ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (136-138), Month: January - March 2021, Available at: www.researchpublish.com

METHOD AND SYSTEM FOR DATA LOSS PREVENTION MANAGEMENT

Rafiq Ajmal Khurshid[1], Saad Farhan Al-Anazi[2], Abdullah Tariq Al-Essa[3]

[1,2]Affiliation None

[1,2]Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **A method and system are required for improving data loss prevention Incident Investigation Process by shifting from a traditional, reactive approach to proactive approach and from a manual to automated incident management process. This will involve all stakeholders and result in a reduction of the risk of data leakages. This article describes a computer-implemented method that includes: detecting an incident that violates a Data Loss Prevention (DLP) rule of an enterprise, wherein the DLP rule specifies contents that are reserved for within the enterprise; automatically alerting one or more members of the enterprise of the incident based on a report detailing the incident; and receiving a response from each of the one or more members of the enterprise.**

Keywords: **Data Loss Prevention, Data Leakage Prevention, Incident Management Process, Incident Investigation Process.**

I. INTRODUCTION

More companies are looking for the protection of an organization's data from both outside threats as well as individuals within an organization that may compromise the data. Accordingly, many organizations use various investigative entities to identify and review data transfers that may violate one or more security policies.

Data loss prevention (DLP) is the practice of detecting and preventing confidential data from being "leaked" out of an organization's boundaries for unauthorized use. The proposed method and system for data loss prevention management introduces a selection of concepts to extend DLP capabilities in a decentralized management of security operations for large enterprises to restrict end-users from sending sensitive or critical information outside the corporate network.

It describes a computer-implemented method that includes: detecting an incident that violates a data leakage prevention (DLP) rule of an enterprise, wherein the DLP rule specifies contents that are reserved for within the enterprise; automatically alerting one or more members of the enterprise of the incident based on a report detailing the incident; and receiving a response from each of the one or more members of the enterprise.

II. DETAILED DESCRIPTION

The proposed DLP method and system, which involve all stakeholders, have been designed to expedite the DLP incident investigation and provide granular visibility into and control over user activities.

A method may include obtaining, from a user device, a first feedback from a first predetermined party regarding a data loss prevention (DLP) event through a graphical user interface (GUI). The method may further include determining whether the DLP event is authorized using the first feedback. The method may further include transmitting, automatically in response to determining that the DLP event is not authorized, a request for a second feedback by a second predetermined party using the GUI. The second predetermined party may be selected for the request automatically according to a routing queue. The method may further include obtaining, in response to transmitting the request for the second feedback, a selection of a security action regarding the DLP event using the GUI. The method may further include transmitting, automatically in response to the selection of the security action, a command that initiates the security action.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (136-138), Month: January - March 2021, Available at: www.researchpublish.com

Fig. 1 below illustrates the proposed DLP incident investigation process.

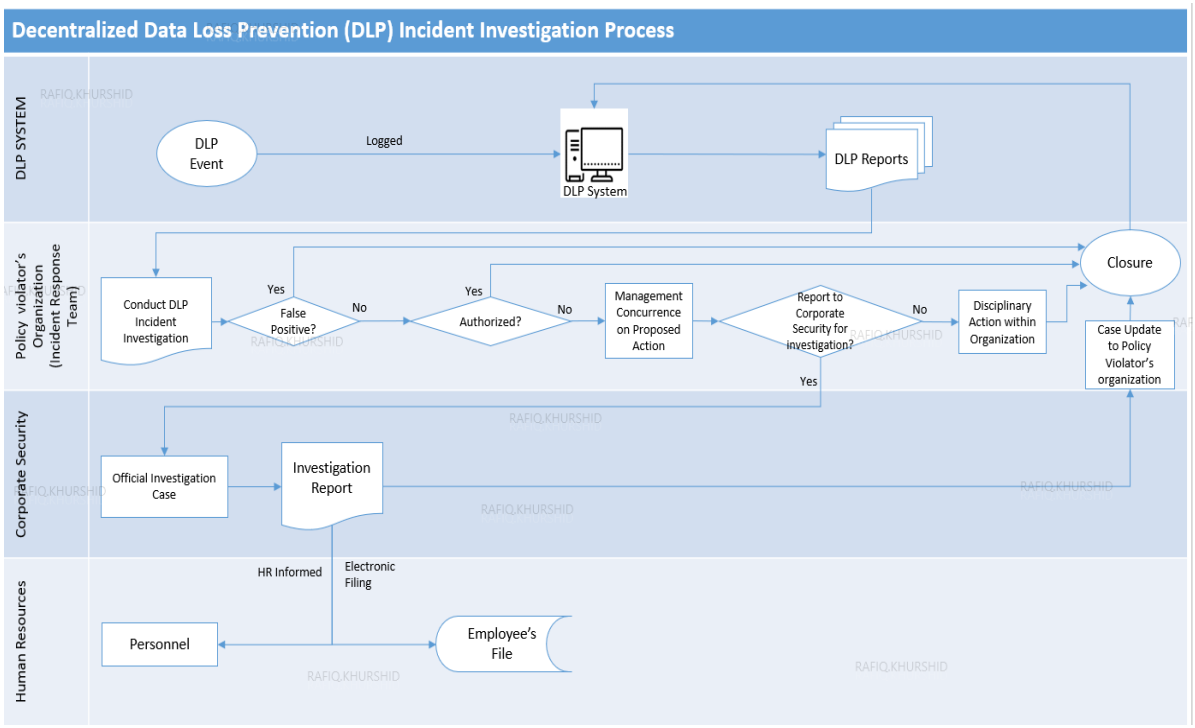

Fig. 1: DLP Incident Investigation Process

The main features of the proposed DLP method and system are as follows:

- Online review and approval of DLP incidents by all stakeholders
- Electronic Filing of DLP Investigation Report
- Integrate with the Corporate HR system
- Conduct DLP Incident Investigation and make recommendation (By Incident Response Team of policy violator)
- Secure concurrence from Organization Head of DLP Policy violator's organization on assessment made by DLP Incident Investigation Team
- Conduct Investigation by Corporate Security organization and complete DLP Investigation Report
- Secure approval from Org. Head of Corporate Security organization on DLP Investigation Report
- Personnel Department & DLP Policy violator's organization to be notified on DLP Investigation Report
- DLP Investigation Report to be filed electronically in the HR Employee Filing System

The method includes routing DLP incidents, when flagged, automatically to the Incident Response Team of policy violator (a role to be defined in each organization for reviewing DLP incidents) for assessment and recommendation. User Interface is provided to Incident Response Team to review and capture their feedback on the incident as follows:

- Identify DLP incident as False Positive OR
- Identify DLP incident as Authorized OR
- Identify DLP incident as Un-Authorized:
- For Unauthorized Incident, User input is required to select:
  - "Require Disciplinary Action within Organization" OR
  - "Report to Corporate Security organization for Investigation"

After completion of assessment by the DLP Incident Response Team, the method further includes automatically routing DLP incident details to the Organization Head of DLP Policy violator's organization for review and approval. When incident marked "Un-Authorized" and approved by Organization Head of DLP Policy violator's organization, DLP Investigation Report to be generated and filed electronically within Corporate Human Resource (HR) system as part of employee's (Policy violator) electronic filing system (eFile).

The method further includes automatically routing DLP Investigation Request with Incident details to Corporate Security organization to conduct a formal investigation and securing approval on DLP Investigation Report from Org. Head of Corporate Security organization in accordance with company policy.

In the end, the DLP Investigations report, prepared by the Corporate Security organization, automatically routed to Organization Head and Personnel Department for further action. Also, file the Investigation report electronically in the Corporate Human Resource (HR) system as part of the employee's (Policy violator) electronic filing system (eFile).

III. CONCLUSION

To maximize the business value of your Data Loss Prevention (DLP) solution, transformation is required from traditional and reactive incident management approach to pro-active incident management approach to protect sensitive data and to gain granular visibility into and control over user activities. Online review of DLP incidents by all stakeholders along with approval and filing of DLP Investigation Report electronically will expedite the DLP incident investigation and reduces the risk of data leakage.

REFERENCES

[1] "EY_Data_Loss_Prevention - Insights on governance risk and compliance", October 2011, Ernst & Young, https://www.coursehero.com/file/16255515/EY-Data-Loss-Prevention/