How to Handle Breach Incidents Involving Personal Information

Flavio Gerbino
Defense Department, scip AG
flge@scip.ch
https://www.scip.ch

Marc Ruef (Editor)
Research Department, scip AG
maru@scip.ch
https://www.scip.ch

Keywords: Assessment, Cloud, Detect, Forensic, Fraud, Gender, Identity, Identity Theft, Law, Legal

1. Preface

This paper was written in 2014 as part of a research project at scip AG, Switzerland. It was initially published online at *https://www.scip.ch/en/?labs.20140410* and is available in English and German. Providing our clients with innovative research for the information technology of the future is an essential part of our company culture.

2. Introduction

Companies typically have sophisticated security incident procedures in place to handle all kinds of issues emerging from possible security events related to their IT environment. Many of those procedures do not consider the affected assets enough and are restricted to IT components. That's why I have created a short overview on how to respond to and manage an information security incident with the primary focus on breach incidents involving Personal Information on paper or on IT systems.

3. Prerequisites

To be able to include the suggestions I am outlining in this article a company should already have established an appropriate security incident response and breach notification plan. This plan should consider the local legal and regulatory accounts as well as business and functional needs. A Risk Management System with appropriate risk measurement guidelines is as well an inevitable instrument that must already be in place.

4. Definitions of Important Terms

- **IT systems:** Computer hardware and software, network elements, Databases, Notebooks, Smartphones, and other electronic devices used to process, transmit, or store information (Clouds are also included here).
- **Personal Information:** Any information (as defined by local Data Protection Legislation) relating to an identified or identifiable person; an identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to factors specific to his physical, physiological, mental, economic, cultural or social identity. This includes information such as name, home address, office address, e-mail address, age, gender, family information, profession, education, professional affiliations, salary, health information and credit card numbers.
- **Data Security Incident (Breach Incident):** Based on the above definition of Personal Information this means loss or misuse of Personal Information, the accidental, unauthorized and/or unlawful access or handling of Personal Information, or any other act or omission that compromises the security, confidentiality and/or integrity of Personal Information. Data Security Incidents include, among other things, the loss of paper files and a portable electronic device, such as laptops and CDs, containing Personal Information.

Here are some Data Security Incidents as examples to see the different focus compared to *classic* incident response which is more IT driven (not conclusive…)

- Loss or theft of a server, desktop, laptop, mobile device, disk, tape, paper files, USB sticks or other storage device containing Personal Information, even if such information is appropriately protected (i.e. encrypted data or redacted)
- Loss of storage devices
- Loss of Data in a cloud
- Violations of established privacy and information security policy
- Violations of company policies designed to safeguard the privacy and security of Personal Information such as the unencrypted transmission of sensitive Personal Information that the company requires to transmit securely
- Unauthorized access to Information from the outside
- A successful intrusion of the Company's IT systems containing unencrypted and unredacted Personal Information or unauthorized access onto property that enables the intruder to access hard copies containing personal information
- Unauthorized internal access. Access rights should be clearly governed in appropriate access policy.
- Inadvertent disclosure: This means the disclosure of Personal Information to an unauthorized person via electronic mail, post or any other means; this includes the situation where e-mails or paper documents are sent to the wrong recipient.

5. Additional Tasks and Members for the Existing Incident Response Team in Case of Breach Incidents Involving Personal Information

To be ready to handle breaches with Personal Data involved an existing Incident Response Team should additionally be charged with the following tasks:

- Analyse, review and investigate the circumstances of the incident related to Data Privacy
- Secure the affected systems (e.g. for further forensic analysis)
- Review and report on legal requirements regarding whether to notify law enforcement and/or affected individuals
- Establish notification requirements to government authorities or affected individuals

When an Incident includes the breach of Data Privacy the response Team must include additional representatives to assure a proper handling according with legal requirements (especially in cases involving employee fraud or misconduct)

- Legal Department (Data Privacy)
- Human resources in cases involving employee data
- Information Security (e.g. CSO)
- Corporate Security (e.g. CSO)

The team should also include senior (management) members from the following departments, depending on the severity and characteristics of the incident

- Internal auditing (IT compliance)
- Communications, Media- / Public Relations
- Finance- / Purchasing & Administration (if there is third party involved)
- External legal counsels
- Forensic analysts

6. Handling of Data Security Incidents

The Action Plan should include the following simplified key steps (not conclusive):

1. **Preparative Assessment:** As a preliminary duty for a Data Security Incident, the Incident Response Team should take the following appropriate preparation actions:
    1. Nominate an individual to investigate possible circumstances of the incident. This individual should bring experience and enough authority to conduct the initial investigation, document the findings in a written report and make recommendations to the Incident Response Team. Typically this person is a senior security representative (e.g. from the CSO Team/organization). From a Data Privacy point of view the following facts need to be checked (additionally to what is anyway being investigated as part of security incidents in any case):
        - The type of systems or files that were compromised (IT Systems, paper files or other)
        - The type of information involved (including whether any Personal Information is at risk and if so, the origin of such data)
        - The persons involved in or responsible for the breach.
    2. Consider whether any external resources are required for assistance. (Including law enforcement in the investigation, consult with outside legal counsel, or enlist other third-party assistance such a forensic analyst).
    3. Identify the need to assemble a broader team to deal with the Data Security Incident.
    4. Determine the need to report
    5. Detect the circumstances of the Security Incident.
2. **Risk Assessment:** In the second step the type and amount of Personal Information at risk, the extent of the incident, the persons affected by the incidents and the risk of harm to individuals and the company should be assessed.
    - The understanding and awareness of following factors is necessary to evaluate the risk:
        - What type of Personal Information is involved?
        - What is the sensitivity of the information? Generally, the more sensitive the information, the higher the risk of harm. (A combination of Personal Information should be valued as more sensitive than a single piece of information. However sensitivity alone is not the only criteria in assessing risk, as expected harm to individuals is also extremely important.)
        - How many individuals are affected by the breach? Assessing the number of individuals affected will help you to estimate the severity of the problem and will be relevant in deciding whether or not to notify local privacy authorities.
        - With lost data, what protections were in place to protect the information at the time of the breach (e.g. encryption and was the Personal Information adequately protected).
        - Who is affected by the incident (employees, contractors, public, clients, service providers, other)
        - Can the Personal Information be used by third parties for fraudulent or otherwise harmful purposes.
        - Was the breach inadvertent or intentional
        - Is there a risk of further exposure of the Personal Information

        - If the Personal Information was stolen, can it be determined whether the Personal Information was the target of the theft.
        - Can the Personal Information be recovered
    - After having clarity about the above factors risk of harm to Individuals should be evaluated (Identify whether harm to individuals may result from the Incident):
        - If the data has been stolen, what is the potential risk of misuse?
        - What harm to the individuals could result from the breach?
            - Identity theft
            - Financial loss
            - Loss of business or employment opportunities
            - Humiliation, damage to reputation or relationships
    - After having a conclusion from the risk evaluation, the Incident Response Team will be able to decide whether notification to individuals and appropriate privacy authorities is required or indicated.
3. **Notification:** The Legal Department should take responsibility for providing any required notice to governmental authorities, including authorities in other jurisdictions, if required. (If notification is required by law, the affected individuals should be notified as promptly as possible, consistent with both the terms of the applicable law and the need to conduct and complete any investigation. Even if notification is not required by law, notification is strongly recommended if the Data Security Incident presents a risk of fraud or identity theft to affected individuals.
4. **Prevention:** A final incident report should include short and long term steps to prevent further incidents:
    - A security audit of security measures
    - A review of policies and procedures, necessary to reflect the lessons learned from the incident
    - Ban on bulk transfers of data onto removable media without adequate security protection
    - Secure couriers and appropriate tamper proof packaging in the transport of bulk data, where applicable to the breach situation.
    - Some Data Security Incidents should be immediately reported to senior Management :
        - Incident where data concerning a substantial number of individuals is involved or where highly sensitive data are concerned
        - Where incident is likely to be published in a national or international newspaper
    - Good reporting gives also overview of data security incidents and is required to document main issues and gaps that have been learned from the incidents. In addition, reporting ensures compliance with disclosure obligations, where applicable, as well as a timely and complete information to the Board.

7. Conclusion

Reading newspapers and seeing the increasing amount of incidents reports related to data privacy today should open your eyes and raise your awareness about the very important fact that privacy and data protection matters more than ever! Establishing appropriate technical, conceptional as well as organizational protection and safeguards to protect sensitive data is the first step of adequate attention to your data.

The constant care and due diligence during its lifecycle would be the second step. But apart from that you still need to be ready for emergencies in order to avoid bad surprises related to breach incidents involving personal information and sensitive data. This can be accomplished by considering the special characteristics and exceptional value of your data assets in your existing incident response procedures from the beginning to ensure an effective and professional handling in case of an incident.