Incident Response Plan

1.0 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handling various security incidents.

2.0 Purpose

This policy is designed to protect the resources of Shredding & Storage Unlimited and their clients against intrusion and loss of confidential data.

3.0 Incident Response Goals

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Notify affected clients.
5. Determine how the attack was done or the incident happened.
6. Prevent future attacks or incidents.
7. Improve security and incident response.
8. Prosecute illegal activity.
9. Keep management and clients informed of the situation and response.

4.0 Incident Definition

An incident is any one or more of the following:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification).
3. Theft of physical asset including computers, storage devices, printers, boxes, files, shredded material etc.
4. Damage to physical assets including computers, storage devices, printers, boxes, files, etc.
5. Misuse of services, information, or assets.
6. Infection of systems by unauthorized or hostile software.
7. An attempt at unauthorized access.
8. Unauthorized changes to organizational hardware, software, or configuration.
9. Reports of unusual behaviors.

10. Responses to intrusion detection alarms.

5.0 Incident Planning and Reporting

1. Roles and Responsibilities
    1. Dan Gornall
        1. A first responder to scene of incident
        2. Inquires the nature of the incident and determines severity
        3. Manages the control or elimination of the incident
        4. Notifies incident response team
    2. Chrisy Gornall
        1. Collect any and all pertinent information about the incident
        2. Notify affected clients of incident and keep them informed as soon as possible
    3. Josh Gornall
        1. Assist in the collection of all pertinent information about the incident
        2. Research incident and possible preventive measures
    4. All members of Incident response team
        1. Establish new procedures and/or security measures to prevent future incidents of this and other nature
2. Reporting of incident
    1. Computer Incidents (Virus, Hacker, Data Theft, System Destruction)
        1. Follow instructions to record any known information about the incident on the "Computer Incident Reporting Form"
        2. Consult the computer security company (available list is attached) on other information that should be included
    2. Off-Site Incidents (Any data-breach incident that does not take place at a company warehouse or office)
        1. After the first response team has been notified, contact Chrisy Gornall and Josh Gornall
        2. Describe the incident in detail and answer all questions in as much detail as possible
        3. Chrisy Gornall or Josh Gornall will complete the "Security Incident Reporting Form" based on the information they receive
    3. On-Site Incident (Any data-breach incident that takes place at a company warehouse or office)
        1. After the first response team has been notified, contact Chrisy Gornall and Josh Gornall

2. Describe the incident in detail and answer all questions in as much detail as possible
3. Chrisy Gornall or Josh Gornall will complete the "Security Incident Reporting Form" based on the information they receive

6.0 Incident Response Life cycle

1. Incident Preparation
    1. Policies and Procedures
        1. Computer Security Policies
            1. Password Policy
                1. All passwords should contain at least one number, lower case letter, and upper case letter.
                2. All or part of the password cannot be found in any dictionary
            2. Network Sharing Policy
                1. Any document that contain a birthdate, SSN, or any sensitive information cannot be shared or sent over the network
            3. Virus and Intrusion Detection and Prevention Policy
                1. Any emails or links that are not expected and from a trusted sender should never be opened
                2. Anti-Virus software should be kept active and up to date
                3. Anything suspicious should immediately be reported
        2. On-Site Policies
            1. Off-Site Record Destruction
                1. Upon receiving records, all records should stay in the possession of an access employee until they have been destroyed
                2. Any containers used to transport records have to have the ability to close and lock. The containers cannot be overflowing
                3. Any records that are not in direct possession of an access employee at any time must be in a locked container and stored in a secure, non-public location
                4. Access employee will ensure that all documents are destroyed at that time. Access employee will ensure that no documents have fallen out of the container or shred unit
        3. Off-Site Policies

1. Security
    1. Camera system will be in working order with a 90 day memory at all times
    2. Containers will remain locked and securely stored when not handled by an access employee.
    3. The containers are logged upon receipt and destroyed within 48 of receipt.
2. Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
3. Post warning banners against unauthorized use at system points of access.
4. Establish Response Guidelines by considering and discussing possible scenarios.
5. Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
6. Establish Contacts - Incident response team member contact information should be readily available. An emergency contact procedure should be established. There should be one contact list with names listed by contact priority.
7. Test the process.

2. Discovery - Someone discovers something not right or suspicious. This may be from any of several sources:
    1. Employee
    2. Intrusion detection system
    3. A system administrator
    4. A business partner
    5. A monitoring team
    6. The security department or a security person.
    7. An outside source.
3. Notification - The emergency contact procedure is used to contact the incident response team.
4. Analysis and Assessment - Many factors will determine the proper response including:
    1. Is the incident real or perceived?
    2. Is the incident still in progress?
    3. What data or property is threatened and how critical is it?
    4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    5. What system or systems are targeted, where are they located physically and on the network?
    6. Is the incident inside the trusted network?

5. Response Strategy - Determine a response strategy.
    1. Is the response urgent?
    2. Can the incident be quickly contained?
    3. Will the response alert the attacker and do we care?
6. Containment - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:
    1. Disconnect the affected system(s)
    2. Change passwords.
    3. Block some ports or connections from some IP addresses.
7. Prevention
    1. Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.
    2. Take steps to prevent an immediate re-infection which may include one or more of:
        1. Close a port on a firewall
        2. Patch the affected system
        3. Shut down the infected system until it can be re-installed
        4. Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
        5. Change email settings to prevent a file attachment type from being allow through the email system.
        6. Plan for some user training.
        7. Disable unused services on the affected system.
8. Restore Affected Systems - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following
    1. Re-install the affected system(s) from scratch and restore data from backups if necessory. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
    2. Make users change passwords if passwords may have been sniffed.
    3. Be sure the system has been hardened by turning off or uninstalling unused services.
    4. Be sure the system is fully patched.
    5. Be sure real time virus protection and intrusion detection is running.
    6. Be sure the system is logging the correct items
9. Documentation - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.

10. Evidence Preservation - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.
11. Notifying proper external agencies - Notify the police if prosecution of the intruder is possible.
12. Assess damage and cost - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
13. Review response and update policies - Plan and take preventative steps so the intrusion can't happen again.
    1. Consider whether an additional policy could have prevented the intrusion.
    2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
    3. Was the incident response appropriate? How could it be improved?
    4. Was every appropriate party informed in a timely manner?
    5. Were the incident response procedures detailed and cover the entire situation? How can they be improved?
    6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    7. Have changes been made to prevent a new and similar infection?
    8. Should any security policies be updated?
    9. What lessons have been learned from this experience?

7.0 Disaster Recovery

1. In cases of data loss, access backups from cloud service provider for the lost data
    1. Database – Azure
    2. Internal Programs – Azure
    3. Individual Computers - Carbonite
2. Resume as much of normal procedures as possible. Do not continue any operation that cannot be performed up to NAID AAA standards.
3. Notify customer of any change of schedule.
4. For any immediate services utilize third party companies and resources to assist in service. Notify customers of any changes related to these services. A list of companies that agreements have been made with and can be utilized is available in the Incident Response Folder.