DATA BREACH INCIDENT RESPONSE PLAN

Incident Response Team Members

- Executive manager
- IT department manager
- Salles department manager

Incident Response Team Roles and Responsibilities

IT DEPARTMENT MANAGER

- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice, as needed
- Contacts members of the Incident Response Team, as needed
- Determines which Incident Response Team members play an active role in an investigation
- Escalates to executive management, as appropriate
- Monitors progress of an investigation
- Ensures proper evidence gathering, chain of custody, and preservation practices are in place
- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Monitors for signs of a firewall breach
- Contacts external Internet service provider for assistance in handling an incident / including AWS server team/
- Takes necessary action to block traffic from a suspected intruder
- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity
- Monitors business applications and services for signs of attack

- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Technology Operations Center with any information relating to a suspected breach
- Collects pertinent information regarding the incident
- Reviews systems to ensure compliance with information security policies and controls
- Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
- Reports any system control gaps to management for corrective action

Incident Response Team Notification

The Technology Operations Center will be the central point of contact for reporting computer incidents.

All computer security incidents must be reported to the Executive Manager.

All security incidents connected with personal data leaks must be reported to the affected sites. / Amazon, PayPal, eBay, Banks, etc./

Incident Types

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of Personal Information
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak

Personal Information

Personal information is information that is, or can be, about or related to an identifiable individual. Most information an organization collects about an individual is likely to be considered personal information if it can be linked to an individual or used to directly or indirectly identify an individual.

For our purposes, personal information is defined as an individual's first name (or first initial) and last name used in combination with any of the following data:

- Home address
- Telephone number
- E-mail

Breach of Personal Information: Overview

This Incident Response Plan outlines the steps our organization will take upon discovery of unauthorized access to an individual's personal information which could result in harm or inconvenience to the individual (e.g., fraud or identity theft). The individual can be either a customer or employee of our organization.

Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by Tradefy. Good faith acquisition of personal information by an employee or agent of our company for business purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

Requirements

When Notification is Required

The following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.
- An intruder has broken into database(s) that contain personal information on an individual.
- A department or unit has not properly disposed of records containing personal information on an individual.
- A third-party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

Breach of Personal Information: Incident Response

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

Technology Operations Center

The TOC will serve as a central point of contact for reporting any suspected or confirmed breach of an individual's personal information.

The TOC is responsible for performing the following actions.

1. After documenting the facts presented by the reporter and verifying that a privacy breach or suspected privacy breach occurred, the TOC will open a Priority Incident Request. This will begin an escalation process to immediately notify the Executive Manager.

2. The TOC will notify the primary and secondary Information Security Office contacts. The TOC will advise that a breach or suspected breach of an individual's personal information occurred. After the Information Security Office analyzes the facts and confirms that the incident warrants incident response team activation, the Incident Request will be updated to indicate "Incident Response Team Activation – Critical Security Problem."

IT Department Manager (ITDM)

The ITDM is responsible for performing the following actions.

1. Once notified by the TOC, performs a preliminary analysis to determine the nature and scope of the incident.

2. Informs that a possible privacy breach has been reported and provide them an overview of the situation.

3. Contacts the individual who reported the problem.

4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of an individual's personal information. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).

5. Reviews the preliminary details.

6. Activates the Incident Response Team if warranted once a privacy breach affecting personal information is confirmed. Contacts the TOC and advises them to update the Incident Request with "Incident Response Team Activation – Critical Security Problem."

7. The IT Department Manager is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.

8. Contacts all appropriate database and system administrators to assist in the investigation effort. Directs and coordinates all activities involved with Incident Response Team members in determining the details of the breach.

9. Contacts appropriate Incident Response Team members.

10. If the breach occurred at a third-party location, determines if a legal contract exists. Works with the Legal Department, and Data Owner to review contract terms and determine next course of action.

11. Determines the type of personal information that is at risk, including but not limited to:

    - Name, address, phone number, e-mail address

12. If personal information is involved, requests that the Data Owner determine who might be affected. Coordinates next steps with the Legal Department

13. Determine if an intruder has exported or deleted any personal information data.

14. Determines where and how the breach occurred.

    - Identify the source of compromise and the timeframe involved.

    - Review the network to identify all compromised or affected systems. Consider e-commerce third-party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.

    - Document all internet protocol (IP) addresses, operating systems, domain name system names, and other pertinent system information

15. Takes measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third-party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

    - Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.

    - Do not access or alter the compromised system.

    - Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).

    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

16. Monitors systems and the network for signs of continued intruder access.

17. Preserves all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensures that the format and platform used is suitable for review and analysis by a court of law if needed. Documents all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Records all forensic tools used in the investigation. Note: Visa has specific procedures that must be followed for evidence preservation.

18. Notifies the CTO. Provides a summary of confirmed findings and of the steps taken to mitigate the situation.

When a Privacy Breach occurs

1. After confirmation that a breach of personal information on individuals has occurred, notify the Executive Manager.
2. Coordinate activities between business area and other departments (e.g., Human Resources, if necessary).
3. If necessary, notify the appropriate authorities (e.g., Amazon, eBay, Paypal, Banks), etc.)
4. Coordinate with Public Relations on the timing and content of notification to individuals.
5. If the Information Security Office determines that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place once law enforcement determines it will not compromise the investigation.
6. Notification to individuals may be delayed until the CTO is assured that necessary measures have been taken to determine the scope of the breach.
7. Follow approved procedures for any notice of unauthorized access to personal information about individuals.