A Very Important Incident

## Date: 2017-04-01

## Handler: George P. Burdell

# Executive Summary

This is a summary of what happened. It should be written in standard paragraph form. It should likely have 3-6 sentences. To the extent possible use words of no more than three syllables and sentences of no more than 20 words. Try to explain in words that a non-technical person would understand. This should contain as much information as is necessary to convey what happened to executive leadership, but not more. For instance:

On 2017-03-27 at 10:00AM department X notified the SOC about unusual behavior on one of their servers, server-a. On investigation Information Security found that a malware strain known as BadStuff was present on the system. While BadStuff is known to steal credentials investigations into network traffic leads Information Security to have a high degree of confidence that no actual information was breached before the system was shut down. On 2017-03-28 at 09:00AM department X was authorized to reimage the system and resume normal operations.

Unless the Incident is specifically about an account, accounts should likely not be mentioned here. In addition, please note that the notifying entity was a department and not a person. It’s best to use department names and titles, and not the names of individuals involved in the incident or the investigation.

# Background

Sections from here to, but not including, Lessons Learned may be combined if the incident is small. This includes background on what systems, services, and accounts were involved and what they normally do. It also includes how and when Cyber Security was notified of the incident.

# Findings

This is an optional outline of what happened. It is not a restatement of your investigative log. It is intended to convey to management and technical leadership what we believe happened to the system. It frequently makes sense to present this chronologically, though it does not have to be if some other ordering conveys the information more succinctly. In some cases, a bulleted timeline may work, but frequently paragraphs work better. If you choose to use chronological paragraphs the time, as closely as you can derive it, should be close to the beginning of each paragraph.

# Actions Taken

This is a statement of what actions were taken in response to the incident. This informs management of how the incident has been contained and what effort has been taken to restore service.

# Financial Impact

|  |  |
| --- | --- |
| Item | Cost |
| This section optional, but should be a table | $10 |
| It is highly recommended if seeking criminal charges or if impact is significant | $100,000 |
| It should include both direct costs and investigative costs1 | $25,000 |
| Labor2 | $50,000 |
| Total | $175,010 |

1. Include footnotes to document how costs were calculated. For example, 25 investigative hours x $1,000 per investigative hour = $25,000
2. Labor cost should always be included. Your organization may include a standard way to compute this, but if not you should assume that all time spent on the incident multiplied by the employee’s hourly rate is attributable to the incident.

# Lessons Learned

This section is not optional.

## Successes

* Outline where things worked
* This includes controls that helped you find it
* Make sure you include other departments who performed well

## Opportunities for Improvement

**Issue:** An item that could have been better including security controls as well as investigative procedures

**Recommendation:** How it could be improved. It helps to talk this through with other parts of the organization if it affects them.

**Action Item Owner:** Who should be responsible for fixing it