INFORMATION SECURITY & PRIVACY DOCUMENT

Incident Response Plan

Created May 29th, 2017
Last Modified Jan 29th, 2018
By Mark LeVell

Incident Response Plan Introduction and Commentary

In accordance with industry 'best practices' and to comply with numerous compliance regulations, 4Thought Marketing has implemented various procedures, policies and guidelines in order to protect the confidentiality, integrity and availability (CIA) of their critical client data and computing resources. This Incident Response Plan is one such procedural document intended to prepare our team to address such sacurity incidents. Regular testing and refinement of this plan will help 4Thought Marketing prepare for adverse security incidents and ultimately help us to manage and minimize risk.

Note that it may be appropriate to use this plan in conjunction with 4Thought Marketing's Disaster Recovery Plan which can be found at <Path Redacted for Public> for internal use or as a link at www.4ThoughtMarketing.com/Trust.

It is anticipated that as new technologies and new requirements are introduced this document will need to be modified and should be reviewed at least annually. This function will be performed by members of the security team at the direction of the Chief Security Officer.

Note that at 4Thought Marketing our "DPO" or Data Privacy Officer (which is a requirement of GDPR) is the same role/person as our Security Officer.

Revision History

Version	Who	Date	What
1.0	Mark LeVell	5/28/2017	First Release
Notes			
1.1	Mark LeVell	1/29/2018	Minor Mods due to GDPR
Notes			

Notes	

Incident Response Plan Overview

There are many different security incidents that can occur with assorted severity levels and not all incidents will require focus on each step. However it is important to be prepared and understand that typically different phases exist in responding to an incident, and the goals and objectives of each phase. The different phases of a security incident response plan at 4Thought Marketing are as follows:

- Prepare
- Identify
- Contain
- Eradicate
- Recover
- Review
- Notification

Prepare

In preparing for security incidents several items need to be addressed.

- Incident handling team should include our security officer, system analysts from our TMAS team, and depending on the type of data lost, human resources personnel
- End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
- Contact information is included as an appendix to this document and should be available in hard copy for:
    - personnel that might assist in handling an incident
    - key partners who may need to be notified
    - business owners to make key business decisions
    - outside support analysts with security expertise
- Backups should be taken and tested!
- Supplies to assist the team in the event of an incident (sometimes referred to a jump bag)
    - An empty notebook (Thorough documentation should be done throughout an incident to include hand written notes in a fresh notebook.)
    - Boot CDs to analyze hard drives and recover passwords
    - Petty cash (food, cabs, batteries as needed)

Identify

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Best practices suggests to declare that an incident has occurred when security officers' sense that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved, to save all key system files or records such as log files and start detailed documentation as soon as possible.

Ultimately business owners need to be involved in many security incidents to decide what are the goals in handling a particular incident, such as immediate business recovery or forensic examination.

Contain

Following basic procedures can contain many incidents. Specific procedures will frequently depend on the nature of the incident, as well as the direction of the business owner. Remember that a compromised machine might not present valid data! Basic steps to consider include:

- Obtain and analyze as much system information as possible including key files and possibly a backup of the compromised machine for later forensic analysis.
- Powering off a machine might lose data and evidence. Preferably disconnecting the LAN cable facilitates containment and forensic activity. (Putting the computer on a separate network with a network analyzer might help analyzing network activity)
- If one machine has been exploited others might be vulnerable. Actions that might need to be taken on a large scale might include:
    - Download security patches from vendors
    - Update antivirus signatures
    - Close firewall ports
    - Disable compromised accounts
    - Run vulnerability analyzers to see where other vulnerable hosts are
    - Change passwords as appropriate

Eradicate

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Boot CDs should be used to access data on compromised machines. (Rootkits installed on compromised machines might affect basic system level utilities and discourage use of a compromised host)
- If machines OS has been compromised it needs to be rebuilt using hardened machines on appropriate platforms
- Test any backups prior to restore and monitor for a new incident.
- Document everything.

Recover

The recovery phase's goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

- Retest the system preferably with a variety of end users.
- Consider timing of the return to production.
- Discuss customer notification and their concerns
- Discuss media handling issues
- Continue to monitor for security incidents

Review

This phase is to allow 4Thought Marketing to better handle future security incidents. A final report should be written describing the incident and how it was handled using the Incident reporting form. Suggestions for handling future incidents and reworking this document should be included in this report.

Notification

Notification of breaches is limited to breaches of PII (Personally Identifiable Information) unless such information is encrypted with a reasonable expectation that such encryption will not be breached. A breach of PII shall be treated as "discovered" as of the first day on which such breach is known to the organization.

Notification does not necessarily occur at the end of the above processes but rather will typically occur in parallel with the above events and at many stages depending on who is being notified and geographical impact.

- **Internal Notification**
  - This occurs typically as soon as breach awareness or even possible breach awareness occurs.
- **Impacted Customer & Partner Notification**
  - Within 4 business hours of discovery or sooner if possible, upon confirmation of impact to a customer or partner
  - If Individuals of customers are impacted, it is the sole responsibility of the customer to notify those individuals
- **EU DPO Notification**
  - Announcement to Data Privacy Authorities of GDPR Countries
    - Required within 72 hours of discovery to comply with GDPR Article 33

- **Notification of Individuals**
  - Notification to EU Citizens shall comply with Article 34 of GDPR
  - Announcements to other individuals based on geographical legal requirements
  - (As previously mentioned) If Individuals of customers are impacted, it is the sole responsibility of the customer to notify those individuals
- **General / Public Announcement**
  - As and when determined appropriate by marketing, customers, and ETeam.

Notification Content:

The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the PII fields that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved), if known;
- Any steps the Customer should take to protect Customer data from potential harm resulting from the breach.
- A brief description of what 4Thought is doing to investigate the breach, to mitigate harm to individuals and Customers, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which may include our 800 number, an e-mail address, a web site, or postal address.

Notification Methods:

4Thought Customers will be notified via email or phone or both within the timeframe for reporting breaches, as outlined above.

Incident Logging

Incident logging shall occur within the standard applicable security logs and the standards applicable and documented for those logs shall apply.

Roles and Responsibilities

Task/Responsibility	Assigned To:	Notes
Identify & Contain Breach	Head of TMAS	
Communicate Breach	CSO & CEO	For EU as per GDPR (Within 72 Hours to DPO as per Article 33, and to Data Subjects as per Article 34)
Eradicate Breach	Head of TMAS	
Recover & Restore	Resources assigned by Head of TMAS	
Review	Security Team (CEO, CSO, Head of TMAS)	
Document Post Mortem	CSO	
Notification -Internal	CSO	
Notification -External	Head of Mktg	

Contact Information for Incident Response Roles

Role	Contact Information
CEO	<Redacted for Public Version>
CSO*	<Redacted for Public Version>
Head of TMAS	<Redacted for Public Version>
Head of Marketing	<Redacted for Public Version>

*Includes GDPR mandated role of DPO

<End Incident Response Plan of 4Thought Marketing>