Information Leakage and Data Loss Prevention

Luke Wang
7/13/2010
# TABLE OF CONTENTS

What is Information Leakage and Data Loss .................................................. 3

Causes

Accidents ........................................................................................................... 3
Intentional actions ......................................................................................... 3

Recent Cases

AT&T .................................................................................................................. 4
Heartland Payment Services ........................................................................... 5
Massachusetts Secretary of State Office ......................................................... 5

Impact of Incidents

Extent of data leakage incidents ................................................................. 6
Cost to organizations ....................................................................................... 6
Victims/customers ......................................................................................... 7

Data Loss Prevention

Culture and leadership .................................................................................... 7
Risk assessment .............................................................................................. 7
Policies and enforcement ............................................................................... 8
Education, training and communication ...................................................... 8
Technology and tools .................................................................................... 9

Annotated Bibliography .................................................................................. 11
INFORMATION LEAKAGE AND DATA LOSS PREVENTION

What is Information Leakage and Data Loss?

Data loss is different from information leakage. Data loss refers to an event where an entity unforeseeably loses its data or information. If the data released is sensitive and is subsequently acquired by someone else, the incident would be called information leakage. However, information leakage can occur without the original entity losing any data.¹ For instance, a hacker may penetrate a network of a software company to steal a copy of valuable source codes, but leaving the original source codes intact.

Causes

Accidents

Data loss or information leakage may occur accidentally. Data loss may happen as the result of loss of hardware such as external storage devices (e.g., USBs, CDs, and external hard drives), laptops, or PDAs. Research commissioned by Cisco has found that 9% of employees admitted to have lost or had their company devices stolen in the past. 26% of them have experienced multiple incidents per year.² Similarly, employees can also damage these equipments due to lack of care, such as dropping them on the floor. Sometimes, employees commit administration errors where data is accidently deleted.

Information may also be lost due to natural causes. Power failure or surges can destroy volatile memory. Hard drive failures are also very common. Other causes of data loss include software crashes, bugs, and data corruption. Unusual events are also known to destroy hardware and data, such as fires, floods, earthquakes, and other natural disasters.³

Multiple studies have shown that the most common causes of data loss are hardware failures and human errors, accounting for three quarters of all incidents.⁴

Intentional actions

Data loss or information leakage may also occur as the result of intentional actions. Criminals can steal hardware from the company, especially portable devices as mentioned earlier. Hackers can penetrate a

---

network directly or plant viruses and other malwares to extract sensitive data. These people are often sophisticated and profit-oriented, sometimes backed by organized crime or governments. But, the chance of these occurrences is relatively low.

The biggest risk, however, resides with the employees. Disgruntled employees may seek financial gains or seek vengeance through sabotage. Survey conducted by Symantec Corp. revealed that 59% of responding ex-employees admitted to have stolen confidential company information (i.e. employee records, e-mail lists, etc.). This number is astonishingly high and shows the prevalence of information leakage through employees. Their profit motive is satisfied when, for example, the stolen customer list is sold to a competitor.

In addition to malicious acts against the company committed by employees, they have also adopted practices that increase the risk of information leakage without realizing that their actions are unsafe. Some common behaviour include talking about sensitive information loudly in public, misuse of company computers, and not maintaining restricted physical and logical access. IT professionals believe that the unauthorized use of computer programs have caused a majority of information leakage incidents.

Employees are increasingly using the computers for personal use (e.g., personal emails, online banking, online shopping, and instant messaging) and accessing risky websites (e.g., pornography and gambling). Furthermore, employees are rendering the physical and logical access controls useless by permitting non-employees to navigate company facilities, failing to log off their computers, and sharing passwords. Thus, the internal threat is much greater than the threat posed by cyber criminals.

Recent cases

Incidents of data loss and information leakage are very common, indicating a very serious issue in the age of information technology. Some recent and prominent incidents took place at AT&T and Heartland Payment Services which involved external hackers. The case about the Massachusetts Secretary of State Office was due to employee negligence.

AT&T

Network vulnerabilities at AT&T were exploited by a hacker group called Goatse Security. As a result, the e-mail addresses and ICC ID numbers of more than new 114,000 iPad owners were compromised.

Among the affected customers include New York Mayor Michael Bloomberg, film mogul Harvey Weinstein, dozens of CEOs, military officials, and top politicians, etc. There are several ways that the stolen information can be utilized. The hackers know that the victims of this incident will be receiving e-mails from Apple and AT&T concerning the matter. They can mimic the legit emails and plant malicious software in them. The iPad users could also be vulnerable to spam marketing. According to a security researcher, the breach can have more serious consequences. The stolen ICC ID number can be used to extract an IMSI number, which can be used to retrieve customer’s billing address, phone number, and the location of mobile devices. It is also possible for the hackers to listen in on the victim’s phone calls and text messages.

Heartland Payment Services

Heartland Payment Services is a large credit and debit card processing company that serves over 250,000 businesses. In 2008, a cyber attack compromised more than 100 million customer accounts. Malware implanted on Heartland’s system allowed the criminals to extract unencrypted data. They have captured card numbers, expiration dates, and customer names. Although the hackers will have difficulty using the card numbers to do shopping online or over the phone because more information is needed, they can clone the cards and swipe them in stores. The breach was considered the largest in US history.

Massachusetts Secretary of State Office

In June 2007, the Massachusetts Secretary of State Office accidently released confidential information of 139,000 investment advisers. The office originally intended to send a list of registered investment companies to an industry publication as requested. But it mistakenly attached the Social Security Numbers, dates and location of birth, height, weight, and other personal information of the registered investment advisers. The publication returned the CD once it discovered the mistake, but it is uncertain whether any information has been leaked.

---

Impact of Incidents

Extent of data leakage incidents

According to Privacy Rights Clearinghouse, a non-profit organization that advocates consumer privacy, over 355 million of records containing sensitive personal information are involved in security breaches in the US since January 2005. This is a fairly conservative estimate because for some incidents the number of records affected is unknown. The number of data loss incidents has increased by 1,700 percent worldwide for large organizations since 2004.

Cost to organizations

When data is lost, it can either be recoverable or the loss is permanent. Research has show that data can be recovered 83% of the time. In the case of a permanent loss, the cost to the organization depends on the value of the lost data. If it can be recovered, expenditures will be incurred for computer support specialists or other technical services. Meanwhile, some productivity is lost. If the incident is not publicized and the adverse effects are not pervasive, the cost to the organization should stop here.

If it is an episode of information leakage that gets out to the public, the cost can be significantly higher. In addition to the above-mentioned costs, the company will incur direct costs to notify the public and offer after-the-fact response such as hotline support. The organization may also face class action lawsuits and regulatory penalties. However, the more significant costs are indirect and difficult to measure.

Depending on the situation and the industry, the affected company will likely experience damages to its reputation and brand integrity, and loss of customer trust and confidence. A study by the Ponemon Institute has estimated the average cost of information leakage to be $202 per customer record, of which $152 is related to indirect costs such as abnormal customer turnover. The costs were found to be higher for financial and healthcare industries because more sensitive data are collected and customers have higher expectation for the safety of those data. In the same study, the average cost of data leak per organization was found to be $6.65 million.

---

In some specific cases, companies could lose their trade secrets, details of contracts, sensitive company information, customer lists, or overall competitive advantage.\textsuperscript{18} The costs to these companies are simply immeasurable and could direct impact their going-concern.

Victims/customers

In some cases, information leakage could lead to incidents of identify thefts which directly impact the victims. In the hands of more sophisticated criminals, victims may suffer other serious consequences. Other times the thieves are only interested in the hardware and not what is stored within.\textsuperscript{19} In any case, customers will lose confidence in the company and will likely switch over to a competitor if available.

Data Loss Prevention

Due to the fact that data loss and information leakage can be the result of a multitude of causes, a comprehensive approach to prevention is needed.

Culture and leadership

Organizations should foster a culture were security is a key priority and not a burden or a hindrance to day-to-day activities. The environment should be open and trusting where employees feel comfortable reporting suspicious activities and security incidents. The importance of data as a resource should be communicated to the employees. Data protection should be everyone’s responsibility and not just limited to the IT staff. A study has shown that 41% of employees do not follow security procedures because they believe that if something goes wrong, IT is there to save them.\textsuperscript{20} Organizations should establish clear leadership by having executive commitment and accountability. The executives can lead by example to emphasize the importance data protection and security in general.

Risk assessment

Organizations should evaluate employee behaviour to identify the associated risks with respect to data security. The threat environment should be continuously monitored and analyzed to assess the risk of interaction between employees and network, endpoints, data, applications, and other employees.\textsuperscript{21}

Policies and enforcement

According to a survey, 25% of companies don't have security policies regarding the access and use of information. Security policies and business processes should be established to address the assessed risks. Employee participation in designing the policies may ensure their willingness and ease of compliance. The policies should be clear about people’s responsibilities and accountability. Enforcement should be simplified by limiting the number of policies, making them easily understandable, and integrating them into business processes. The following policies and conducts should be established at a minimum:

- Restrict computer use to only authorized applications
- Using company devices for personal purposes should be limited or prohibited
- Prohibit the visit of inappropriate websites
- Prevent or limit the sharing of work devices
- Restrict the sharing of passwords

For companies with security policies, 25% of them do not respond to violation of the rules. The policies must be enforced or they would be useless. Depending on the severity of the violation, organizations should consider disciplinary actions up to termination.

Education, training and communication

According to a study conducted by Cisco, 40% of employees, and surprisingly 20% of IT staff, did not know security policies existed. Employees should be provided with proper education and training about information security and company policies and procedures. IT staff should educate employees on common security mistakes, areas of vulnerability, how to protect data, and how to report incidents. New hires should begin education and training during the orientation stage. Any updates to policies and procedures should be supplemented with either verbal communication, newsletter, or website updates in addition to emails. Emails may be ignored or accidentally deleted. It is also harder for employees to retain the information if it was read from an email relative to communication in person.

---

Technology and tools

Organizations should try to identify and categorize their data based on importance, confidentiality, and privacy levels, and establish controls and access over them accordingly. It is also recommended that they implement tools and processes to track data’s movement to monitor where it is stored, how it is accessed, and which users are using it.\(^\text{27}\)

To combat viruses and malwares, anti-virus programs should be properly maintained and timely patched. Firewall should be in place to deter and prevent unauthorized external access.\(^\text{28}\) Security settings should be implemented on all company devices and employees should not have the option to override them.\(^\text{29}\) Encryption techniques should be adopted or improved to ensure the secure transmission of data.

Physical access controls can be improved by adding physical locks to hardware, especially portable devices. Physical access to company facilities should be limited to employees only. ID cards and security guards can be used to manage access. In terms of logical access, procedures should be in place to terminate access rights to employees that have left the company. Password creation techniques should be sound and passwords should be stored securely.\(^\text{30}\)

The use of privacy filters can prevent over-the-shoulder viewing from strangers or unauthorized individuals in general.\(^\text{31}\)

To protect data from power failure, companies should consider having multiple power circuits with battery backup and a generator. To guard against certain hardware and software failures, a journalizing filing system with RAID storage can be implemented.\(^\text{32}\)

Lastly, many software vendors offer data loss prevention solutions. These technological solutions should be evaluated based on the following criteria before purchase.\(^\text{33}\)

---


- Comprehensive channels coverage
  - Data can be leaked through many channels, such as email or instant messenger. A good DLP system should cover all network channels.

- Enforcement
  - In addition to detecting data breaches, a good DLP system should be able to block the transmission of protected data.

- Content inspection
  - A good DLP system should be able to inspect the content of data being transmitted to determine whether it's protected

- Accuracy
  - A good DLP system shouldn't make any errors, both false positives and undetected leaks. If the protected data went under simple modifications, such as text-reformatting, a good DLP system should still be able to detect it.

- Non-duplicating protected data
  - A good DLP system should not copy the protected data into its internal database, which would lead to additional risks instead of preventing leaks.
**Annotated Bibliography**


**Annotation:**
The article describes data loss as the leakage of confidential data caused accidentally or intentionally. The worldwide impact of data loss incidents is also described.


**Annotation:**
The paper describes the many causes of data loss such as hardware failure, human errors, theft, and natural disasters. The author identified the various costs associated with a data loss incident and estimated the average cost of an incident to be $4,000. The estimate is conservative because lost sales and reputation damages are not considered.


**Annotation:**
Article defines data loss as the unforeseen loss of data or information. It is caused by various reasons such as crimes, disasters, intentional and unintentional actions, and various failures. DLP suggestions include regular backup, anti-virus, and having multiple power circuits.


**Annotation:**
Data breach is defined as unintentional release of sensitive information. If an incident is publicised, the bad publicity is very costly. Other losses could include the loss of trades secrets and sensitive corporate information.


**Annotation:**
Data breach at AT&T exposed the e-mail addresses of 114,000 Apple iPad users. Hacker group is called Goatse Security. iPad owners may be vulnerable to spam marketing and emails containing malicious attachments.

**Annotation:**
According to Privacy Rights Clearinghouse, a non-profit customer organization that advocates consumer privacy, over 355 million of records containing sensitive personal information are involved in security breaches in the US since January 2005.


**Annotation:**
Heartland Payment Services, a large credit card processing company that serves 250,000 businesses, was breached in a cyber attack that compromised more than 100 million customer accounts. Malware was discovered on Heartland’s system that allowed thieves to sniff unencrypted data such as card numbers.


**Annotation:**
Study showed that "insider threats" are more prevalent than external threats. Employees could be sabotage company data or purposely leaking them out. Or, they can simply be negligent and careless. Best practices address all of these insider threats.


**Annotation:**
Employees are conducting risky behaviour despite of policies and procedures. These behaviours include the unauthorized use of applications, misuse of computer computers, unauthorized access, and misuse of password. DLP responses to these risks are to better manage and guard corporate data by implementing policies, communicating them, and enforcing them.


**Annotation:**
IT security policies are usually not well documented, communicated to employees, or outdated. Employees don’t follow procedures for various reasons such as lack of care and the perception that IT will solve the problem. Suggestions to this problem including simplifying enforcement, increase awareness, and communicate policies more effectively.
Since 2005, more than 250 million customer records containing sensitive information have been lost or stolen. Direct costs include outlays for detection, escalation, notification, and after the fact response. Indirect costs include in-house investigation, economic impact of lost customer trust and confidence. The average cost of a data breach is estimated to be $202 per customer record.

59% of respondents to the study admitted to stealing confidential company information. 24% of respondents were still able to access employer’s system or network after leaving. Theft could have been prevented from better data loss prevention measures.

The 5 ingredients to a good DLP system are: comprehensive channels coverage, enforcement, accuracy, content inspection, and non-duplicating protected data.

SIM card numbers stolen by hackers can be used to derive another set of numbers that allow them to obtain billing information of customers. They may also listen in on phone conversations and read text messages.

The Massachusetts secretary of state’s office mistakenly released confidential information of 139,000 registered investment advisers. Social security numbers, birth dates, and other information were mistakenly sent to an industry publication company.