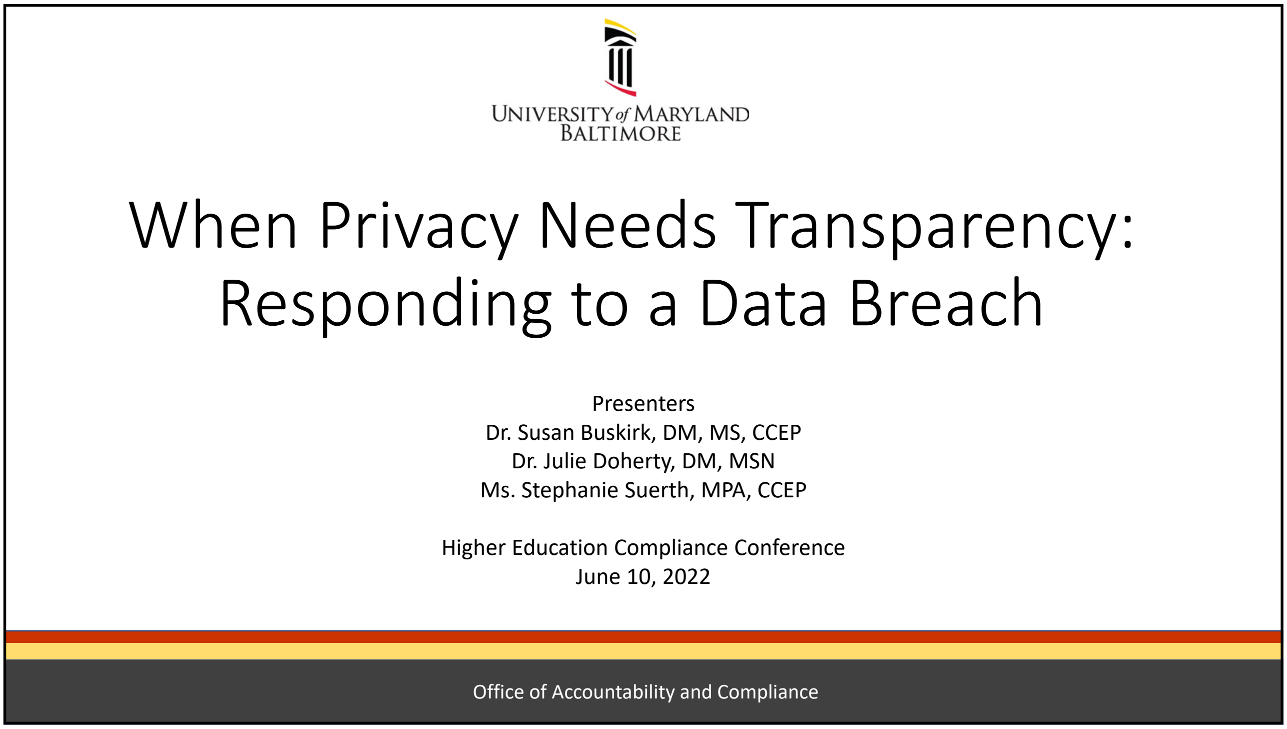


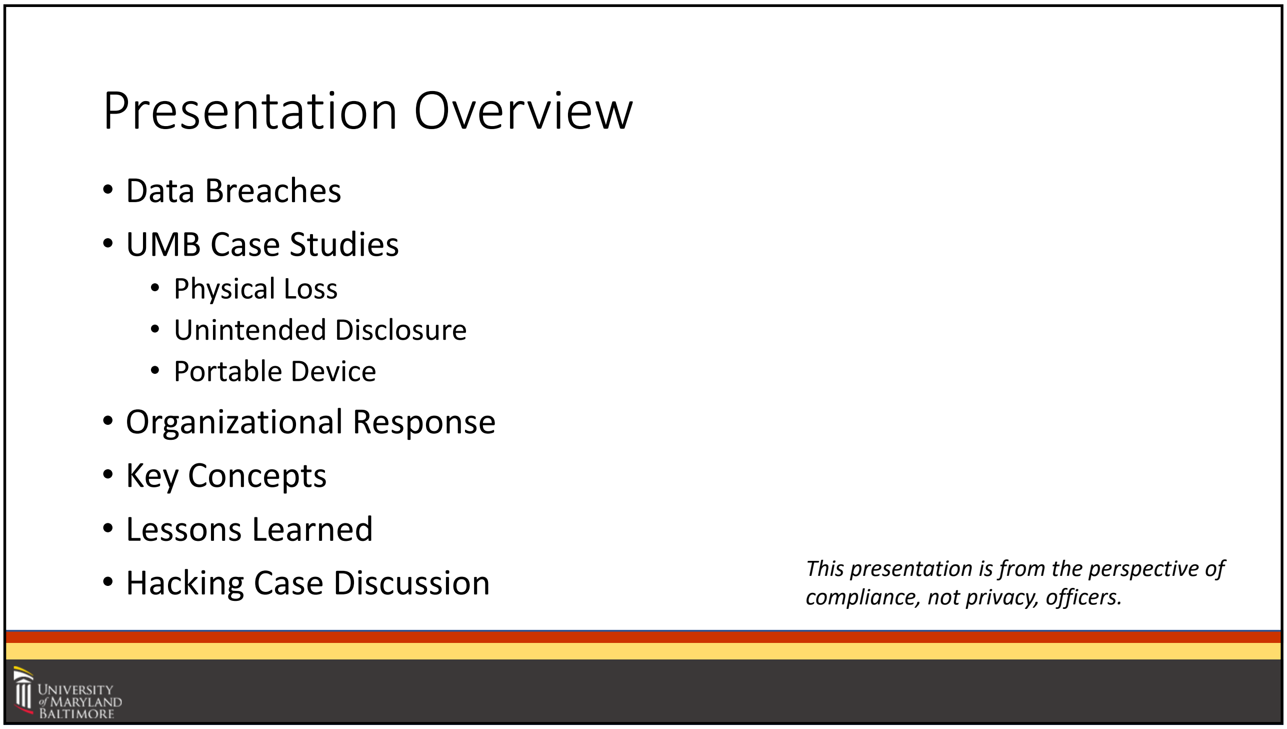
When Privacy Needs Transparency: Responding to a Data Breach

Presenters
Dr. Susan Buskirk, DM, MS, CCEP
Dr. Julie Doherty, DM, MSN
Ms. Stephanie Suerth, MPA, CCEP

Higher Education Compliance Conference
June 10, 2022

Office of Accountability and Compliance

1



Presentation Overview

- Data Breaches
- UMB Case Studies
  - Physical Loss
  - Unintended Disclosure
  - Portable Device
- Organizational Response
- Key Concepts
- Lessons Learned
- Hacking Case Discussion

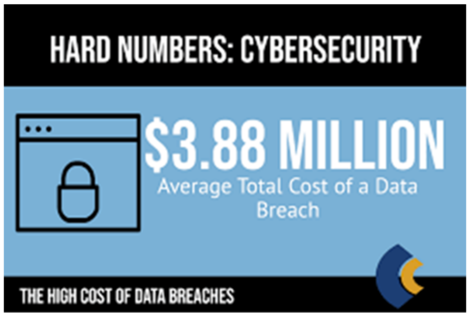
This presentation is from the perspective of compliance, not privacy, officers.

2

Risky Business – Threats to Data

The risks to data are as varied as the information you are protecting:

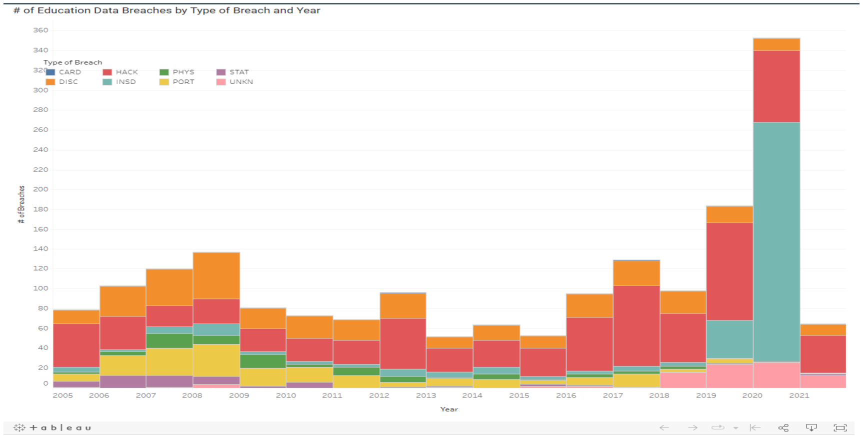
- Physical Theft
- Ransomware
- Phishing
    - Spear-phishing
- Malicious Insiders
- Human Error
- Malware
- Social Engineering Scams
- Water holing


HARD NUMBERS: CYBERSECURITY
$3.88 MILLION
Average Total Cost of a Data Breach
THE HIGH COST OF DATA BREACHES

Retrieved from: https://www.collegeconsensus.com/resources/university-data-breaches/

3

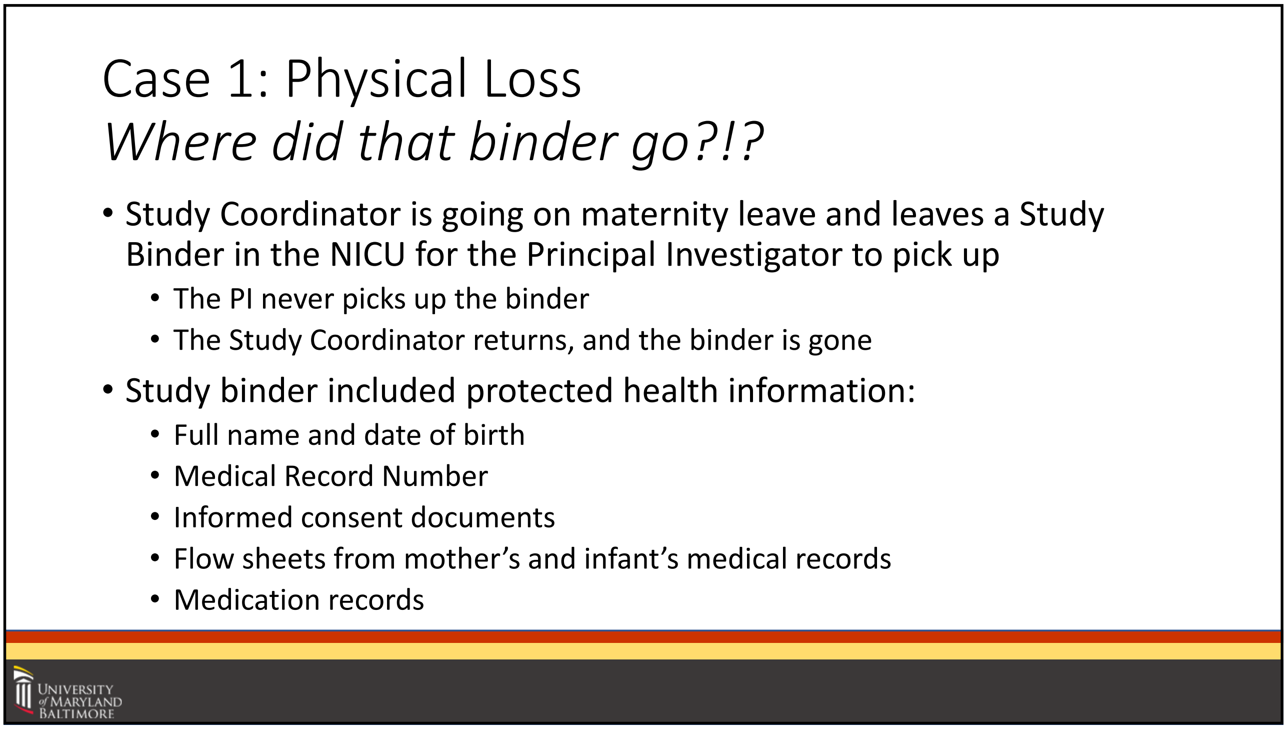
Common Data Breach Types in Education



Breach definitions: Card (debit/credit card not via hacking, e.g. skimming), Hack (outside party or malware), Insd (insider–employee, third-party, or customer), Phys (paper documents), Port (portable devices, e.g. laptops, memory sticks, and hard drives), Stat (stationary computer), Disc (unintended disclosure, e.g. sensitive information posted publicly), Unkn (unknown).

Retrieved from: https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/

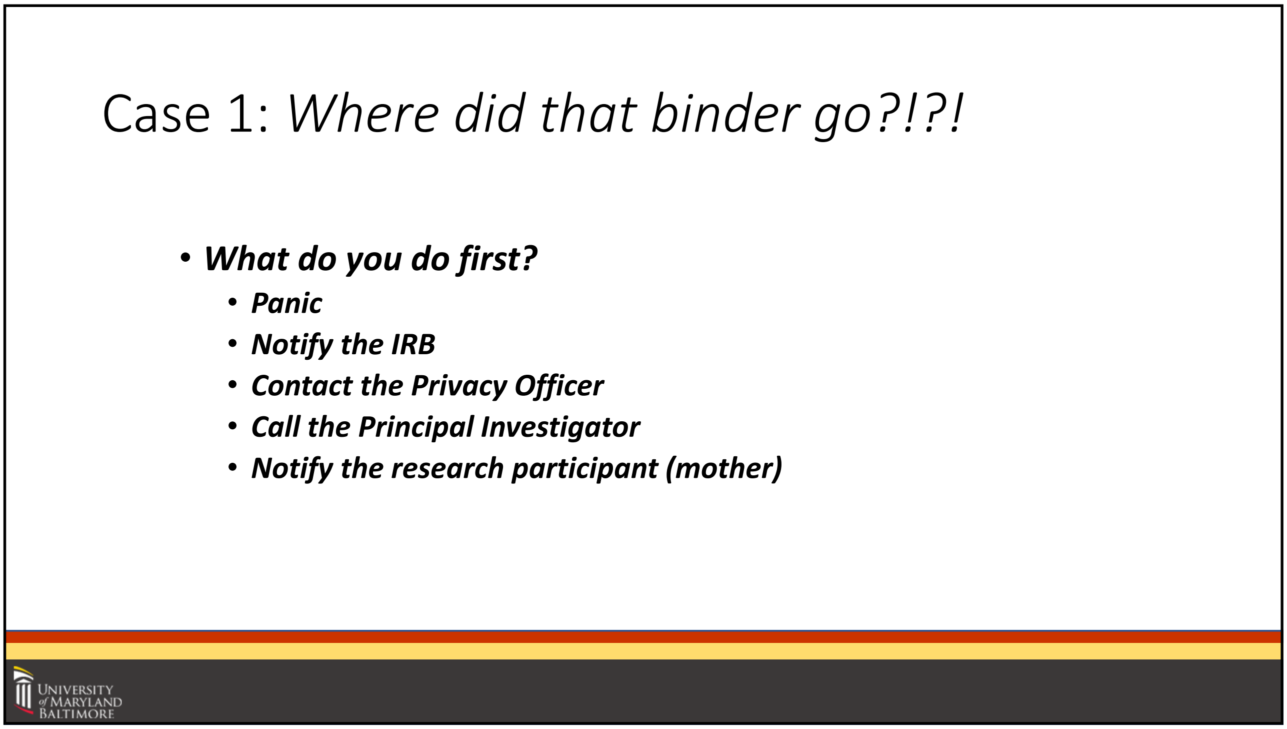
4



Case 1: Physical Loss
Where did that binder go?!?

- Study Coordinator is going on maternity leave and leaves a Study Binder in the NICU for the Principal Investigator to pick up
  - The PI never picks up the binder
  - The Study Coordinator returns, and the binder is gone
- Study binder included protected health information:
  - Full name and date of birth
  - Medical Record Number
  - Informed consent documents
  - Flow sheets from mother’s and infant’s medical records
  - Medication records

5



Case 1: *Where did that binder go?!?!*

- ***What do you do first?***
  - ***Panic***
  - ***Notify the IRB***
  - ***Contact the Privacy Officer***
  - ***Call the Principal Investigator***
  - ***Notify the research participant (mother)***

6

Case 1: *Where did that binder go?!?*

https://tenor.com/view/dont-panic-hitchhikers-guide-to-the-galaxy-stay-calm-gif-12660494

Keep Calm and Assess Your Risks

Operational

- *What are the potential risks to operations of the organization, external partners?*

Functional

- *What are the potential risks to the integrity of the study?*

Financial

- *What are the potential financial risks?*

Reputational

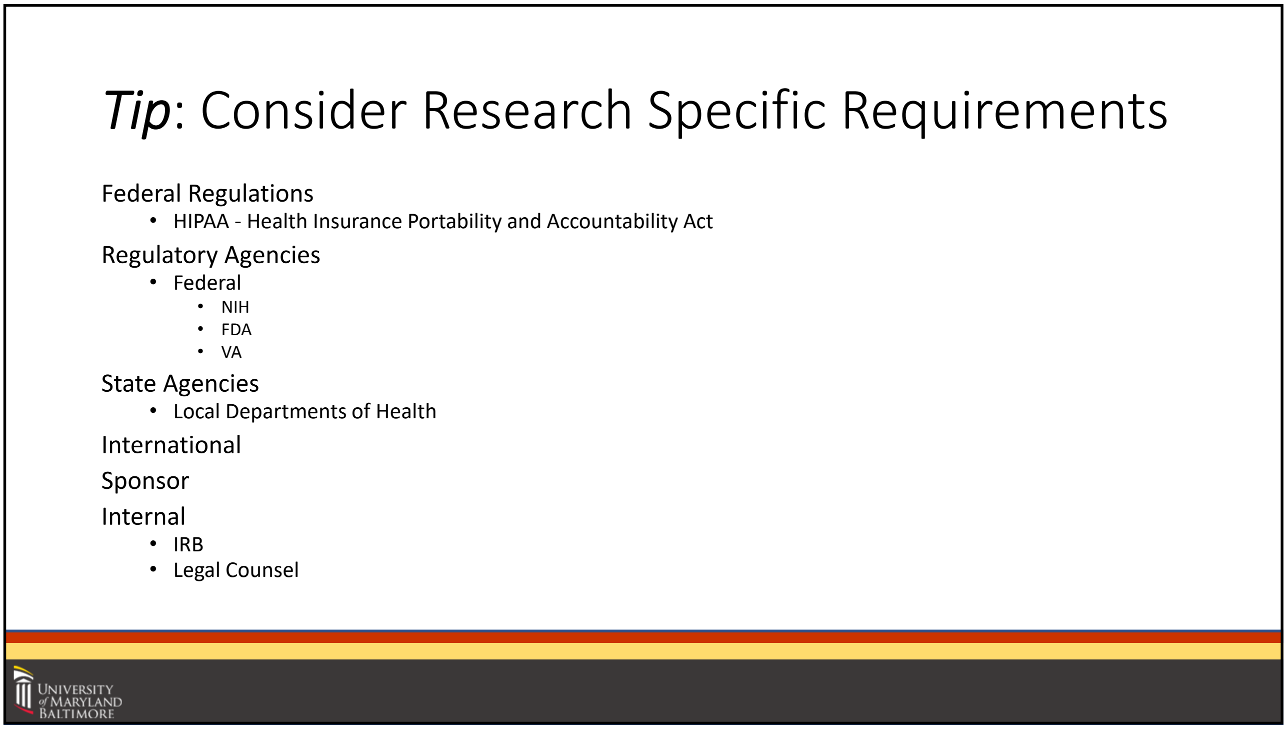
- *What risks are there to the reputation of the organization, external partners, and associated persons?*

Regulatory

- *What regulations apply to the breach?*

Legal

- *What are the potential legal risks?*



Tip: Consider Research Specific Requirements

Federal Regulations
- HIPAA - Health Insurance Portability and Accountability Act

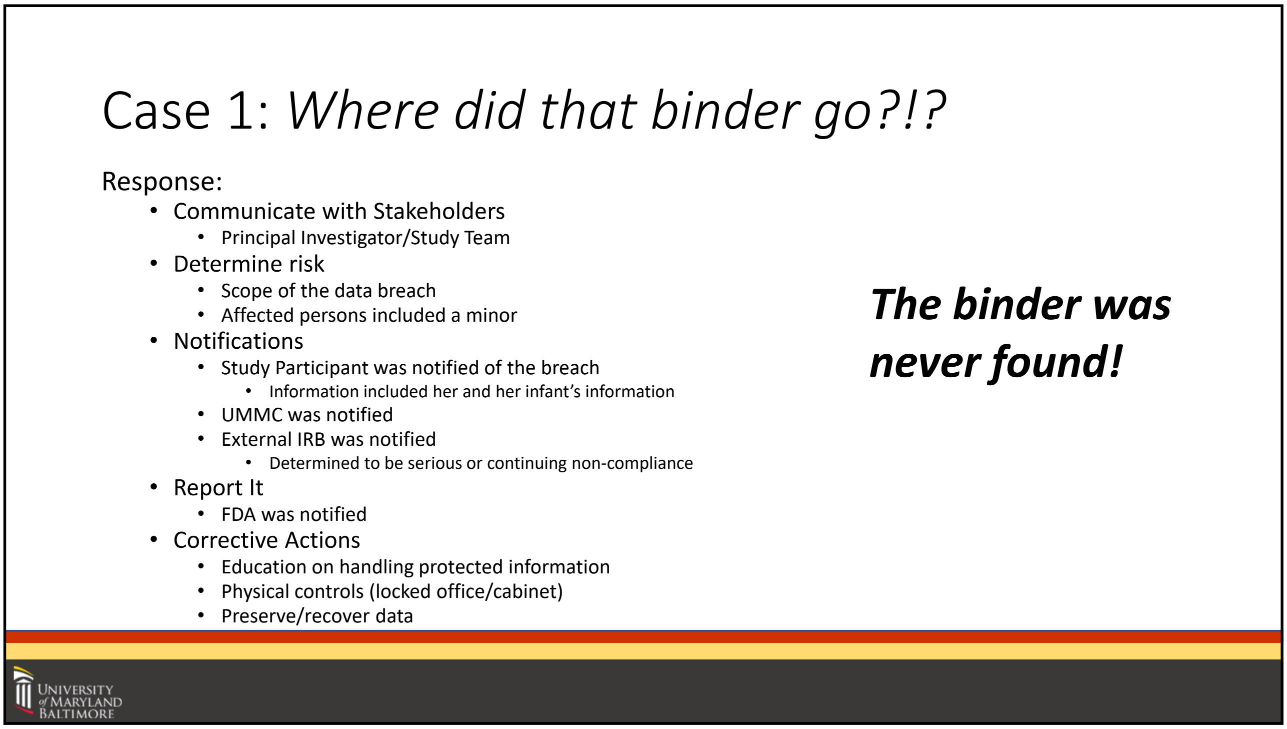
Regulatory Agencies
- Federal
  - NIH
  - FDA
  - VA

State Agencies
- Local Departments of Health

International

Sponsor

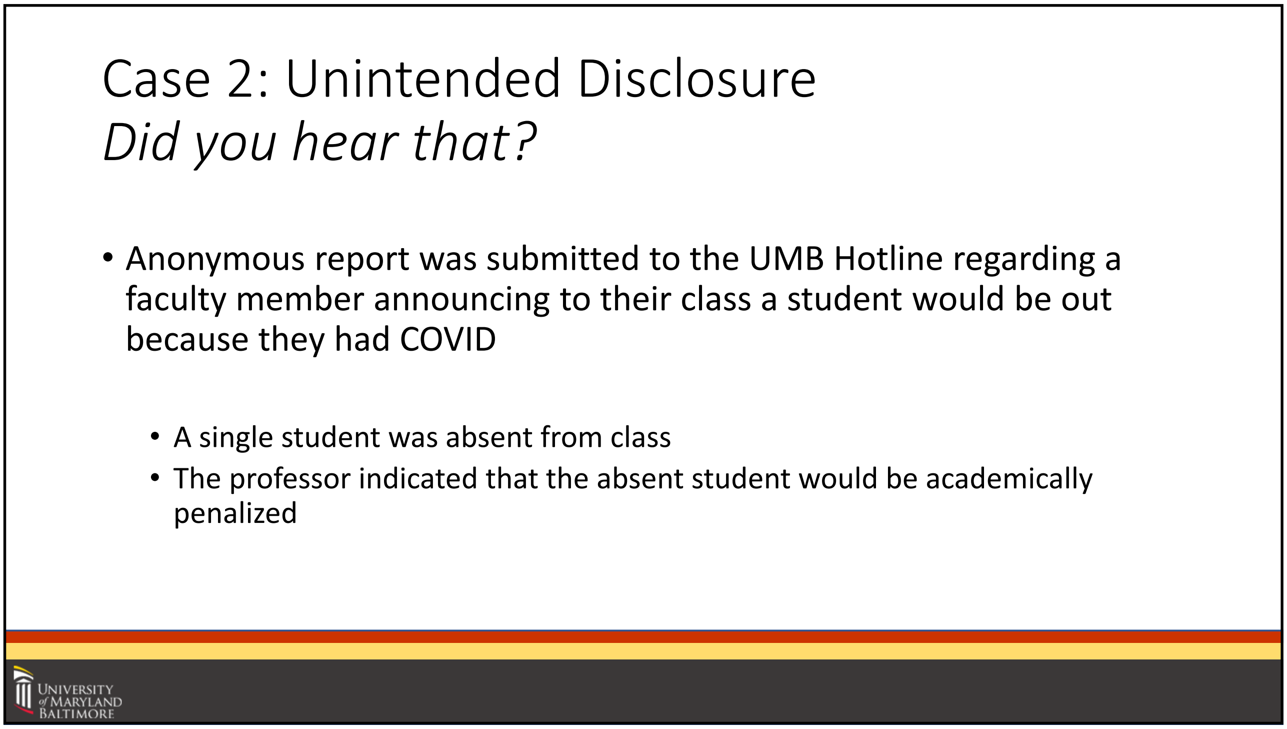
Internal
- IRB
- Legal Counsel



Case 1: *Where did that binder go?!?*

Response:
- Communicate with Stakeholders
  - Principal Investigator/Study Team
- Determine risk
  - Scope of the data breach
  - Affected persons included a minor
- Notifications
  - Study Participant was notified of the breach
    - Information included her and her infant's information
  - UMMC was notified
  - External IRB was notified
    - Determined to be serious or continuing non-compliance
- Report It
  - FDA was notified
- Corrective Actions
  - Education on handling protected information
  - Physical controls (locked office/cabinet)
  - Preserve/recover data

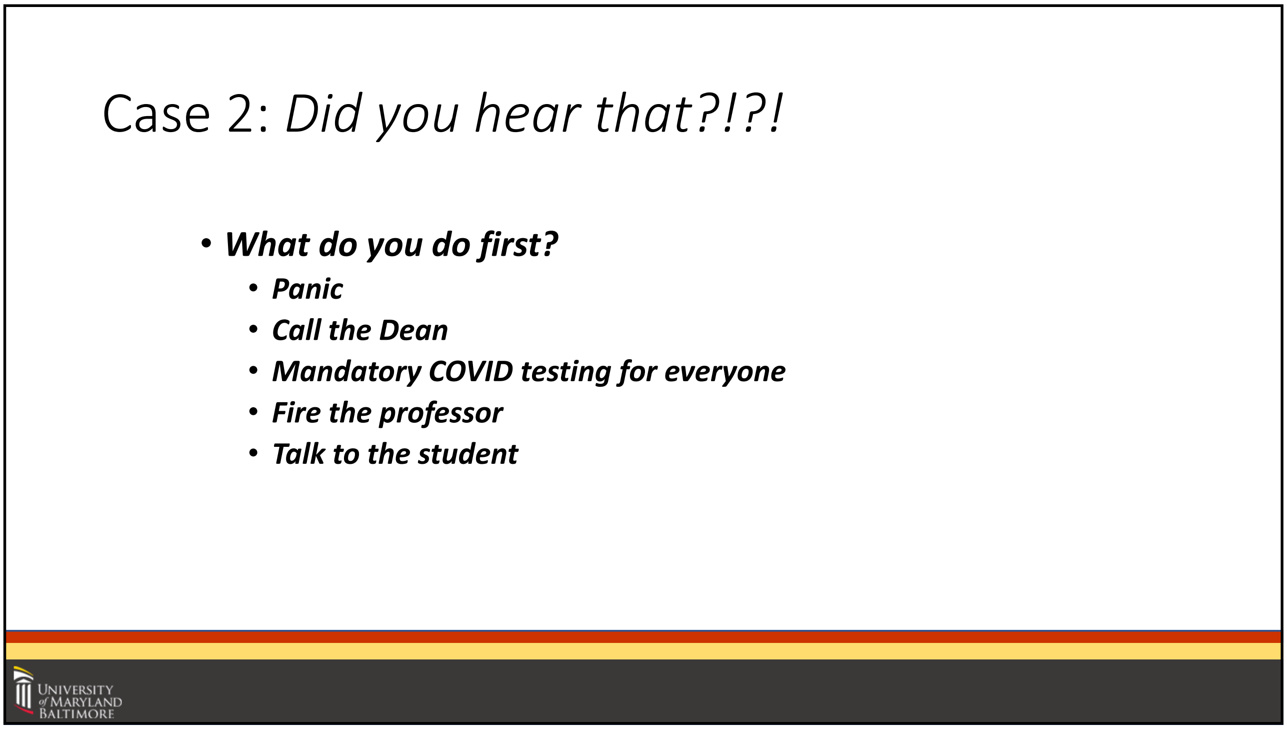
The binder was never found!



Case 2: Unintended Disclosure *Did you hear that?*

- Anonymous report was submitted to the UMB Hotline regarding a faculty member announcing to their class a student would be out because they had COVID
  - A single student was absent from class
  - The professor indicated that the absent student would be academically penalized

11



Case 2: *Did you hear that?!?!*

- ***What do you do first?***
  - ***Panic***
  - ***Call the Dean***
  - ***Mandatory COVID testing for everyone***
  - ***Fire the professor***
  - ***Talk to the student***

12

Case 2: *Did you hear that?!?*

https://tenor.com/view/dont-panic-hitchhikers-guide-to-the-galaxy-stay-calm-gif-12660494

Keep Calm and Assess Your Risks

Operational

- *What are the potential risks to operations of the organization?*

Functional

- *What are the potential risks to the school providing educational services?*

Financial

- *What are the potential financial risks?*

Reputational

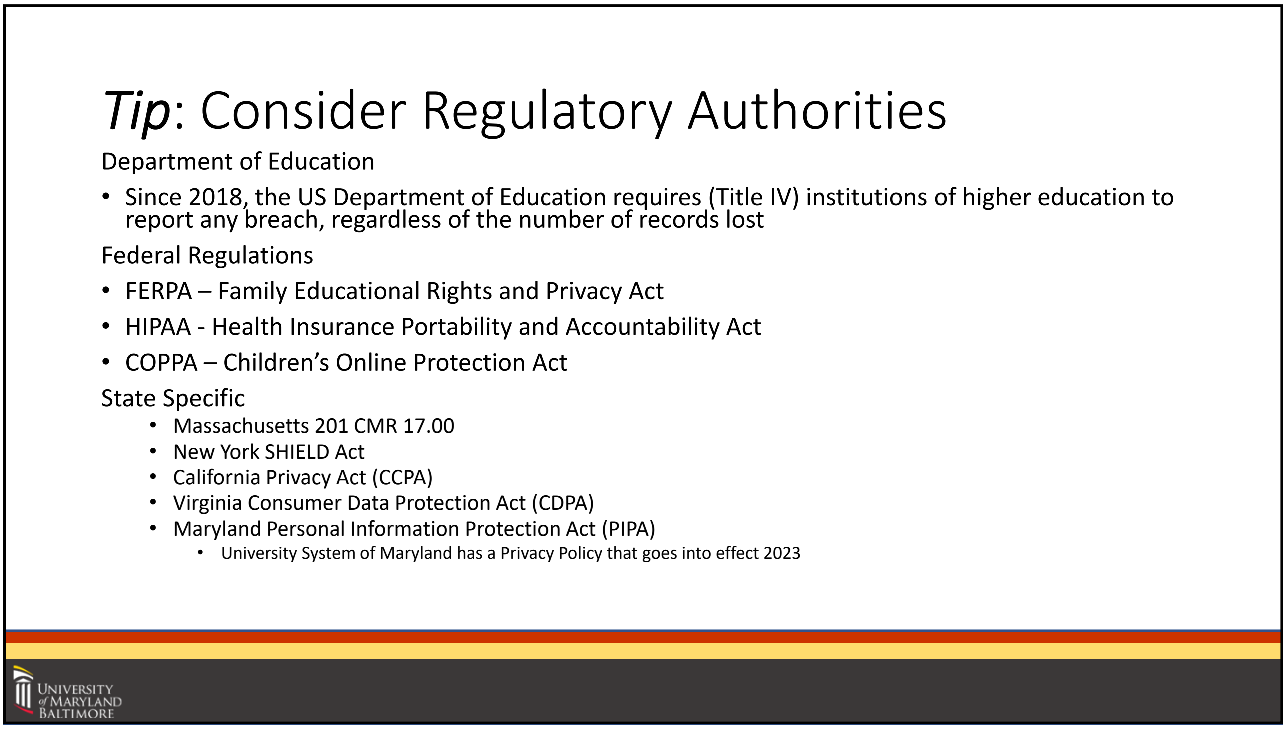
- *What risks are there to the reputation of the organization?*

Regulatory

- *What regulations apply to the breach?*

Legal

- *What are the potential legal risks?*



Tip: Consider Regulatory Authorities

Department of Education

- Since 2018, the US Department of Education requires (Title IV) institutions of higher education to report any breach, regardless of the number of records lost

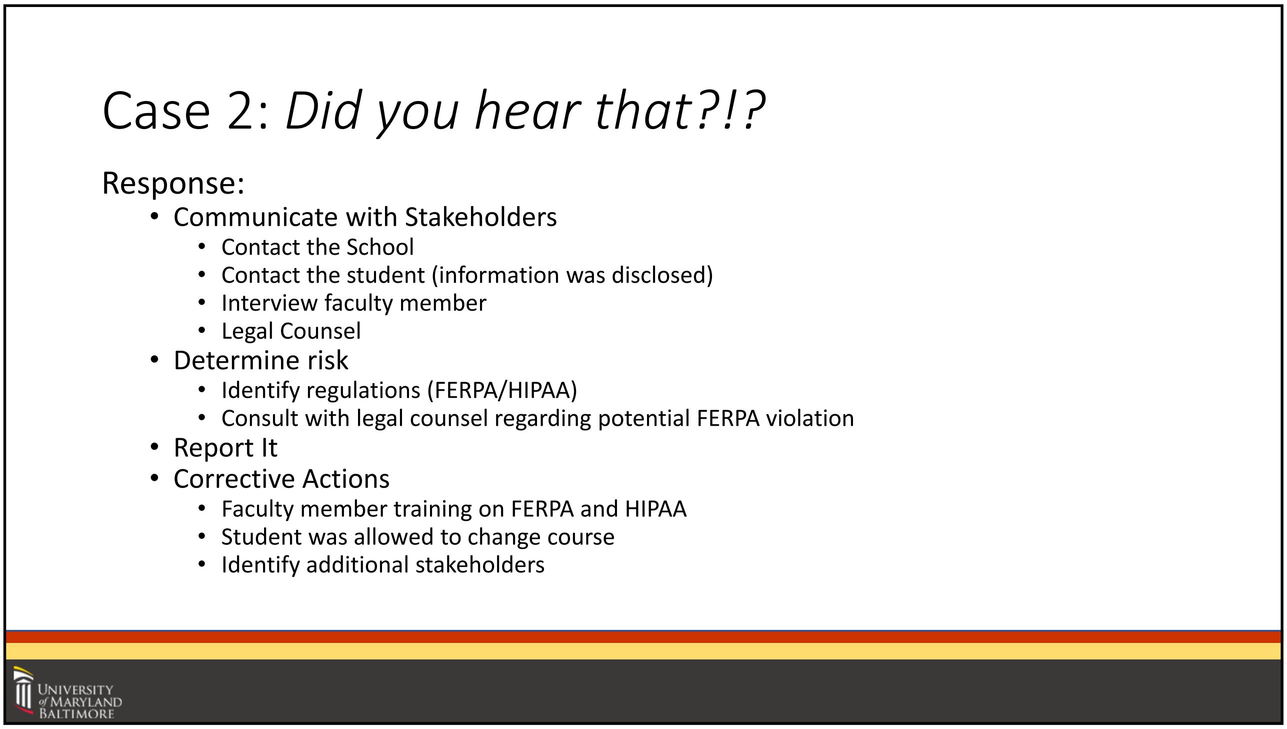
Federal Regulations

- FERPA – Family Educational Rights and Privacy Act
- HIPAA - Health Insurance Portability and Accountability Act
- COPPA – Children's Online Protection Act

State Specific

  - Massachusetts 201 CMR 17.00
  - New York SHIELD Act
  - California Privacy Act (CCPA)
  - Virginia Consumer Data Protection Act (CDPA)
  - Maryland Personal Information Protection Act (PIPA)
    - University System of Maryland has a Privacy Policy that goes into effect 2023

15

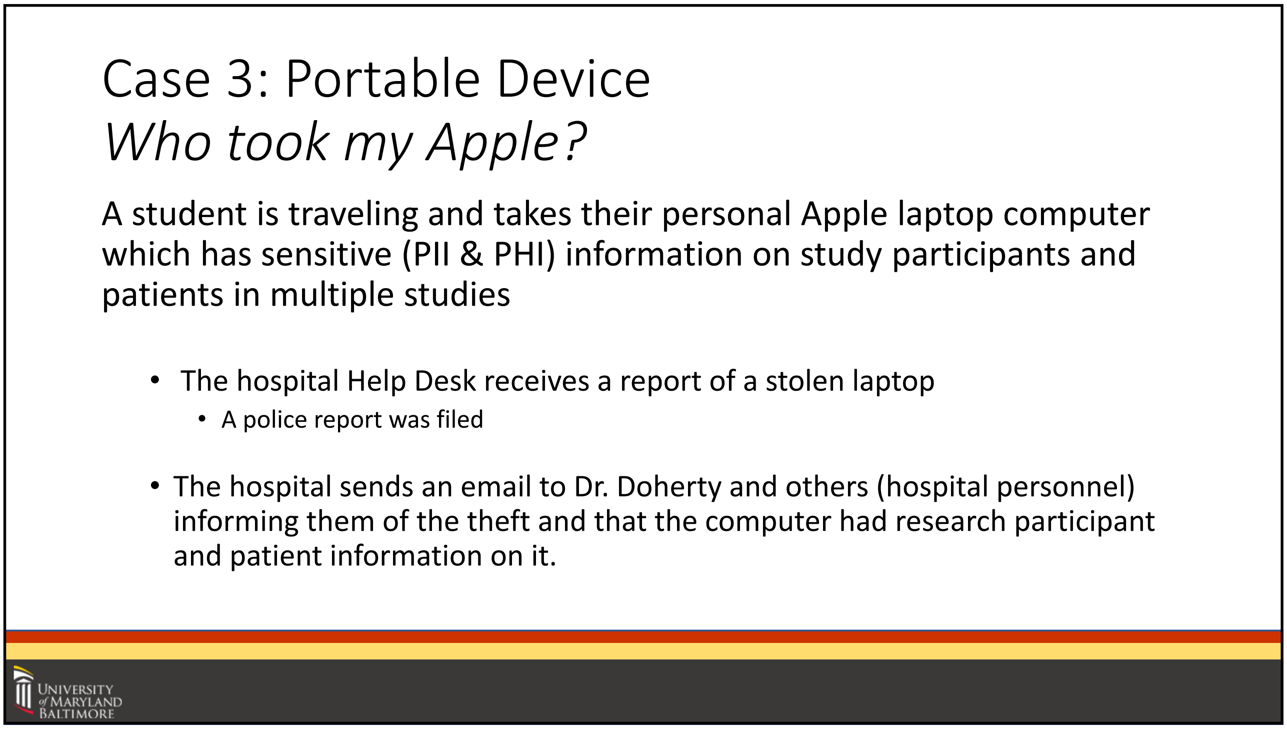


Case 2: *Did you hear that?!?*

Response:

- Communicate with Stakeholders
  - Contact the School
  - Contact the student (information was disclosed)
  - Interview faculty member
  - Legal Counsel
- Determine risk
  - Identify regulations (FERPA/HIPAA)
  - Consult with legal counsel regarding potential FERPA violation
- Report It
- Corrective Actions
  - Faculty member training on FERPA and HIPAA
  - Student was allowed to change course
  - Identify additional stakeholders

16

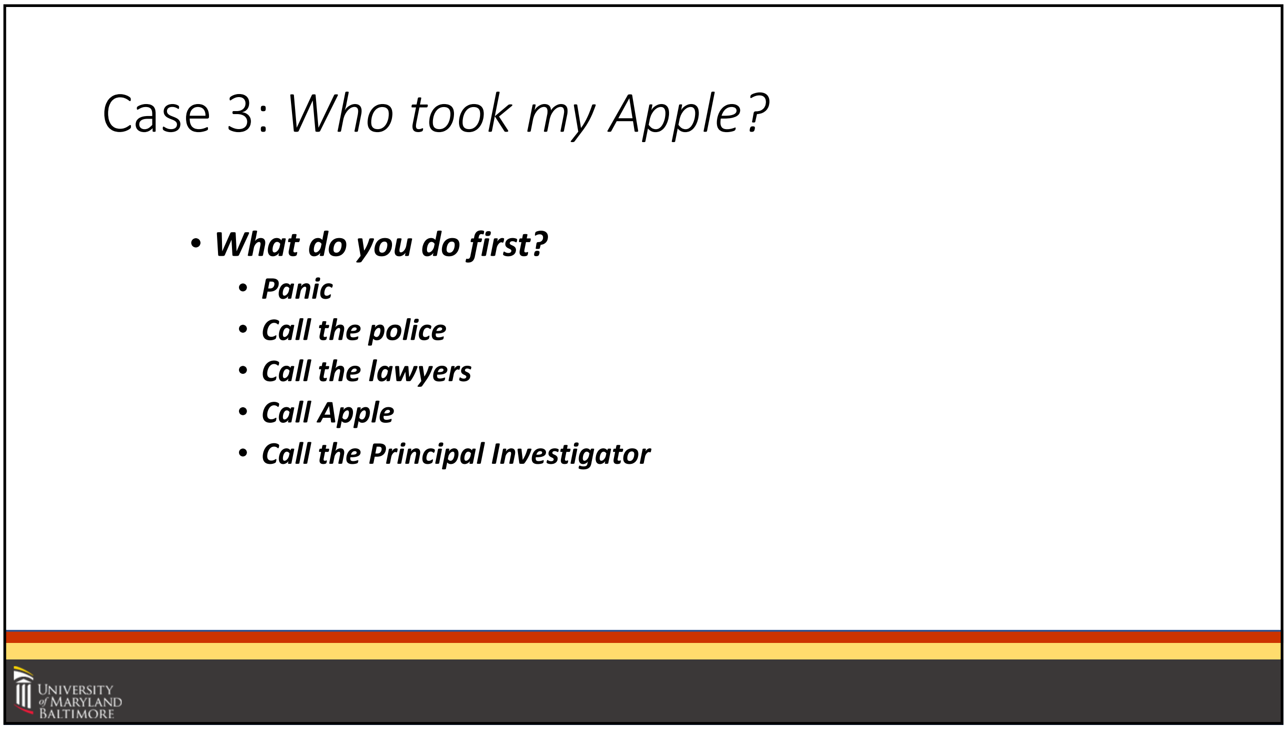


Case 3: Portable Device *Who took my Apple?*

A student is traveling and takes their personal Apple laptop computer which has sensitive (PII & PHI) information on study participants and patients in multiple studies

- The hospital Help Desk receives a report of a stolen laptop
  - A police report was filed
- The hospital sends an email to Dr. Doherty and others (hospital personnel) informing them of the theft and that the computer had research participant and patient information on it.

17



Case 3: *Who took my Apple?*

- ***What do you do first?***
  - ***Panic***
  - ***Call the police***
  - ***Call the lawyers***
  - ***Call Apple***
  - ***Call the Principal Investigator***

18

Case 3: *Who took my Apple?*

https://tenor.com/view/dont-panic-hitchhikers-guide-to-the-galaxy-stay-calm-gif-12660494

19

Keep Calm and Assess Your Risks

Operational

- *What are the potential risks to operations of the organization, the hospital?*

Functional

- *What are the potential risks to the integrity of the study, to the hospital providing clinical care?*

Financial

- *What are the potential financial risks?*

Reputational

- *What risks are there to the reputation of the organization, the hospital?*

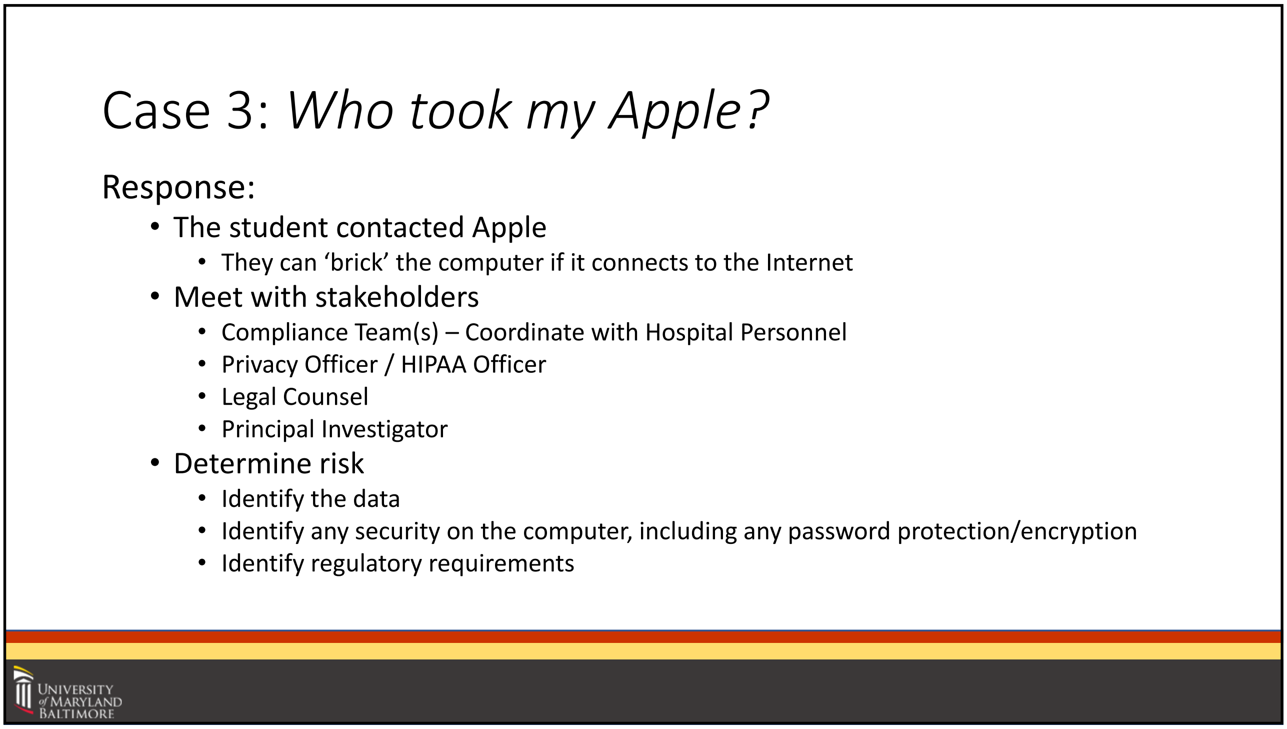
Regulatory

- *What regulations apply to the breach?*

Legal

- *What are the potential legal risks?*

20

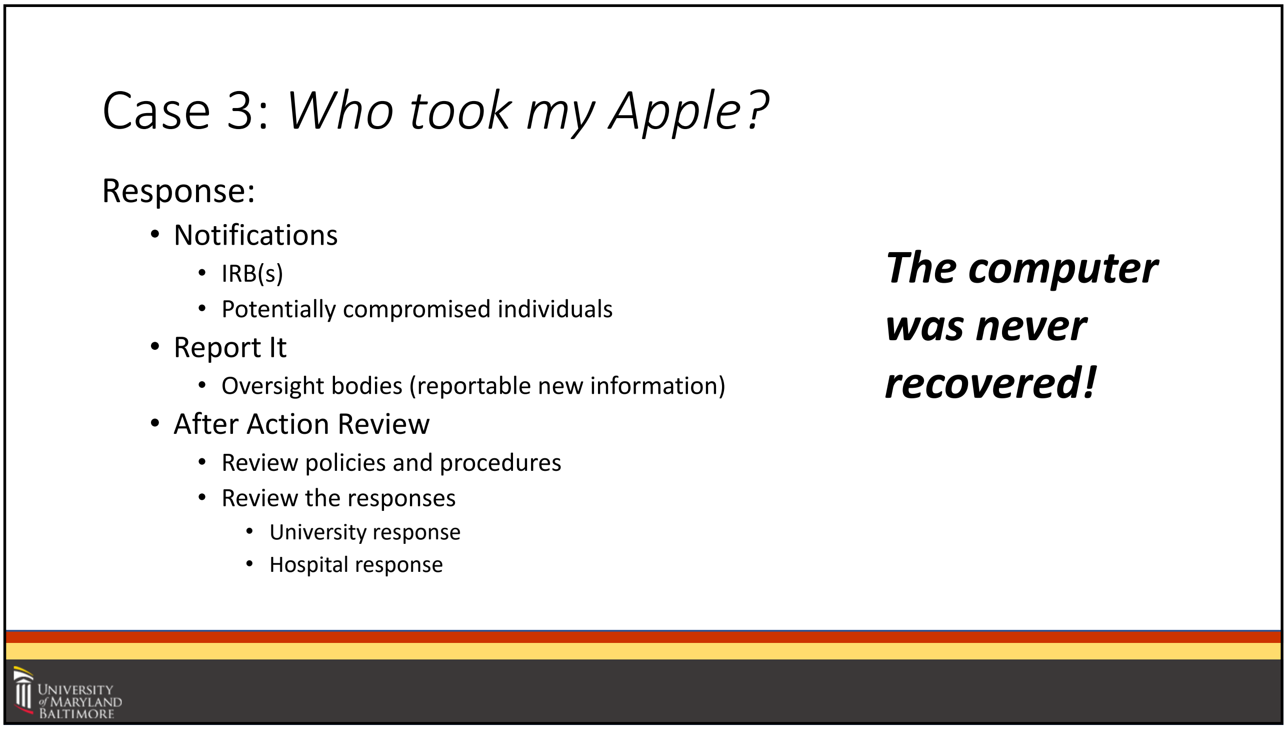


Case 3: *Who took my Apple?*

Response:

- The student contacted Apple
  - They can ‘brick’ the computer if it connects to the Internet
- Meet with stakeholders
  - Compliance Team(s) – Coordinate with Hospital Personnel
  - Privacy Officer / HIPAA Officer
  - Legal Counsel
  - Principal Investigator
- Determine risk
  - Identify the data
  - Identify any security on the computer, including any password protection/encryption
  - Identify regulatory requirements

21



Case 3: *Who took my Apple?*

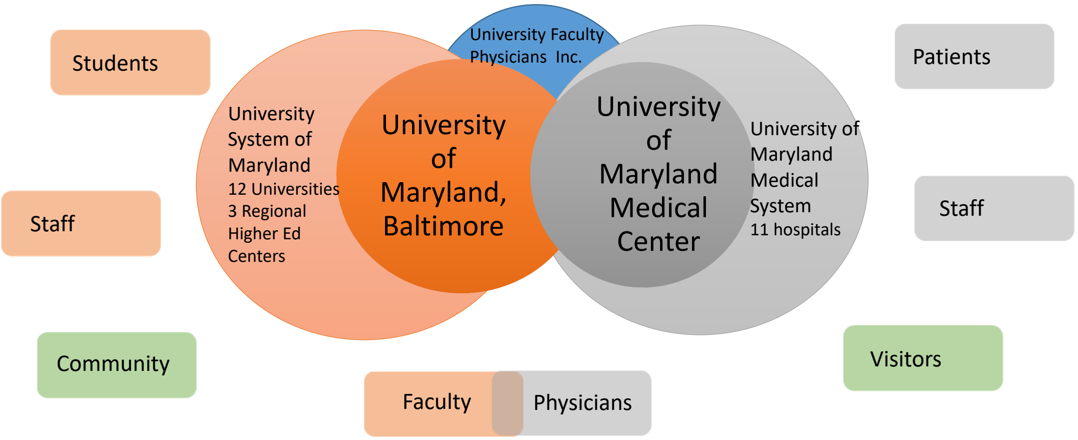
Response:

- Notifications
  - IRB(s)
  - Potentially compromised individuals
- Report It
  - Oversight bodies (reportable new information)
- After Action Review
  - Review policies and procedures
  - Review the responses
    - University response
    - Hospital response

The computer was never recovered!

22

Who We Are:



Students

Staff

Community

University System of Maryland
12 Universities
3 Regional Higher Ed Centers

University of Maryland, Baltimore

University Faculty Physicians Inc.

University of Maryland Medical Center

University of Maryland Medical System
11 hospitals

Faculty

Physicians

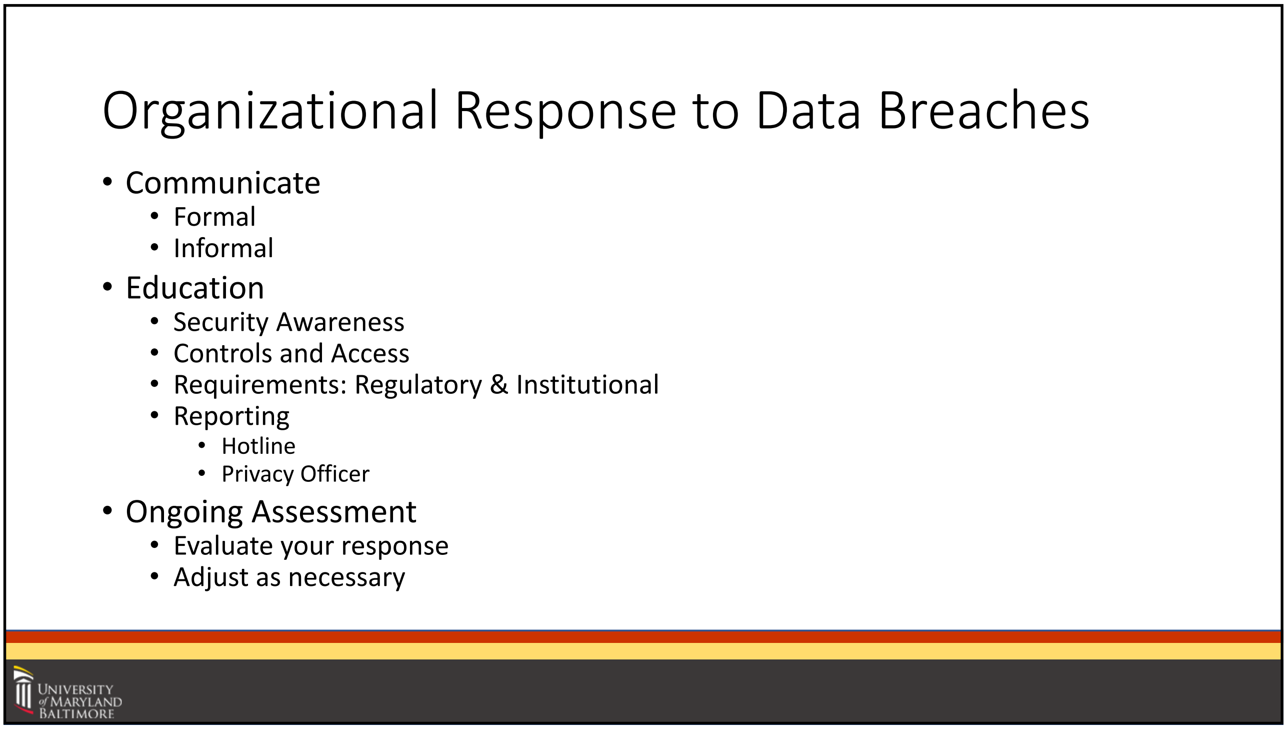
Patients

Staff

Visitors

Organizational Response to Data Breaches

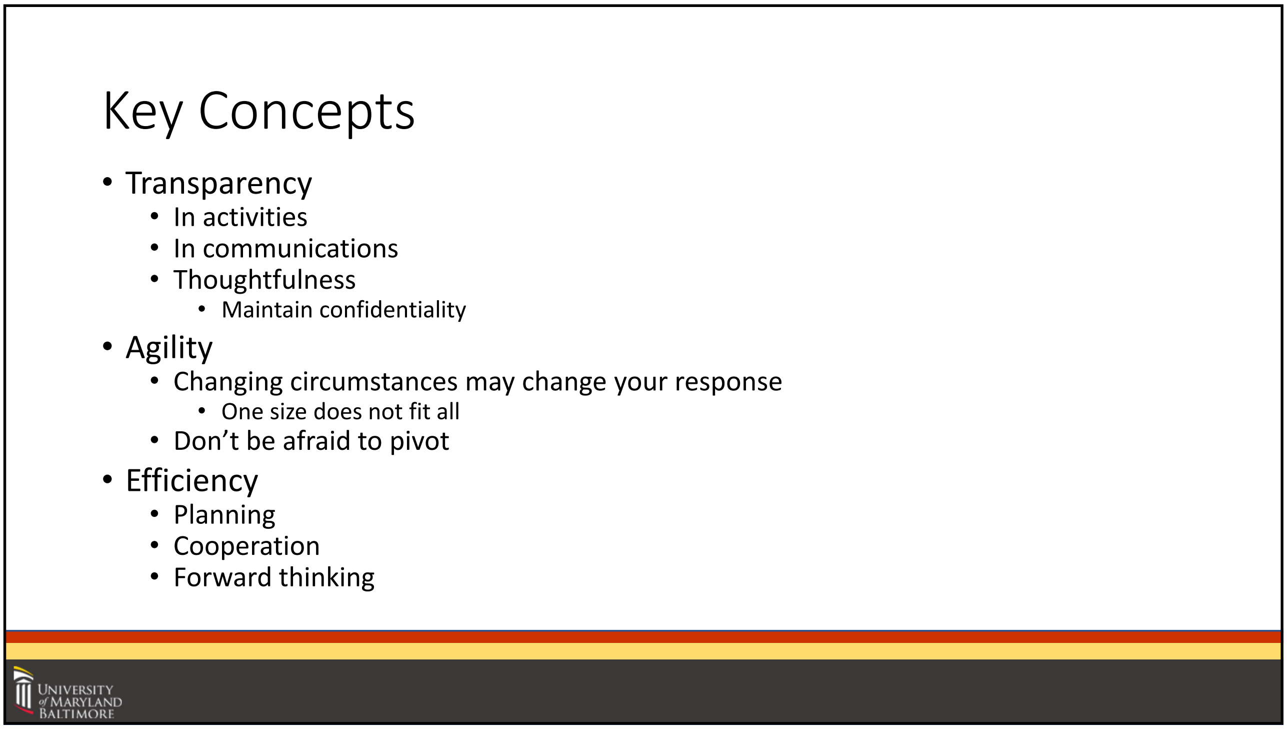
- Identify key partners
  - Internal
  - External
- Identify the scope of risk
  - Operational
  - Functional
  - Financial
  - Reputational
  - Regulatory
  - Legal
- Plan the response
  - Coordinated and collaborative
  - Cross organizational boundaries
  - Identify root cause



Organizational Response to Data Breaches

- Communicate
  - Formal
  - Informal
- Education
  - Security Awareness
  - Controls and Access
  - Requirements: Regulatory & Institutional
  - Reporting
    - Hotline
    - Privacy Officer
- Ongoing Assessment
  - Evaluate your response
  - Adjust as necessary

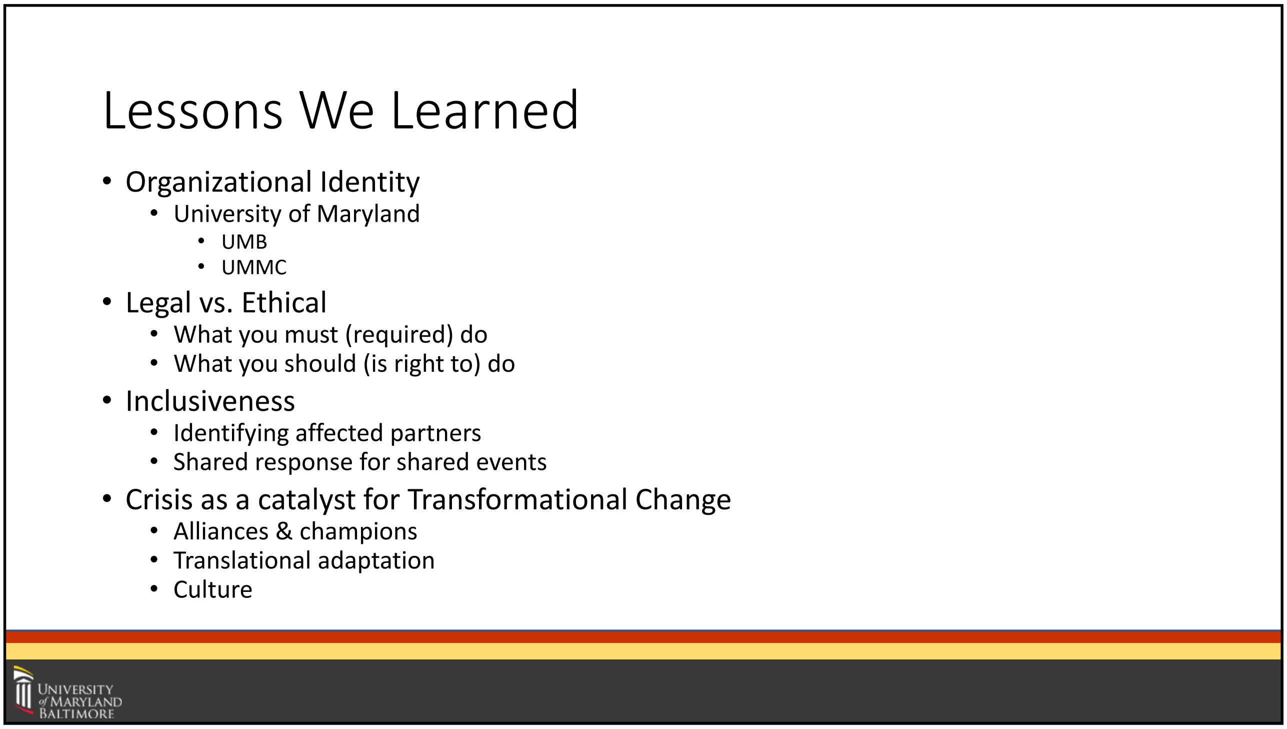
25



Key Concepts

- Transparency
  - In activities
  - In communications
  - Thoughtfulness
    - Maintain confidentiality
- Agility
  - Changing circumstances may change your response
    - One size does not fit all
  - Don't be afraid to pivot
- Efficiency
  - Planning
  - Cooperation
  - Forward thinking

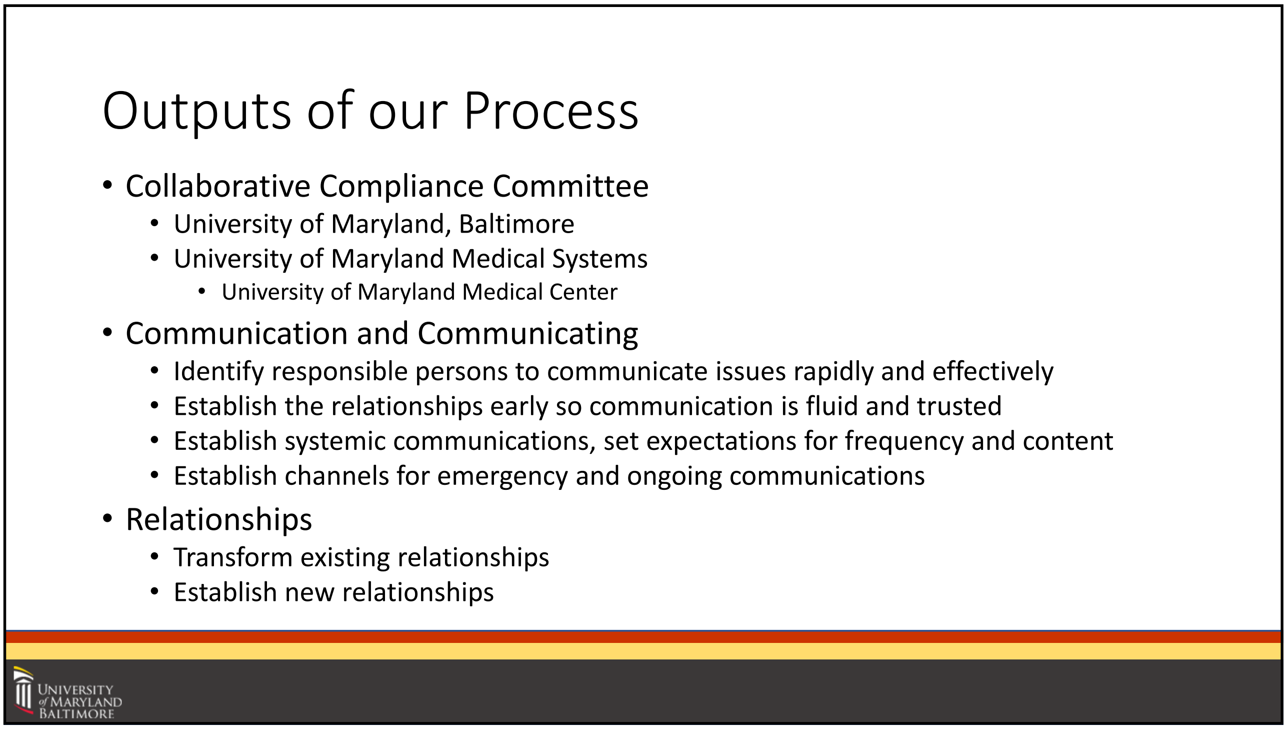
26



Lessons We Learned

- Organizational Identity
  - University of Maryland
    - UMB
    - UMMC
- Legal vs. Ethical
  - What you must (required) do
  - What you should (is right to) do
- Inclusiveness
  - Identifying affected partners
  - Shared response for shared events
- Crisis as a catalyst for Transformational Change
  - Alliances & champions
  - Translational adaptation
  - Culture

27



Outputs of our Process

- Collaborative Compliance Committee
  - University of Maryland, Baltimore
  - University of Maryland Medical Systems
    - University of Maryland Medical Center
- Communication and Communicating
  - Identify responsible persons to communicate issues rapidly and effectively
  - Establish the relationships early so communication is fluid and trusted
  - Establish systemic communications, set expectations for frequency and content
  - Establish channels for emergency and ongoing communications
- Relationships
  - Transform existing relationships
  - Establish new relationships

28

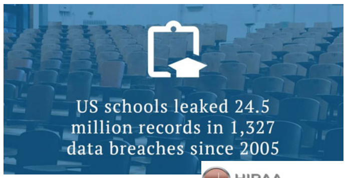
Case Discussion and Q&A

29

Data Protection Matters

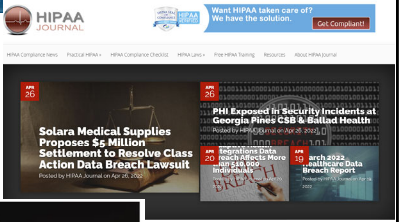
Huge Risks and Potential Rewards

- Data breaches are big news
- Costs of a data breach
- Comprehensive and transparent response – crisis management
- Successfully protecting data can lead to positive attention
- Strengthen your organization(s)



US schools leaked 24.5 million records in 1,327 data breaches since 2005

Retrieved from: https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/



APR 26 Solara Medical Supplies Proposes $5 Million Settlement to Resolve Class Action Data Breach Lawsuit

Posted by HIPAA Journal on Apr 26, 2022

APR 26 PHI Exposed in Security Incidents at Georgia Pines CSB & Ballad Health

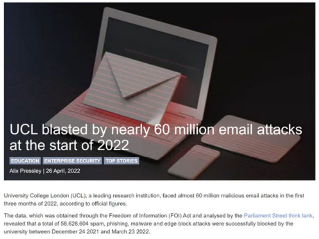
Posted by HIPAA Journal on Apr 26, 2022

APR 20 tegrations Data reach Affects More ɪan 510,000 Individuals

Posted by HIPAA Journal on Apr 20, 2022

APR 19 arch 2022 ealthcare Data Breach Report

Posted by HIPAA Journal on Apr 19, 2022



UCL blasted by nearly 60 million email attacks at the start of 2022

EDUCATION ENTERPRISE SECURITY TOP STORIES

Alix Pressley | 26 April, 2022

University College London (UCL), a leading research institution, faced almost 60 million malicious email attacks in the first three months of 2022, according to official figures.

The data, which was obtained through the Freedom of Information (FOI) Act and analysed by the Parliament Street think tank, revealed that a total of 58,628,604 spam, phishing, malware and edge block attacks were successfully blocked by the university between December 24 2021 and March 23 2022.

Retrieved from: https://www.intelligentcio.com/eu/2022/04/26/ucl-blasted-by-nearly-60-million-email-attacks-at-the-start-of-2022/#

30

Privacy and Transparency

- Privacy
  - Individual
  - Organizational
- Transparency
  - Within the organization
  - Across stakeholders
  - External
- Trust
  - Ongoing Effort – A daily exercise
- Culture
  - High level/executive support

Contact Information

Susan Buskirk, DM, MS, CCEP
Vice President
Chief Accountability Officer
Institutional Official
sbuskirk@umaryland.edu

Julie Doherty, DM, MSN
Assistant Vice President, Research Compliance
jdoherty@umaryland.edu

Stephanie Suerth, MPA, CCEP
Director, Special Projects
Acting Title IX Coordinator
ssuerth@umaryland.edu