Security Incident Response Guide

Abstract
This document serves as a guideline for institute personnel in establishing cyber incident response capabilities while outlining how to handle security incidents efficiently and effectively. It provides guidelines for cyber incident handling, including analyzing incident-related data and determining the appropriate course of action as it pertains to each incident.

Georgia Institute of Technology
Security Operations Center
404-385-CYBR (2927)
soc@gatech.edu

IMPORTANT NOTE: If you believe a security incident is an illegal act or life threatening, contact the Georgia Tech Police Department: (404) 894-2500, or Emergency: 911 **immediately.**

Table of Contents

1 Introduction

1.1 Purpose

This document is intended to provide a framework and consistent processes for Georgia Tech's incident response team to reference and develop for a given computer security-related scenario. Georgia Tech Cyber Security strives to build a foundation of support for the Institute's Strategic Plan[1] by managing cyber-risks and creating a secure environment in which the Institute's goals and objectives can be realized. In particular, the information security architecture focuses on assuring the Institute's information confidentiality, data integrity and systems availability.

To achieve these goals, our team has adopted security best practices derived from standardized incident response processes such as those published by the National Institute of Standards and Technology (NIST) Special Publication 800-61[2] and other authorities.

[1] See the *Strategic Plan* at http://www.gatech.edu/about/strategic-plan for more details.

[2] *NIST 800-61 (Computer Security Incident Handling Guide) can be found at https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final*

1.2 Audience

Georgia Tech Cyber Security acts on behalf of the Institute's community and asks for cooperation and assistance from community members as required. This includes students, faculty, staff and any individual using computers and technology devices connected to the Georgia Tech network.

2 Security Incident Scoping

2.1 Definitions

Event

An event is any observable occurrence in a system or network.

Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

Security Incident

A security incident is an event, as determined by Georgia Tech Cyber Security, that violates an applicable law or Institute policy including the violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident could also be established based on the potential for harm to the confidentiality, integrity, or availability of Georgia Tech IT resources.

Examples of security incidents include: unauthorized access to a computer or network; the presence of a malicious application, such as a virus or worm; inappropriate computer usage; probes or reconnaissance scans; or the presence of unknown/unexpected programs.

3 Roles and Responsibilities

Georgia Tech IT Resource users

As outlined in the Institute's Code of Conduct policy[3], all members of the community are expected to escalate any suspected or observed incidents to the appropriate party for further examination. This includes the inherent responsibility toward protection of the Institute's intellectual property.

Computer Support Representative (CSR)

The CSR is assigned to coordinate IT Incident response for an individual business unit, college/school, or department. The CSR is responsible for interacting with Georgia Tech Cyber Security to help contain and eradicate the vulnerability.

[3] See the *Code of* Conduct Policy at http://www.catalog.gatech.edu/rules/19/ for more information.

Security Incident Response Team

To react quickly in the midst of a major incident, Georgia Tech employs an on-call rotational model to provide 24/7 response and support. In particular, the daily schedule tracks the Security Incident Response Commander and Security Operations Handler role as well as backups should a security incident occur.

- **Security Incident Response Commander**
  Coordinates and manages all aspects of a severe incident response effort including documenting all pertinent data, communicating with the appropriate parties, and providing status updates throughout the investigation.

- **Security Operations Handler**
  Communicates with all members of the incident response team to effectively diagnose the security event and initiate a prompt response plan.

Executive Incident Response Committee

During a severe security incident, it may be necessary to convene members of the Executive Incident Response Committee to assist with critical decision-making regarding incident response strategies, communications, and reporting/notification responsibilities.

Key members	*Additional members
• Associate VP and Chief of Staff for the Office of the President • Chief Information Officer (CIO) • Vice President for Legal Affairs and Risk Management • Chief Information Security Officer (CISO) • Office of Legal Affairs • Institute Communications • Internal Audit	• Georgia Tech Police Department • Data Steward(s)[4] • Representatives from affected campus units

*Dependent upon affected data sources

[4] See the *Data Access Policy* at https://policylibrary.gatech.edu/data-access for more details regarding data stewards.

4 Reporting an Incident

4.1 Criminal Activity

If you believe a security incident is an illegal act or life threatening, contact the Georgia Tech Police Department: (404) 894-2500, or Emergency: 911 **immediately.**

If the event falls under the jurisdiction of law enforcement, Georgia Tech reserves the right to direct the reporter to the Georgia Tech Police Department or appropriate law enforcement agencies.

4.2 Abuse

If you suspect that your network, systems, or services may have been negatively impacted by resources at Georgia Tech, please report them to the Georgia Tech Cyber Security via email to: abuse@gatech.edu.

4.3 Reporting Responsibilities by Affiliation

If a Georgia Tech IT Resource user suspects or has observed an event that would satisfy the definition of a security incident, they should report the suspicion immediately to the system administrator or unit technical lead.

Users may also report a suspected security incident directly to the Georgia Tech Cyber Security team for further examination: https://security.gatech.edu/report-incident.

Students

If you are a current Georgia Tech student, you should contact the Technology Support Center (TSC). If you live on-campus, you may also contact Wreck Techs for help.

Faculty & Staff

If you are a Georgia Tech faculty or staff member, you should first try to contact your department's Computer Support Representative (CSR). If your CSR is unavailable, you should contact the Security Operations Center (SOC) at 404.385.CYBR (2927) or soc@gatech.edu.

CSRs and other IT Professionals

If you are a CSR or other IT Professional, you should follow the Security Incident Response Procedure.

Not affiliated

If you are not affiliated with Georgia Tech, please contact the Security Operations Center (SOC) at 404.385.CYBR (2927) or soc@gatech.edu.

4.4 Initial Remediation Steps

Please follow these steps:

1. Stop work on the machine immediately.
2. Do NOT disconnect the network or power cables from the machine(s) so that we can use our approved endpoint software to respond to the incident.
3. Do NOT attempt to investigate or remediate the incident on your own. Wait for instructions from the SOC. There may be compliance requirements, a 'bigger picture', or other 'complications' that you may not know about.
4. Provide us with as much information as you can about the user(s), GT account(s), and/or endpoint(s) that are affected. Some helpful scoping information is outlined in the Security Incident Response Document.
5. Do NOT send sensitive information via email. Provide it over the phone or wait to add it to a Security Incident Response Task (SIT) inside our Security Operations Management Tool.

4.5 Requested Scoping Information

Basic Information

1. Contact information:
    a. Name
    b. Email address
    c. Phone #
2. What's your affiliation to Georgia Tech?
3. Did you work with research data?
    a. If so, what types of research data?
4. Does the machine have an Endpoint agent installed?

User Activity

1. What is the date and time of the incident?
2. What were you doing during the incident?
3. Did you notice any strange things about the computer around that time?
4. Did you notice a change in computer performance?
5. Did you install any software or updates?
6. Did your antivirus software complain or alert?
7. Did you receive any strange emails, or open any unknown attachments?
8. Did you enter credentials (username, password) on any sites?
9. Did you receive any strange Instant Messages?
10. Do you use the computer for non-work-related functions?
    a. If so, what function(s)?
        i. Facebook/social media?
        ii. Internet Radio?
        iii. Email?
        iv. Online Banking?

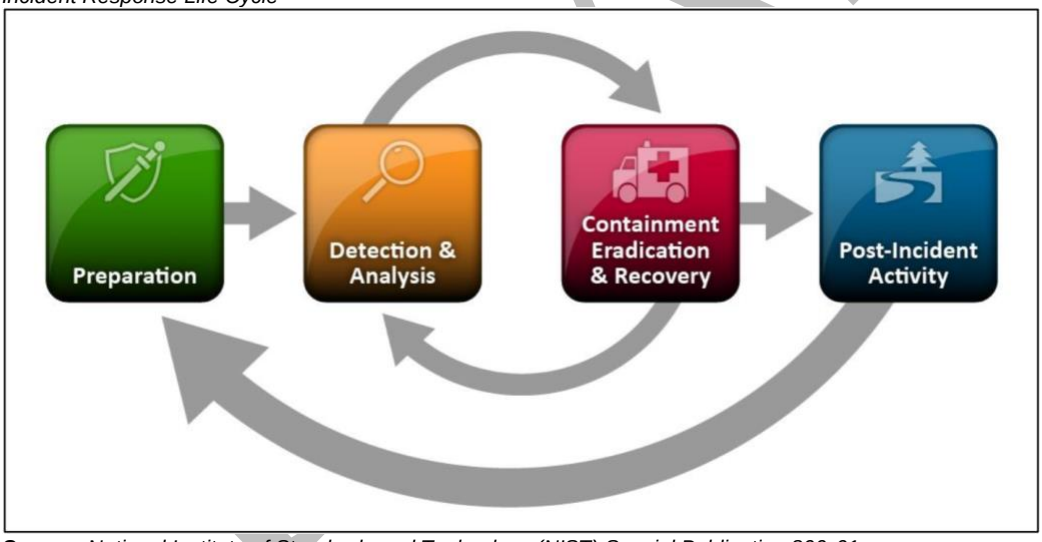
Data Categorization

11. What category of data exists on the host?
12. Does the user work with sensitive or covered PII data?
    a. If yes, what types of sensitive or covered PII data?
13. What files did the user access during the time of the incident?
14. Does the user use university or departmental enterprise systems?
    a. If so, what level of access does the user have?
15. Does the user have access to shared network storage?
16. Are the shared drives automatically mounted?
17. Who else shares the data in those folders?
18. Did the user use encryption on files?

5 Security Incident Response Methodology

As a University System of Georgia (USG) participant, the Institute uses the best practices outlined in *NIST 800-61 (Computer Security Incident Handling Guide*) to adhere to the guidelines set forth in Section 5 of the USG handbook[5]. The incident response lifecycle consists of six phases: preparation, detection, analysis, containment, eradication, and post-incident activity. The figure below illustrates the general lifecycle of these phases; however, many of the phases do occur in parallel. With that said, this document serves as the primary guide for incident preparation

Incident Response Life Cycle



Source: *National Institute of Standards and Technology (NIST) Special Publication 800-61*

[5] *https://www.usg.edu/assets/information_technology_services/documents/IT_Handbook.pdf*

5.1 Protocol for notifying affected individuals

The Executive Incident Response committee is responsible for ensuring notice is sent to individuals when a breach of notice-triggering data elements occurs. Notice-triggering data elements are any data elements that require notification according to Georgia, United States, or international laws. The response committee may choose to send notification when not required by prevailing law. Notification must be sent in a timely manner and no later than is required by prevailing law. Content of notifications as well as methods of notification will be determined individually for each incident, but should generally follow guidelines developed by the Cyber Security team.

6 Prioritization

The Security Incident Response Commander in consultation with the Executive Incident Response Committee will determine if and when an incident should be referred to external authorities.

All incidents determined to be severe incidents must be reported to the University System of Georgia Cyber Security team. The initial report should be submitted through the USG ServiceNow system at https://usg.service-now.com. In addition, upon completion of the incident investigation a final incident report should also be submitted through the USG ServiceNow system.

Severe incidents include the following:

- Incidents involving the loss of Category III or IV data[6]
- Incidents requiring reporting to regulatory bodies (e.g. Department of Education or the European Union)
- Incidents involving the compromise of more than 10 user accounts or more than 10 computers

7 Additional Information

7.1 Contact Information

More information regarding the Security Incident Response Plan and associated procedures, please contact the Security Operations Center (SOC) at 404.385.CYBR (2927) or soc@gatech.edu.

[6] *https://security.gatech.edu/DataCategorization*

7.2 Revision History

Revision Number	Date	Author	Description
1.0	6/25/2018	Andrew Nyhan	Initial Draft
1.1	8/1/2018	Andrew Nyhan	Revised Draft: Roles and Responsibilities
1.2	8/6/2018	Andrew Nyhan	Revised Draft: Requested Scoping Information
1.3	8/14/2018	Andrew Nyhan	Final Draft
1.4	8/24/2018	Jimmy Lummis	Revised Draft: Prioritization
1.5	9/25/2018	Andrew Nyhan	Revised Draft: Formatting

Note: *This document should be reviewed on an annual basis by a manager from Georgia Tech's Security Operations team along with the Chief Information Security Officer to examine how the current procedures satisfy Georgia Tech's needs.*