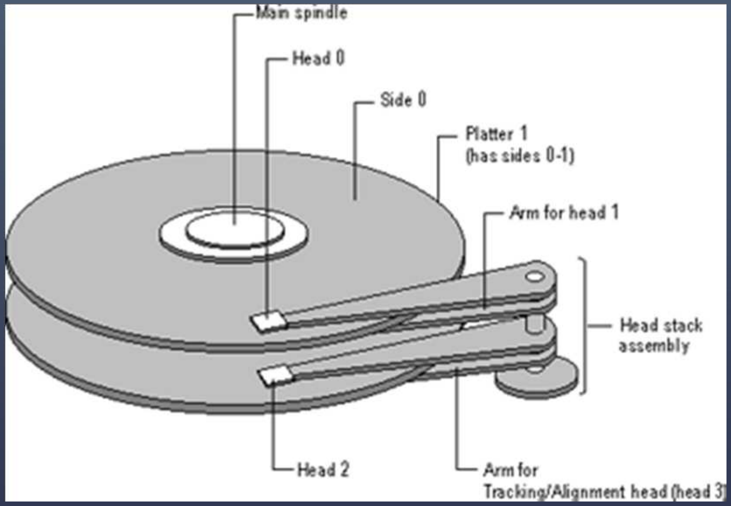


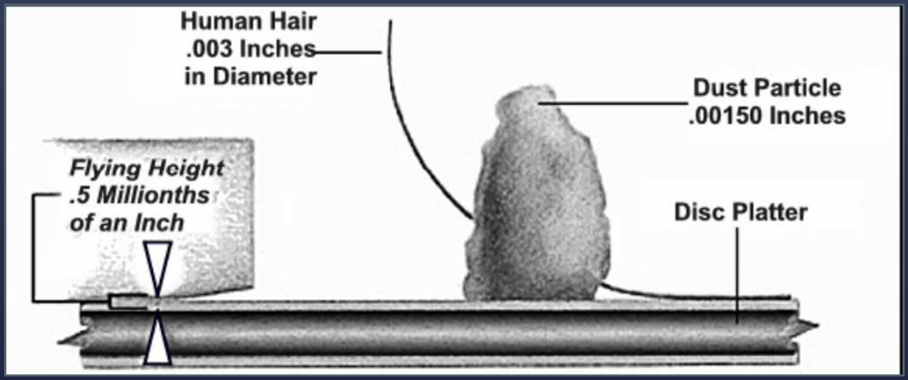
Forensic Analysis – Potential Contents of a Hard Drive

- A forensic examination can find:
  - Hard drive format date, time zone settings, profile creation and last login, last shutdown time for Windows and last activity date/time
  - Browsing history (included in unallocated space)
  - Preferred locations for storage, email clients used
  - External drives (serial number) plugged into the device
  - CDs, DVDs burned
  - Files accessed at specific dates/times
  - Backup files for the computer as well as devices such as smartphones
  - Recover deleted email/webmail from unallocated space
  - Chat sessions
  - Use of cloud storage
  - LNK files—Windows shortcuts of recently opened documents shows MAC dates and where stored
  - Shell bags—shows what folders were browsed on network, hard drive and external devices

Forensic Analysis – How is Data Stored?

Visualize a HD as an old LP turntable – but much more delicate.

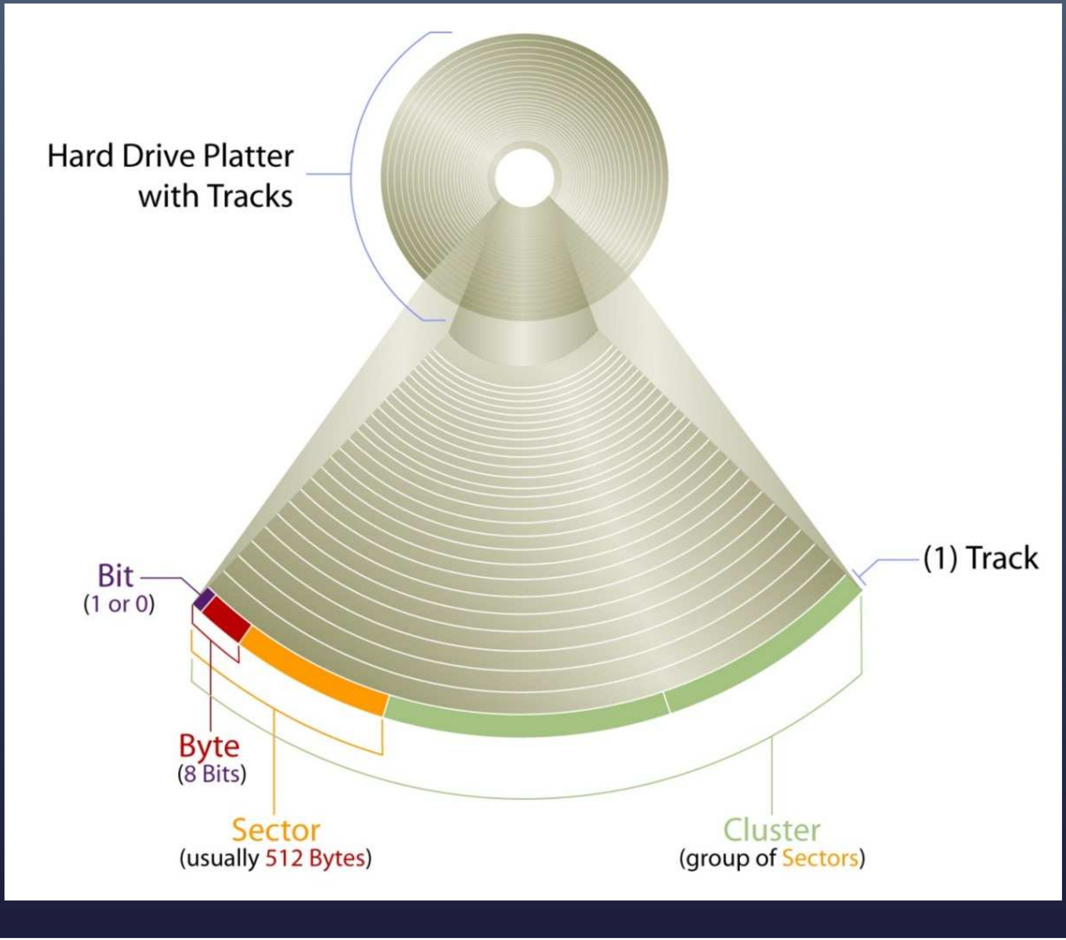




An executive at Seagate once made the analogy that a HD operation is:

"Equivalent to *an F-16 fighter jet flying at 813 times the speed of sound and one-sixty second of an inch off the ground while counting every blade of grass as it goes!"*

Forensic Analysis – Peeling the Onion



Response and Restoration – Detection and Tracking

Detection – determine what took place

- Timing Challenges: Discovering and tracing event; pulling team together

The first 24 hours is critical.

- Forensic Challenges: preserving the evidence before it is overwritten or lost

- Logistical Challenges: tracing compromised data back to affected individuals

Response and Restoration – Notifications

- Legal / Factual Analysis
  - Residence of affected individuals
  - Jurisdictional considerations
- Compliance with notification content requirements
- Logistics
  - Distribution of notice
  - Call center
  - Additional measures
    - Credit monitoring
    - ID theft insurance

Response and Restoration – Restoring Security

- Identifying security flaws
- Assessing and selecting enhancements
- Training, education and implementation
- Validating and testing enhanced security
- Preserving evidence of remedial measures adopted
- Post-Mortem / After-Action Review

For those attorneys participating by teleconference, please note the following code on your attendance sheet:

CLE VERIFICATION CODE:

2013-A005

Upcoming, Final Webinar in this Series

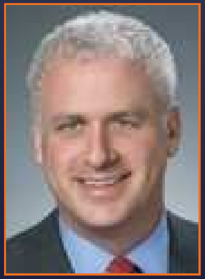
- 10/30: Cybersecurity Risk Transfer
  - Joe DePaul – Arthur J. Gallagher & Co.
  - Laurey Harris – Huron Legal
  - Rene Siemens – Pillsbury Winthrop Shaw Pittman

- Please complete our Cybsecurity survey: http://pillsburylaw.draft-cybersecurity-survey.sgizmo.com/s3/

Contact Details

Carolyn Southerland– Managing Director
Huron Legal
csoutherland@huronconsultinggroup.com
2929 Allen Parkway, Suite 2700
Houston, Tx. 77019
Ph 713-222-5940

Catherine Meyer – Counsel
Pillsbury Winthrop Shaw Pittman LLP
catherine.meyer@pillsburylaw.com
725 South Figueroa Street - Suite 2800
Los Angeles, CA 90017-5406
Ph +1.213.488.7362



David Stanton – Partner
Pillsbury Winthrop Shaw Pittman LLP
david.stanton@pillsburylaw.com
725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Ph +1. 213.488.7271