Cyber Security Articles

DATA LEAKAGE PREVENTION (DLP)

12 Practical Tips for Success

PART 1

Illyas Kooliyankal,
SVP & Chief Information Security Officer, Abu Dhabi Bank.
Email: illyaskool@gmail.com

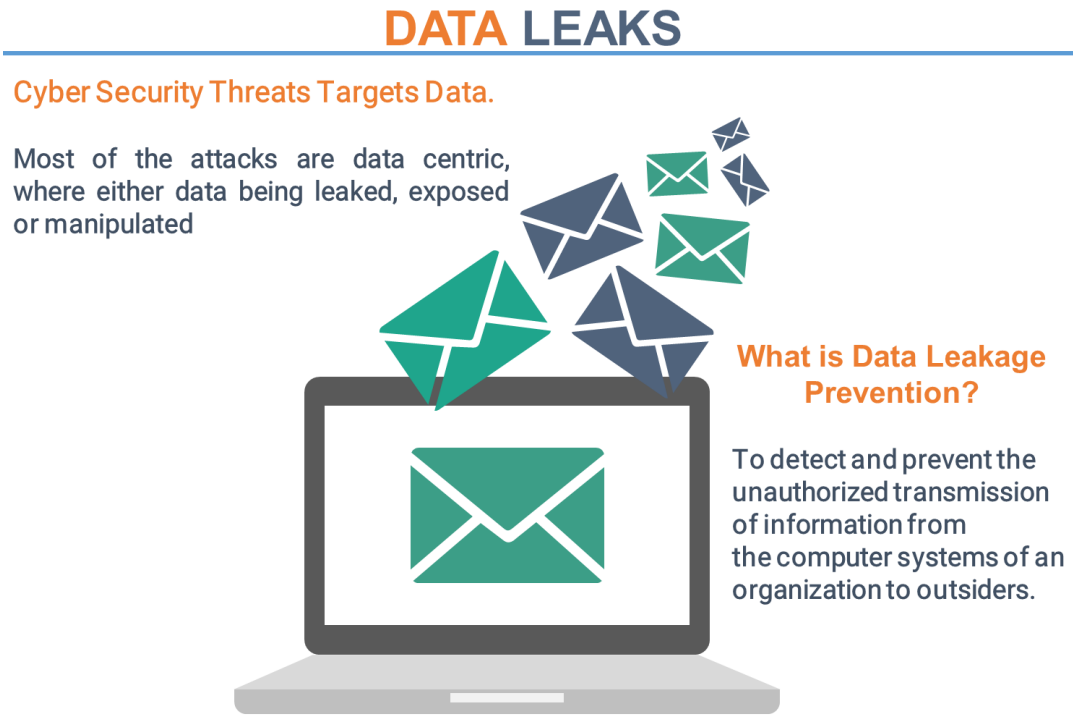
Table of contents

Introduction

CYBER SECURITY TRENDS & DATA-CENTRIC SECURITY

Cyber Security trends show that organisations are now realising the importance of data-centric security than relying on perimeter controls only. Information is the most valuable asset that any organisation possesses. Modern businesses entirely depend on data, irrespective of its size and location.

Flexible and easy-to-use data is the business driver, which combine with cost-effectiveness lead to the aggressive adoption of cloud and related technologies. Perimeters and business isolations are the subjects of the past now.



One of the biggest concerns organizations have is Data Leaks, but overlooked in the past and till now

Multi-tenancy, Cloud, Big Data, Artificial Intelligence, FinTechs, and IoTs - all require data and mobility. Business engagements, analysis, reporting, advisory services, auditing, and consultancy - everywhere easy and quick access to information is unavoidable.

The digital transformation and technological advancement across all walks of life demonstrate the significance of protecting the organisations from data leakages.

Consequences of Data Leakage

The challenge in front of Cybersecurity professionals is how to protect the organisation from data leakages without impacting genuine business activities.

Current and future technology direction and adoption leads to more avenue for data leaks

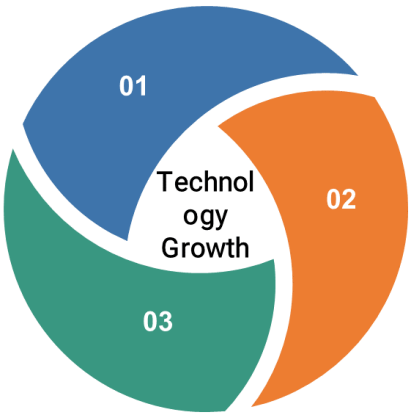
WHAT CAN ELEVATE THE RISKS?

Digital Transformation

Digitalization of all sectors, including business and governmental services

Mobility and Flexibility

Users and Business needs mobility and flexibility in services



Cloud & Big Data

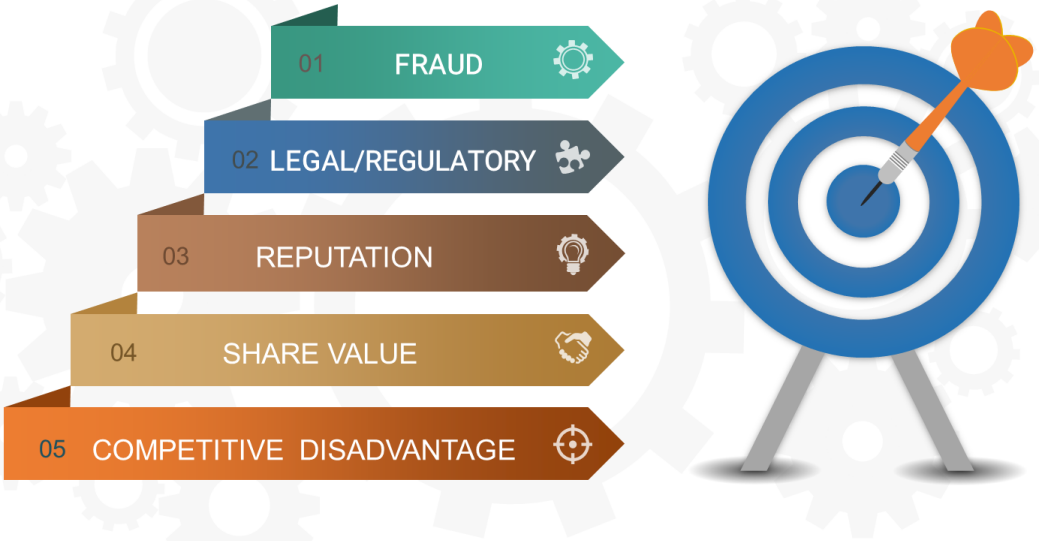
Perimeter based controls are not any more applicable for data security

Data Leakage Prevention (DLP) is at the heart of any information security programs but often overlooked due to the efforts involved and lack of expertise available. Even today, most organisations fail miserably in implementing controls around data leakage.

The list of companies at the wrong end of this includes Facebook, Google and many bigger names. Unauthorized data leakage is the root cause of most of the current age frauds happening in the industry.

Any lapses around data protection could end up in not having the right level of controls around sensitive information, and can potentially lead to financial, reputational, legal/regulatory or competitive losses to the organisation.

What are the CONSEQUENCES?



Data Leaks can lead to significant damages to organization and services

FOCUS AREAS

In this article, we look at some of the critical mistakes around data leakage prevention programs and how to address those to meet the targeted Cyber Security objectives.

Right process, trained and skilled users, and the appropriate technology - This is the holistic and effective approach to take by organizations to manage information leakages.

Technology alone cannot solve the problem, but a holistic approach can!

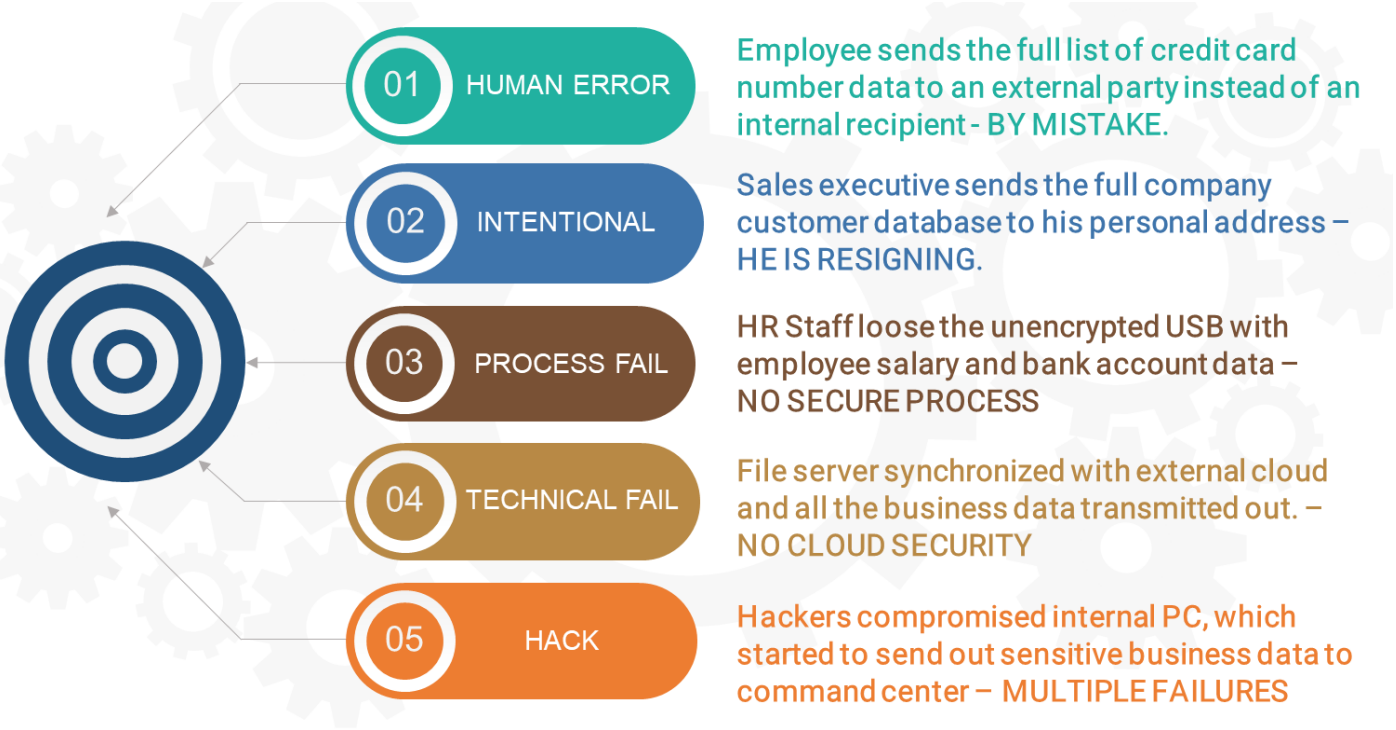
Technological limitations or ineffectiveness often being blamed for failure in Data Leakage Prevention (DLP) initiatives, but in fact, that is only one angle of the whole problem.

Lack of defining and adhering to appropriate processes and failure in educating the people around it significantly hinders a successful DLP program.

HOW TO SOLVE ?

What could go Wrong?

Data leaks can happen due to numerous factors, including Human error, process failure, technology failure, hacking or an intentional malicious attempt by an internal employee.



Data leakages can happen due to many reasons –
It could be due to People, Process and Technology

What is missing in DLP Programs?

1 Lack of a comprehensive data security policy, and governance framework including classification schema/levels.

The absence of management approved policy and a defined framework, could lead to an inconsistent approach and ineffective implementation of DLP controls.

Solution

The starting point for any DLP implementation is an explicit policy with business relevance, in alignment with organisational Cyber Security Policy.

Following the DLP Policy, it is recommended to have a detailed Data Security Governance Framework to define roles, responsibilities, activities, procedures, data flow diagram, and data schemes etc.

2 Lapses in effectively identifying information, that needs to be classified and protected.

Most organisations lack an up-to-date inventory of information assets. Firms try to create the inventory by collecting the details of only documents or on an ad-hoc basis.

This method of inventory creation is a challenge for implementing effective data leakage prevention measures, since the lack of effectively identifying the valuable data, means, the organisations may not have the control to protect it.

The essential prerequisite for any information security assessment is an accurate asset inventory at the organisation. However, most of the time, it doesn't happen to be the case.

The lack of asset inventory is an additional burden to the data classification team, as the starting point is to have the right inventory of services, processes, and data associated with those.

Solution

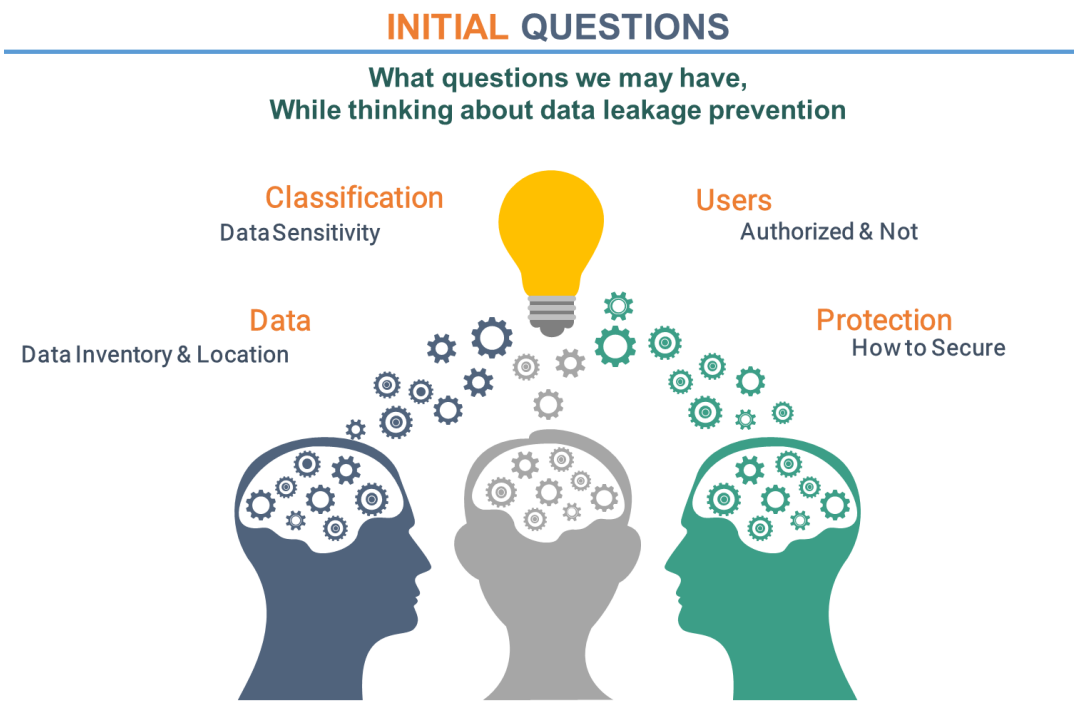
organisations must seriously consider having a comprehensive asset inventory, that is regularly updated.

The inventory shall include the digital assets as well. If one is not available, collect the data from multiple sources, including the Active Directory data, IP addresses, information from procurement, finance, Enterprise Architecture team etc.

Past risk assessment, other internal engagements must have data collected for the purpose, that also could be reviewed, prepare an initial list of assets.

Needs to brainstorm and identify all the possible sources of data for an asset inventory, which includes the list of business/support services & products, processes, software and hardware assets, and information asset.

File Shares, Business Impact Analysis (BIA) data from the Business Continuity Team, past risk assessment data are some of the sources.



Also, valuable inputs can be obtained from Intranet/Internet, Service Catalogues, Configuration Management Database (CMDB), SOPs (Standard Operating Procedures), and Product & Services list from business departments.

3 The absence of a structured approach to collecting information

Once the organisation identifies the need for information collection and classification, the next question would be where to start and how to execute that? The biggest challenge here is the absence of any guideline, policies and procedures.

In the typical case, the Information Security Team will either meet the concerned department or ask them to provide the data. Alternatively, they may refer to the available documentation.

These adhoc process may lead to incomplete, inefficient, and very time-consuming process, and at the end a less than desirable result regarding asset inventory and classified data for leakage prevention.

Solution

Based on the defined policy and governance framework, and identified innovative approaches to execution, the source of data collection needs to be listed.

This source could include the BIAs, Fraud Investigation Reports, past incident reports, DLP (if existing solution) events/incidents, HR disciplinary records, File shares, and Intranet portals.

InfoSec teams should have the right template for the information collection and right questions for classifying the data. Before meeting and interviewing/collecting information from the business departments, carry out maximum background work, and fill the templates.

Revalidation and refinement of the data collected should be the target objective for the direct engagement with the business, which reduces the overhead on them and much quicker progress in the exercise.

Also, the technical solution for identifying/discovering and labelling of data is a complementing approach to have a more comprehensive data classification process.

4 Failure to conduct comprehensive classification exercise

Even after having the inventory of data, most organisations don't have the right process or criteria to classify the information.

Without ensuring an effective classification, it leads DLP to focus on a massive amount of data, that may include non-sensitive and could lead to inefficient policies, and wastage of investments.

Thousands of false positive alerts are another significant challenge that originates from a weak classification process, which will, in turn, makes it impossible for the security team to monitor and respond.

Solution

Based on the Data Classification Policy and Governance Framework, organisations need to conduct a data classification exercise. This classification process may have to go through multiple iterations to get maximum accuracy.

Definitely, the InfoSec team needs to prioritise and set clear expectations and outcome. Data classification may be extended to define the data flow diagram, to understand the legitimate business activities and related data path, to reduce the false positives.

During the classification exercise itself, the team can identify the business impact of the data breach, and then the controls required for the classified data based on criticality, and business needs.

InfoSec team needs to play a significant role in reducing overhead to the business and also provide the right visibility on the risks, and potential controls for the business to recommend relevant measures through an informed decision process.

5 No background work, to collect, analyse and gather services, process and information.

Most cases, data classification starts and ends without the real benefit for the organisation. The considerable challenge faced by the organisation is around where to start, and how to proceed, and the sheer size of the data to be collected and analysed. Lack of policy and procedure and an approach document is just added more troubles to this.

Solution

Define a clear roadmap for data classification, with different steps, phases, activities, ownership, constraints, risks, challenges, and proactive solutions. Analyse the data in hand, sources of the same, correlate those to identify as much information as possible.

6 Lack of total visibility of data - including data that is being received by the organisation.

Most organisations may have the visibility of data it produces, including the documents created by employees, or reports produced from applications.

Many other data sources/locations may be missing for the data identification and classification exercise.

The absence of total visibility leads to incomplete security around data leakages. It may lead to legal, regulatory and contractual breaches too.

Notably, information received from partners or third parties doesn't get the visibility for data identification and classification.

Contractual and regulatory responsibilities to protect those data also gets overlooked due to this.

Solution

Establish an effective and automated process to ensure that all data location and incoming and outgoing channels are being identified and monitored.

Centralised locations for incoming data, detecting attachments and sensitive data through email and other channels, and establishing a data room for information exchange with third parties can assist towards this.

7 No defined roadmap for data classification and data leakage prevention

Planning for the complete solution, without short terms objectives and quick wins
As in any other initiative, it is not practical to achieve a perfect or 100% accurate output at one go.

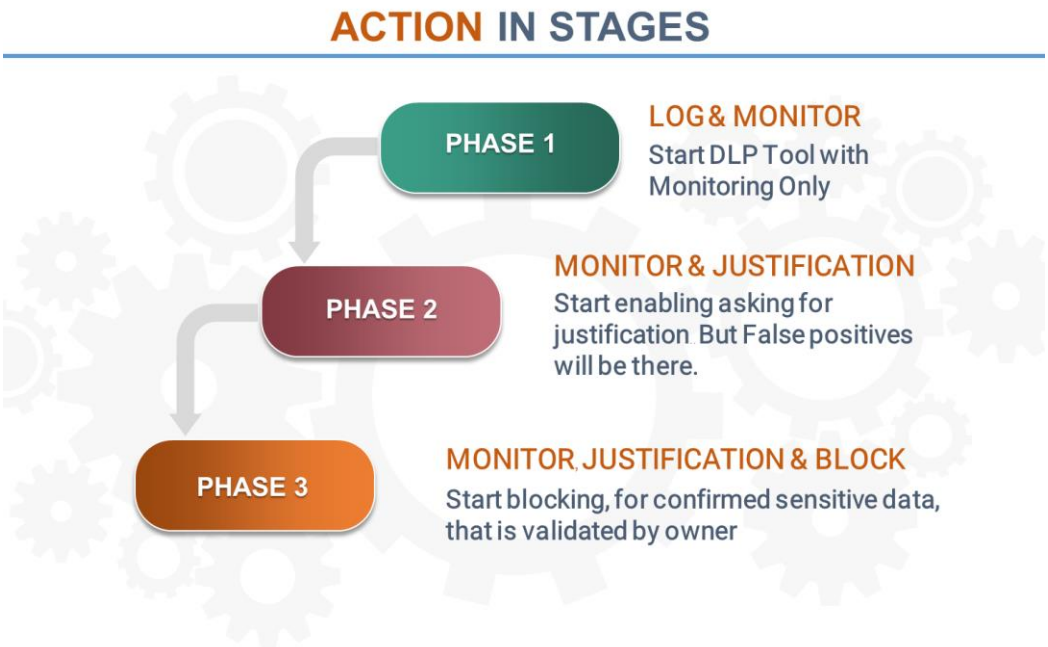
However, in most of the cases, organisations tend to target to finish and get the perfect solution at the outset of the data classification and leakage prevention exercise.

Solution

It is always better to take step by step approach and target a certain maturity level at the initial phase.

Define short-term goals, and work towards that. Instead of aiming the perfect and most accurate output, set reasonable expectations according to business criticality and priority.

However, ensure that the approach and the data are right to quickly compile and iterate for refined accuracy on an ongoing basis. Ensure continual improvement with a defined KPI.



8 Lack of Right Technology for Data Classification & DLP

Many organizations procure data labelling and DLP solutions without understanding and defining the requirements and business environment adequately. Selection of the solution may be done in an ad-hoc manner, influenced by market trends or vendor sales pitch.

Many case the procurement and implementation done without understanding the functionalities required, and without the right clarity about the solution objectives. Technologies being sold as a magic band for all security problems, including data leakages.

In the end, solutions may be implemented but without any real business benefit or effective control of data leakages.

Solution

A comprehensive risk assessment shall be conducted in consideration with data leakage aspects, covering the vulnerabilities and threats. Potential threat agents and channels of data leakages shall not be overlooked.

A detailed Request For Proposal (RFP), Business Requirements Document and Functional Specification Document must be developed with a focus on target objectives and outcomes of the program.

Solutions need to be procured, that can mitigate the risks, in an effective and efficient manner, without impacting the business operations.

Selection of the product or combination of products shall be done based on well-defined evaluation criteria, and comprehensive process that may include running a POC (Proof Of Concept).

Implementation and configuration of the solutions must be done with qualified and experienced professionals in order to configure and maximise the usage of all available functionalities in alignment with the risk scenarios and business needs.

9 The absence of a defined process for DLP rule creation, and refinement

Organisations miss defining the risks and channels of data leakage and what levels of policies to apply. Also, it could lead again to ineffective policies, and can cause business disruption, and may not detect or respond to critical data leaks.

Business inputs and decision also may be missing, if the right visibility and discussion to define the rules are not taken.

Solution

Business logic and data flow mapping could be analysed to determine the business needs of data transfer. Authorised activities and relevant stakeholder identification help to determine the genuine data transmissions and potential leakages.

Policies can be defined to detect, prevent or asking for justification based on the significance of the data and the consequence due to its leakage.

10 Ineffective and inappropriate reporting and responding procedures

Data classification and leakage prevention could be ineffective, if the process around it is not well defined, which includes how to report and respond to the different activities around.

In case of any detected incident or potential incident, most of the time lack of clarity is lacking on how to report, what actions to take, whom to contact, and who is authorised to take the decision.

Considering the sensitivity of the incidents, lapses in these could lead to organisational resistance, impact the employee morale, and business disruptions.

Solution

Incident Response procedure, with a defined subcategory for data leakage incidents, shall be defined with clear roles and responsibilities and escalation matrix.

The sensitivity of the incidents, parties involved, and the consequence of the leakage may be referred to define appropriate procedures and escalation levels.

Also needed is to define the violation levels, disciplinary process, reporting management, and corrective actions - in alignment with relevant organisational policies and procedures.

11 Lack of process and commitment to continue the classification process on an ongoing basis

Even if the first time exercise is completed successfully, the real effectiveness of data classification and leakage prevention depends on how good the company maintains and improve its data classification process and leakage prevention mechanisms.

Solution

Policy and procedures must be defined with assigned responsibilities to make sure that the data classification and leakage prevention is an ongoing exercise.

Relevant data labelling tools, its integration with data leakage prevention (DLP) solutions, defined and automated processes, employee education and awareness are crucial for the effectiveness of ongoing adherence to relevant controls.

12 A scarcity of skilled resources, who understand and can effectively achieve DLP Objectives

Traditional methods and thinking cannot produce the desired results in data classification and data leakage prevention (DLP) activities, especially considering the complexity and magnitude of the work involved.

Lack of quality resources with holistic experience in security and business acumen and that too with an innovative mindset is a significant challenge for organisations.

Solution

Define the frameworks, templates, processes, and implement the right technology for data classification and leakage prevention. Identify and hire good talent with technology and process related skills and experience, with a mindset to learn and understand the business services and processes.

The resource needs training and nurturing to support the organisational data leakage prevention objectives.

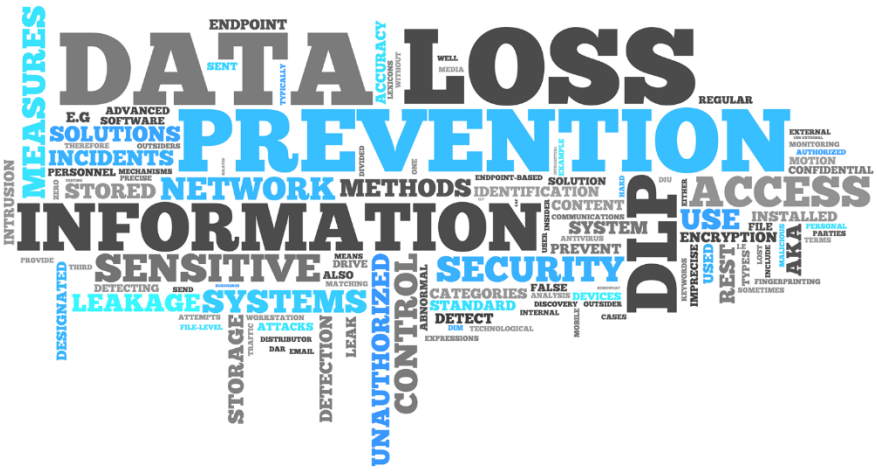
Robust planning and controls around people is key to the success of Data Leakage Prevention Program

Overall Summary of DLP Challenges and Proposed Solutions

Summary of the challenges around DLP & proposed solutions depicted in the infographics below.

Pain Areas and Solutions

Pain Areas		Solutions	
Data	Size, Inventory, Location *Data Size, No Inventory, without location tracking, or sensitivity understanding, data owner*	Data	Comprehensive Inventory *Services, Process, Assets Inventory by collecting data through multiple sources/channels.*
Governance	Process Absence *No strategy, policy, framework, structured approach, guidelines, ownership of process.*	Governance	Strategy, Roadmap, Policies *Define a framework consists of a clear roadmap, policies, procedure, guidelines, standard.*
Technology	Ineffective/Absent Technology *Weak/Absent – DLP, Labelling, Discovery, DRM, Cloud Security*	Technology	Technology - Risks and Requirements *Technology based on risk assessments and implement in alignment with defined requirements*
Operation	Policy Design, and Configuration *Inefficient/ineffective policies and management. False Positives, False Negatives, Weak Monitoring*	Operation	Defined configuration and monitoring *Inventive and innovative policy design and configuration. Risk and priority based monitoring with automation*
Response	Detection, Response & Improvement *Untimely/No detection, No defined response process, Lack of corrective & disciplinary actions*	Response	Defined detection and Response process *Pre-defined process for detection of breaches and corrective actions with Improvement plans*
Buy In	Executive, Business, Info Sec, IT *Lack of understanding the risks, value, process, innovative approaches, and response plans*	Buy In	Strategic, Tactical & Operational Support *Business objectives linked risks, and the value of data leakage prevention with defined KPIs*



About the Author

Illyas Kooliyankal is a renowned Cyber Security Transformation Leader, serving as SVP & CISO in a leading bank in Abu Dhabi. He is currently a member of prestigious UAE Bank Federation Information Security Committee and former Vice President of ISC^2 (UAE Chapter). Winner of many international awards, including the EC Council (USA) Global CISO Award (Runner Up), ISACA CISO and Emirates Airlines CISM Award and a celebrated keynote speaker at international conferences in the USA, UK, Singapore, Dubai, etc. With more than 15 industry certifications and many whitepapers and articles, he brings in his innovative thoughts to transform organizational security landscape.

About Secure Reading

Established by a team of visionary leaders in the global cyber security arena, and closely mentored by prominent CISOs, **Secure Reading** is an online portal, a complete knowledge base with cyber security news, advisory services, training etc. We also provide cyber security consultation for enabling individuals and businesses to fight the toughest of cyber challenges.

Corporate Head-Quarters

41/406 E, 4th Floor
Beejay Towers, Rajaji Road
Cochin 682035

Ph: +91 9995531819,
+91 9744303817
Email: info@securereading.com

UAE

G-19, AFNAN Building
The Square-Dubai
PO Box: 98981

Phone: +971 4 269 5669
Email: info@rightclickuae.com

Learn more at www.securereading.com

SECURE READING