# Responding to Incidents

## Introduction

Dealing with incidents once they have occurred is an important part in mitigating the effect of overall risks within an organisation. Champions within civil society groups must deal with everything from lost phones to sophisticated government attackers. This module highlights some services that can be utilised in the event of incidents occurring and also some useful references that can be used for helping champions prepare and respond to incidents.

## Learning Goals

- Understand commons information security problems affecting civil society groups
- Understand frameworks for dealing with information security incidents
- Explain first line response procedures for potential incidents
- Describe the different offerings of various groups who can help - timescale, resources etc.
- Understand what is needed for forensic analysis at a later point

## Assessment Goals

Add incident response plan for major information security risks to the assessment

## Recommend Preparations

N/A

## Suggested Time

45 Minutes

## Notes

N/A

## Activity

**Incident Simulations**
Break participants into two groups. Each will be given a different scenario.

***Scenario One*** A hacking group hostile to your organisation has sent out a tweet with screenshots of a few sensitive internal files containing information on the pay and personal details of a few of the staff. They say this is just the beginning and they have access to lots more. What will you do?

***Scenario Two*** A colleague of yours in traveling for the past week in a high-risk country to gather sensitive evidence from witnesses about human rights abuses in a country. They recently called you to say they were arrested by intelligence officials of the local government on the way to the airport. They could not say anymore. You can assume they have all of their sensitive information and devices with them. What will you do?

Trainers Note: It is often most productive to assign specific roles to individuals within the groups themselves, in order to stimulate discussion and also to ensure that a variety of viewpoints are being represented. Experience shows that people often underestimated who is involved in responding to incidents and how much of their time and resources are necessary. For example, in scenario two, some of the roles could include people such as:

- IT Champion
- Organisational Director
- Social Media or Public Relations Manager
- Family of the staff member
- Individual who provided testimony and is now concerned
- Finance team
- Embassy representative of the person detained
- Government representative of the person detained or of the country which detained the individual
- Google/Facebook/Cloud host Representative (if the group decides they want to have )

## Discussion

- What lessons did we learn from the scenarios?
- What did we think we handled well?
- What did we think we did not handle well?
- How could we make ourselves better prepared to deal with incidents?
- Who might be involved in responding to incidents in our own organisations?
- What sort of incidents do we think this process would be useful in helping us address?

## Inputs

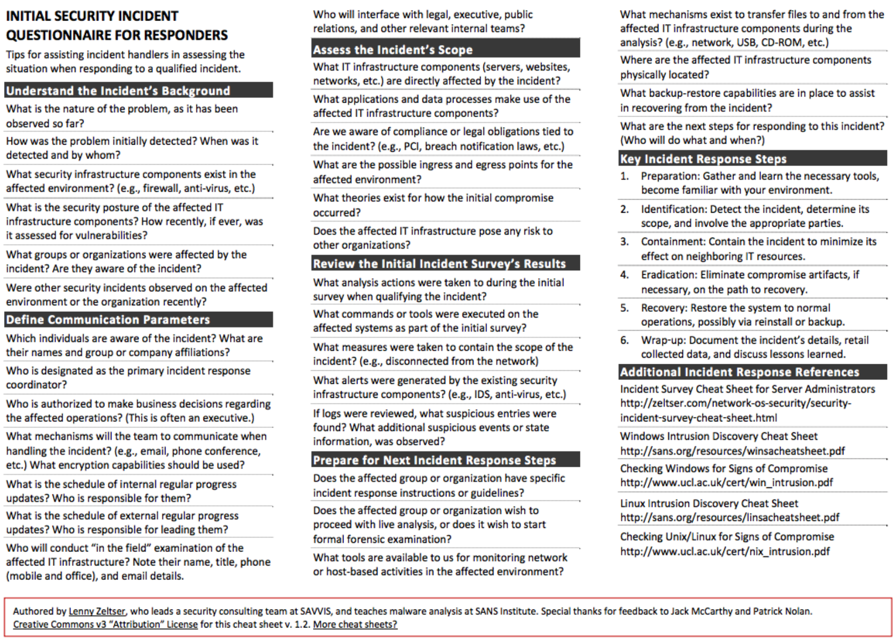
There are a number of sources of support for civil society groups when they experience a digital security incident.

These include organisations such as:

- Access Now
- Security without Borders
- Digital Security First Aid Kit
- Security First

## Deepening

Participants will now break into groups to conduct discussions where they review best practice documentation on how to respond to incidents. The should examine each document and discuss points such as:
-How useful is the document?
-Do the understand everything I would need to be able to use it correctly?
-What would the need to add, remove or modify to make it useful for themselves?



**INITIAL SECURITY INCIDENT QUESTIONNAIRE FOR RESPONDERS**

Tips for assisting incident handlers in assessing the situation when responding to a qualified incident.

### Understand the Incident's Background

What is the nature of the problem, as it has been observed so far?

How was the problem initially detected? When was it detected and by whom?

What security infrastructure components exist in the affected environment? (e.g., firewall, anti-virus, etc.)

What is the security posture of the affected IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?

What groups or organizations were affected by the incident? Are they aware of the incident?

Were other security incidents observed on the affected environment or the organization recently?

### Define Communication Parameters

Which individuals are aware of the incident? What are their names and group or company affiliations?

Who is designated as the primary incident response coordinator?

Who is authorized to make business decisions regarding the affected operations? (This is often an executive.)

What mechanisms will the team to communicate when handling the incident? (e.g., email, phone conference, etc.) What encryption capabilities should be used?

What is the schedule of internal regular progress updates? Who is responsible for them?

What is the schedule of external regular progress updates? Who is responsible for leading them?

Who will conduct "in the field" examination of the affected IT infrastructure? Note their name, title, phone (mobile and office), and email details.

Who will interface with legal, executive, public relations, and other relevant internal teams?

### Assess the Incident's Scope

What IT infrastructure components (servers, websites, networks, etc.) are directly affected by the incident?

What applications and data processes make use of the affected IT infrastructure components?

Are we aware of compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)

What are the possible ingress and egress points for the affected environment?

What theories exist for how the initial compromise occurred?

Does the affected IT infrastructure pose any risk to other organizations?

### Review the Initial Incident Survey's Results

What analysis actions were taken to during the initial survey when qualifying the incident?

What commands or tools were executed on the affected systems as part of the initial survey?

What measures were taken to contain the scope of the incident? (e.g., disconnected from the network)

What alerts were generated by the existing security infrastructure components? (e.g., IDS, anti-virus, etc.)

If logs were reviewed, what suspicious entries were found? What additional suspicious events or state information, was observed?

### Prepare for Next Incident Response Steps

Does the affected group or organization have specific incident response instructions or guidelines?

Does the affected group or organization wish to proceed with live analysis, or does it wish to start formal forensic examination?

What tools are available to us for monitoring network or host-based activities in the affected environment?

What mechanisms exist to transfer files to and from the affected IT infrastructure components during the analysis? (e.g., network, USB, CD-ROM, etc.)

Where are the affected IT infrastructure components physically located?

What backup-restore capabilities are in place to assist in recovering from the incident?

What are the next steps for responding to this incident? (Who will do what and when?)

### Key Incident Response Steps

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.
2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3. Containment: Contain the incident to minimize its effect on neighboring IT resources.
4. Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6. Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

### Additional Incident Response References

Incident Survey Cheat Sheet for Server Administrators
http://zeltser.com/network-os-security/security-incident-survey-cheat-sheet.html

Windows Intrusion Discovery Cheat Sheet
http://sans.org/resources/winsacheatsheet.pdf

Checking Windows for Signs of Compromise
http://www.ucl.ac.uk/cert/win_intrusion.pdf

Linux Intrusion Discovery Cheat Sheet
http://sans.org/resources/linsacheatsheet.pdf

Checking Unix/Linux for Signs of Compromise
http://www.ucl.ac.uk/cert/nix_intrusion.pdf

Authored by Lenny Zeltser, who leads a security consulting team at SAVVIS, and teaches malware analysis at SANS Institute. Special thanks for feedback to Jack McCarthy and Patrick Nolan.
Creative Commons v3 "Attribution" License for this cheat sheet v. 1.2. More cheat sheets?

Figure 1: Zelstser Incidnet Questionnaire

Examples of basic incident reponse documentation include:

- Lenny Zelstser's "Initial Security Incident Questionnaire for Responders - example above
- SANS Incident Handler's Handbook
- OWASP Top 10 Considerations For Incident Response
- OWASP Anti-Ransomware Guide

## Synthesis

Participants should turn to their assessment documentation and consider how their organisation deals with the subject matter covered in this module. Where necessary they should ask questions and work with other participants to identify any:

- Issues they have found that affect their organisations
- Possible solutions they have learned
- Possible difficulties they may face in implementation (ideally using the time and experience of trainers and other participants)
- Things would need to overcome these difficulties
- Connections to other organisations or individuals that would help them
- Timeline, resources and costs for implementation

This should be noted in their assessment, for future use.

In line with keeping this curriculum as an updated community tool, we would also ask that participants provide comments, feedback and new ideas for this module on the project website and/or Github!

TODO
-Conduct a series of short scenarios games based on the most likely threats risks faced by the participants in the training. -Emphasis the need for threat information sharing. Suggest methods for doing that (procedural - NDA etc.) and technical (IOC, MISP etc.)

## Resources