

Emory Office of Information Technology (OIT)

Security Review Process in Human Subject Research Studies

Mike (Mo) Davidson

Associate Director, Information Security Architecture

Topics:

Part 1

- **Cyber Threat Landscape**
- **Examples of Sensitive Data**
- **Why Emory Cares About Data Security**
- **Preventing Data Breaches**

Part 2

- **Security Review Process in Human Subject Research Studies**

Topics:

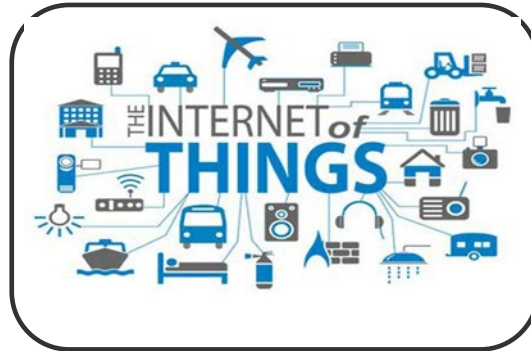
Part 1

Cybersecurity Background Information

Cyber Threat Landscape



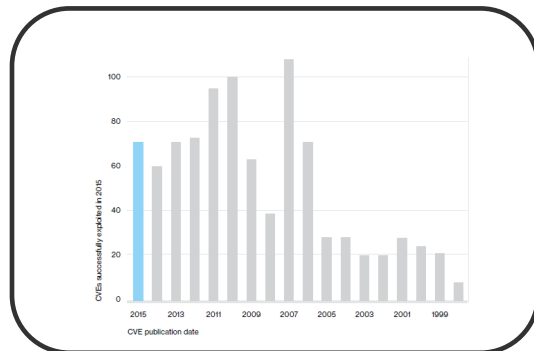
Sophisticated and Motivated Actors



Exploitation of the Internet of Things



Rise of Advanced Ransomware Threats



Attacks Continue to Target Old Vulnerabilities

1.1 Billion
Records Breached

In U.S. Since 2005

16.7 Million
Identity Theft Victims
per Year

\$16.8 Billion Stolen

Cyber Threat Landscape



Phishers/Spammers



Malware



Financial Fraudsters



Nation States

Primary Threat Actors

1000
Unique Attackers

Identified and Quarantined
Every Month

235 Million
Malicious
Communications

Blocked Every Month

**4 Major Incidents &
315 Minor Incidents**

Last 12 Months

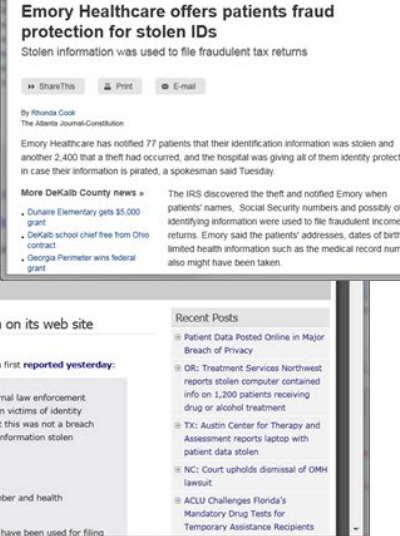
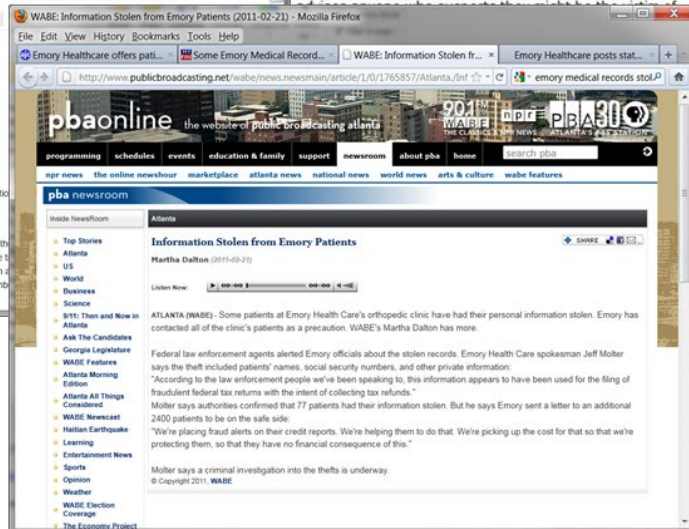
Examples of Sensitive Data

- Identifiable Electronic Protected Health Information (ePHI).
- Individually Identifiable Health Information (IIHI)
- Human subject research data containing Personally Identifiable Information (PII)
- Combinations of Personally Identifiable Information that could readily be used for identity theft:
 - Social security numbers, when combined with any form of the corresponding name
 - Driver's license numbers, when combined with any form of the corresponding name
- Non-directory student information
- Passwords
- Credit/Debit card numbers
- Financial records that could lead to identity theft or fraud
- Any data deemed to be restricted by the data owner
- Any data that, if acquired by unauthorized individuals would require notification of affected parties
- Any data that Emory is legally, contractually, or ethically obligated to encrypt

Why Emory Cares About Data Security

- It's the law (HIPAA, FERPA, PCI, etc.)
- Financial Impact
 - Forensic analysis \$5K to \$15K per system
 - Notifying affected parties \$1 per individual
 - Credit monitoring \$6 per individual
 - Fines and Penalties Can easily exceed \$1,000,000
 - Lawsuits Unlimited
 - Incident costs are allocated to the department where the breach occurred
- Damage to Institutional Reputation
 - Negatively affects recruitment of faculty and students
 - Negatively affects fundraising
 - Could negatively affect ability to get grants
 - Negatively affects the willingness of other institution to share sensitive data
- Breach of computer security / confidentiality identified as one of Emory's top risks during every Enterprise Risk Management assessment

Why Emory Cares About Data Security



Why You Should Care About Data Security

- **Legal Consequences** – HIPAA contains criminal penalties for violating privacy requirements. Up to \$250,000 fine and/or up to 10 years in jail.
- **Identity theft and financial fraud** – a compromised account could give an attacker access to your own Personally Identifiable Information.
- **Personal reputation** – breach notification letters are signed by leadership within the business unit where the breach occurs.
- **Data loss or corruption** – research data could easily be modified, destroyed or corrupted.

Preventing Data Breaches

- Ask your local IT support for help securing sensitive data
- Eliminate or minimize the use of SSN (and other sensitive data)
 - Use substitute identifiers
 - Truncate or Mask
 - Change business practices
- Move sensitive data to secure central storage solutions
 - Don't store sensitive data on workstations, laptops, USB drives, smartphones, etc.



Preventing Data Breaches

- Tightly control who can access or modify sensitive data
- Ensure data transfer agreements are in place before transferring data to other institutions
- Delete old files that are no longer needed
- Encrypt Devices and Media
 - Laptops
 - Workstations that must store sensitive data
 - Servers
 - Removable media



Manning

Assange



Preventing Data Breaches

- Physically securing any systems or media containing sensitive information
- Never leave unsecured devices or paper containing sensitive information unattended
 - Especially in your car
- Choose a strong password, never share it with anyone else, and change it periodically



Preventing Data Breaches

- Log out, disconnect, or lock your workstation when you step away
- Backup your data to secure central storage solutions
- Shred, erase, or otherwise destroy paper records or electronic media containing sensitive data before disposing of them



Preventing Data Breaches

- Only send sensitive information via email if it is encrypted
- Don't store sensitive data on unapproved external services like Google Docs, DropBox, Carbonite, IDrive, iCloud, etc.
- Ensure that appropriate audit logging is in place for sensitive data regardless of its location



Preventing Data Breaches

- Ensure that audit logs are regularly reviewed
- Ensure that your systems stay current on all patches and anti-virus updates
- Understand your obligations
 - Regulations
 - Policies (policies.emory.edu)
 - Grant and Contract requirements
- **NSPM-33**: National Security Presidential Memorandum 33
 - National Security Strategy for United States Government-Supported Research and Development



LAWS & POLICIES



Preventing Data Breaches

- Complete all required security and privacy training
 - HIPAA Modules
 - NSPM-33 required cybersecurity training
 - Foreign Travel Requirements (forthcoming)
- Use applications that have already been vetted for use with sensitive data
 - Search for “OIT Reviewed Apps” on the Emory home page
 - [https://it.emory.edu/security/protecting-data/software for research.html](https://it.emory.edu/security/protecting-data/software%20for%20research.html)
- Request a security scan or security review of your systems via ServiceNow



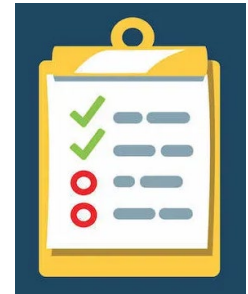
Topics:

Part 2

Security Review Process in Human Subject Research Studies

Security Review Process in Human Subject Research Studies

- In addition to the IRB review process, a security review may be conducted by the Office of Information Technology (OIT) Information Security Architecture Team
- An OIT Security Review could be needed:
 - If a study is using PHI
 - If a study is using IIHI
 - If a study is handling sensitive data which may need some additional review to ensure the handling / storing / transmission is secure



Security Review Process in Human Subject Research Studies

- Additionally, until a system or service has been vetted and added to the Approved for Research using Identifiable Information list, a security review will need to be conducted
- Finally, if the IRB identifies that there are any other parameters for a study that may warrant a closer look, the IRB may require an OIT Security Review be performed



Security Review Process in Human Subject Research Studies

- Documentation which may be requested in the course of a security review for IT components of an IRB study
 - Diagram of how the IT component will be used (architecture diagram)
 - Data flow diagram
 - Security questionnaires
 - Security info or attestations from IT vendors and medical device manufacturers
 - DUA / DTA / BAA
 - Evidence of encryption (in transit, at rest)
 - The study protocol



Security Review Process in Human Subject Research Studies

- Timeline / duration of a security review
- Depends on several factors but primarily:
 - Responsiveness from study team members / vendors for requested information
 - Accuracy of information provided to Security
 - Workload (in the request queue) for other security reviews being requested / worked on
- IRB approval will be pending until the completion of the security review



Security Review Process in Human Subject Research Studies

- Typical order of activities for a security review
 - Security review request submitted via ServiceNow
 - Initial review by Security; request(s) for additional info
 - Q&A on aspects of IT solution / passed to vendor(s)
 - Clarification on diagrams / documents / usage
 - Clarification on data classifications (PHI vs IIHI)
 - Data flow identified / clarified (all Emory / 3rd party)
 - Potential information security risks identified in report
 - Preliminary Security Review Assessment Report shared
 - Risks either remediated / mitigated / accepted
 - Accepted risks signed off within document
 - Completed Security Review Assessment Report shared



Security Review Process in Human Subject Research Studies

The following are screenshots of
an example of an OIT
Security Review
Assessment Report



Risk Project Name:	Request Number:	Prepared by:	Date:
Disneyland Main Street U.S.A. public access	REQ # G00F33	Woody the Sheriff	July 17,1955
Division	Business Unit:	Responsible Party	Requestor
Disneyland – Anaheim, California	Main Street U.S.A.	Buzz Lightyear	Mickey Mouse

1. Risk level definitions, mitigation timelines, and risk acceptance criteria

Risk Level	Description	Mitigation Timeline	Risk Acceptance Criteria
<i>Critical</i>	The Security Review has determined that the current level of risk associated with the finding is critical (severe) in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 30 days if system is live. If the system is not yet live, the risk must be fully remediated or mitigated to an acceptable level before the system goes live or is connected to a production Emory network.	Critical risks can only be accepted by Responsible Party such as VP/Dean level leadership. Relevant Executive VP level leadership must be informed that the risk is being accepted by the VP/Dean.
<i>High</i>	The Security Review has determined that the current level of risk associated with the finding is high (substantial) in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 60 days if the system is live. If the system is not yet live, the risk must be fully remediated or mitigated to an acceptable level before the system goes live or is connected to a production Emory network.	High risks can be accepted by Responsible Party such as Director/Chair level leadership. VP/Dean level leadership must be informed that the risk is being accepted by the Director/Chair.
<i>Medium</i>	The Security Review has determined that the current level of risk associated with the finding is medium (moderate) in its current state.	The risk must be fully remediated or mitigated to an acceptable level within 90 days.	Medium risks may be accepted by Responsible Party such as Director/Chair level leadership.
<i>Low</i>	The Security Review has determined that the current level of risk associated with the finding is low (tolerable) in its current state.	Risk remediation is recommended, but not required at present.	Low risks do not need to be explicitly accepted.

2. Description of requested application/service

The Disneyland theme park in Anaheim, California permits the public to access Main Street U.S.A. The current residents of Main Street U.S.A. have requested a Security Review of that public access to their street. The primary residents on Main Street are Mickey Mouse, Minnie Mouse, Donald Duck, Daisy Duck, Goofy, Pluto – and at the far end of Main Street: Cinderella.

3. Security Review Triage

The following questions will determine if a security review is required by OIT-Enterprise Information Security. The triage process quickly identifies projects that do not pose material risks to the institution. A security review is required if any of the responses to the “Answer” column match the adjacent “Review Needed” column.

Triage Questions	Answer	Review Needed
Does solution process, transmit, or store restricted or confidential data? See Emory Disk Encryption Policy for definitions.	Yes	Yes
Does vendor provided solution connect to any on-premise Emory systems and data feeds (e.g. HL-7, FTP/SFTP, API calls, VPN, etc.)? Shibboleth/Emory NetID are not in scope for this question. If solution is not hosted, administered, or remotely supported by vendor, select “no.”	Yes	Yes
Does vendor provided solution integrate with Emory NetID authentication (e.g. Shibboleth)? If solution is not hosted, administered, or remotely supported by vendor, select “yes.”	No	No
Does on-premise hosted solution have network connectivity? If solution is not hosted on-premise, select “no.”	Yes	Yes
<p><u>Triage Result:</u></p> <p>Based on the responses to the Triage Questions, the project associated with this request requires a security review. The possible risks associated with this request are significant enough to merit further review.</p>		

4. Security Review

Data Type: Personally Identifiable Information (PII) for residents of Main Street U.S.A. in Disneyland

Solution Location (which core for on-prem): Disneyland theme park, Anaheim, CA

Support Matrix (who supports the app, hardware, software): Disney support the theme park, Disney cartoons support their houses

Endpoint (how users accesses solution): Public access to Main Street U.S.A. is through the Disney front gate

Audit Logs: Yes, Disneyland keeps track of the visitors to their theme parks

Device Information: OS, encryption, etc.:

- Disney encrypts the data for the public visitors
- However, Disney cartoon characters are not encrypted and their PII data is fully available on Main Street U.S.A.

Shibboleth Integration? If not, How?: No, Disney does not use Shibboleth for authentication

Number of Users: Millions every year

Issues found and were they resolved?: Yes issues found; no – not yet resolved

Have we reviewed this service before?: No, we have not reviewed Disneyland before



5. Risk Assessment Findings

THIS SECTION IS TO BE COMPLETED BY THE ENTERPRISE INFORMATION SECURITY TEAM

Enterprise Security Team member completes the section based on the submitted documentation and then sends the document to a Requestor/Responsible Party.

Risk Assessment Findings					
Item Number	Risk Category	Findings	Findings Description	Recommended Remediation	Risk Level
R-01	Data Protection	The public is allowed access to Main Street U.S.A. in Disneyland with <u>all</u> of the Disney characters PII data available / unencrypted	Public access has been available to Main Street U.S.A. but the PII data for the Disney cartoon characters has been left unencrypted by Disney.	Disneyland should encrypt the PII data for each of the cartoon characters who live on Main Street U.S.A.	High
		# No more risks found #			

6. Risk Mitigation Results

THIS SECTION IS TO BE COMPLETED BY THE REQUESTOR

This section is to be completed by a person who requested the review – Requestor along with the Responsible Party and then sent back to a member of the Enterprise Security Team.

Each of the risks documented in this section must be addressed in a manner that is consistent with the guidance provided in the table in section 1 and should be based on its associated risk level

Risk Mitigation Results				
Item Number	Risk Description	Remediation approach	Estimated Completion Date	Name of Risk Owner(s)
R-01	There needs to be assurance that Disneyland will encrypt the PII for the Disney cartoon characters who live on Main Street U.S.A.	Disney agrees to encrypt the PII data for all Disney cartoon characters who live on Main Street U.S.A. in Disneyland, California.	3 days before Infinity and Beyond	Buzz Lightyear (Representing Disney animators)

7. Residual Risk

THIS SECTION IS TO BE COMPLETED BY THE ENTERPRISE INFORMATION SECURITY TEAM:

The member of the Enterprise Security Team reviews the mitigation efforts performed and classifies any residual risks in the table below and sends the update document to the Requestor/Responsible Party.

If any risk assessment finding is not fully remediated, any residual risk associated with the finding must be formally accepted by a Responsible Party -an organizational leader with sufficient authority to accept the risk given its residual risk level. Please refer to the table in section 1 in this document to identify the appropriate leader to fulfill this role.

Only one leader should fulfill the role of Responsible Party. The leader who is responsible for the highest residual risk(s) should sign off on all risks.

Item Number	Risk Description	Residual Risk	Residual Risk Level	Residual Risk Action (Remediated, In Progress, or Accepted)	Risk Owner(s)
R-01	There needs to be assurance that Disneyland will encrypt the PII for the Disney cartoon characters who live on Main Street U.S.A.	<i>Disney animators agree to encrypt the Disney cartoon characters PII data.</i>	<i>Low</i>	<i>In Progress</i>	Buzz Lightyear (Representing Disney animators)

Security Risk Assessment

8. Residual Risk

THIS SECTION IS TO BE COMPLETED BY RESPONSIBLE PARTY

By signing below, I fully understand and acknowledge the risk(s) identified. Therefore, I agree to accept full responsibility and accountability for all residual risk associated with the findings noted within this document, for which I have been identified as the Responsible Party. In addition, I agree to continue to oversee the remediation of all risk(s) that has remediation plans developed as stated in the table above.

risk remediation in progress

Responsible Party

Date

Security Review Process in Human Subject Research Studies

- How to request an OIT Security Review

- Our ServiceNow Request Form direct link:

- https://emory.service-now.com/sp?id=sc_cat_item&sys_id=13b886852b70f100427d2ca119da1536



- Our ServiceNow Request Form browser navigation:
 - <https://help.emory.edu>
 - Click on “Request Something”
 - From the left-hand menu, click on “Security Management”
 - Center-section of the page, click on “Security Review Process Intake Document”

Security Review Process in Human Subject Research Studies

- A final note about security reviews:
- A Security Review “Bypass”
 - What is it?
 - When could it come into play?



Questions

