Proposed Incident Response Methodology for Data Leakage

Presenting the best processes and procedures tosafeguardyour business while preventing data leakage

Alex Rabello, Junior Goulart, Marcelo Karam, Marcos Pitanga, Reinaldo Gomes Baldoino Filho and Ronaldo Ricioni
IESB University Center
alex.rabello@privamax.com.br, jgoulart@vidalink.com.br, karam@unb.br, marcos.pitanga@talkcomm.com.br,
reinaldo.baldoino@iesb.edu.br and ronaldo@r3force.com

Abstract - Most Brazilian companies disregard the national privacy law (LGPD) by not ensuring data governance and well-managed security controls with technical and organizational measures to prevent data leakage. Brazilian LGPD specifies that organizations must report to the national authority (ANPD) and the data subject if any security incident occurs that could cause relevant risk to the data subject. However, this privacy law lacks information on how to respond effectively to data leakage by embracing preventive measures against data breaches. The appropriate approach to handling data leakage is to invest in trained personnel, cutting-edge technology, and processes, enabling a proper incident response methodology. Organizations will be more willing to comply with the privacy law by administering a more approachable and straightforward path for security and privacy best practices. The development of this methodology is based on the international standard (ISO 27035) and some recommendations from the NIST 800-61 publication. The adaptation of these standards provides a more detailed checklist for determining when to perform incident reporting and transparency to the Brazilian authority (ANPD) and data subjects. Other points discussed are related to properly building the security incident response team, using security automation tools and playbook resources to ensure the application of best practices by handling data leakage processes.

Keywords-Data Leakage; Information Security; Incidents; LGPD.

I. INTRODUCTION

The advent of privacy and data protection laws and regulations worldwide raises one of the most relevant questions for most organizations: Has your company ever suffered a data leak? If so, the business impact of responding publicly with transparency can be massive, with the imposition of significant fines and the loss of customer trust affecting the company's reputation. Otherwise, in most cases, if a company has not had leaked data, it is because it has not yet been the target of attacks or because it has invested in strategic and tactical actions to avoid Information Security incidents.

The purpose of this article is to describe a methodology to propose best practices for the Information Security Incident Management, following the definitions and concepts standardized by the International Standards Organization (ISO / IEC 27035) [6] and some procedures described by the National Institute of Standards and Technology(NIST 800-61) [7] publication, with applicability in the context of personal data protection as it is the evolution of the Information Security applied to the current scenarios of data leakage.

In the media, reports of data leaks, cyber-attacks, and selling of information, including disclosure of confidential data, are frequently published by the Ponemon Institute and IBM Security [5], disclosing the cost of a data breach, for example, on average, the time to identify and contain a data breach is 280 days, and 80% of the breaches relate to the leakage of personal customer data.

Examples of security incidents may include system or service malfunctions, cyber-attacks (such as social engineering or denial of service), unauthorized access to confidential/restricted data, sending or receiving malicious code, changes to a system without owner approval, loss, misplacement, theft of data or equipment containing critical/sensitive information. These security vulnerabilities in organizations are among the greatest threats to privacy and data protection in the 21st century.

In this context, it becomes inevitable for any organization to prioritize incident governance and management of Information Security events to deal with breaches involving personal data leakage.

Some questions that guided the article:

- ***What is the proper way to analyze security incidents?***
- ***How to handle a risk analysis to avoid data breaches?***
- ***How can companies adopt a methodology for Security***
- ***Incident Management involving data leakages?***
- ***What is the appropriate communication and notification to the national authority and data subjects?***

The following Section II describes the standard frameworks applied for information security incident management and their phases to handle a lifecycle of the incident related to data leakage. Section III demonstrates the proposed methodology focusing on the key points to be addressed during incident security response. Topics IV, V, and VI provide specific data leakage scenarios and the appropriate solutions available to address the incident response.

 ISBN: 978-1-61208-894-5

II. Standards and Frameworks for Information Security Incident Management

ISO standards and NIST publications are recommended tools that can help organize and manage security incident response for any organization. The NIST 800-61 publication brings crucial insight into the structure of the incident response team, including three models: centralized, distributed, and coordinated. To choose the appropriate model, size and possible locations of the organization must be evaluated, but there are also other vital decisions, such as defining 24/7 availability, being composed of people working either whole or part-time, having in-person or outsourced work, cost of hiring based on experience and level of knowledge and evaluating stress factors. Regarding the incident response lifecycle, NIST recommends four phases: 1. Preparation, 2. Detection and Analysis, 3. Containment, Eradication and Recovery, and 4. Post-Incident Activities.

ISO/IEC 27035 standard is divided into three parts: Incident Management Principles (ISO/IEC 27035-1), Guidelines for Planning and Preparedness for Incident Response (ISO/IEC 27035-2), and Guidelines for Incident Response Operations incidents (ISO/IEC 27035-3). According to ISO/IEC 27035, a fundamental part of an organization's overall information security strategy must establish controls and procedures to prevent or contain the impact of information security incidents, reducing the direct and indirect costs caused by incidents. The main steps to minimize the adverse effects of information security incidents are 1. Plan and Prepare, 2. Detection and Reporting, 3. Evaluation and Decision, 4. Responses and 5. Lessons Learned.

III. Proposal for an Incident Response Methodology for Data Leakage

Our proposed incident response management methodology for personal data leakage scenarios is based on a response framework adapted to the context of personal data protection. An appropriate incident response plan prepares the team to handle threats, notifies incidents, isolates incidents, identifies severity, contains the attack, eradicates the underlying cause, recovers production systems, and conducts a post-mortem analysis to prevent future episodes.

A. Formation of the incident response team

The incident response team, also known as Computer Security Incident Response Team(CSIRT) [1], consists mainly of members of the privacy, information security, and legal team, with pre-established roles, objectives, and goals for each member of the team. The team will improve upon implementing procedures and processes to dominate the sector in which it operates, bringing the concepts of the cybersecurity ecosystem closer to the operational reality of the organization. It is essential to recruit and train the members in team building, ensuring they have access to the relevant systems and technologies for the best performance quality.

B. Defining the roles and responsibilities

The responsibilities involved are defined in the roles of a Chief Information Security Officer (CISO), Data Protection Officer (DPO) in case of data subject breaches, incident response manager, security analyst, threat researcher, legal representative, corporate communications, risk management, and external forensic security experts.

Among the main objectives of the incident response team, such as incident analysis, documenting the extent, priority, and impact of a breach, to see what assets are affected and whether the incident requires attention. With this, the team must plan and document procedures are containing the description of the incident response plans for different types of occurrences, severity levels, and affected regulatory bodies.

C. Plan and identify the risks

Another relevant procedure refers to implementing a risk assessment in case of cyber-attacks, knowing the most valuable assets and possible critical impacts on the organization's business. In addition to establishing a communication plan declaring the situations that require or not the issuance of internal and external notifications, depending on the level of impact and extent of violations of personal data of the holders. This methodology enforces the contextualization and adequacy given to the treatment of infringements containing personal data, not observed in the ISO/IEC 27,035 and NIST 800-61 standards, such as the figure of the DPO and notifications referring to violations containing personal data. In addition, it should be defined which will use tools to record and document incidents and mechanisms for detection and correlation of events and anomalies to obtain predictability and generate evidence records in audits supporting analysis of the incident.

D. Selecting the proper security tools

Incident response tools work with applied security measures, obtaining response information via network traffic analysis, system logs, endpoint alerts, and identity systems to detect network security-related anomalies. These tools investigate malware infections, password attacks, phishing, information leakage, privilege abuse, and other internal and external threats.

Information gathered from security tools, and IT systems should be kept in a central location, such as a Security Information Event Management (SIEM) [9], which consolidates events and logs from all types of critical computing resources. As a result, this information should be used to create an incident timeline and conduct an incident investigation with all relevant data points in one place. Technology alone cannot detect security breaches therefore, human perception must be trusted where the security operation team carefully monitoring events and behaviors, highlighting the following action approaches:

- Network traffic anomalies on sensitive internally used connections and servers that typically have a stable and predictable traffic volume;
- Access accounts without elite or administrator permission levels for more information and systems than

 ISBN: 978-1-61208-894-5

regular employees. Since employees tend to be the most accessible entry point into cybercrime, it is relevant to closely monitor accounts with administrator profiles, noting the increase in privileges on standard user accounts.

• Excessive consumption and suspicious files when observing an increase in the performance of the memory or hard disks in the environment could signal someone illegally accessing or leaking data.

• Use modern security tools, such as User and Entity Behavioral Analytics (UEBA) [11], which automatically identify anomalies in user behavior or file access. Provides a much better coverage of potential security incidents and saves time for security teams.

E. Handling incidents and threats

After developing an information security team specializing in monitoring threats and anomalies, it is necessary to detail how the organization will handle the incident. In conjunction with privacy and data protection experts, this information security team must determine what types of data are involved and assess the potential harm caused, evaluating any jurisdictional or industry laws that the company needs to comply with.

The proposed methodology gives the incident response team an accurate analysis of the severity of the breach involving personal data and the need for escalation to the national authority (ANPD), as required by various legislations, including the GDPR and the LGPD.

F. Incident investigation and recording

Investigations are based on two types of incident input to be handled: IT systems gather events from monitoring tools, log files, error messages, firewalls, and intrusion detection systems. This data must be analyzed by automated means and security analysts to decide whether anomalous events represent security incidents. There can be a report of a user from any area of the organization who submits a new happening in the system reporting an occurrence stating the cause of the incident, assets, and suppliers involved. This activation carried out via the incident system must follow a treatment flow. There is a prior assessment by a member of the information security team enabling classification of the type of incident, severity, the risk to the business, and possible impacts on personal data.

All evidence and records must be collected and preserved in case any criminal activity is recorded. Preservation of proof during screening and scope should be considered, especially if it becomes apparent that the incident involves illegal activity or data breaches. This methodology extends the need to preserve evidence and records for violations involving personal data, even if it is not criminal activity, aiming at the defense in possible lawsuits based on privacy filed by the data subjects and administrative data by the national authority (ANPD).

Proper preservation of evidence requires establishing a chain of custody procedures that must properly track any electronic evidence.

G. Incident containment, recovery and remediation

The next step in the process, called containment, aims to isolate the security incident to prevent further damage to the organization. The strategy to limit damage to organizational resources involves activating the information security team that works in management and control of confidentiality detection and protection resources to identify which business process is affected so that it is possible to isolate the problem. The priority is to have short-term containment with an instant response so that the threat no longer causes damage, but also to provide for long-term containment, planning corrective actions on affected systems, taking measures to prevent the incident from recurring or augment, such as installing the latest security patches on affected and associated systems, removing accounts and backdoors created by intruders, changing firewall rules involving the intruder's address, etc.

The information security team working on remediation must isolate the root cause of the attack, removing threats and malware, and identifying ways to mitigate vulnerabilities that have been exploited to prevent future episodes. These steps make configuration updates with a focus on minimizing the negative effect on the organization's operations. Choosing the proper way to accomplish this is to limit the amount of data exposed. In acting to recover affected systems, there must be guidelines to minimize the chance of another related incident.

H. Post Incident activities

Therefore, must validate that another incident does not occur by restoring clean backup systems, replacing compromised files with clean versions, rebuilding systems from scratch, installing patches, changing passwords, and strengthening network perimeter security (router access control lists rules, firewall rule sets, etc.). It would help to consider how long it would take to monitor the network system and verify that the affected systems are functioning normally. Therefore, the cost of the breach and the associated damages are minimized.

I. Comunnication and Data Breach notification

In cases of high risk of data breach and possible impacts on privacy, the flow should include an immediate notification to all members of the communication team and crisis team/committee, data protection officer (DPO), third-party vendors and executives involved, as well as actions to preserve all physical evidence regarding the location of the breach with detailed documentation of the incident to be used in the development of the incident response and forensic investigation process when necessary.

This methodology understands that the DPO must be promptly informed about all the steps in handling incidents involving the breach of personal data, especially about the increased risk. So that it is possible to exercise its role as an interlocutor between the organization, national authority (ANPD), and the data subjects, following the federal privacy law (LGPD). If determined during the previous phases of the incident response plan, the responsible team will communicate following the notification process where

 ISBN: 978-1-61208-894-5

strategic communication and dissemination are developed for external audiences and internal staff.

J. Review and Process Improvement (PDCA)

Once critical incidents are addressed, and the systems involved are recovered, the organization should hold a meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices.

Information gathered from these meetings should identify and correct systemic weaknesses and deficiencies in policies and procedures. The security specialist must determine how the incident was managed, revalidating what took action to recover the attacked system, the areas where the response team needed improvement, and the areas where they were effective. Evidence reports provide a clear review of the entire incident and can be used in meetings, as benchmarks for comparison, or as training information for new incident response team members.

K. Development of an incident response playbook

In addition, the root cause analysis must be prepared so that complete documentation is provided with greater accuracy after the incident response process, which also helps to improve the process for prioritizing technical data protection measures aligned with the organization's cyber risks.

Gerard Johansen [3], can elaborate the steps of the incident response plan with a set of instructions and actions described in a playbook process, where the risks of critical threats must be evaluated, indicating the appropriate scenario to be followed.

Due to the large volume of incidents, and the short deadlines present in the legislation for the notification of violations involving personal data, within 48 hours for a response (LGPD) and 72 hours (GDPR), we believe it is necessary that these best predictability practices can be automated with the implementation of a playbook process, building a continuous flow of known approaches to handling recurrent or similar cases. The methods described in this playbook should seek to identify patterns, deeply understanding the TTP (Tactics, Techniques, and Procedures) [8] commonly used by threats, performing governance based on threat scenarios with use cases instead of just rules, and using connected and integrated security platforms using technology such as Security Orchestration, Automation, and Response (SOAR) [12] for a centralized approach with the ability to automate incident response, including personal data breaches.

IV. Scenario Analysis of Data Leakage to Apply DLP Solutions

Technology capabilities for preventing data loss or leakage are defined by a strategic program that detects, monitors, and blocks potential breaches of sensitive data while in use (endpoint actions), in-motion (network traffic), and at rest (storage data).

Following Bose et al. [12], data leakage is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or restore lost information. Data leakage is distinguished from data unavailability, such as that arise from a network outage. According to Xi et al. [13], it is also essential to check the data loss in the use of mobile platforms because there has been a significant growth in the usability of mobile equipment with innovative platforms, unintentional loss of sensitive data due to a malicious agent, an inside job, or an unknown employee can lead to significant financial loss and reputational damage for any organization. To avoid these damages and losses, it is imperative to implement solutions for data loss prevention (DLP) [2], which can include:

- DLP Endpoint (end-user device) when the user has a scope of data on desktop, laptop, USB storage, and virtual desktop.
- DLP for data at rest or storage is usually unstructured data that resides on a server or structured data that resides in databases.
- Network DLP is applied to data that transits or leaves the network to the Internet and.
- DLP for cloud is data residing in Google Workspace, Microsoft 365, and other personal cloud providers.

DLP methods [10] are designed to discover and analyze content and context to determine if the presented data matches a pattern or expression of an identification number or a specific keyword. Once the way is reached, a violation or alert can be generated, and it is sent to a management console for review by an incident triage and support analyst.

When evaluating some proposed scenarios, the possible focus of data leakage should be identified, for example, of a fictitious company that processes medical insurance claims for a regulated health care organization. They are aware that sensitive personal data resides on file servers, but they are unsure where the data is located. In this case, we should prioritize the analysis in the resting DLP solution. The strategy would include an unstructured data discovery scan, which will scan the selected storage and find data matching the keyword pattern (health data) as stated in the scan policy. Another common scenario is when a Human Resources (HR) manager learns that some department members have emailed sensitive files to their email address to work on corporate requests overdue over the weekend. To address this situation, we must prioritize the use of DLP for networks and endpoints. Also, can create a network security policy to prevent file uploads to personal email platforms. DLP for Endpoint can also detect HTTP/HTTPS connections as data leaves the Endpoint to the Internet.

 ISBN: 978-1-61208-894-5

V. CONCLUSION

As a result of applying the proposed methodology, some factors are observed as gaps to be treated about the procedures and recommendations of the NIST and ISO standards. One of these factors is the use of automation in incident processing driven due to the significant increase in recent years and the short deadlines established by legislation for notification of personal data breaches, and the possibility of automating many processing tasks with retransmission to systems and IT tools, reducing the amount of human activity and human decisions required. Suppose the organization already has an incident response team. In that case, it must carefully consider all the team building factors provided in the NIST document, adding professionals with privacy and data protection knowledge, and dual user verification of all processes, except for the DPO. As emphasized by NIST, handling incidents is a complex task, which can customize by implementing security automation.

An important point within this proposal is the massive and in-depth training of information security teams, especially those responsible for handling the response to incidents, so that they prepare adequate documentation for the proper chain of custody, thus tracing the entire timeline along with the proper procedures to safeguard the environment, avoiding the contamination of evidence, which may be necessary for a more in-depth investigation in the civil/criminal scope that can use to prove the truth with the national data protection authorities or in the public judicial spheres for the judgment of the rights of the holders.

In terms of the ISO / IEC 27035 approach, this standard describes and details incident management and allows an organization to apply prevention proactively. However, this approach depends on the effectiveness of the lessons learned and continuous improvement of treating incident management as a linear or cyclical activity.

The adaptation of the incident response methodology also allows for the inclusion of a checklist of actions to decide when it is time to notify the incidents to ANPD, as well as the data subjects, as in the ISO standard and the NIST recommendation, these notification procedures are not as emphasized concerning the importance of this requirement stated in the LGPD law.

REFERENCES

[1] J.Novak, D. Mcintire, A. Hueca, B. Manley, S. Mudd and T. Bills , Technical Report - The Sector CSIRT Framework, [Online]. June2021,Available from: https://resources.sei.cmu.edu/assetfiles/TechnicalReport/2021_005_001_734796.pdf 2021.08.25

[2] A. Gorecki, “Cyber Breach Response that actually works”, Willey 2020.

[3] G. Johansen, “Digital Forensics and Incident Response, 2nd ed.” Packt Publishing, Birmingham, UK, 2020.

[4] LGPD: Lei Geral de Proteção de dados 13.709.[Online]. Available from:http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm 2021.07.23

[5] Ponemon Institute: The cost of a Data Breach report.[Online]. Available from: https://www.ibm.com/security/data-breach

[6] ISO/IEC 27035:Information technology - Security techniques - Information security incident management.[Online]. Available from: https://www.iso.org/standard/60803.html

[7] NIST 800-61:NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide.[Online]. Available from: https://www.nist.gov/privacy-framework/nist-sp-800-61

[8] Threat Intelligence: Radware. [Online]. Available from: https://www.radware.com/getattachment/Security/Hackers-Corner/2218/HackersCorner-TTPsDDoS-FINAL-V3.pdf.aspx?lang=en-US

[9] Security information and event management (SIEM) technology: Gartner.[Online]. Available from: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[10] The practical executive's guide to Data Loss Prevention:Forcepoint.[Online]. Available from: https://media.bitpipe.com/io_14x/io_147455/item_1939907/whitepaper_practical_executives_guide_data_loss_prevention_en%20%283%29.pdf

[11] User and Entity Behavioral Analytics (UEBA): Forcepoint.[Online]. Available from: https://www.forcepoint.com/pt-br/product/ueba-user-entity-behavior-analytics

[12] Security Orchestration, Automation, and Response (SOAR).[Online]. Available from: https://searchsecurity.techtarget.com/definition/SOAR

[13] Bose, Neetu, and N. Vishwanath. "An Improved Method for Preventing Data Leakage in an Organization."

[14] Xi, Ning, et al. "Information flow based defensive chain for data leakage detection and prevention: a survey." arXiv preprint arXiv:2106.04951 (2021).

 ISBN: 978-1-61208-894-5