ZUORA

Security Incident Response Procedure

Last revision date: 07/12/2023

Revision History

Version	Date	Change Log
1.0	01/14/2014	Creation of Policy
1.1	3/11/2015	Annual review of Zuora's Emergency Mode Operation Plan. Updated IRT members and added a reference to the support PROD process.
1.2	01/13/2016	Update IRT members
1.3	02/10/2016	Update to replace Zendesk with JIRA, created Slack Channel, updated titles, included IT as part of IRT.
1.4	03/14/2017	Updated individuals that are part of the IRT.
1.5	3/30/2017	Updated to include that not all IRT members must be involved in all instances and only as applicable.
1.6	8/21/2017	Updated to include the Communication Process (Internal)

1.7	1/29/2018	Update the IRT
1.8	4/4/2018	Updated IRT with new incident type: Key Security Control Missing
1.9	7/23/2018	Updated to include individuals from RevPro
1.10	2/28/2019	Updates to the Incident Response Team
1.11	2/3/2020	Updates to the Incident Response Team
1.12	9/15/2020	Added updated incident response / report template, updated response team
1.13	12/14/2020	Updated response team
1.14	1/7/2021	Updates to some details.
1.15	11/08/2021	Updates to response team
1.16	03/01/2022	Updates to contacts
1.17	05/02/2022	Updates to contacts
1.18	05/03/2023	Updates to the response team contacts
1.19	07/12/2023	Updated Incident Response Process

Table of Contents

- Introduction
- Audience
- Definitions
- Roles
    - IRT Responsibilities
    - Management Responsibilities
    - Incident Response Process
        - Incident Identification/Alert
        - Investigate
        - Respond
- Testing

Introduction

Zuora has documented this incident response procedure as a guide for detecting, analyzing, and responding to computer security incidents as they occur. This document contains specific requirements for dealing with computer security incidents.

Security incidents include, but are not limited to:

- Virus
- Worm
- Trojan horse
- Unauthorized use of computer accounts
- Disclosure of cardholder data and computer system
- Unauthorized wireless access points are plugged into the Zuora network .
- Complaints of improper use of Information Resources as outlined in the Acceptable Use Policy.
- Key security control missing
- Breaches of information from any of the services that Zuora uses or develops (includes, application, APIs, website). These may be internally developed or third party developed.

Audience

Zuora Incident Response Policy applies equally to all individuals that use any Zuora Information Resources.

Definitions

- **Information Resources**: Any and all computer printouts, online display devices, storage media, and all computer related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, servers, personal computers, notebook computers, handheld computers, personal digital assistants (PDA), telecommunication resources, network environments, telephones, fax machines and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.
- **Computer Security Incidents**: Unauthorized wireless access points are plugged into the Zuora network
- **Incident Response Team (IRT)**: Personnel responsible for coordinating the response to computer security incidents in Zuora.
- **Virus**: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.
- **Worm**: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.
- **Trojan Horse**: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by email or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.
- **Security Breach Incident**: In information operations, an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.
- **Key Security Control Missing**: Key Security Controls refer to but not limited to: HIDS, NIDS, WAF, Firewall or central log server would trigger this incident.

Roles

Chief Security Officer (CSO): The designation of an incident response manager is intended to establish clear accountability for setting policy for incident response activities, provide for greater coordination of Zuora’s incident response activities, and ensure greater visibility of such activities within and between Zuora its customers and law enforcement agencies. The CSO has been given the authority and the accountability by Zuora management to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the Zuora. This individual is responsible to executive management for administering the information security functions within Zuora and shall be the internal and external point of contact for all information security matters. The CSO is required to be active in industry organizations and standards groups focused on information security. It is the responsibility of the CSO to incorporate industry developments into Zuora's security and incident response programs.

All IRT team members are required to name a surrogate. The table below lists current IRT members & surrogates, in addition to the members listed here the CEO, SVP of Customer Success, and SVP of Engineering will be notified of all confirmed security incidents. The IRT shall comprise the following personnel, as needed based on the incident:

Role	**Primary**	**Surrogate(s)**
Chief Financial Officer (CFO)	Todd McElhatton (CFO)	Matt Dobson
Chief Security Officer (CSO)	Jayson Franklin CISO	Anu Veluri
Vice President of Technical Operations	Venkat Venkataraman (VP TechOps)	Karunakaran Duraikannu,Abhilash Chintalapudi
Senior Vice President of Legal / General Counsel	Andy Cohen (General Counsel)	Ademuyiwa Bamiduro
Vice President of Support	Andy Newsham (VP Support)	Srinivas Guduru, Michael Cardamone
Chief Information Officer (CIO)	Paul Heard (CIO)	Piyoush Sharma
Chief Product Officer (CPO)	Tom Krackeler (CPO)	Karthik Ramamoorthy, Kyle Kolich, Srinivas Chalavada,Tanmoy Dutta

Senior Vice President R&D Operations	Radhi Chagarlamudi (VP R&D Ops)	Venkat Venkataraman

IRT Responsibilities

1. The IRT provides accelerated problem notification, damage control, and problem resolution.
2. IRT members are granted the authority to fulfil their responsibilities.
3. IRT members:
    a. Investigate, verify, and remedy critical incidents
    b. Manage communication with key clients during incident troubleshooting or service disruption
    c. Ensure that incident evidence is safeguarded for forensic investigation
    d. Conduct and document forensic investigations and post incident evaluations
    e. Coordinate with Media, Security, Legal, and external law enforcement as needed
    f. Maintain and update policy and procedures as required

Management Responsibilities

- Organize and maintain an in-house IRT.
- Prepare, update, revise and regularly test the incident response plan.
- Establish, maintain, and periodically test an incident notification system that enables personnel to report suspected incidents promptly to the appropriate staff
- Provide training (and periodic retraining) for personnel who are expected to follow any phase of the procedure, including those employees who are not on the IRT
- Grant appropriate authority to IRT members to fulfil their responsibilities

Incident Response Process

At a high level, the Security incident response process will follow the Unified - Internal Security Incident Management Process. Due to the high risk associated with security incident all suspected security incidents will be classified as a P0 or P1 and follow an escalated response process.

Incident Identification/Alert

The incident response process is started when Zuora Support or Zuora Security notes a potential incident. Incident discovery can occur in many ways including:

- Email alerts from system monitoring
- Customer notifications of suspected activity.
- Routine inspection of Zuora systems.

Investigate

Zuora will perform a thorough investigation; the Zuora's Security team logs all potential security indents in JIRA, which may originate from Zendesk if it came from a customer, for investigation. Once logged Zuora Security contacts the user in question to determine if the activity reported is the result of normal business operations or malicious activity. In the event the activity does not relate to a specific user, Zuora Security will contact the process owner that is responsible for the activity reported.

- If the incident is a false positive Zuora will note this in the JIRA or Zendesk ticket and close the ticket.
- If the incident is malicious the Security team will notify the appropriate IRT members immediately regarding the incident and the assessment of its impact. Based on the incident, applicable IRT member are included within a Slack channel, which is where communication will occur.
    - IRT will participate in the IRT channel to check the latest status:
        - Login toSlack
        - A conference call number will be set up for keeping participants and IRT members informed about latest situation, progress and impact on business continuity. In addition, incident response activities will be documented in JIRA in an indent ticket for the IRT members to review.
    - Zuora will document detailed information about the incident in JIRA and/or Zendesk including:
        - The type of incident (virus, intrusion, misuse, etc.).
        - If the incident real or perceived.
        - Which equipment or system(s) are being affected, including operating system(s), IP address(es), and location(s).
        - If the incident is still in progress.
        - What property or data are threatened, and how critical are they? Rank affected systems by criticality and address the most critical systems first.
        - What is the impact on the business should the incident occur again? Is the affected equipment business critical? What is the severity of the potential impact?
        - Analysis of legal requirements for reporting compromises (even potential but not confirmed compromises)
        - How the response strategy will support business continuity while preserving forensic evidence.

Respond

1. **Immediately contain and limit the exposure.**Zuora will prevent further loss of data by conducting a thorough investigation of the confirmed compromise of information. To preserve evidence and facilitate the investigation:
    a. The IRT will not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).

   b. The IRT will not turn the compromised machine off. Instead, the IRT will isolate compromised systems from the network (i.e., unplug cable).
   c. The IRT will preserve logs and electronic evidence.
   d. The IRT logs all actions taken on the compromised system.
   e. If using a wireless network, the IRT will change SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.
   f. Zuora TechOps will be on "high" alert and monitor all systems with cardholder data
2. **Alert all necessary parties immediately.** If an incident is suspected or confirmed compromise of cardholder data the IRT must immediately notify the payment brands affected. In addition, Zuora's incident response process must agree with the payment brands response procedures. This Incident Response Procedure has been designed to meet the payment brands incident response procedures. In the event that cardholder data is suspected to be accessed The IRT will contact the brands affected using contact information below. In the event Zuora can confirm cardholder was not access, Zuora still has legal and contractual obligations to notify customers if personally identifiable data was accessed. The VP of Support will coordinate contacting customers.

Brand	**Contact Information**	**Incident Response Procedure**
Visa	Zuora merchant bank or Visa (650) 432-2978 or usfraudcontrol@visa.com	If Compromised Responding to a Data Breach
MasterCard	Zuora merchant bank or MasterCard through MasterCard Online here.	Security Rules and Procedures
Discover	1-800-347-3083 Call Mon–Fri 8:30am to 4:00pm Eastern Time, excluding holidays	Discover Information Security and Compliance
AMEX	Email at EIRP@aexp.com. Zuora must designate an individual as their contact regarding such Data Incident.	Data Incident Management Obligations

If the incident is related to financial fraud, Zuora is required to contact the local office of the United States Secret Service or FBI, Zuora legal will determine the correct notification.
Zuora is legally and contractually obligated to notify customers. The VP of Support and the Director of Customer Success will coordinate contacting customers.

1. **Risk Assessment:** Determine if the security incident is a breach of ePHI
    a. HIPAA requirement §164.402 defines a breach as the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.
2. Response strategies are implemented according to the incident type:
3. Data Theft
    a. Determine the source of the breach and close it
    b. Determine as rapidly as possible the scope of the data breach
- Escalate to the appropriate parties, which may include the CEO and contact legal & law enforcement entities, providing details of the breach
1. Establish a plan to prevent the similar theft in the future
1. Computer Intrusion
    a. Determine the access point of the attack and close it
    b. Preserve evidence and logs needed to conduct forensics investigation
- Determine the purpose, type, source, and seriousness of attack
1. Mitigate the threat
2. Establish a plan to prevent the same or similar attacks in the future
1. Virus Outbreak
    a. Disable, cleanse, or deactivate the virus
    b. Determine the source and extent of the infection
- Establish a plan to prevent similar virus exposure in the future
1. Restoration of Impacted System(s): The IRT returns the affected system(s) to the uninfected state through any of the following or similarly appropriate processes:
    a. Reinstall the affected system(s) from standard image base and restore any needed data from clean backups, ensuring that forensic evidence is preserved for investigation
    b. Require users to change passwords if passwords may have been compromised
- Ensure system hardening by turning off or uninstalling unused services
1. Ensure patches are fully applied

2. Ensure virus protection and intrusion detection are running
3. Ensure host intrusion tool is installed

- Ensure file integrity monitoring tool is installed
- Ensure system(s) are logging the correct events and to the proper level

1. Prevention of Reinfection or Reoccurrence: Depending in the incident's source (e.g., inadequate training, attack through application bug, a port, or unpatched system), the IRT takes steps to prevent immediate reinfection, when appropriate, and reoccurrence.
2. Forensic Investigation: The IRT applies forensic techniques, including:
    a. Reviews of system intrusion logs and detection logs – examine for gaps and evidence of suspicious activity
    b. Interviews of the incident victim and witnesses to determine how the incident was caused and detected.

- NOTE: Only IRT members or law enforcement officials will conduct interviews or examine evidence.

1. Notification
    a. **Provide all compromised payment card accounts to Zuora's customers promptly.** All potentially compromised accounts must be provided and transmitted as instructed by Zuora's merchant bank and the card brand's Fraud Investigations and Incident Management groups. The card brands will distribute the compromised payment card account numbers to Issuers and ensure the confidentiality of entity and non-public information. Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank. (See Appendix A for the report template.)
    b. **Provide all compromised ePHI data to Zuora customers promptly.**
2. **Postmortem conducted.**The IRT produces an after-action evaluation, assessing the following areas of concern:
    a. IRT Performance

1. Was the incident response appropriate, effective, and timely? How could it be improved?
2. Was every appropriate party informed in a timely manner?

- How did the incident impact business continuity? How could continuity be strengthened in future incidents?

    a. Policies and Procedures

1. Was the incident response procedure sufficiently detailed to cover the entire situation? How can it be improved? Was it too broad or too restrictive?
2. Did the incident result from procedures or policies not being followed? What could be changed to ensure that requirements are followed in the future?

- What modifications should be made to existing policies and procedures—including security documents—to prevent further similar incidents?

1. If new procedures were developed during the incident response, have they been properly documented? Are they being implemented?
2. How/when will existing policies and procedures be modified and implemented? How/when will users be trained on the changes?

    a. System Functioning

1. Have changes been made to prevent new or similar occurrences?
2. Are all systems patched, hardened, and locked down? Have passwords been changed, antivirus protections been updated, email policies been set, etc.?

a. Modifying and evolving the Incident Response Procedure, this plan should be updated as Zuora's needs change. After each event Zuora management is required to evaluate the response process and improve the process after considering the following:

1. What lessons have been learned?
2. What industry developments can be adopted?
- What recommendations can be made?
1. How will users be informed about the new incident/threat and be trained to handle and recognize the incident if it occurs again?

The results of the postmortem will be used to evaluate this Incident Response Procedure and update it as necessary to improve the overall process.

Testing

Testing of the IRP shall be conducted at least annually. The IRP test will include a mock security event conducted by a member of the Security team and additional departments as appropriate, not on call to respond to a security event. The security test will include formal documentation of how the security event will be executed. Note, this test does not have to be a blind test and all members responding to the event can be aware that the event is only a test. In any case the entire IRP will be executed as if it were a real security breach.

Note: As the IRP mandates a post incident “lessons learned” session meant to improve the IRP, any incident response conducted during a year is considered a process test and satisfies the annual test requirement.