DLP Assure

Reference Architecture: Envisioning a Data Loss Prevention Team Structure

Author: Denis John Kattithara, DLP Assure

Date: 05th April, 2021

Document Control

Revision History

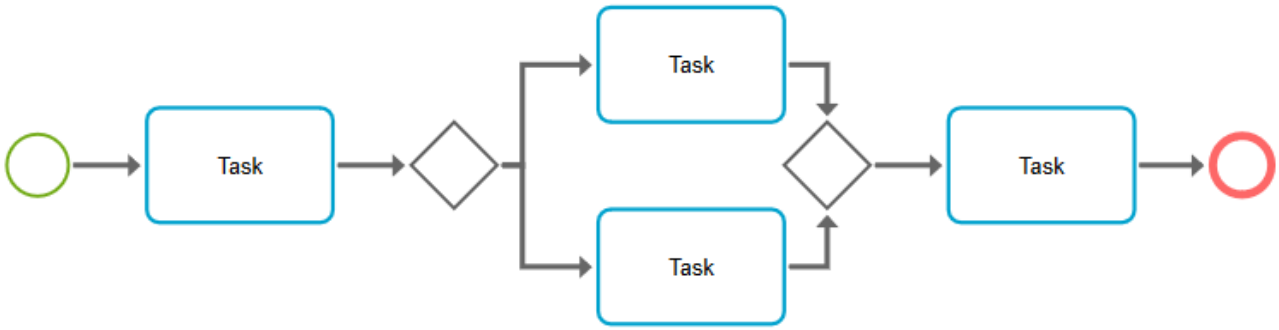
Version	Date	Description	Name
1.0	5th April, 2021	Initial draft	Denis John Kattithara

Contents

Introduction

The intent of this document is to produce a reference architecture around the way Data Loss Prevention (DLP) teams may be structured. This factors best practices based on experience gained by implementing DLP across various global organizations, as well as lessons learned over time.

DLP is a unique solution that is not just about technology, but a lot of people and processes. It is very much like having a "**Bentley**", yet it is not uncommon to see DLP programs go south. This failure is often attributed to legacy DLP solutions, but ***have you ever wondered if this was less of the solution and more of us (people and processes) being a contributor?*** The analogy from "***Who moved my Cheese?***" could be helpful in understanding this puzzle, i.e. "***If You Do Not Change, You Can Become Extinct***".



1) Why do DLP programs fail?

There are various reasons why a DLP program may fail for an organization, and below is an overview of few common aspects:

Vision and Motivation

What are your organizational goals with DLP? DLP is often seen as a mere compliance requirement that must be satisfied, and investment of time or budget is constricted thus envisioning DLP as an IDS / IPS solution. As a result, it is not uncommon to see DLP leveraged as a redundant solution that is simply generating an audit log of user activities. It is imperative that we start with a clear vision and motivation of the longer term goals with a DLP program.

Return of Investment (ROI)

It is natural to expect ROI from any investment made by an organization, but the case for DLP is a bit unique. It is difficult to quantify ROI in the short term, but this is rather articulated in terms of risk reduction over an extended period of time. We see organizations adopt aggressive strategies in an attempt to quickly showcase ROI, and this is often counterproductive to the goal of having a DLP solution.

Engagement with business

A DLP solution should be seen as a way to complement business by adding value, but this is not possible without extensive involvement of various stakeholders. DLP teams often need to operate in an autonomous / semi-autonomous manner, indirectly determining the way a business functions. This is detrimental to the interest of an organization, and sometimes backfire on the DLP initiative.

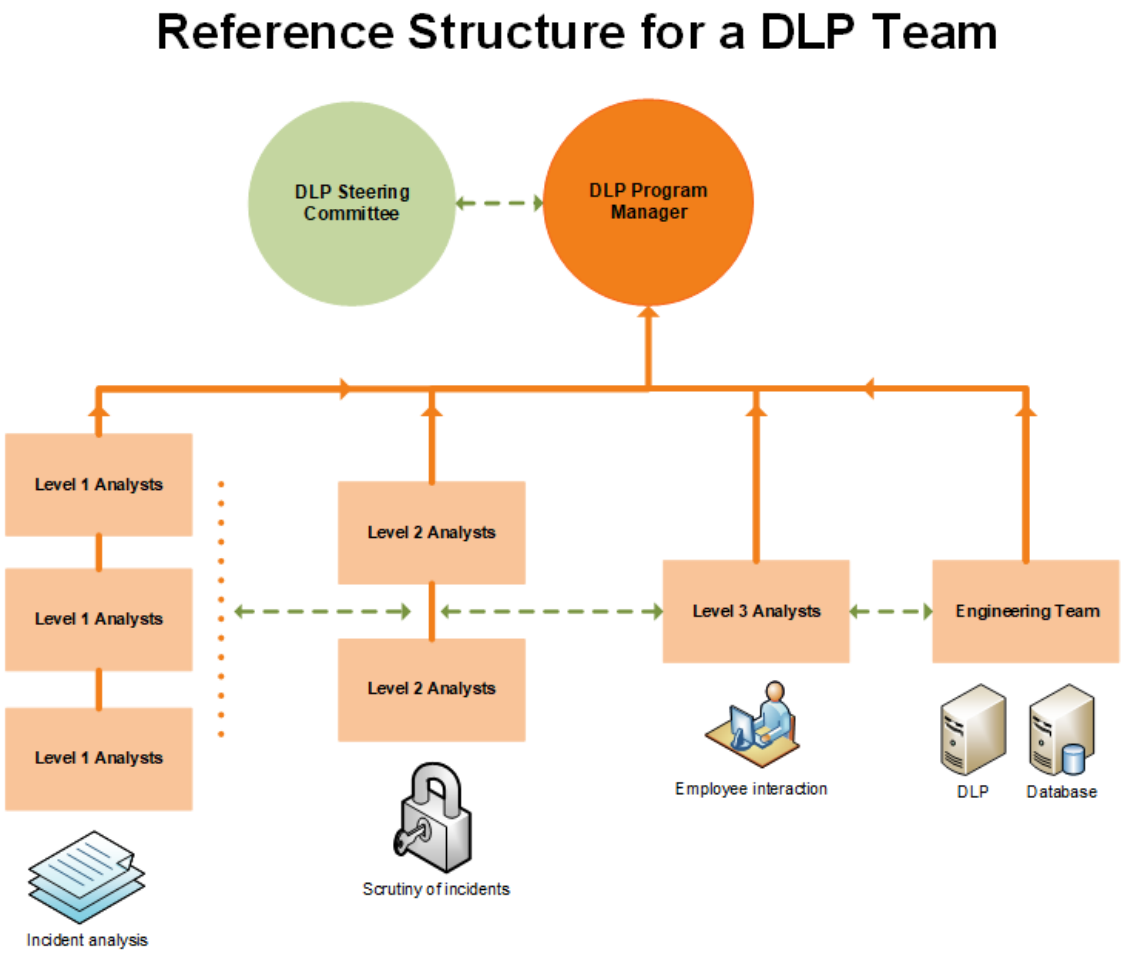
It is natural for an employee to ignore / delay a certain task, in case they cannot perform the same in a convenient manner. ***Have you factored the invisible cost that an organization assumes, when a couple thousand employees exhibit this behavior?*** The best way to manage this is through extensive engagement with business, where every security risk is articulated and either accepted via a signoff or carefully mitigated.

Ongoing involvement

The criticality of data keeps changing with time, and data that is critical today may not be critical tomorrow. Thus it is imperative that we frequently review and improvise our data protection strategies, in lieu of constantly changing dynamics. This is a common reason owing to which some DLP programs moves southward.

2) Staffing for a DLP team

A successful DLP program requires an ongoing investment into resources, and this involves various different roles. We recommend leveraging a hybrid management model of a hierarchical, flat and adhocracy based structure. Below is a reference model for staffing a DLP team, but this is likely to differ (*i.e. responsibilities may be consolidated to specific roles*) based on the size of each organization as well as the maturity stage of a DLP program. Moreover, several organizations also consider outsourcing specific roles to managed DLP service providers.



DLP Program Manager

The first step towards defining a DLP program is to resource a '**Program Manager**'. While the title of this resource may vary across organizations, the vision is that he/she will be seen as a '***Champion of the DLP program***'. In many cases a DLP program manager initially assumes multiple roles and responsibilities within the DLP initiative, while rest of the team are staffed and responsibilities delegated. In summary the key responsibilities of a DLP program manager include:

- Lead and manage the DLP team
- Provide thought leadership on various aspects of DLP
- Recommend business process changes that may mitigate Data Loss
- Engage with the DLP steering committee with the aim to review and mitigate risks
- Liason with the Incident management team to assess the risk landscape

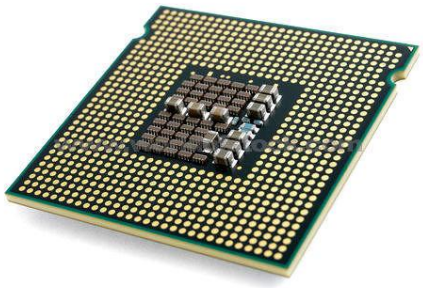
It is strongly recommended that this role is assigned as a KPI (Key Performance Index) to a dedicated full time resource. The presence of a KPI is the driving force and motivation, thus ensuring that we see traction in DLP over time.

DLP Steering Committee

The steering committee is truly the '**North star**' of a DLP program. This may involve stakeholders like C-level executives, cyber security, business, compliance, privacy etc (*ideally anybody interested and required for the success of DLP*). The DLP program manager plays an important role in driving the steering committee to meet on a periodic basis, with an aim to make decisions and steer in a defined direction. Below are few examples where a steering committee may add value:

- ✓ **Budget decisions / support**
  - *"We have been able to identify a huge volume of potential risks, and here is a high level report. The only way we can investigate these risks, is to staff 'x' Incident analysts, that requires an additional annual budget."*
  - "*We have identified a new security risk, which can be mitigated with the use of encryption technology. There are various market leading technologies that have been evaluated, and we will need budget approval for driving the same further."*
- ✓ **Business risk mitigation**
  - *"We have identified that a huge volume of finance employees have been using removable media for performing day to day tasks. Our options for mitigation involve 'x, y & z'. Is this acceptable to business?"*

DLP Engineering Team



The engineering team is responsible for building and maintaining the DLP technology infrastructure. This role is typically handled by a dedicated resource(s) within large organizations, whereas this may be an additional responsibility for an existing resource in certain organizations or the initial stage of a DLP program.

The key responsibilities of a DLP engineer include the below:

- Design and lead technical functions for DLP projects
- Develop secure system solutions to meet DLP program requirements
- Perform impact assessments for any DLP related aspects from a technology standpoint
- Operational monitoring and optimization of DLP systems

DLP Incident Management Team

The incident management team is a key pillar of any DLP program, and may include two or three levels of tiering (with responsibilities distributed as per organizational requirements). The implementation of performance KPI's for such teams may prove counterproductive, as people tend to emphasize on quantity instead of quality. Thus a hybrid flat adhocracy based model fostering innovation and creativity is preferred.

An incident management team adds value in the form of risk reduction over a period of time, through various aspects including but not limited to the below:

- Analyze and assess user behavior
- Identifying broken business processes
- Evaluate loss of critical data

✓ **Level 1 Analysts**

The key role of a Level 1 analyst if to funnel potential true positives, by eliminating false positive incidents. While experience with DLP or similar incident management solutions is preferred, an individual with corporate work experience and a quest to understand problems in the most simplistic manner could add value. We recommend a blended mix of both skillsets thus fostering an environment with different perspectives towards risks.

✓ **Level 2 Analysts**

The key responsibilities of a Level 2 analyst include the below:

- Scrutinize potential true positive incidents, and escalate for investigation where required
- Mentor Level 1 analysts by fostering a culture of working together
- Recommend DLP policy optimization measures, thus reducing the volume of false positives being generated
- Recommend changes to business processes with a risk reduction mindset
- Recommend other technologies that may complement the DLP program
- Develop risk reduction reports on a periodic basis

✓ **Level 3 Analysts**

A Level 3 analyst performs various functions, with investigation being one of the most frequent task. The personality attributes to explore in a level 3 analyst are maturity of thought as a social individual, and secondarily experience or aptitude for performing DLP investigations. Interactions that occur between a level 3 analyst and company employees, portray an image of the organizational culture and there can be no compromise on that. The key responsibilities of a level 3 analyst include the below:

- Investigate escalated incidents. This may involve collaborating directly with end users, end user managers, department heads, HR etc
- Mentor Level 1 & 2 analysts by fostering a culture of working together
- Lead the effort to optimize DLP policy rules
- Work with business stakeholders to identify / qualify critical data, with an aim to author new DLP policies. This will involve building relationships and conducting workshops with various business stakeholders
- Perform impact assessments for any DLP related aspects from a strategy standpoint
- Documentation of various DLP program processes

Continued below…

3) Planning an implementation strategy

Implementing a DLP solution is a long term effort, which could take anywhere between months to years (differs for each organization based on size and other aspects). You may consider leveraging the below strategy:

Phase 1 → Define your requirements

The first step towards any engagement is defining your requirements, and it's even more important with DLP. Moreover, we must also factor compliance requirements for various locations etc. As an example, implementing DLP for Swiss banking requires on premise servers, on premise staff and zero remote access. Likewise, there are hundreds of such compliance guidelines for various regions that must be studied and factored.

Phase 2 → Implement the DLP technology

It may be a good idea to start with implementation of the DLP technology, as this is a key dependency in determining your later strategy. Each technology vendor has certain limitations, and we must factor the same for further planning.

Phase 3 → Plan a staffing structure

We have seen some organizations start with a single role initially, that could be a DLP engineer or a DLP Program Manager while gradually expanding the organization chart to accommodate more roles. In either case, you must plan a timeline and budget for scaling the staffing structure.

Phase 4 → Deploy few initial high level policies

The initial stage of a DLP program might seem like being in a dry desert, but even a desert has resources. The best way to move DLP into production is to deploy high level monitoring policies, e.g. PCI, PII etc (preferably just one at a time). This will provide the DLP team with sufficient breather to analyze incidents as well as learn from the initial experience. The idea is to leverage the incident data to produce a high level user behavior dashboard, based on which further strategies may be devised.

Phase 5 → Create repeatable processes

It is crucial that we create repeatable processes for dealing with investigations, communication, mitigation, reporting etc. This is an important step towards showcasing maturity of a DLP program, and is extremely useful for achieving compliance with various regulatory frameworks. This is an exercise that must be done for every policy / critical data type. Few examples include:

- Process and collateral for conducting critical data identification workshops
- Documentation of interviews performed with various people handling data
- Documentation for each DLP policy being implemented, with a change management trail
- Impact assessment documentation:

- Data Privacy Impact Assessments for GDPR
- Data qualification / impact assessments for DLP, i.e. ***What is the impact if this data is leaked outside the organization?***
- Outcome of risk assessments

- **DLP Damage Control Protocol**: In most cases we are late the very moment we identify an instance of leaked data. However, there are certain scenarios where we can control known-unknown damage before it occurs. It is imperative that we create a suitable damage control protocol / process that must be invoked in such scenarios. This may involve a committee or suitable points of contact globally 24/7, who may be counselled for direction in case an event occurs. Few examples of damage control may involve the below:
  - Issuing legal notices / warnings to the concerned parties
  - Voluntary data loss disclosures performed in a timely manner
  - Implementing measures that may reduce potential impact, e.g. early dissemination of a public report that was leaked before the due date

These recommendations aim to serve as a reference point for architecting a DLP team structure, and we hope you find the same helpful. Please feel free to reach out in case we may be of any assistance.

About DLP Assure

DLP Assure evolved as a knowledge sharing platform offering solutions towards various ***'Data Protection'*** strategies. This involves the entire life cycle ranging from the way data is stored, protected, disseminated or handled.

DLP Assure

Email: info@dlpassure.com
Web: https://www.dlpassure.com