San Francisco State University
Information Technology Services (ITS)

Incident Management

Description

An **Information Security incident** is an event that violates SF State information security policy and has the potential to compromise the confidentiality, integrity or availability of SF State information technology assets.

Incident management is the structured approach of handling information security events to both limit their impact and prevent them from recurring.

Overview of Incident Management Procedures

Detection
Campus Functional Unit employees identify potential information security events.

Initial Assessment
The local Point of Contact (PoC) conducts a preliminary investigation to screen out false positives. Users are interviewed. Relevant evidence is collected, analyzed, stored, and secured.

Containment
The local PoC quarantines information assets suspected of being compromised.

Escalation
The PoC encounters indications of a breach and requests the involvement of the ITS Security Team.

Investigation
The ITS Security Team evaluates the event to further determine the potential level of risk.

Notification
In the case of a breach involving protected data, stakeholders are informed and updated.

Recovery
Controls are implemented to minimize the impact of the incident, resume normal operation, and prevent recurrence.

Lessons Learnt
The previous incident response will be reviewed. Potential improvements will be identified.

Detection

The incident response cycle begins when a suspicious event is observed. The source can be an individual user or, more commonly, a Point of Contact (**PoC**) who represents a campus functional unit.

News of the event should be submitted in the form of a **Service Desk** ticket (e.g. https://sfsu.service-now.com/). When submitting a ticket for a suspected incident the "Urgency" field should be set to "Security/Health/Safety." The "Assignment Group" field should be set to the campus functional unit that owns the asset in question (e.g. endpoint, network switch, server). The "Short Description" field should begin with the phrase "INFOSEC Incident" followed by the name of the caller and a brief synopsis of the incident. For example:

```
INFOSEC Incident - Jonas Salk Phishing Data Loss
```

A more detailed synopsis should be placed in the "Description" field.

If a breach of sensitive data is suspected, please keep in mind that incidents possess the highest priority. Be prepared to make yourself available to field additional requests by the UTS Security Team.

Initial Assessment

Next, the PoC needs to conduct a preliminary assessment of the event. Guidelines for doing so are provided in the **ITS Incident Response Form**. The results of this initial assessment should be included in the description of the service desk ticket.

A link to the current ITS Incident Response Form can be found under SF State's **Incident Management Policy**.

https://adminfin.sfsu.edu/incident-management

Keep in mind that the underwriter for SF State's cyber insurance policy requires that incidents be formally disclosed *within at most 30 days* of their occurrence. Also, while speed is important it's even more crucial that the PoC provides a narrative that's as complete as possible. A handful of carefully posed, context sensitive, queries can easily replace several days of otherwise unnecessary digging.

In a nutshell, the PoC should strive to answer pertinent information with respect to who, what, when, where, why, and how. The PoC is in a unique position to do so because (as a unit-level liaison) they typically have immediate access to compromised assets, commission them, maintain them, understand normal baselines of system behavior, and maintain tighter links with departmental personnel.

Ultimately the goal is to determine if there has been a breach of Level 1 or Level 2 data. In lieu of a core network service being paralyzed by an attack the ITS Security Team is primarily focused on maintaining the confidentiality and integrity of Level 1 and Level 2 data. Desktop computers can always be rebuilt.

Software can always be reinstalled. But once protected data has been accessed by an intruder it's a whole different ballgame.

Containment

When an information security event has occurred, the first thing the PoC should do after completing their initial assessment is to ensure that a compromised system has been taken off the network and is quarantined in a physically secure area. This will stop malware from receiving command & control messages, safeguard against further data loss, and protect against tampering with evidence.

Escalation

If, and only if, the preliminary investigation produces evidence that Level 1 or Level 2 data has been breached, the issue should be escalated from the PoC to ITS. In the interim the PoC should complete the "In-Depth Synopsis" portion of the Incident Response Form and attach it to the corresponding service desk ticket.

Investigation

The ITS Security Team will re-appraise the POC's submission to further determine the level of risk associated with the incident. Additional evidence may need to be procured by the PoC. High risk incidents may necessitate communication using alternate channels.

Digital artifacts related to the incident should be archived in the Security Team's Box share in the "ITS InfoSec Level 1 Data" directory, under the "s_incidents" sub-folder.

In particular, they should be placed in a sub-folder that adheres to the following naming convention:

```
\yyyymmdd-sequence# issue=TicketNumber UserName Short description
```

For example:

```
\20160330-01 issue=96586 Jose Lema Email Attachment Malware
```

The sequence number exists to help sort incidents in the scenario that multiple security events take place on the same day.

Physical assets that require further examination by ITS must be signed in and released using the paper access logs located in a 3-ring binder on the top shelf of the ITS Security Team's filing cabinet. This filing cabinet is locked with a combination lock. Please see the ISO for the combination.

Keep in mind that an incident could very well end up in court. This means artifacts can quickly turn from dust collectors into legal evidence. Maintaining chain of custody and the integrity are vital.

If a laptop is involved in an incident it may have its drives encrypted. Data recovery keys are usually escrowed by whomever built the system. Key material should be conveyed outside of the ticketing system using an alternate channel. It goes without saying that key material should be stored securely.

The exact nature of the secondary evaluation by the ITS Security Team will vary. It depends upon the nature of the incident. Functional units should attempt to confirm assumptions, eliminate dead-ends, and follow-up on promising leads during their initial triage. Timeline analysis is a good starting point. Bear in mind that the primary goal is to determine if sensitive data has been put at risk and if so to limit the severity of a breach.

Don't hesitate to ask the PoC for additional information if something needs to be clarified. With the exception of cases involving sensitive meta-data, the entire process should be archived in the ticketing system and related digital evidence should be stored in Box.

Notification

In the event of a data breach entailing **protected information** (e.g. Level 1 or Level 2 data) the campus Information Security Officer will need to issue formal notices to other groups. The specifics depend on both the type of data and the number of records that have been disclosed. The details are spelled out in CSU policy. See the "CSU Information Security Policy and Standards" document maintained in the CSU's policy library. In particular, the section entitled "K. ISO Domain 16: Incident Management Standard," subsection 6.

Recovery

Having assessed the severity of the incident, SF State is in a position to respond with appropriate controls. The type of response and the priority assigned to the incident will vary according to the nature of the incident.

For example, catastrophic scenarios may entail a formal disaster recovery process where a backup site is brought online, and external resources are conscribed, to restore core business operations. Less severe cases may simply involve migrating a user to a temporary system while their compromised machine is quarantined for further investigation.

Regardless of the controls that are deployed the underlying goal is to minimize the impact of the incident, resume normal operation, and prevent recurrence.

Once an incident has been dealt with successfully, its ticket status should be marked as "Resolved" and notification should be sent out to any internal and external groups who have become involved over the course of the response cycle.

Lessons Learnt

Once recovery has been achieved a post-mortem review may be conducted. The requirement for a review depends upon the extent of business impact and the judgement of the ISO. This review should be recorded and archived. If need be, a formal document can be issued to the ITS Director and whomever else the ISO deems relevant.

The goal of the review is to evaluate the effectiveness of existing policies, procedures, and controls. To derive insights from an incident that can be used to improve SF State's information security profile. Such an appraisal may identify new threats, vulnerabilities, and corresponding controls.

Revision History

Version	Revision Date	Revised By	Summary of Changes	Sections Revised
1.0	2016-05-04	Blunden	Original version	All
2.0	2019-01-10	Blunden	Review of Process	-
3.0	2019-01-10	Blunden	Service-Now adjustments	
4.0	2020-01-05	Blunden	Contact Information	Notification
5.0	2023-06-20	Blunden	Revision	All