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 in such a way that it has the potential to seriously compromise the confidentiality, integrity or availability of SF State information technology assets.

Incident management is a structured approach to handling information security events in a manner that both limits their negative impact and helps to prevent them from arising in the future.

Overview of Incident Management Procedures

Detection
Unit employees identify potential information security events. Sources of information may vary.

Initial Assessment
The local Point of Contact executes a preliminary investigation per the ITS Incident Response Form to screen out false positives. Users are interviewed. Relevant evidence is collected, analyzed, and secured.

Containment
The local Point of Contact isolates information assets that are suspected of being compromised.

Escalation
If the local point of contact suspects that the identified event is actually an information security incident they'll request the involvement of the ITS Security Team.

Investigation
The ITS Security Team will evaluate the submission to further determine the level of risk associated with the incident. Additional evidence may be collected, analyzed, and secured.

Notification
In the event of a breach of protected data the appropriate internal and external parties should be informed and updated as necessary.

Recovery
Suitable controls should be implemented to minimize the impact of the incident, resume normal operation, and prevent recurrence.

Lessons Learnt
The incident response will be reviewed. Potential improvements will be identified. ITS will update response procedures and the campus risk profile as necessary.

Detection

The incident response cycle begins when a suspicious event is observed. The source tends to be either an individual user or, more commonly, a point of contact (**PoC**) who represents a local I.T. help desk (AT, CHSS, etc.) or an ITS team.

Regardless of the source, news of the event should be submitted to the ITS Security Team in the form of a **Service Desk** ticket (e.g. https://sfsu.service-now.edu/). 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 "ITS Security L2." 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 Malicious Email Attachment
```

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

Of the various types of issues that ITS Security handles, incidents have the highest priority. This means dropping everything to address them until a suitable stopping point has been achieved.

Initial Assessment

After an information security event has been detected 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 submitted to ITS. If it's missing you should ask the PoC to complete one.

The current ITS Incident Response Form is available at:

http://tech.sfsu.edu/content/sfsuincidentreport

Keep in mind that the underwriter for SF State's cyber insurance policy (Alliant) requires that incidents be formally disclosed *within at most 30 days* of their occurrence. Yet while speed is important it's even more crucial that the PoC provides a chronological 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 and tighter links with departmental personnel.

Ultimately the goal is to determine if there has been a breach of Level1/Level2 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/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 been alleged, the first thing the PoC should do after completing the 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

At this point the issue has officially been escalated from the PoC to ITS. The ITS Security Team should review the PoC's assessment and decide if they agree with the PoC's conclusion or not. In the interim the PoC should complete the "In-Depth Synopsis" portion of the Incident Response Form and attach it to the service desk ticket.

Investigation

The ITS Security Team will evaluate the POC's submission to further determine the level of risk associated with the incident. Additional evidence may need to be collected, analyzed, and stored securely. High risk incidents may necessitate communication using alternate channels.

Digital artifacts related to the incident should be stored on the ITS share in the following folder:

```
\\s.ad.sfsu.edu\ITS\infosec\s_incidents\Incidents SFSU 20yy
```

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. Hence maintaining chain of custody and the integrity of forensic data is an overriding necessity.

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.

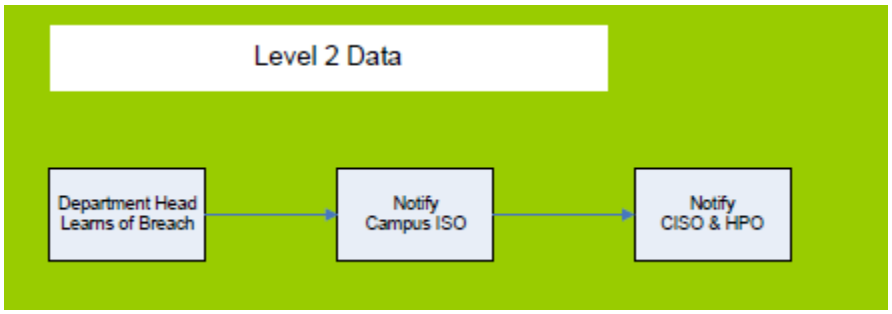
The exact nature of the secondary investigation conducted by the ITS Security Team will vary. It depends upon the nature of the incident. Try to confirm assumptions, eliminate dead-ends, and follow-up on promising leads. Timeline analysis is a good starting point. Bear in mind that the primary goal is to determine if sensitive data has been put at risk and if so to limit the negative impact.

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 the Incidents directory on the ITS network share.

Notification

In the event of a data breach entailing protected information (e.g. Level 1 or Level 2 data) you'll need to issue a formal report to other groups. The specifics depend on both the type of data and the number of records that have been disclosed.

For example, if an incident is limited strictly to Level 2 data the campus ISO will need to notify the CSU's Chief ISO in Long Beach. The basic report structure is as follows:

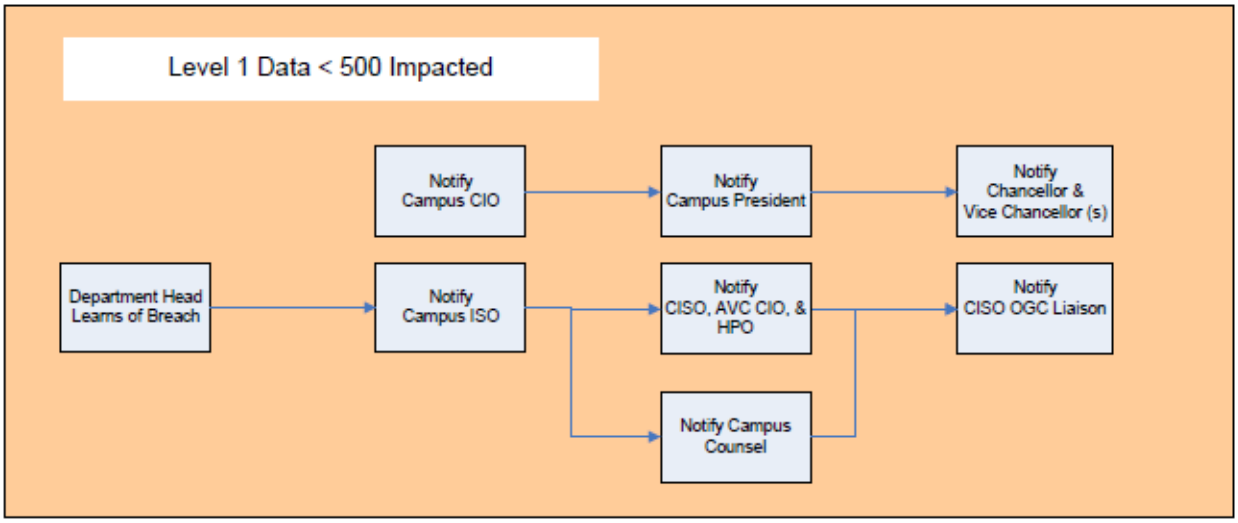


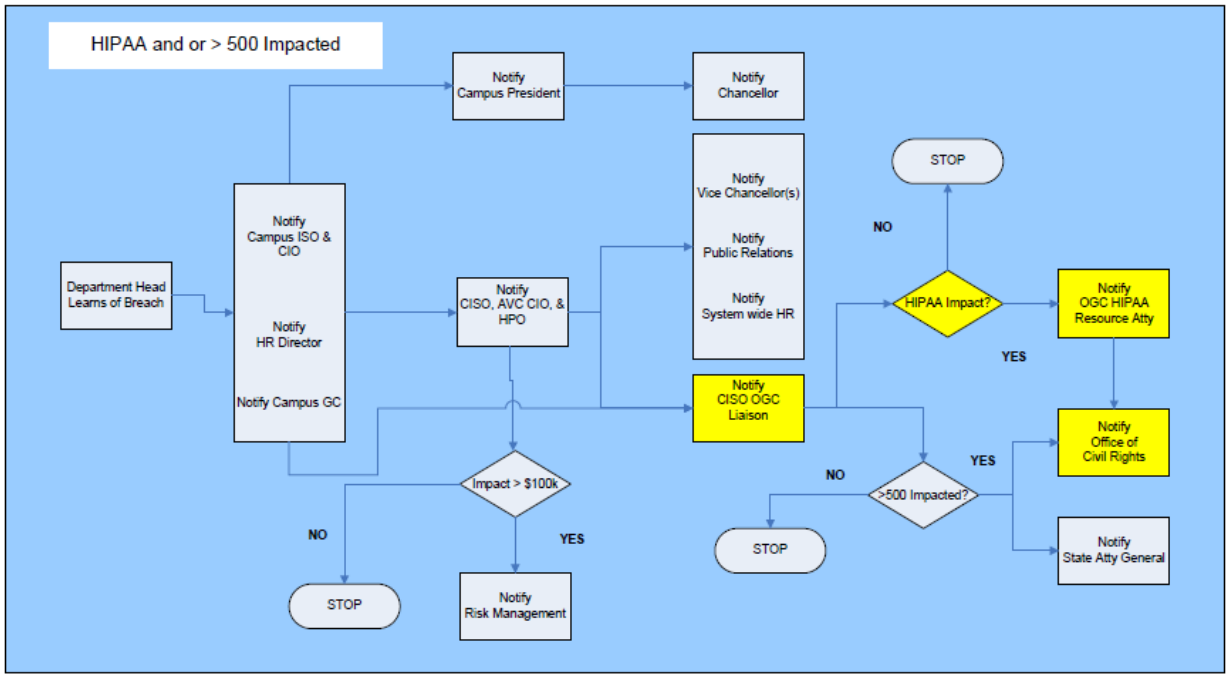
Having said that, the ISO's contact information is as follows:

ADM 123
(415) 338-7013
mmorshed@sfsu.edu

If the ISO isn't available, you should contact the acting CIO.

In the event of a Level 1 data breach, things get a little more involved. In this case two distinct channels of communication need to be established. One channel goes to directly to the Chancellor's Office in Long Beach and the other proceeds internally to the office of the SF State President. Looking at the flow charts below it's clear that a breach involving more than 500 records is a more serious affair and therefore involves more people. This type of breach is a full-blown crisis.





From the perspective of a lowly ITS security analyst in the trenches both flow charts encapsulate the same basic logic: immediately contact the ISO, or their stand-in, so that they can launch internal notification at SF State and then concurrently begin a similar notification process with the Chancellor's

Office in Long Beach. They central idea to this process is to make sure that no one at SF State receives a surprise call from the Chancellors Office.

In other words, the operating maxims are as follows: no one likes to be blind-sided, especially the university President. But at the same time no one likes false alarms so be careful when you decide to crank up the siren. Have your facts laid out, double-checked, with a concise summary to present to the higher-ups. Once the process begins you can expect to be on call for several days.

Recovery

Having assessed the severity of the incident the ITS Security Team is in a position to respond with appropriate controls. The type of response conducted 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. More pedestrian 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 that underlying goal is the same: to minimize the impact of the incident, resume normal operation, and prevent recurrence. In addition, measures implemented by the Security Team should be recorded in the incident's help desk ticket.

Legal questions during this phase should be directed to the SF State University Council:

Alison Kleaver
akleaver@calstate.edu
(562) 951-4500

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.

When a compromised system is finally returned to its originating unit it should be processed to eliminate remaining threats. The option which prevents the least degree of risk is to flatten the impacted system, reformat the drive, and rebuild it from a pristine image.

Lessons Learnt

Once recovery has been achieved a post-mortem review can 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. Resulting updates to SF State security policies, standards, or guidelines should be transmitted to users through the existing Security Training and Awareness program.

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