Data Leak Prevention of Financial Institutions

Mohammad Ali ACMA
Assistant Vice President
Internal Control and Compliance Division
Dhaka Bank Limited
3rd Floor, 39 Karwan Bazar, Dhaka
Email: alicma2014@gmail.com

Engineer Quazi Shaklain
Senior Assistant Vice President
Head of IS Audit
Internal Control and Compliance Division
Dhaka Bank Limited
3rd Floor, 39 Karwan Bazar, Dhaka
Email: qshaklain@yahoo.com

Abstract:

Information is a critical aspect of organizational success. It is obvious that the information security defenses that are implemented by the government and organizations to prevent data loss are not totally effective. Malware and malicious individuals and organizations are wreaking havoc for many enterprises by capturing their sensitive data. These events became known as data breaches. Data classification has to be defined first before identifying data breaches. The organization must know where data is stored and what mode. There must be a Policy and guideline for protecting data and authentication is needed for accessing each type of data. Monitoring and admin team need to be formed to ensure organization's data is safe and secured. It's not possible to track data breaches manually so automated DLP solution needs to be implemented. Challenges are if employees are not honest and loyal for the organization then it's really difficult to ensure 100% data protection.

Keywords: APT, Malware, Data at rest, Data in Motion, Data in use, Confidentiality, Integrity and Availability.

1.00 Introduction

Data Leakage involves tapping or leaking information out of the computer. This includes APT (Advance Persistent Threat) and malware attacks, dumping files to paper or stealing computer reports, pen drive and CD/DVD. Unlike product leakage, data leakage leaves the original copy, so it may go undetected. Fundamentally, data leakage involves the unauthorized transfer of sensitive or proprietary information from an internal network to the outside world. Ways that this information can leave the organization include Intranet, Extranet, instant message (IM), social media, email, file sharing, taking photo snap and memorizing the information in brain.

Common controls to prevent data leakage have also been covered including identifying assets, classifying them

and in information security management system, including policies and procedures.

In Bangladesh, data leakage occurred in Supreme Court of Bangladesh, Privet and Government Banks. Outside of the Bangladesh, 5 of the biggest data breaches ever happened in Yahoo, First American Financial Corp, Facebook, Marriott International and Friend Finder Network.

2.00 Objective of the study:

To understand DLP, its risk along with challenges and how to overcome for implementing DLP in a Financial Institution.

3.00 Methodology of the study:

Both primary and secondary sources of data were used for this study. The primary data relates to the information gathered while working with ICT Security Risk of a private bank, discussion with employees of other banks. Secondary data were collected from various reports of national and international reputed firms.

4.00 Objective of DLP

Enterprise DLP solutions can significantly reduce the risk of data loss due to inadvertent employee behavior and broken business processes, the causes of 95 percent of data loss incidents.

Companies can no longer rely on traditional perimeter security solutions to guard high risk data, and must consider DLP strategies to include data-at-rest, data-in-use, and data in- motion.

5.00 DLP is related with state of data

Effectively implementation of DLP system depends on data life cycle of the organization. A data life cycle is a detailed outline of the phases involved in effectively preserving and managing of data to be used and reused. According to the state of data, we can classify it as follows:

1. Data at rest: Data stored in PC, Server or Cloud.
2. Data in motion: Data travelling through the network.
3. Data in Use: Data movement due to actions taken by end users on their work stations.

6.00 Understanding the DLP

To understand DLP meticulously, we have to understand and answer following 04 questions related with any organization:

a) What Information is of value to an organization?

The first and most important step of DLP implementation is the identification and classification of organizational information. Industry best practice proposes two information classification standards for public (government) and private institutions: classification by level of importance and impact of its disclosure or destruction. The classification should follow a risk-based approach. The classification standard for public information interprets the potential risk impact in terms of national security and stability, as depicted in figure below:

Public Information Classification	
Classification	**Description**
Top Secret	Disclosure of Top-Secret data would cause severe damage to national security
Secret	Disclosure of Secret data would cause severe damage to national security but those are considered less sensitive than that of Top-secret.
Confidential	Confidential data exempt for disclosure under relevant laws
Secret but unclassified (SBU)	SBU are not considered vital but their disclosure would do some harm to the national securities. Many agencies/NGOs classify their data collected from citizens as SBU.
Unclassified	Unclassified data are not classified or sensitive.

Information employed in private institutions is classified in accordance with the impact of risk on the achievement of enterprise objectives; this is usually depicted in monetary form as per table below:

Private Information Classification		
classification	**Description**	**Examples**
Sensitive	These data are to be most restrictive. They do much damage to the organization if disclosed.	Password, Encryption Key, Payment Card details etc.
Confidential	These are data that are less restrictive for the company but cause much harm, if disclosed.	Internal Market research, Audit Report etc.

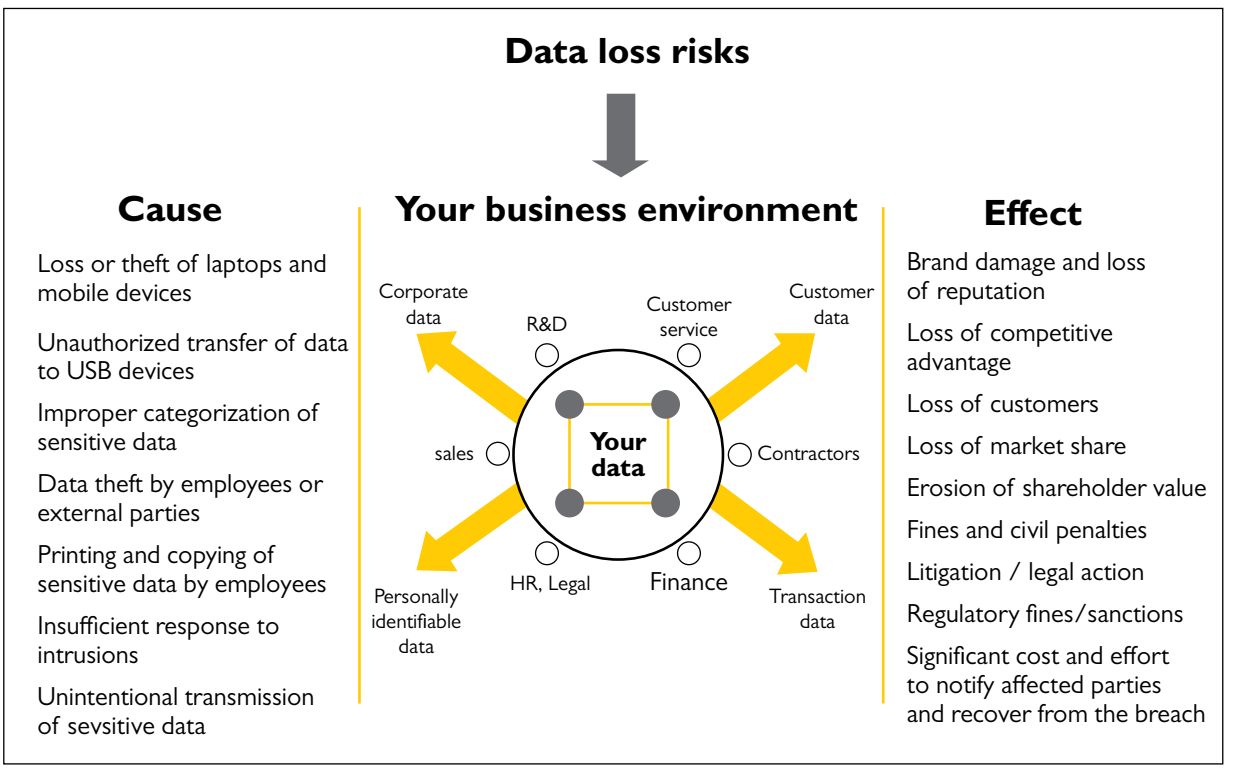
Private	Private data are compartmental data that do not damage severely but restricted for some quality issues.	Human resources related information.
Proprietary	Proprietary data can be disclosed on a limited because it may deter competitive advantage.	New product research.
Public	Public data are least sensitive data.	Mission & vision statement of an organization.

b) Who is Responsible for the Protection of Organizational Information?

The responsibility for protecting organizational information rests with all stakeholders at different levels of the organization.

Business owners and mission owners (senior management) create the information security program and ensure that it is availed the necessary resources and given appropriate organizational priority.

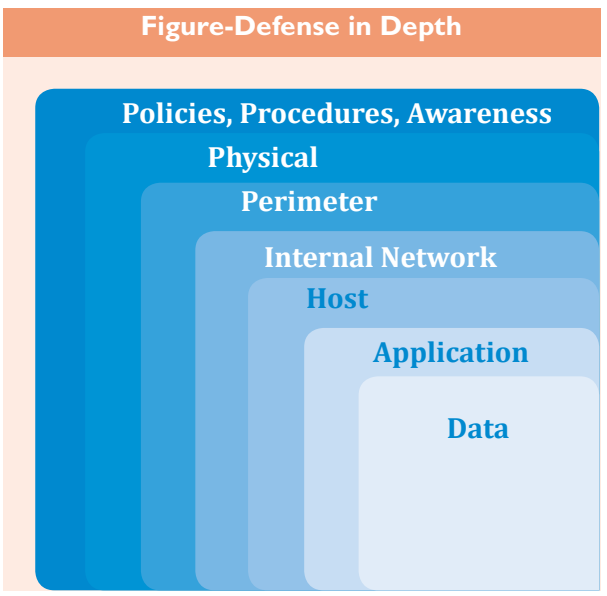
Organizational data loss risks:



The data owner (also called information owner) is a manager responsible for ensuring that specific data are protected. Data owners determine data sensitivity labels and the frequency of data backup. An organization with multiple lines of business may have multiple data owners. The data owner performs management duties, while custodians perform the hands-on protection of data.

c) How Can Organizational Information Best Be Protected?

To effectively protect organizational information, a holistic approach should be adopted, one that targets information in its various states—in use, in transit and at rest. Industry best practices for information security recommend the adoption and implementation of a multilayered or defense-in- depth (DiD) strategy as follows:



d. How effective is the DLP Program?

To effectively monitor and manage the performance of a DLP program, several metrics have to be defined and managed.

A key risk indicator (KRI) is a measure used by management to indicate the risk level of an activity. They are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. As part of its information communications and technology (ICT) and organizational risk management exercise, an organization should actively track its information risk and ensure that it is kept within acceptable thresholds in line with the organization's risk appetite. A risk register is used to document and report identified risk.

7.00 Lessons learned from Bangladesh Bank due to leakage of sensitive data

What happened?

In February 4th, 2016, hackers used stolen credentials to send money transfer requests that supposedly originated from the central bank of Bangladesh. The requests were sent over the SWIFT banking network, a computer network operated by a consortium of banks that processes sensitive financial communications.

The requests were sent to the Federal Reserve Bank of New York. They specified that funds from Bangladesh Bank's accounts at the Fed be transferred to various recipients in the Philippines, Sri Lanka, and other countries.

The attackers installed malware at Bangladesh Bank that kept the SWIFT system from working properly and alerting workers of the suspicious transactions. The malware also prevented the Federal Reserve Bank of New York's inquiries into the transactions from getting through.

As a result, the Fed went ahead and processed the transactions, sending $81 million USD to overseas accounts.

How did the breach originate?

Bangladesh Bank was breached and malware was placed on their system to prevent employees from discovering the fraudulent transactions before it was too late. Their SWIFT access credentials were also stolen.

SWIFT was not breached directly, but their system connects thousands of banks around the world. An attack on one bank in the SWIFT network could potentially have ripple effects affecting any other bank. In fact, the system has been used in a series of other attempted thefts.

Key Takeaways:

For financial services firms, protecting one's own IT systems is priority number one. Security programs should not only meet but exceed regulatory requirements and take into account the Latest threat intelligence.

However, focusing on internal security alone is not enough. Comprehensive financial services risk management programs should also focus on third and fourth parties who have access to sensitive information or resources and the risk they pose to the organization.

8.00 DLP Implementation steps

For proper implementation of any DLP systems, there are ten key steps to be considered and if these steps are followed would help an organization to adequately implement the DLP systems for protection of their confidential data. These steps are as follows:

Step 1 : Develop policies and Manual;
Step 2 : Implementation of a universal technique based on risk assessment;
Step 3 : Set right people in right place;
Step 4 : Identify sensitive data and understand how they are to be handled;
Step 5 : User Acceptance Testing based on progress
Step 6 : Don't burden / overload system performance and business operations;
Step 7 : Implement effective event review and investigation mechanisms;
Step 8 : Provide analysis and meaningful reporting;
Step 9 : Implement security and compliance measures;
Step10 : Implement an organizational data flow and oversight mechanism.

9.00 Challenges in DLP implementation and it's countermeasures

Three major challenges of DLP implementation:

i. The inability to enforce data use and handling policies.

ii. Data protection and privacy requires more than just regulatory compliance efforts.

iii. Rapid growth of data: In total, 2.7 Zettabytes of data exists in our digital universe , 149513 numbers of emails are sent every minute, 3,3 million (undoubtedly extremely insightful) Facebook posts are created every minute, 3.8 Google million searches are performed each minute, Each minute, 65,972 Instagram photos are uploaded, 500 hours of YouTube videos are uploaded every minute and many more.

Countermeasures:

i. Awareness of handling data;

ii. Adherence to policy;

iii. Updating policy as per scalability and requirements;

iv. Access right to be categorized properly based on their level of permission;

v. Encrypting system for data transmission;

vi. Proper classification of data.

10.00 List of commercially available automated DLP solutions

I. "Symantec" Data Loss Prevention;

II. "McAfee" Total Protection for DLP;

III. "Digital Guardian" Endpoint DLP;

IV. "Check Point" Data Loss Prevention.

11.00 Conclusion

A successful DLP program are the organization's to decide. Developing an understanding of what data are sensitive and where to find them, being aware of the threats and associated risk to data loss, identifying the causes of data loss (i.e., internal vulnerabilities) to implement measures to prevent them, Understanding DLP product differences and selection criteria to better evaluate vendor tools and techniques, Determining the best practices to follow when developing and implementing a DLP program.

As long as there is human involvement, the areas of concern will continue to evolve. It is essential to maintain vigilance to avoid and eliminate weakness in cyber and work environments.

References:

"Data Loss Prevention and Challenges Faced in their Deployments" by Victor O. Waziri, Ismaila Idris, John K. Alhassan, and Bolaji O. Adedayo Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.

https://www.bitsight.com/blog/lessons-learned-from-3-major-financial-services-data-breaches

https://bankingjournal.aba.com/2018/09/banks-turn-to-the-courts-for-data-breach-claims/

Proven Data Loss Prevention for European Union (EU) Data Protection Directive by Symantec Corporation© 2008.

8Tips for Implementing Employee Monitoring and Data Loss Prevention Solutions in a Data Privacy and GDPR Governed World by Alp Hug. (https://itsecuritycentral.teramind.co/2019/04/23/8-tips-for-implementing-employee-monitoring-and-data-loss-prevention-solutions-in-a-data-privacy-and-gdpr-governed-world/)

Insights on governance, risk and compliance by EY on October-2011.

CISA Study Manual, 2019.