FSU INCIDENT RESPONSE

October 2016

ITS SECURITY AND PRIVACY OPERATIONS
JOE THOMAS

OVERVIEW INCIDENT RESPONSE

- Security Goals
- Incident Benefits
- University Policies
- General Procedures
- Reporting to FSUPD, HR, FDLE,

INCIDENT RESPONSE

- Phishing - Accounts Compromised
- Compromised File
- Ransomware
- Stolen Property
- Final Comments

WHAT IS AN INCIDENT

A **computer security incident** is any action or activity – accidental or deliberate – that compromises the confidentiality, integrity, or availability of data and information technology resources.

Incidents also include the use of technology for criminal activities such as: fraud, child porn, theft, etc…

Policy violations may also be considered security incidents.

INCIDENT RESPONSE GOALS

- Preserving the confidentiality, integrity and availability of enterprise information assets.
- Minimizing the impact to the university.
- Providing management with sufficient information to decide on appropriate course of action.
- Providing a structured, logical, repeatable, and successful approach.

INCIDENT RESPONSE GOALS (CON'T)

- Increase the efficiency and effectiveness of dealing with an incident
- Reduce the impact to the university from both financial and human resources perspectives.
- Provide evidence that may become significant should legal and liability issues arise.

UNIVERSITY POLICIES

- The university has policies requiring action from IT administrators to report and respond to Security Incidents.
  - 4-OP-H-5 Information Technology Security
  - 4-OP-D-2-G Payment Cards
  - 4-OP-H-12 Information Privacy policy

TEAM LEADERSHIP AND DUTIES

- CISO or Operations Team Lead usually acts as CSIRT Leader
  - Convene the CSIRT (Computer Security Incident Response Team).
  - Select additional support members as necessary for the reported incident.
  - Contact the Chief Information Officer.
  - Conduct meetings of the CSIRT.
  - Ensure meetings are documented.
  - Direct team training on an ongoing basis.
  - Periodically report status of incidents to the CIO.
  - Manage incidents.
  - Ensure Class 2 and Class 3 incidents are documented.
  - Coordinate team incident research and response activities.
  - Conduct a debriefing of lessons learned and report to the CIO.

TEAM EXPERTISE

- Chief Information Office (CIO)
- Chief Auditor Office
- Legal
- Human Resources
- Information Security (CISO or Representative)
- Registrar
- Public Information Officer
- Platform Specialists
- Financial Administrators
- Law Enforcement

ROLE OF THE CSIRT

- The role of the CSIRT is to serve as the first responder to computer security incidents within and to perform vital functions in identifying, mitigating, reviewing and reporting findings to management.

RESPONSIBILITIES OF THE CSIRT

- Classify security incidents.
- Convene upon notification of a reported computer security incident.
- Conduct a preliminary assessment to determine the root cause, source, nature, extent of damage.
- Recommend response to a computer security incident.
- Select additional support members as necessary for the reported incident.
- Maintain confidentiality of information related to incidents.
- Assist with recovery efforts and provide reports to the CIO.
- Document incidents as appropriate. Examples include: lessons learned and recommended actions.
- Report incidents to the Information Security and Privacy Office.
- Maintain awareness of and implement procedures for effective response to computer security incidents.
- Stay current on functional and security operations for the technologies within their area of responsibility.

CLASSIFICATION OF SECURITY INCIDENTS

The CSIRT will classify each incident as a Class 1, Class 2, or Class 3 incident based upon risk severity. The following criteria are used to determine incident classification:

CLASS 1 INCIDENT: LOW SEVERITY

A Class 1 incident is any incident that has a low impact to university information technology resources and is contained within the unit.

- The following criteria define **Class 1** incidents:

1. **Data classification:** Unauthorized disclosure of confidential information has not occurred.
2. **Legal issues:** Lost or stolen hardware that has low monetary value or is not part of a mission critical system.
3. **Business impact:** Incident does not involve mission critical services.
4. **Expanse of service disruption:** Incident is within a single unit.
5. **Threat potential:** Threat to other information technology resources is minimal.
6. **Public interest:** Low potential for public interest.
7. **Policy infraction:** Security policy violations determined by the university.

CLASS 2 INCIDENT: MODERATE SEVERITY

A Class 2 incident is any incident that has a moderate impact to university information technology resources and is contained within the unit.

- The following criteria define **Class 2** incidents:

1. **Data classification:** Unauthorized disclosure of confidential information has not been determined.
2. **Legal issues:** Lost or stolen hardware with high monetary value or that is part of mission critical system.
3. **Business impact:** Incident involves mission critical services.
4. **Expanse of service disruption:** Incident affects multiple units within the university.
5. **Threat potential:** Threat to other university information technology resources is possible.
6. **Public interest:** There is the potential for public interest.
7. **Policy infraction:** Security policy violations determined by the university.

CLASS 3 INCIDENT: HIGH SEVERITY

A Class 3 incident is any incident that has impacted or has the potential to impact other external information technology resources and/or events of public interest.

- The following criteria define **Class 3** incidents:

1. **Data classification:** Unauthorized disclosure of confidential information has occurred outside the university.
2. **Legal issues:** Incident investigation and response is transferred to law enforcement.
3. **Business impact:** Threat to other university information technology resources is high.
4. **Expanse of service disruption:** Disruption is wide spread across the university and/or other entities.
5. **Threat potential:** Incident has potential to become wide spread across the university and/or threatens external, third-party information technology resources.
6. **Public interest:** There is active public interest in the incident.
7. **Policy infraction:** Security policy violations determined by the university.

REPORTING PROCESS

The CSIRT Leader reports and documents all incidents classified or reclassified as a Class 2 or Class 3 incidents. The Report should include the following:

- Executive Summary
- Description of the Incident
- CSIRT Members Participating
- CSIRT Findings
- Conclusions
- Recommendations

GENERAL PROCEDURES

- End users need to communicate computer incidents to unit ISMs.
- Information security managers must immediately notify the FSU IT Security Incident Officer of Incident.
- Payment card data breach – the department head notifies the Security manager who then notifies the Director of Information Security and Privacy of the incident.
- Information security manager notifies the Police Department involving threats to human beings, property, child pornography, or breach of CJIS information.
- External Law enforcement if needed will be referred to the FSUPD who will serve as liaison during the Security Investigations.
- General Counsel, Director of Information Security and Privacy, and FSUPD must be notified when a subpoena is issued.

REPORTING OF IT SECURITY INCIDENTS

- Different departments will become involved in the remediation of an incident.
- Criminal activities should be reported to FSUPD
- Employee misconduct, both criminal and otherwise should be reported to HR.
- Incidents of technical nature from an external source should be reported to the Director Information Security & Privacy.
- All University data should be classified into one of three levels:
  - Level 1 – Protected
  - Level 2 – Private
  - Level 3 – Public

IT SECURITY INCIDENTS REPORTED TO FSUPD

- Electronic transmission / storage of child pornography
- Electronic transmission of threats to the physical safety of human beings or physical assets
- Harassment and other criminal offenses involving user accounts
- Loss or theft of computing device
- Using FSU computing resource in the commission of a fraudulent activity against the university, individual, or outside entity.
- Incidents involving a breach of CJIS information.

IT SECURITY INCIDENTS REPORTED TO HUMAN RESOURCES

- Misuse of FSU IT resources is described in 4-OP-H-5 with some examples below:
  - Commercial use of IT resources that is not pre-approved
  - Advertisement for personal gain in FSU.EDU websites
  - Use of IT resources that interferes with the performance of employee's job
  - Use of IT resources that result in an incremental cost to the University

TYPES OF MAJOR SECURITY INCIDENTS REPORTED TO THE FSU DIRECTOR OF INFORMATION SECURITY AND PRIVACY

- Breach of Personal Identifiable Information (PII).
- Root or system-level attacks on mission critical information system(s) desktop, laptop, tablet, server, storage device, or network infrastructure.
- Compromise of restricted protected service accounts or software installations, for data classified as “Protected” or “Private”.
- Denial of Service attacks that Impair FSU resources.
- Malicious code attacks including malware infections on devices that allow an unauthorized user access to data.

TYPES OF MAJOR SECURITY INCIDENTS REPORTED (CON'T)

- Open mail relay used to forward spam or other unauthorized communications with FSU email system.
- Compromise user logon account credentials.
- Denial of service on individual user accounts
- Other attacks that may constitute a risk to confidentiality, integrity, or availability of university data or systems.

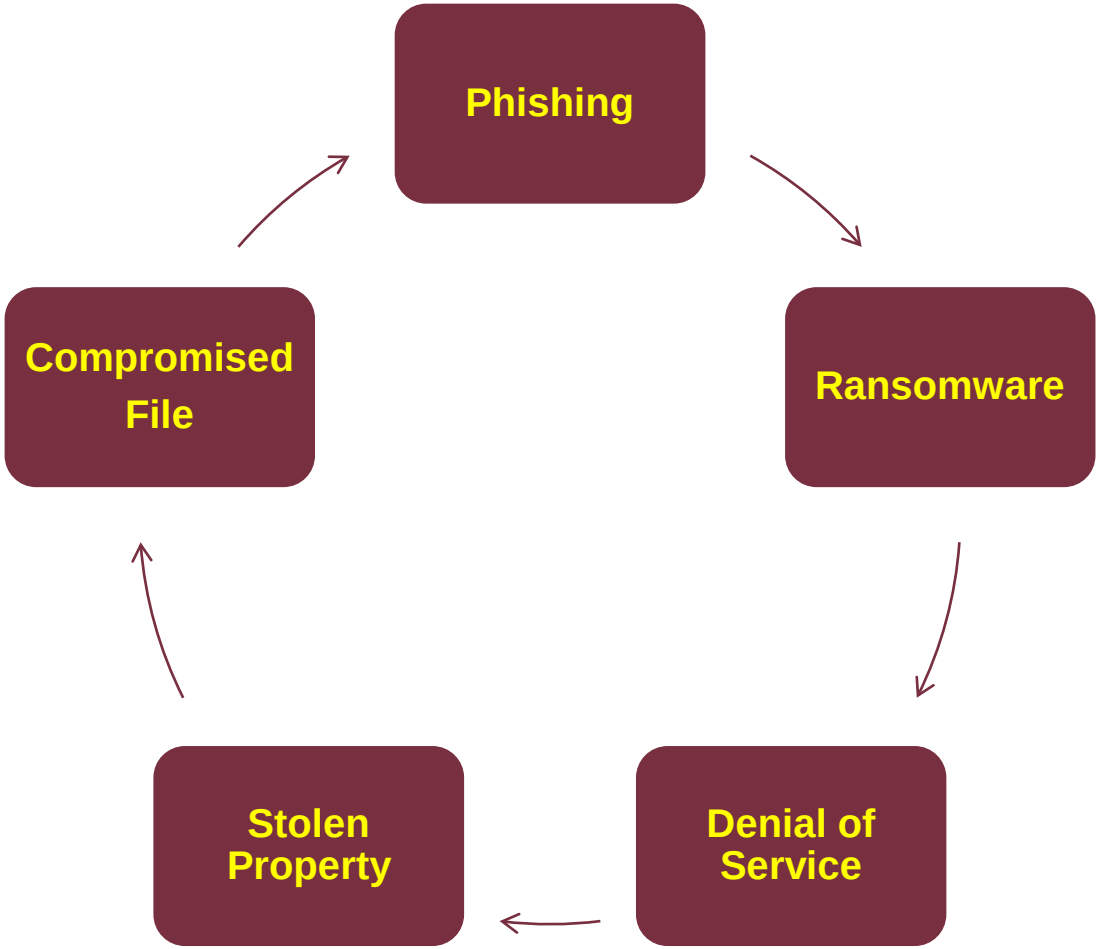
TYPES OF MINOR SECURITY INCIDENTS

- Virus infections on servers and end-points

DEPARTMENTAL RESPONSE TO IT SECURITY INCIDENTS

- Isolation and Protection of Compromised Devices
  - Discontinue use of that device immediately
  - Do not power off the device
  - Disconnect the Network Cable at the Network Jack
  - Isolate computer to prevent any further use.
  - Preserve logs
  - Contact FSUPD, HR, Director of Information Security and Privacy, to assist in investigation
  - If necessary get a backup of the hard drive.
- Identification of Personally Identifiable Data
- Calculation of Campus Unit Fiscal Cost to Remediate

TYPE OF ATTACKS



FINAL COMMENTS

Any Questions?