Coralogix

INCIDENT MANAGEMENT PROCEDURE

Version 5.0

Table of Contents

Version Control

Version	Developed by	Changes	Approved by	Date
1.0	Oded David	Initial Version		
2.0	BDO	Update according to ISO 27701		30/05/2020
3.0	Shiran Wolfman	Update according to PCI-DSS and GDPR		17/10/2021
4.0	Shiran Wolfman	Annual Review		18/01/2022

5.0	Shiran Wolfman	Annual Review	Oded David	17/01/2023

Description

1. An Information security incident can occur at any time leaving Coralogix exposed. An incident that is anticipated, improves the ability to effectively respond and manage the incident.
2. The Incident Management Process is designed to handle security incidents and should be used as a baseline or reference document for dealing with information security threats.
3. The Incident Management process is a component of Coralogix's Information security program.

Incident Reporting and Investigation Process

- User notifies CISO upon discovery of a suspected incident or
- Security monitoring software issues an alert.
- The incident is then classified:
    1. Information Security: Information lost or stolen
    2. Information Security: Privacy or Security Breach
    3. Information Security: Risk Notification/Non Compliance
    4. Information Security: Suspicious Activity
- Examples of possible incidents:

Denial of Service	Social Engineering
Malicious Code Attack	Theft, Fraud or Espionage

Unauthorized Access	Customer data breach
Probes and Network Mapping	Third Party Data breach
Other incident	

- The CISO will notify the appropriate people of an incident for follow-up.
- An incident summary shall be written, containing additional information which can include: date, time, contact details, country, region, data, sensitivity etc.)
- The CISO must:
    1. Analyze the causes of the incident.
    2. Implement a containment process if possible e.g. wipe phone.
    3. Involve other teams to plan and implement corrective action to prevent recurrence.
    4. Communicate with those affected by or involved with recovery from the incident.
    5. Escalate to Senior Coralogix Management.
- The CISO must determine the alert level based on information gathered and inform relevant parties.
- Consistent with Coralogix Information Security Policy, it is the responsibility of the CISO to notify the IT team, who will log any and all incidents. Security incidents resulting in harmful effects known to Coralogix will be mitigated to the extent practical.
- Coralogix will notify the customers about every security breach in the cloud environment.
- The notification will be communicated to all the customers via email within 48 hours.

Table 1 : Security Incident Alert Levels

Alert	Impact Details	Privacy	Availability	Employee Impacted
High Threat	Control of production servers, or code insertion	User/Customer privacy impacted	System availability issue which is not under control or is	most affected

			longer than 1 hour	
No to Low Threat	Threats such as IP scans	None	System availability issue which is short and under control	Some users affected

Incident Recovery Process

The incident recovery process is not always required in its entirety.

1. CISO is the Recovery Lead for leading the response and recovery.
2. The responsibilities and authority of Recovery Lead include:
    1. Continuous updating of all parties.
    2. Collecting evidence.
    3. Shutting down, isolating or disconnecting systems that are significantly impacting production.
    4. Status reporting: dates, times, impact, still-in-progress, data lost or stolen data.
    5. Recovery effort.
    6. Coordinate recovery activity with other organizations where necessary.
3. After a suspected or actual system compromise:
    1. Change all access including all privileged and user passwords to the affected system.
    2. Test system for other vulnerabilities if required – Ethical hack, application testing.Harden against further attacks.
    3. Validate system prior to it being released back into operations.
    4. Monitor for any unusual activity or unknown services on the network.
    5. Recover systems from backup if required – including patches and changes to prevent re-occurrence.

    6. Look for backdoor, Trojans and other malicious code which can be very well hidden and may be programmed to lie dormant for a time, prior to activating.
4. The CISO must gather and document lessons learnt and areas of risk and what can be done to improve the security posture based on the incident.
5. The CISO must inform the Insurance Company within less than 72 hours from the start of the incident.
6. The CISO in consultation with Legal must determine if authorities must be involved (could be the law depending on the country and what occurred).
7. The Recovery Lead must document the recovery process followed and coordinate with the return to normal business.
8. Lost transactions due to restore from previous backup must be communicated.
9. The CISO must update the Information Steering Committee on the incident.
10. Coralogix will periodically review information system activity records—including audit logs, access reports, and security incident tracking reports—to ensure that implemented security controls are effective and that ePHI and/or credit card information has not been potentially compromised.

Rules for Evidence Guidelines

1. Information Security violations are not the same as physical violations. Not handling the evidence correctly can disqualify it in a court of law, making prosecuting an individual impossible. Training in handling evidence or obtaining outside help from experts who do this is required. The legal evidence can be classified into various categories, some of more value to a legal case than others.
2. For external actions evidence will conform to the following rules:
    - All evidence must be gathered with the intention of using it in a court of law through accepted legal means.
    - More evidence rather than less must be gathered and retained.

Admissibility of Evidence Guidelines

1. For evidence to be admissible in a court of law, evidence must meet certain key requirements. All evidence to be of value to any legal proceeding must be relevant, legally permissible, reliable, properly identified, and properly preserved.
    - The evidence must be related to the security breach/crime and demonstrate or verify that the security breach/crime was committed.
    - The relevant evidence must also provide information detailing the crime including the time it occurred and the perpetrator's motives.
    - All evidence must be obtained within the boundaries of the law.
    - Evidence must be free from modification and tampering.
    - All Identification evidence must be substantially identified without modifying or degrading the evidence.
    - Preservation of evidence must not be subject to damage or destruction:
        - Power must not be prematurely removed.
        - Where possible hard disk images must be backed up and evidence write protected.
        - Evidence should be stored in properly controlled physical conditions (heat and humidity) and away from the proximity of magnetic fields.
2. Without a structured process to maintain evidence, the evidence collected may not be admissible evidence to the incident. This may be the hurdle when taking this case to court.
3. Coralogix may involve a lawyer, specialist or an insurance company early in any contemplated legal action and take advice on the evidence required.

Definition of Breach

1. In the context of this policy, a Breach means the acquisition, access, use, or disclosure of PII or "Sensitive Information" (as it may be defined in applicable data privacy laws/regulations) in a manner not permitted under the HIPAA Privacy Rule, GDPR (defined as "Personal Data") or applicable data privacy laws/regulations) and PCI-DSS that compromises the security or privacy of the PII/PHI/Sensitive Information. An impermissible use or disclosure of protected health information is presumed to be a Breach unless Coralogix demonstrates that there is a low probability that the PII/PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PII/PHI involved, including the types of identifiers and the likelihood of re-identification
- The unauthorized person who used the PII/PHI or to whom the disclosure was made
- Whether the PII/PHI was actually acquired or viewed
- The extent to which the risk to the PII/PHI has been mitigated
- Coralogix has the discretion to provide the required Breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the PII/PHI has been compromised.

Definition of Unsecured Protected Health Information

1. Unsecured protected health information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of Health and Human Services—"the Secretary"—(essentially, through use of encryption technology where there is a low probability of assigning meaning without the use of a confidential process or key to decrypt the PHI).The following encryption technologies have been judged to comply with the Secretary's guidance:

    - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.1
    - Valid encryption processes for data in motion are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

Breaches that Require Notification

1. Breaches that trigger a notification requirement under the HIPAA Breach Notification Rule are those that involve Unsecured Protected Health Information only. No notification under the HIPAA Breach Notification Rule is required if the PHI that is the subject of a Breach is encrypted.

2. Breaches that trigger a notification requirement under PCI-DSS Requirement 12 are those that involve credit card information of customers. Breaches in this regard triggers the notification of affected customers and their corresponding payment brands.

Assessing the Risk

3. The Chief Information Security Officer (CISO) or Data Protection Officer (DPO) ,or a designated person, will investigate the Breach and prepare a Breach Report. (See Appendix A)
4. The report will follow the U.S. Department of Health and Human Services Office for Civil Rights guidance on Breach Management and will consider the following:

    - How the Breach occurred
    - The type of personal data involved
    - The number of data subjects affected by the Breach
    - Who the data subjects are
    - The sensitivity of the data breached
    - The harm that could be incurred to the data subjects. For example, the Breach could result in identity theft or fraud, physical harm, psychological distress, humiliation, or damage to reputation.
    - The potential outcome if the personal data is used inappropriately or illegally.
    - Whether there are any protections in place, such as encryption, for the personal data that has been lost or stolen.

- The measures taken, or proposed to be taken, to address the personal data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Whether the Breach is required to be notified to the Covered Entity customer or the U.S. Department of Health and Human Services Office for Civil Rights. In the event that it is decided such notification is unnecessary, the reasoning behind the decision, including reasons why the Breach is unlikely to result in a risk to the rights and freedoms of individuals

1. If the breach could result in a high risk to the rights and freedoms of the affected users, the users must also be notified. Consider the dangers of 'over-notifying'.

Notification

2. After becoming aware of a personal data breach, Coralogix will notify the relevant controllers without undue delay.
3. Notification to data subjects may be via a variety of means, depending on the number of data subjects affected, the severity of the breach, the urgency of notification or other factors. Notification can take place via:
    - Email to all affected data subjects
    - Web page banner with a means to have users confirm that they have seen the notice.
1. The notification shall:
    - Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
    - Communicate the name and contact details of the Data Protection Officer or other contact point from whom more information can be obtained.

- Describe the likely consequences of the personal data breach.
- Describe the measures taken, or proposed to be taken, by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- Where, and insofar as, it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay.
- Coralogix shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken.

Remedies to Customers Related to Personal Data

1. Data subjects who believe that Coralogix's processing of personal data relating to him or her does not comply with relevant regulations, have the right to lodge a complaint with a supervisory authority, relating to the infringement of his or her rights.

2. The complaint should be lodged with the supervisory authority of the data subject's habitual residence, the data subject's place of work, or the place of the alleged infringement

Appendix A: Incident Response Sequence of Events

1. The person who discovers or suspects the incident will e-mail company CISO, or whoever is on call in his place, with "INCIDENT REPORT" in the Subject line.

Persons discovering and reporting incidents can include employees, customers, partners, contractors or other contacts at the physical office.

1. When the incident report email is received, the CISO or on-call staff member answering will decide if the incident warrants further escalation, and then create a “short incident report (SIR)” with the following details:
    - Reporting contact
    - Time of the report
    - Contact information for the reporter
    - The nature of the incident
    - What equipment or persons were involved?
    - Location of equipment or persons involved
    - How the incident was detected?
    - When the event was first noticed that supported the idea that the incident occurred
2. The report will be the basis for escalation or for documentation purposes in the case that the incident turns out to be a false positive.
    1. CISO will refer to the Incident Response Contact List and notify the relevant factor.
        - CISO will communicate the log of information received in the previous step AND add the following details (to the best of their ability):
        - Is the impacted equipment/software business critical?
        - What is the severity of the potential impact?
        - Name of system being targeted, along with operating system, IP address, and location.
        - IP address and any information about the origin of the attack.
    2. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
        - Is the incident real or perceived?
        - Is the incident still in progress?
        - What data or property is threatened and how critical is it?
        - What is the impact on the business should the attack succeed? Minimal, serious, or critical?

- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?
- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care? (Sometimes it is imperative to not let the attacker know that we are on to him)
- What type of incident is this? Example: virus, worm, intrusion, abuse, physical or nonphysical damage.

3. The incident ticket will be updated. The incident will be categorized into the highest applicable level.
4. If CISO and Coralogix management are convinced that user data has been breached or leaked or that there is enough evidence to support the suspicion that such breach or leak has occurred, then the following steps will be taken:
    - Change all internal access passwords to the application
    - If there is a suspicion that an attacker may have entered the system, change all customer account passwords
    - Inform all customers of the breach or the suspicion of a breach
    - Inform the insurance company (cyber policy)
5. Team members/response team will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only personnel authorized by the Incident Response Team should be performing interviews or examining evidence.
6. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
7. Upon management approval, the changes will be implemented.
8. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
    - Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    - Make users change passwords if passwords may have been sniffed.

- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real intrusion detection is running.
- Be sure the system is logging the correct events and to the proper level.

Appendix B: Categorization of Security Incidents

Security incidents are categorized according to their source and potential effect. Attack methods may include:

1. Data Privacy Incidents;
2. PHI disclosure;
3. Credit Card information disclosure;
4. Wiretapping and eavesdropping;
5. DoS and DDoS;
6. Degradation of service;
7. Masquerading;
8. Unauthorized data copying;
9. Scanning and traffic analysis;
10. Trapdoors and covert channels;
11. Tunneling;
12. IP spoofing;
13. Trojan horses, viruses and worms;
14. Session hijacking;
15. Timing attacks;
16. Logic bombs;
17. Password sniffing;
18. Misuse of privileges.

Appendix C: Examples of Security Events and Responses

Suspected exposure of PHI/credit card information: hard copy or electronic copy obtained by an unauthorized party	
LEVEL	HIGH
RESPONSE	The CISO investigates the events leading to the incident. The information owner is informed. Corrective measures are taken to prevent additional incidents.

Suspected damage to a data stored in an information system in terms of confidentiality, integrity and availability	
LEVEL	MEDIUM
RESPONSE	Relevant system and database logs are retrieved. Data is restored from backup. The information owner is informed. Configuration of the information system and authorization system of the endangered data are corrected. Disciplinary measures are taken if a policy/procedure was violated by an employee.

Unsuccessful login attempts using the username and password of an employee	
LEVEL	MEDIUM
RESPONSE	The user is contacted to check if he/she trying to log in but have forgotten the password. The password of the user is changed. The authentication mechanisms of the system are inspected.

User activity at irregular times	
LEVEL	LOW
RESPONSE	The user is contacted to check if he/she is responsible for the activity and if it has been approved. If the user is not responsible for the activity, the account is locked and enabled only after the username and password have been changed.

A virus is detected on a computer of Coralogix network	
LEVEL	HIGH
RESPONSE	The infected computer is isolated by disconnecting it from the network. The IT Manager carries out the initial assessment of the virus to determine if it is new or known and its impact. Other computers are scanned for viruses.

	Anti-virus software is updated immediately after the update is released. The virus is removed from the infected computers. Information damaged by the virus is restored.

Signs of penetration attempts to the communication equipment	
LEVEL	HIGH
RESPONSE	The source of the attack is identified and blocked, for example, by adding an emergency rule to the firewall. A warning is sent to the attacker. Legal action is considered.

Appendix D: Incident Report

Incident Management Report

Incident Title		Customer Name	
Priority		Customer Location	
Date and Time of Incident Detection		Support Personnel Name	
End Date and Time of Incident		Law Enforcement	

Incident Summary

Type of issue Detected	Denial of Service	Unauthorizd Access	Malicious Code	Unplanned Downtime	Unauthorized Use	Other
Description						

Names and Contacts of Others Involved

Example: IT Manager						

Incident Notification and Escalation

Mgmt	HR	IT & MIS	Finance	R&D	InfoSec
Insurance company	Response Team	Customers	Israeli Privacy Authority		
Business Impact and Scale					