# Compliance, Contracts, & Cybersecurity

# IT Security / Regulatory Update for Campus Leadership

# Agenda

- Current Climate
- Security Incident Protocols
  - What to do if you suspect Ransomware
  - Security Incident Response at Carthage
- GLBA Regulation – effective 6/9/2023
  - Highlights:
    - Catalog of Data and Services
    - Third Party Agreements

# Current Climate

- Education continues to be among the most heavily attacked sectors.
- Increasingly difficult to qualify for Cyber Liability insurance
- Schools continue to go offline due to cyber attacks
  - ie Morehead State in July / network still offline
- 3rd party breaches continue to impact Higher Ed
  - ie MoveIT incident impacted TIAA, National Student Clearinghouse

# Security Threats – A Day in the Life @Carthage

- INTERNET: Thousands of exploit attempts blocked on our firewall daily and tens of thousands of known malicious IPs
- EMAIL: Google and Proofpoint block more than 50% of inbound email - Email is the preferred and most common threat vector
- PCs: Daily investigation of alerts triggered from computers
- Proactive Actions:
  - Bad Actors lured into our honeypots - 3,000 / day
  - Daily threat intelligence feeds get loaded to the firewall
  - Threat bulletins manually evaluated daily (software & hardware vulnerabilities, exploits, coding vulnerabilities, zero days, etc.
  - Software security patches issued every Tuesday

# Top Incidents @Carthage

- 3rd party vendors have breaches & inform us
- People accidentally send incorrect attachments or intended attachments to unintended recipients
- Adware impersonating malware
- Individual machines with viruses

# What to do if you've been impacted by RANSOMWARE


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

# Don’t Panic …

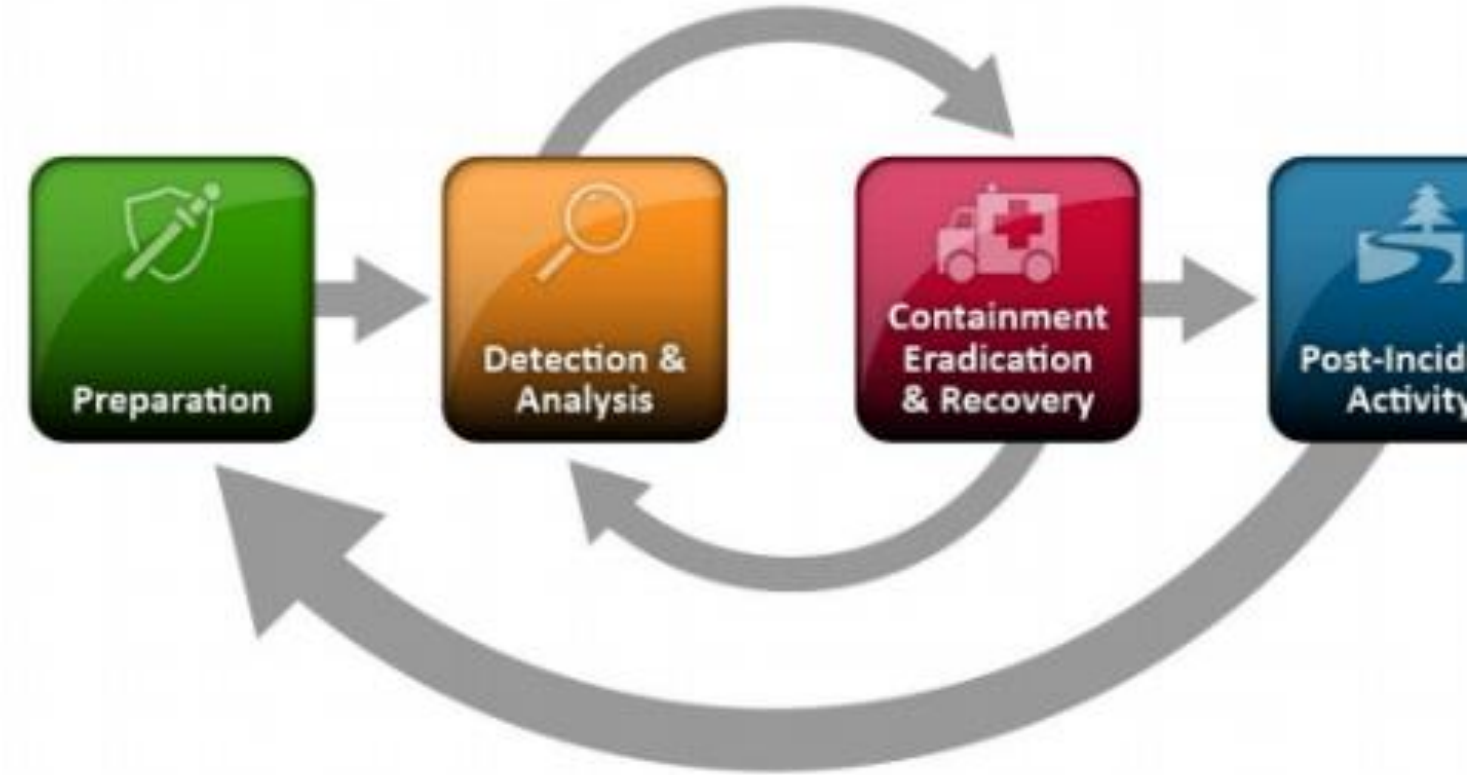
1. User your phone to take a photo of the screen/display
2. Disconnect from the network and/or shut down (important to minimize potential spread)
3. Contact LIS directly in person or on phone

# What Happens if we suspect Ransomware?

- Incident Response Procedure and Ransomware Runbook are referenced
  - Basically an Emergency Response effort
- LIS leads the a ‘war room’
  - HL140 or Tennis Center and/or Virtual
- How we notify you will vary based on the situation:
  - You might be called upon as a member of the Emergency Response team
  - If we believe there is intruder, but there are no signs of encryption or data exfiltration, we would be using offline communications
  - May take systems offline as a protective measure

# Response Stages

Carthage's incident response plan includes the following stages:




1. Detection & Analysis
2. Containment
3. Eradication & Recovery
4. Post-Incident Activity

# 1) Detection & Analysis

- Determining what is affected, type of compromise & if there was lateral movement
- Call in for Assistance from Insurance who will bring in a Cybersecurity Forensics Firm, May contact the FBI

# 2) Containment

- May require shutting down access to the network and specific systems and services
  - Time to start communicating, if we haven't already: impact to classes, services, etc..
  - Communications team would be engaged for broad messaging

# 3) Eradication & Recovery

- Need to ensure the exploit is eliminated before restoring service
- Need system copies for post-incident forensics

- If there was a breach, the appropriate department of the college will participate in the stakeholder communications

# Communications

- Incident vs Breach
  - We work an “incident” until we call in a professional who would be qualified to determine if there was a “breach” or a specific attack such as ransomware
    - You might hear *“IT is investigating an incident”*
    - Or “*We’ve taken down some services out of an abundance of caution as we investigate the incident.”*
      - This is a very common action to take before the scope is known
      - We have diversified our technology, so it is unlikely that both cloud and on-premise services would be impacted in a single incident, so some channels of communication will likely be available.

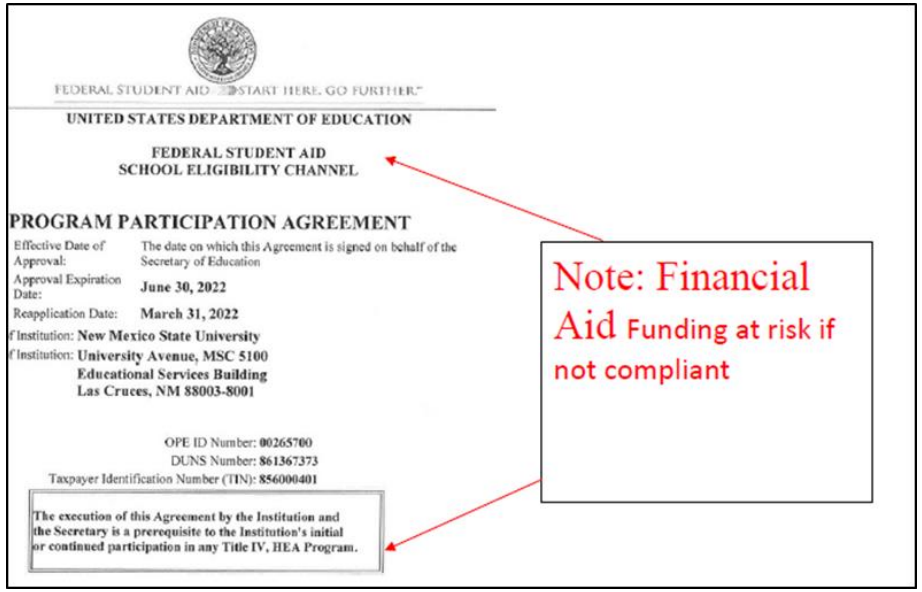
# GLBA Safeguards Rule

# GLBA Safeguards Rule

- Required to follow as a condition of administering Federal Financial Aid
- Audited on compliance as part of the Single Audit (CLA will shortly be auditing for period ending 6/30/23)
- Department of Education receives the Single Audit Compliance Report
- DOE shares GLBA findings with FTC

- Penalties can include fines,

  loss of federal financial aid, & prison time



# New GLBA Safeguards Rule

## December 9, 2021

- 1. Qualified employee to coordinate the information security program
- 2.1. Written Risk assessment
  - 2.1a. Criteria for the evaluation and categorization of identified risks
  - 2.1b. Criteria for the assessment of the confidentiality, integrity, and availability of information systems and customer information; include adequacy of existing controls
  - 2.1c. Documented mitigation or acceptance of residual risk
- 2.2 Periodic additional risk assessments
- 3. Implement safeguards to threats identified in the risk assessment
- 3.1. Implement and periodically review access controls, technical and physical, to:
  - 3.1a. Limit access to customer information
  - 3.1b. Limit user access to based on their duties
- 3.2. Identify and manage data, personnel, devices, systems, and facilities
- 3.3. Encrypt customer information held or transmitted in transit and at rest
- 3.4. Adopt secure development practices for in-house developed application; Test the security of externally developed application
- 3.5. Multi-factor authentication for any individual access any information system
- 3.8. Implement policies and controls designed to monitor and log user activity, and detect unauthorized access or tampering of customer information
  - 3.6a. Develop customer information disposal procedures
  - 3.6b. Periodically review data retention policy
  - 3.7. Adopt change management procedures
- 4.1. Regularly test the effectiveness of the safeguards' key controls, systems, and protocols, including those to detect actual or attempted attacks
- 4.2. For information systems, monitoring and testing includes continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring, then:
  - 4.2a. Annual penetration testing
  - 4.2b. Semi-annual vulnerability assessments, or upon material changes to operations
- 5. Implement policies and procedures to ensure personnel can enact the information security program, by providing:
  - 5.1. Security awareness training
  - 5.3. Security updates and training to information security personnel
  - 5.2. Qualified information security personnel, either employed internally or an affiliate or service provider
  - 5.4. Verification key information security personnel maintain current knowledge of changing threats and countermeasures
- 6. Oversee providers, by:
  - 6.2. Vendor contractual requirement for safeguard implementation and maintenance
  - 6.1. Vendor selection process with consideration for appropriate safeguards of customer information
  - 6.3. Periodically assessing service providers based on their risk and continued adequacy of their safeguards
- 7. Evaluate and adjust the information security program in light of the testing and monitoring required by section 4; material changes in operations or business arrangements, material impacts, or based of off results from 2.2, or any other circumstance.
- 8. Establish a written incident response plan. The plan should address:
  - 8.1. The goals of the incident response plan
  - 8.2. Internal processes for responding to an event
  - 8.3. Defined roles, responsibilities, and levels of decision making
- 9. Annual formal reporting to BOD or governing body by Qualified employee, includes:
  - 9.1. Overall program status
  - 9.2. Material matters, such as risk assessment, risk management and control design, service provider arraignment, testing results, security events, and recommended program changes

## In Effect: June 9, 2023





Requirements apply to both on-premise and third-party hosted information

# Identify and Manage Data & Systems

## The importance of systems “inventory”

- **For security purposes:**
  - It is a requirement that we keep track of ALL systems used by the College, how they are authenticated, and what data is stored there
  - We call this the “Service Catalog”
  - If a system is compromised, we need to know about it!  (Herff Jones, e.g.)
  - When a new system is being considered, it needs to go through a security evaluation (more on that coming up!)
  - For all systems, we send a Google form asking for various pieces of information, including who the office contact is.
  - Any communications about breaches, end of service, etc. need to be passed along by the office contact to LIS.
  - LIS may ask you to request periodic updates from the vendor; we collect vendor contact info on the form.

# Identify and Manage Data & Systems

## The importance of systems “inventory”

- **For support purposes:**
  - When users contact the Information Desk about systems, it is important that we know about systems and who users should contact if support is not provided by LIS (GET app, Nelnet, e.g.)
  - We need information on how a system authenticates (SSO or something else) so we can help people with their logins, whenever possible
  - Information on when systems will be available or will cease to be available helps manage user expectations (my.carthage, GET app, e.g.)
- **For cost-saving purposes:**
  - Cataloging our systems helps avoid duplication and paying for things we no longer use
- **Note about physical computers:**
  - We will need to know what computers (laptops, desktops, etc.) that you have so we can also better support and protect those.

# Procedural Requirements

- Data Retention Policy & Procedure
- Mandatory Security Awareness Training
- Annual Reporting to the Board

# Technical Protections

- Multi-Factor Authentication
- Encryption of Data in Transit & At Rest
- System Monitoring

# 3rd Parties … Oversee Providers

We must hold our 3rd parties accountable for meeting the requirements, specifically including…

- We must evaluate and select appropriate service providers, considering the GLBA requirements
- Require them by contract to maintain security and confidentiality
- Periodically assess their cybersecurity compliance

# Takeaways

- Work with LIS on new technology acquisitions
  - Plan for more extensive vetting with vendor & LIS
  - Vendors must provide written evidence of their security compliance & security audits
  - Vendors must agree to our security terms & conditions

Plan to reach out to vendors annually for copies of their security audit documentation & help LIS hold them accountable

- Work with LIS ahead of any renewals, so we can get these things worked into existing vendor contracts