Global Privacy Office (GPO)
Privacy Incident Response Plan

Confidential

Revised November 2017

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

Table of Contents

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

Purpose

The purpose of the Privacy Incident Response plan is to ensure that compromises of Cargill Personal Information ("Personal Information") are *detected*, *contained*, and *reported* to the appropriate individuals and organizations; to *comply* with applicable laws and regulations; and to *identify* the root causes of those compromises.

Scope

The scope of this document includes all privacy incidents involving Personal Information in any format or location, and any building, device, or computing environment.

Privacy Incidents may include, but are not limited to:

a. lost or stolen laptops, computers, servers, tapes, CD ROMs, flash drives, phones, personal-data assistants, and any other mobile data-storage medium containing Personal Information;
b. lost or stolen paper documents containing Personal Information;
c. attack to or compromise of Personal Information in a database or server;
d. e-mails or paper documents containing Personal Information sent to an unauthorized party;
e. electronic transmissions of Personal Information sent outside Cargill's network unencrypted;
f. unauthorized access of Personal Information;
g. an intentional defeat or malfunctioning of the physical access controls to facilities where Personal Information is stored;
h. an intentional defeat or malfunctioning of the logical access controls within the computing environment where Personal Information is stored or processed;
i. saving a file containing Personal Information to a widely accessible storage location, such as a corporate common file directory or in a network DMZ; and
j. notification by Cargill's third parties, law-enforcement authorities, government agencies, credit-reporting agencies, or financial institutions that there has been a suspected or confirmed breach of the computing environment where Personal Information is stored or processed.

Roles and Responsibilities

TGRC Privacy Incident Response Team (TGRC PIRT)

The TGRC PIRT is responsible for the privacy incident response process for all suspected privacy incidents and participating in the remediation of the incident. TGRC Cyber Security Incident Response Team (CSIRT) owns the overall incident response process at Cargill. The PIRT is formed to support the CSIRT process and may include resources from the CSIRT team. The coordination of the incident is determined together with CSIRT and Global Privacy Office (GPO) depending on the nature and scope of the incident.

The TGRC PIRT's responsibilities include, but are not limited to:

- Conducting up-front due diligence and information gathering of the suspected incident.
- Managing the Privacy Incident Response Process.
- Reviewing all reported Privacy Incidents within one business day of receipt, or in a reasonable time period as established by the Global Privacy Office Manager.
- Determining the nature, scope, and priority of each incident.
- Coordinating investigations crossing organizational boundaries (internal and external).
- Capturing and documenting information relating to the incident in Archer
- Coordinating breach notifications to law authorities, banks, credit card companies, employees, customers, and other parties as necessary.
- Reporting privacy incident response status to the CISO.
- Participating in incident response testing, maintenance and Post-Mortem review sessions to identify potential opportunities for improvement of the Privacy Incident Response Plan and Process.

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

Global Privacy Office Manager
The Global Privacy Office Manager will act as a Chair for TGRC PIRT. The Global Privacy Office Manager is responsible for managing and/or delegating the privacy incident response process. During an incident, the Global Privacy Office Manager is responsible for convening the appropriate individuals and leading them through the privacy incident response process.

The TGRC PIRT Chair's responsibilities include, but are not limited to:

- Owning the Privacy Incident Response Plan
- Coordinating the annual testing of the Privacy Incident Response Plan to identify potential opportunities for improvement
- Reviewing, maintaining and obtaining approval for privacy incident response process procedures
- Coordinating remediation of privacy incidents at an enterprise level within Cargill
- Escalating suspected incidents to the TGRC PIRT and the CISO

Privacy or Risk Analyst
The Privacy or Risk Analyst is responsible for supporting the Global Privacy Office Manager and the TGRC PIRT during the privacy incident response process: Their responsibilities include, but are not limited to:

- Maintaining and updating the Privacy Incident Response Plan
- Assisting in the coordination of and participating in the annual testing of the Privacy Incident Response Plan
- Assisting in the remediation of privacy incidents at an enterprise level
- Escalating suspected privacy incidents to the Global Privacy Office Manager or the TGRC PIRT
- Assisting the Global Privacy Office Manager and TGRC PIRT during privacy incidents as needed.

Employees and Contractors
All employees and contractors are responsible for immediately reporting suspected Privacy Incidents to the Service Desk at myglobalit.cargill.com. Service Desk agents will then connect with TGRC CSIRT. Further, all employees and contractors are responsible for assisting the PIRT when requested to do so.

Third Parties
Non-Cargill individuals and organizations with contractual relationships to Cargill will report suspected Privacy Incidents within 24 hours, or as contractually obligated, to the Service Desk at myglobalit.cargill.com

Privacy Incident Response Steps

This section provides summaries of the key tasks of each core step of the Incident Response Process.

Incident Detection and Triage

Privacy incidents are detected or captured in a variety of manual and automated ways, including from employees, third parties, law enforcement and information systems. It is the responsibility of all Cargill employees, contractors and business partners to report suspected incidents when they are detected.

Events should immediately be reported to the Service Desk at myglobalit.cargill.com and Service Desk agents will then connect with CSIRT. CSIRT will escalate suspected privacy incidents to the GPO. Further reporting and escalation is determined by the Global Privacy Office Manager.

CSIRT and GPO perform initial triage to determine whether the event is a suspected privacy incident. If so, CSIRT and the GPO determine the coordination responsibilities of the incident response process. Initial triage includes scope determination (type and number of records, data subjects, technology, exposure time and audience). Based on the scope of the incident GPO forms the PIRT team and schedules a meeting for further analysis.

Analysis and Containment

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

When an incident is confirmed to be a suspected privacy incident, the PIRT will convene and follow the incident response process. The objective of analysis and containment is to fully understand the incident scope and take actions to limit the impact of the incident.
In the analysis and containment phase the PIRT will conduct an investigation, determine the root cause, assess the risk level as well as the legal and regulatory obligations. The containment includes both technical and administrative actions needed to limit the incident. The following are key areas to cover as a part of Analysis and Containment step.

Systems and technology involved
One of the objectives of incident investigation is to identify which systems, applications, and other technologies are impacted and determine if there are known vulnerabilities or security gaps leading to the incident.

Privacy implications
Investigation should confirm the type and amount of Personal Information included as well as privacy implications to individuals. Privacy implications may vary depending on the location and categories of individuals. It will be necessary to assess the sensitivity of the Personal Information involved and the potential harm to the individuals whose information was compromised. This is one of the most important factors in assessing the potential impact of a privacy incident. Cargill Law should be consulted to review potential legal obligations relevant to the incident.

Legal and regulatory
Depending on the scope and severity of the incident, the TGRC PIRT should work with Cargill Law to determine legal or regulatory obligations. The legal and regulatory obligations may depend on the jurisdictions of the affected individuals, the location of the incident, and the requirements of the laws in the affected jurisdictions. Cargill might also have contractual obligations to a third party or compliance responsibilities specific to an industry sector that need to be evaluated.

In case of breach notification, Cargill Law will provide guidance to the PIRT. The final decision on whether to notify affected person(s) and parties is made by the CISO in consultation with Cargill Law.

Business Operations
Part of investigation should determine the potential impact to Cargill's business operations. This might include ceasing processing of Personal Information, changes to processes or procedures, or availability of technology. An incident investigation may require making key individuals available for the duration of the incident investigation.

Third party involvement
Potential impact to third parties should be evaluated as a part of analysis phase. There may be contractual obligations for Cargill or the third party depending on the nature of the incident and in whose environment it happened.

PIRT may also consider using third party services specializing on incident related activities such as investigation, forensics, breach notifications, legal counsel, etc.

Forensics investigations
The analysis phase might also include forensics investigations to determine the full impact of the breach, identify the avenue of attack, and trace the root cause of the incident back to the source. The nature of the investigation will depend on the type of breach. The investigation may be strictly internal or it may involve cooperation with law enforcement or third-party investigators. Forensics investigations should be approved according to the established process.

Containment
Containment includes immediate technical and administrative actions taken to limit the spread of the incident and damage caused by the incident. Containment plans should cover the direct effects of the incident as well as what side effects containment itself may have on other business units, network segments, users or services.
Containment strategy should consider the following:

- Potential damage to resources

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

- Need for evidence preservation
- Service availability
- Time and resources impact
- Effectiveness of containment
- Duration of the containment solution

The PIRT is responsible that the above-mentioned steps are completed as appropriate to the scope and severity of the incident. The PIRT may escalate or delegate any analysis and containment steps outside immediate team as needed.

Reputation Impact:
This refers to the potential for adverse publicity and impact to Cargill's reputation. Reputational impact is often driven by scope and harm but can also be greatly influenced by how Cargill responds to the incident.

Financial Impact:
This refers to whether, as a result of the compromise, Cargill may incur remediation costs, fines, penalties or reduced revenue from lost business.

Business/Operational Impact:
This refers to the risk of not meeting the needs of Cargill's customers, contractual obligations, or business operations and initiatives.

Remediation and Restore

In the Remediation and Restore phase the PIRT will determine the necessary actions to correct the situation caused by the incident. These actions may include the following:
Actions to bring back the technical, business and privacy capabilities to the state prior to the incident
Actions to meet legal obligations
Protection measures to affected person(s)
Remediation plan review and approval by the stakeholders
Prepare Internal and External Communications including front-line briefing materials and/or scripts for use.

PIRT, together with the appropriate stakeholders, will assign owners to the remediation and restore plan action items.

Incident Closing and Post-Mortem

Once an incident has concluded, the TGRC PIRT should hold a Post-Mortem review of the incident. The goal will be to obtain input from all participants regarding the procedures, tools, communications, and protocols involved in the incident response and to identify elements of the response that worked well and elements with opportunities for improvement. The Post-Mortem review can be accomplished by a formal meeting or via email depending on the nature of the incident.

Incident Communication and Documentation

Internal and External Communications

Privacy incident communication includes incident operations communication, informative communication about the incident, and formal statements and media releases. Depending on the scope and severity of the incident the TGRC PIRT should work with Business Owner, Law and Corporate Communications to develop and distribute internal and external communications regarding the incident.

In general, GPO owns communication regarding incident operations within the PIRT team, CISO, and third-party breach notification service provider. TRCM and Business Owners communicate with the Cargill Business and Functions as well as to impacted employees. The CISO owns the communication to external investigative authorities, and Law communicates with external regulatory or compliance authorities as necessary.

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

Informative communication about the incident is mainly owned by the CISO. Any formal statements or media releases are undertaken by Corporate Affairs or the CISO together with Cargill Law.

Breach Notification

There may be several parties that need to be notified in the event of a breach. These parties might include, but are not limited to, employees, law enforcement agencies, credit card companies, regulatory authorities, customers, and other third parties.

The decision to notify depends upon the jurisdictions of the affected individuals, the location of the incident, and the requirements of the breach notification laws in the affected jurisdictions. The trigger for notification to affected persons varies by breach notification law. As laws and regulations often change, Cargill Law should always be consulted to obtain the most up-to-date information as it relates to breach notification laws.

In the U.S. Cargill has partnered with an external service provider to provide support for notification writing and production. The TGRC PIRT should work with the service provider to facilitate and monitor the quality of this process.

The service provider will provide a template for the notification letter as well as other necessary help during the notification process. Cargill Law must review all breach notification communications prior to distribution.
The service provider will also perform breach notification and call management for the breach event as well as provide staffed support line as a part of breach notification service.

Outside the U.S., the first point of contact for Law should be the Cargill Law Privacy contact for the region. The Cargill Law Privacy contact will facilitate the required activities in conjunction with local resources and the PIRT team. It should be noted that some jurisdictions have specific time periods within which regulatory authorities must be notified of a data breach.

Website and Support Line

In the event of a mass breach affecting a large number of customers, some breach laws require a business entity to host a website as a mechanism to reach affected customers. The hosted website should indicate the notice of a breach and provide a mechanism to address customer concerns. A typical mechanism to address customer concerns may include creating a staffed, toll-free hotline number to allow affected customers to contact Cargill regarding the breach.

Documentation

Privacy incidents are logged and documented in the Archer system. GPO and CSIRT are responsible for ensuring that a sufficient level of incident process documentation as well as evidence material relevant to the incident are captured and saved in Archer.

Legal Actions

Depending on the nature of the incident and whether it becomes public knowledge, it is possible that legal actions may be initiated. To manage this risk, the TGRC PIRT should keep Cargill Law informed of all details of the incident and must forward any incoming calls or letters concerning possible legal actions to Cargill Law immediately.

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.

Plan and Process Maintenance

The Privacy Incident Response Plan and related Incident Response processes should be reviewed annually to keep all elements up to date and relevant to Cargill's needs. The Global Privacy Office Manager is responsible for the maintenance of the Privacy Incident Response Plan.

Under the direction of the Global Privacy Office Manager, the GPO will review and update the Privacy Incident Response Plan accordingly. The review will address changes to the following elements:

- New country or state breach notification laws or changes to existing laws
- New or updated Cargill Policies and procedures
- Organizational changes, new contacts or new TGRC PIRT team members, transfers or departures which would impact the contact list in the PIRT Process Worksheet.
- Process improvements identified through periodic testing process.

General information about global breach notification obligations can be located here. Cargill Law should be consulted on specific guidance and interpretation of data breach and data privacy laws.