HUSCH BLACKWELL

Information Security Trends and Best Practices for Colleges and Universities

MHEAC - March 9, 2021

Sean Tassi
Chris Budke

Presenters

Sean Tassi

816.983.8330

Sean.Tassi@huschblackwell.com

Chris Budke

816.983.8391

Christopher.Budke@huschblackwell.com

Agenda

- The Typical Lifecycle of a Security Incident
- Internal / External Roles during a Security Incident
- Dos and Don’ts
- How to Prepare For a Security Incident
- Ransomware and Other Threats
- Case Study – The Dark Overlord
- ED Notice re Campus Cybersecurity

HUSCH BLACKWELL

Lifecycle of a Security Incident

Detection (internal or external)

Notify executive management team (internal counsel)

Notify insurer

Select breach counsel (external counsel)

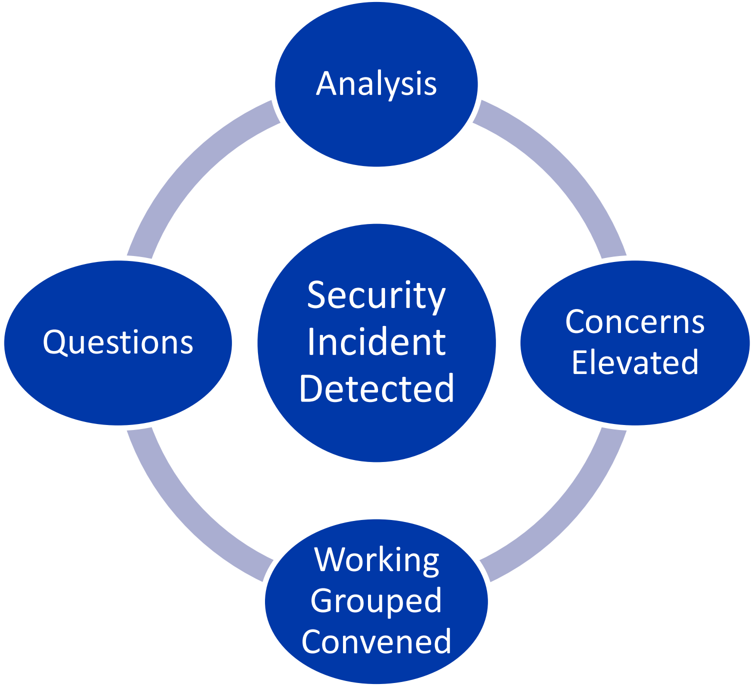
Select forensic firm

Consider public relations firm

The Incident Response Trap

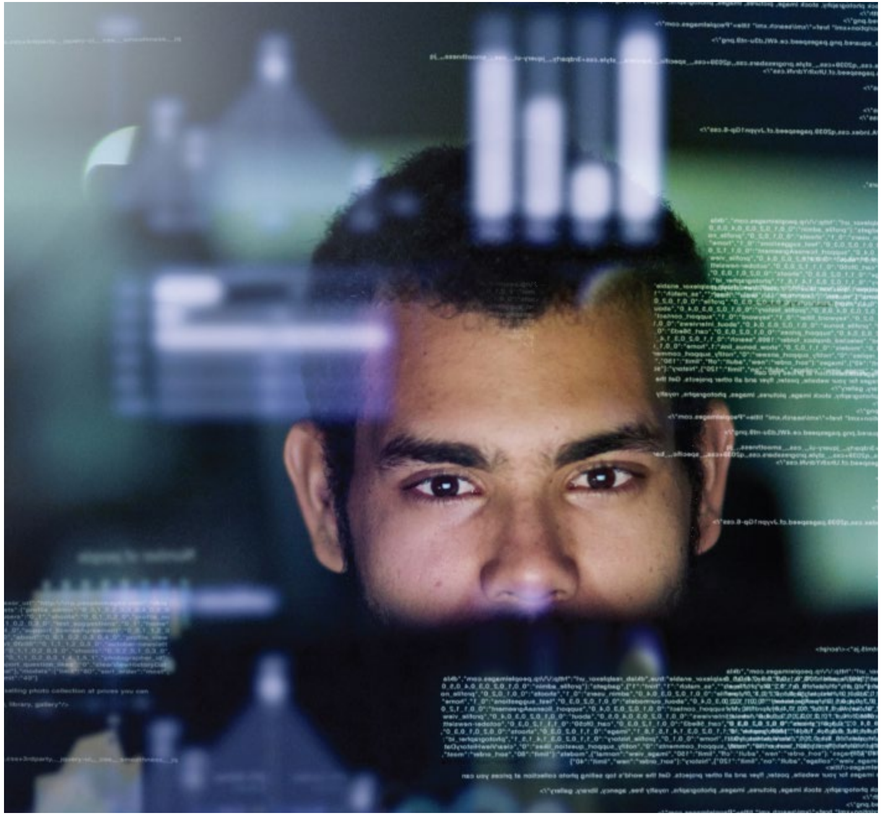
"It's a Trap!"

-Admiral Ackbar



External Counsel's Role — Quarterback The Incident

- Direct the forensic investigation
- Evaluate legal risk and potential notification obligations
  - Regulators
  - Impacted individuals
- Lead daily/weekly status calls to ensure that key campus stakeholders have real-time information to help make strategic business decisions
- Work closely with PR (internal or external) on messaging
- Coordinate any necessary notifications



This is everyone’s problem!

Forensic firm	• Collects evidence and conducts forensic investigation at the direction of counsel
Internal information technology and security	• Works hand-in-glove with forensic firm
Executive management	• Makes decisions based on recommendations from counsel and the forensic firm
Public relations	• Help style the messaging

Pre-Incident Dos and Don’ts

- Develop an incident response plan and practice it
- Coordinate with IT to ensure that logging exists for critical systems (firewall, systems and application logs)
- Understand your policy and coverage
  - Preselect vendors if possible
- Data mapping

Post-Incident Dos and Don’ts

- Notify insurer and engage counsel ASAP
- Take a breath
  - Limit internal written correspondence
  - Do not make public statements until they have been vetted by cyber counsel

Post-Incident Dos and Don’ts (cont.)

- Ensure forensic evidence is preserved
  - Do not tromp around the crime scene
  - Time is of the essence – it is critical to preserve the integrity of the evidence
    - Consider taking compromised systems off-line
- The priority will be containment
- Once the matter is contained, the investigation and fallout can be determined

Create An Incident Response Plan

1

Create an evaluation and response team

- Members will vary, but the key is to include stakeholders who can ensure prompt action
- Understand your policy and coverage prior to an incident

2

Identify and select external resources

- Screen attorney and forensic panels prior to incident
- Include key contact information of external resources that have been selected

3

Differentiate incidents

- Ransomware, phishing and other unauthorized access, loss or theft of equipment
- Major/minor incidents
- Empower stakeholders to respond quickly

4

Checklist

- Record the date of the incident and steps taken
- Engage external resources ASAP when necessary
- Attempt to take compromised system off-line without impacting forensic integrity

5

Review and update plan

- Simulate an incident and evaluate the effectiveness of your plan
- The plan should not come off the shelf for the first time during an actual incident!

2021 Cyber Security Threats for Higher Education

Ransomware:

- Education sector is the second most frequent target of Ransomware attacks.
- Devices are no longer the target, but rather disabling enterprise-wide systems is the goal.
- Greater impact = Larger Ransom Demands. In 2020, the average cost of a ransomware attack increased to $447,000.
- Rapid growth in "Double-Extortion" Ransomware attacks. These types of attacks now account for nearly half of all reported Ransomware incidents.
- Highly successful nation state hacker groups are offering Ransomware-as-a-service (RaaS), wherein support services are sold to other cyber criminals.

2021 Cyber Security Threats for Higher Education

“Double-Extortion” Ransomware:

- Involves demanding a ransom, not just to decrypt the stolen data, but also to refrain from publicly releasing the stolen data.
- Even when the victim is able to restore the data from backups, they may still be forced to pay a ransom to prevent data exposure.
- Targets of these attacks tend to be entities with fiduciary or regulatory obligations to protect sensitive data.
- Cyber criminals exploit these obligations as well as the threat of reputational harm.

2021 Cyber Security Threats for Higher Education

Botnet targeted Data Breaches:

- Data thefts by nation states are becoming regular occurrences for Institutions of Higher Education.
- University sign-on credential lists are heavily trafficked on the dark web.
- The FBI reports 86% of observed university networks show evidence of inbound botnet targeting.

2021 Cyber Security Threats for Higher Education

Phishing Attacks:

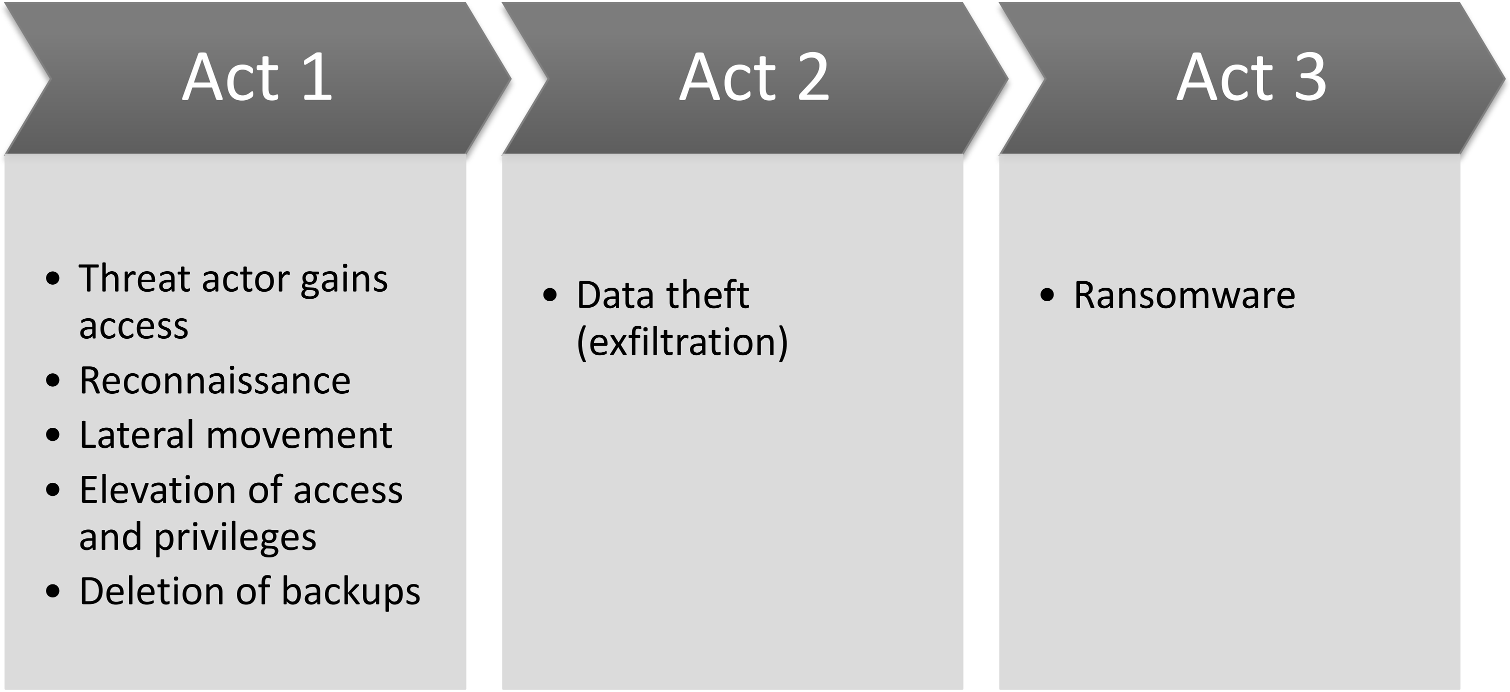
- Industry security groups report a 700% increase in the number of phishing attacks since the beginning of the COVID-19 pandemic.
- The sophistication and quality of Phishing Attacks continue to improve, increasing their success rates.
- Phishing is the most common delivery method for malware used in Ransomware and other forms of data breaches.
- The rapid expansion of remote access brought on by the pandemic has left many employees and students struggling to recognize and address these improved Phishing threats.
- Education and training to address elevated threats has never been more important.

2021 Cyber Security Threats for Higher Education

Business Email Compromise:

- Second fastest growing cyber crime threat behind Ransomware.
- May indicate a breach in your systems, but often results from breaches in vendors’ systems.
- Accounts payable employees must never change payment instructions without first verbally verifying the change request with a previously known point of contact. Telephone call – not email.
- FBI Recovery Asset Teams (RATs) have established streamlined communications with financial institutions in order to assist with the recovery of funds transferred to domestic financial institution accounts under fraudulent pretenses. However, recovery is time sensitive.
- Typically, the FBI must respond within 24-72 hours following the fraudulent transfer in order to recover funds.

Typical Ransomware Lifecyle



Act 1

- Threat actor gains access
- Reconnaissance
- Lateral movement
- Elevation of access and privileges
- Deletion of backups

Act 2

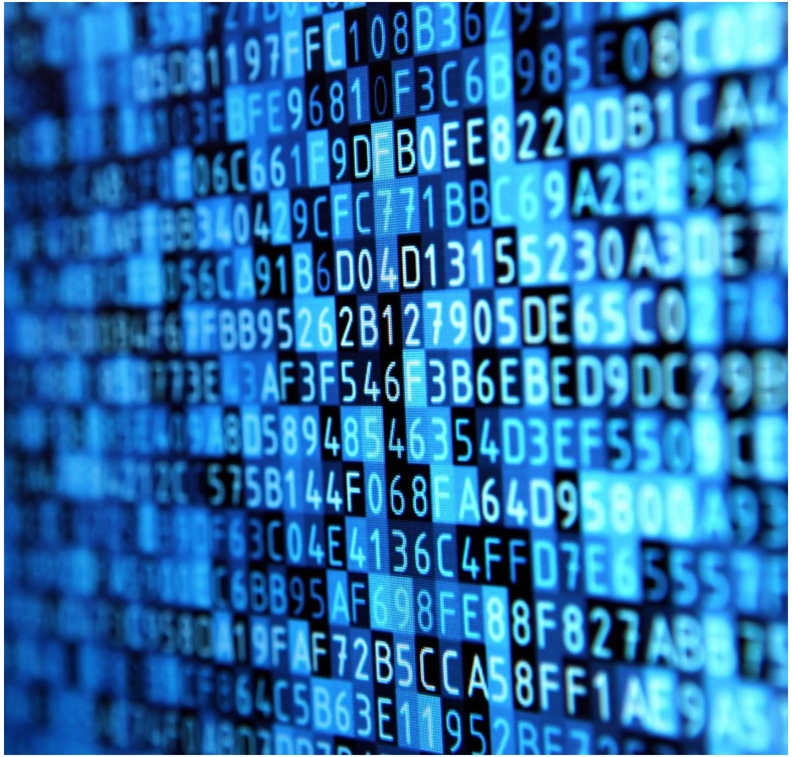
- Data theft (exfiltration)

Act 3

- Ransomware

HUSCH BLACKWELL

Extortion Considerations



- Nature of the information
- Backup
- Threat actor reliability
- Cyber coverage
- Data theft or extortion
- OFAC / Department of Treasury sanctions

HUSCH BLACKWELL

Case Study: The Dark Overlord

- Victim company maintained sensitive data which they had an obligation to secure on a rarely used and outdated server.
- The outdated server remained outwardly connected to the company's network in case the data needed to be accessed. However, the security software was not updated because the server was rarely accessed.
- The Dark Overlord used Botnets deployed to identify and penetrate unsecured servers throughout the Internet.
- Once the victim company's server was penetrated, The Dark Overlord exfiltrated sensitive data and encrypted the server.
- Bitcoin was demanded from the company to prevent the public release of the sensitive data and to obtain the decryption key to allow access to the data.

Case Study: The Dark Overlord

- Company contacted the FBI and was advised not to pay the ransom because The Dark Overlord often demanded follow-up ransom payments. A business decision was made to pay the ransom.

- The Dark Overlord provided the victim company with a contract for the payment of the ransom, which agreed to provide the decryption key and promised to destroy the exfiltrated data following the full payment of the ransom.

- After the ransom was paid, The Dark Overlord sent the victim company a "Customer Satisfaction Survey" and asked them to rate the services provided.

- Approximately one year later, The Dark Overlord re-contacted the victim company, asking that they be a reference for new victims.

- When the victim company refused, The Dark Overlord claimed a violation of the contract and demanded a second ransom under the threat that he would release the sensitive data that he had never destroyed.

Case Study: The Dark Overlord

Lessons Learned:

- It is critical to have an accurate accounting for the status of all outwardly facing servers and the type of data they contain.
- Security software must be updated and maintained on any outwardly facing server.
- Consideration should be given to archiving or at least disconnecting outdated servers and/or the removal of sensitive data from networks when access to that data is rarely necessary.

Other Resources:

FBI InfraGard Program

- Operated by the FBI’s Office of Private Sector.
- Every FBI field office sponsors an InfraGard group.
- Designed to support strategic relationships between private industry, academia, and governmental intelligence agencies for the timely exchange of appropriate threat analysis in order to protect economic and national security.
- To start your partnership, go to www.cisa.gov/cybersecurity-training-exercises or contact your local FBI field office and ask to speak with the Private Sector Coordinator.

Other Resources:

Cybersecurity and Infrastructure Security Agency (CISA) Training and Exercises:

- CISA is an agency of the Department of Homeland Security.
- Offers online topical cybersecurity training webinars. www.cisa.gov/cybersecurity-training-exercises
- Can assist organizations with cybersecurity assessments and tabletop exercises.

December 2020
Announcement From ED

Expect new guidance from the U.S. Department of Education in 2021

- Federal Student Aid announced on December 18, 2020 that it is finalizing the Campus Cybersecurity Program framework:
  - Multi-year phased implementation.
  - Compliance with National Institute of Standards and Technology Special Publication 800–171 Rev. 2.
  - Start with a self-assessment to evaluate readiness to comply.
- ED stated its "intention is to partner … with IHEs … to enhance the resilience and maturity across IHEs by establishing a cybersecurity baseline … and overseeing compliance with NIST 800–171 Rev. 2 and other cybersecurity requirements."
- View the announcement here: https://ifap.ed.gov/electronic-announcements/121820CybersecurityProtectStudentInfoComplianceCUInGLBA

HUSCH BLACKWELL

Questions?

Thank You

HUSCH
BLACKWELL