Information Leakage and Data Loss Prevention

ACC 626 - Section 1

Instructor: Kieng Iv

Student Name: Kiren Dulku

Date: June 27, 2014

# Table of Contents

Executive Summary .................................................................................................................. 3

Introduction ................................................................................................................................. 4

Information Leakage .................................................................................................................... 4 - 5

Impact of Information Leakage .................................................................................................. 5 - 8

Controls to Prevent Information Leakage .................................................................................. 9 - 11

Data Loss Prevention Tools ........................................................................................................ 12 - 14

Current Issues with Information Leakage and Data Loss Prevention ........................................ 14 - 15

Conclusion ................................................................................................................................. 15 - 16

Appendices .................................................................................................................................. 17

Works Cited ............................................................................................................................... 18 - 19
Executive Summary

Information leakage is a serious issue today that impacts everyone, personally and broadly. Impacting someone personally can be a stranger getting a hold of one's name, phone number or email address or can become more serious such as a stranger getting a hold of your personal credit card number and PIN. Information leakage impacting someone broadly can mean an information leakage issue that may have occurred at their workplace or in the community, such as a data breach with a company or a local store. Hence, information leakage affects everyone and therefore, everyone should be aware of it, its risks and how one can protect their own personal and confidential information as well as any prevention mechanisms they can use in order to prevent the loss of any data.

Although information leakage can affect anyone, there are also methods to prevent someone from stealing private and confidential information as long as individuals are aware of the impact of information leakage and what the consequences are to them or their company or community. This is where internal controls come in, which are necessary in a company setting in order to educate employees regarding the issues of information leakage and how to ensure they are not part of the leaking of confidential company information. C-Suite executives as well as auditors and consultants play a vital role in educating employees and ensuring that the company has the security controls in place to protect company data.

These issues above will be discussed in this report from the perspective of businesses and how information leakage may impact a company along with controls to prevent information leakage from their employees or by external threats. Furthermore, the report will focus on data loss prevention tools for businesses in order to mitigate the risks that arise from a data breach or to prevent another data breach from occurring again in the future. Finally, the report will discuss current issues that involve the leakage of information and the impact of the data breach in each situation.
Introduction

Information leakage and data loss prevention are important issues today that impact everyone. These issues impact anyone that may have any type of information that they do not want others to obtain. For example, people have personal information, such as a Social Insurance Number in Canada, that they do not want others to have access to since it can lead to significant risks, such as identity theft. Therefore, they will use mechanisms to prevent others from gaining access to this personal information, such as keeping it written in a safe and hidden place or not written down at all. However this is one specific example of information leakage and data loss prevention, and there are several others that could have an impact at an individual level, to having an enormous impact on an entire nation! The scale varies greatly, however, the focus of this report is on information leakage and data loss prevention as it impacts businesses, as well as how it may impact the employees of different levels of an organization and the impact on the accounting profession.

Information Leakage

In simple terms, information leakage is, "the leaking of "internal" information, such as personal information and confidential company information, to the outside world". Information leakage is therefore, any inside information that is meant to stay within the organization, being revealed somehow to anyone external to the organization. One needs to first determine where this information originates from and then what the possible methods are for this information to be leaked to the outside world.

Information can enter an organization from any part of the organization, whether it is from the lower level employees or from the top level executives. Information within organizations can come from the CEO, CFO or a manager, a board of directors meeting, the company's Intranet or information system or from the company's annual report. There are different methods of communicating information such as through the Intranet or Internet, in meetings, Emails, information being passed via a USB key, information on paper being passed through hands or a simple discussion between two employees, whether it is inside the workplace or outside of it. Information is then transmitted via these methods and hence creates a possibility of information leakage.

---

to be leaked to the outside world. Information can also be extracted by someone external to the organization by simply hacking into the company's information system or the network itself.

Besides the methods listed above, other forms of internal information leakage include instant messaging between employees or an employee with an external party, web mail, web logs / wikis, malicious web pages, hiding in SSL, File Transfer Protocol (FTP), other removable media / storage, security classification errors, hard copy of information, cameras, inadequate folder and file protection and inadequate database security. Other forms of external information leakage include data theft by intruders, SQL injection, malware, dumpster diving, phishing, social engineering and physical theft.

Appendix 1 was created on the basis of information from the report, "2008 Survey Report of Information Security Incident" by NPO Japan Network Security Association. The study confirmed that the majority of information is leaked through paper-based mediums, accounting for 55.9% of cases due to handling errors, management errors and loss or misplacement. Further, most large-scale incidents involving information leakage have occurred as a result of information being leaked through paper-based mediums, at 59.5% of cases. From Appendix 1, it is evident that information leakage from means such as the Web and Email were not as prominent as the traditional, paper-based means in 2008. These results are contrary to the information leakage prevention techniques that are being used today. The prevention techniques today mainly use technology in order to protect information within a company and to prevent information from being accessed by unauthorized users. These techniques and further data loss prevention tools will be discussed in this report. Note that information leakage through technology-based means could be more prominent today in 2014, however paper-based means of information leakage is definitely still an issue to be aware of and needs to be dealt with in organizations.

**Impact of Information Leakage**

Information leakage can occur intentionally or unintentionally by anyone inside or outside of the organization. It can also have a small impact or a detrimental impact on the organization.

---

3 Ibid
5 Ibid
6 Ibid
depending on the level of confidentiality of the information that was leaked. For example, if something written in the annual report is leaked before the annual report is released, the impact is not as large, especially because the annual report will eventually be open to the public. However, if personal customer information is leaked to the outside world, this can have a detrimental impact on the future operations of a company and its reputation. One example where information leakage had a larger impact on a company is when there was a data breach with Target in December 2013. Information regarding customer’s payment card data was accessed by unauthorized users and affected approximately 40 million credit and debit card accounts. Later it was revealed that some 70 million customers’ personal information such as names, mailing addresses, phone numbers and Email addresses were also stolen. As a result of this data breach, Target's reputation was damaged and customers lost trust in the system used at Target to protect their credit card payment information. This is proven by the drop of 35 points (from 26 to -9 points) in Target's brand on the BrandIndex’s scale from the week before the announcement of the data breach to immediately following the announcement. This demonstrates the impact of information protection and prevention of information leakage for large companies such as Target if such a company wants to maintain their reputation and continue to be successful in the future.

The impact of information leakage can also affect certain individuals, whether they are employees or parties connected to the company. These parties include C-Suite executives and individuals part of the professional body of accountants, such as auditors. The impact on these individuals is discussed next.

**C-Suite Executives**

Information leakage has a large impact on C-Suite executives since they are the face of the organization they are running. If there is a leakage of information, especially sensitive information, then these executives could face high levels of scrutiny from the media and the public in general. For example, returning to the Target data breach, the CEO Gregg Steinhafel stepped down from his position as a result of the security breach, despite the fact that he had been

---

8 Ibid.
with Target for 35 years\textsuperscript{11}. Clearly this information leakage had such a significant impact that it caused the CEO to resign from his position. This shows the impact that information leakage may have on C-Suite executives, especially those of large public companies.

As a result of the impact that information leakage may have on these C-Suite executives, their chief concerns regarding information leakage would be the ability to prevent and detect any information leakage in the first place. The ability to prevent information from being leaked would be a higher concern for executives as opposed to detecting it, since detection is a control after the fact, and prevention will ensure information is not leaked in the first place. Further, if a C-Suite executive leads by example and explains to his or her employees the importance of protecting the confidential information of the company, then it sets an environment where employees are more aware of the methods they are using to transmit information and they are more likely to ensure they are retaining information within the company. This is an important part of the control environment, which will be discussed later.

\textit{Accounting Profession}

Information leakage is an important issue that accounting professionals, especially auditors, need to be aware of. Although an auditor is not responsible for information leakage within the company they are auditing, if they are aware of what it is and what can cause information leakage, then they would recognize indications of a data breach within the company they are auditing. They would then be able to inform management if they are unaware of the issue and the auditor may need to change the scope of their audit as a result of the news of a potential data breach.

As an auditor, there is a requirement to demonstrate professional skepticism and a questioning mind while conducting an audit\textsuperscript{12}. This means that an auditor should ensure that they evaluate the internal controls of a company and if there are suspicions of inside information being leaked, then they need to discuss the issue with management. It could be that management was unaware of the issue or that they were attempting to hide the issue from the auditor so that the auditor would not


\textsuperscript{12} Kerler, William A. \textit{The Effects of Auditors’ Trust in Client Management on Auditors’ Judgments}. Blacksburg, Virginia: n.p., 27 June 2005. PDF.
tell management that they would have to disclose the issue or take other immediate and expensive actions.

From a different perspective than the client having an issue of information leakage as a result of their own actions or their employees, the client may have a concern about the auditor protecting the information that they provide during an engagement. As part of the Fundamental Principles created by the International Ethics Standards Boards for Accountants, an accountant has an obligation to protect the information that they gather regarding an engagement with a client and ensure it is not disclosed to anyone that is unauthorized to view or hear the information. Information that is provided to an auditor during an audit tends to be confidential, with the client firm trusting the auditor to safeguard this confidential information and to ensure it does not get exposed to unwanted users. This includes information that the auditor gathers as a result of their engagement or information that the client provides to the auditor. Providing information to unwanted users includes giving client information to anyone that the auditor has not been provided with permission from the client to provide such information to. Therefore, information leakage is not only something that an auditor needs to be aware of at their client sites, but they also have to be careful not to take part in the leaking of information.

Thus, it is evident that the issue of information leakage impacts everyone within an organization, especially C-Suite executives within client firms and auditors and other accountants in the accounting profession. Other large scale impacts of information leakage on an organization can be loss of sales due to a potential hack into their system that impacts their ability to sell products or services and loss of control over their system and operations. Also, consequences such as a damaged reputation and financial penalties from fines or lawsuits have a large impact on companies that have faced data leakage in the past. Fortunately, there are controls to help these parties prevent information leakage from occurring, and these controls will be discussed next.

Controls to Prevent Information Leakage

There are several controls that C-Suite executives can implement at their companies in order to prevent information leakage from occurring. Professional accountants that are working with a client, whether as a consultant or an auditor would also be interested in these controls to aid with their engagement. Strong internal controls are paramount for the success of companies in today's society and must be implemented in order for a company to see the results of these strong internal controls. First and foremost, an important component of the internal control integrated framework, Committee of Sponsoring Organizations (COSO), is the control environment within a company\textsuperscript{15}. The strong control environment is important in order to reduce the risks in a company such as the loss of assets and to ensure the financial statements are reliable and compliant with standards\textsuperscript{16}. The control environment consists of multiple layers, such as integrity and ethical values, commitment to competence, board of directors and audit committee, management's philosophy and operating style, organizational structure, assignment of authority and responsibility and human resource policies and practices\textsuperscript{17}. These components are all important controls to prevent the leakage of information from within a company and how these controls can be approached to prevent information leakage is discussed below:

- Integrity and ethical values - This includes having a code of conduct that sets the expected standards within the company and that prevent a person to be incited to behave mischievously\textsuperscript{18}. This control can prevent information leakage from occurring intentionally by an employee from within the company as they will be deterred from doing so as a result of the code of conduct that should discuss the importance of retaining confidential information within the company and the consequences of not doing so.

- Commitment to competence - This includes having the appropriate people completing tasks within the scope of their knowledge and skills\textsuperscript{19}. This control is important to prevent information leakage, especially between departments, as there can be confidential information that is required to stay within certain departments and this information

\textsuperscript{15} Wainberg, J. (2014, June 4). Lecture presented in Assurance and Governance. University of Waterloo. Waterloo, ON
\textsuperscript{16} Internal Control - Integrated Framework. N.p.: Committee of Sponsoring Organizations of the Treadway Commission. PDF.
\textsuperscript{17} Wainberg, J. (2014, June 4). Lecture presented in Assurance and Governance. University of Waterloo. Waterloo, ON
\textsuperscript{18} Internal Control - Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission, Dec., 2011. PDF.
\textsuperscript{19} Ibid
should not be shared with other employees in different parts of the company. Having the right personnel with the necessary skills working in the right departments can ensure that the information does not stray where it should not. This can also be relevant to employees without the proper knowledge approaching sources external to the company to aid them with job tasks that include confidential information.

- **Board of directors and audit committee** - This includes having independent members of the board as well as having an audit committee that is competent in financial reporting. This control provides an oversight over any operating or financial reporting issues within the company and could perhaps reveal any potential information leakage before the external auditor, if one exists, finds it.

- **Management’s philosophy and operating style** - This includes tone at the top and management displaying honest and ethical behaviours that they would want their employees to also demonstrate. This control is important in preventing information leakage since it sets the atmosphere that is expected at the company, which includes employees protecting confidential information and not taking part in any unethical behaviours such as leaking inside information. This control is related to the integrity and ethical values control discussed above.

- **Organizational structure** - This includes having a structure that complements the organization's planning, directing and controlling operations, along with having an information systems steering committee. This is important for the prevention of information leakage since it allows for employees with concerns regarding the information system and controls to reach out to the committee, who then in turn can help resolve any issues or concerns. Some issues and concerns may include an employee with suspicions that inside information is being leaked through the information system by another employee or that the system has been compromised by a hacker.

- **Assignment of authority and responsibility** - This includes defining, assigning and limiting the authority and responsibility of employees in the company. This is important to prevent information leakage since it forces employees to be accountable for their actions.

---


21 Ibid

22 Ibid

actions and decisions and they should understand that they will face the consequences of any misbehaviour, including leaking inside information.

- **Human resource policies and practices** - This includes ensuring that employees that are hired are properly trained, promoted and compensated\(^{24}\). This is important for the prevention of information leakage since employees that are trained and appropriately compensated should not be motivated to leak inside information on the basis of getting revenge for being treated unfairly at the company. However, this control may not be as strong as the others discussed above since some employees have a natural tendency to be unethical regardless of being properly trained and compensated. These are simply deterrents that can help prevent the leaking of inside information.

These components of the control environment are therefore strong controls to help prevent the leaking of confidential information within a company. Although the other components of the internal control framework are important for strong internal controls, the control environment is definitely important to help prevent information leakage as it is directed at the employees and their conduct. Another control to prevent information leakage would be monitoring, which is also part of the internal control framework\(^{25}\). Monitoring by the board of directors and audit committee can reveal instances where information has been leaked or any other suspicions regarding the potential leakage of information.

As mentioned earlier, the internal control framework is important to professional accountants in helping their clients, whether they are in the role of an auditor or a consultant to the client. As a consultant, an accountant would want to ensure their client is aware of creating and maintaining a strong control environment, especially if information leakage has been an issue in the past. When conducting an audit, the auditor will want to look for strong internal controls, which includes the control environment and its components as discussed above. Further, if the auditor finds that components of the control environment are lacking in the organization, they would want to further investigate these issues to determine any negative impact the absences may have on the organization and discuss any issues with management.


\(^{25}\) Ibid
Data Loss Prevention Tools

The most common reasons of data breaches tend to be innocent mistakes by employees, such as a lost or stolen device or the unintentional misuse of corporate assets\textsuperscript{26}. Therefore, there is a greater need to focus attention on preventing the loss of important and confidential data that occur by other means as well as by human error as human error is natural and inevitable.

Along with the controls to prevent information leakage discussed above, there are several data loss prevention tools that can be used by organizations to protect their confidential information further. To begin, data loss prevention helps to ensure that confidential information remains safe and secure at all times\textsuperscript{27}. As mentioned earlier, most data loss prevention tools are technology-based and therefore help prevent the loss of information from technology-based information sources, such as Email, laptops and mobile devices. Most of the data loss prevention tools discussed below would be useful for C-Suite executives and their managers to use, however, a CA practitioner that may be a consultant to a client may provide some of these tools as options to use in order to prevent any data from being lost in the future.

Some data loss prevention tools and reasons as to why they are useful are discussed below:

- **Downloadable and Purchasable software** - This includes AntiVirus, AntiSpyware and AntiPhishing programs designed to protect computers and networks from viruses and malware\textsuperscript{28}. Also, a company can install firewalls and an intrusion detection system to prevent outside users from getting into the company's network. Furthermore, a company can purchase data leakage protection tools that have been created by companies such as Cisco, in order to assess risk and prevent data loss at times of highest risk\textsuperscript{29}. Another company, Sophos, has solutions to prevent the leakage of information through Email with advanced content filtering and encryption, built-in device control to block anyone from

\textsuperscript{28} Gordon, Peter. Data Leakage - Threats and Mitigation. N.p.: SANS Institute InfoSec Reading Room, Oct. 2007. PDF.
using removable storage, optical media drives and wireless networking protocols, as well as the ability to block applications and have network access control\(^\text{30}\).

- **Upgrading Information System** - The first step to upgrading the information system is by hiring an information systems expert/consultant that can review the company's operations and implement a customized information system that is based on the needs of the organization. Note that upgrading the system may not be necessary, however, a change to the current information system may be required to help the system protect company data.

- **Rules/Codes of Conduct** - As mentioned earlier as part of the control environment, implementing rules such as the appropriate use of the Internet at the workplace and rules regarding the use of personal and work Emails can help prevent the loss of data. For example, having unauthorized or unsafe websites blocked can prevent malicious software called malware from entering and infecting the organization's network. Also, prohibiting the use of personal Email as well as disallowing employees from downloading any attachments from external users can prevent viruses from entering the system. Malware or other viruses can lead to information being stolen by an unauthorized user and can also provide full access to the company's network\(^\text{31}\).

- **Mobile devices** - Mobile devices are commonly used in the workplace today. Information sent over mobile devices such as laptops, hand held devices and tablets can be encrypted on both ends, and to further protect the data, a company can require the device to be locked with a password and also allow the IT department to be able to wipe the data clean remotely if the device is lost or stolen\(^\text{32}\).
  - Note that encryption may also be used to send information through Emails on stationary devices such as a computer

- **Security Controls** - A company will want to have strong physical access controls to prevent unauthorized users from being able to enter the company physically by simply walking through the front door. Basic security controls are having electronic pass codes to enter through doors, with a picture of the employee on the card, as well as restricting physical access to certain departments and rooms to authorized personnel only. This can


be done by having special security access inputted on individual pass codes or having physical keys provided to the authorized personnel within the company only.

**Current Issues with Information Leakage and Data Loss Prevention**

Today, there are several issues related to information leakage and data loss prevention that affect multiple people, whether they are impacted through their business or personally affected by the issue. One issue that has been discussed above is the data breach that occurred with Target. Some other issues that have impacted a large number of people will be discussed below.

*Heartbleed*

Earlier in 2014, Heartbleed, which is "a security bug or programming error in popular versions of OpenSSL", was discovered\(^33\). Although not a virus or malware, it could be used by cybercriminals and malware\(^34\). The issue is that it could extract the keys used in these "secure" websites, essentially any site that is meant to be protected by showing the lock symbol beside the URL or the "https"\(^35\). These keys could be decoded and read by the bug and it has been proven through tests that information such as user names, passwords, instant messages, Emails, business documents and business communications could potentially be available to cybercriminals\(^36\). This issue impacted many Canadians as even the Canada Revenue Agency website was infected by the bug, with 900 Social Insurance Numbers stolen\(^37\). Clearly, this is an example of a nation-wide issue and it impacted any Canadian that wanted to file their 2013 tax returns since the Canada Revenue Agency website was shut down to deal with the security hole\(^38\). Therefore, this is an example where individuals must be aware of potential data breaches that could occur within their own computers with personal information stolen, and it emphasizes the need for people to be aware of information leakage issues and data loss prevention tools to protect themselves and their private and confidential information. This issue not only impacted Canadians on an individual level, but it impacted larger organizations, such as the Canadian government, which demonstrates the severity of information leakage. It also proves that even with the highest security protection,

\(^34\) Ibid
\(^35\) Ibid
\(^36\) Ibid
\(^37\) Ibid
\(^38\) Ibid
anyone can be the victim of a data breach, and therefore everyone should be aware of it in order to protect themselves and their information in any way.

Michaels Stores Inc.
Also early in 2014, Michaels announced that 2.6 million debit and credit cards may have been impacted by a security breach\textsuperscript{39}. The information that may have been stolen included payment card numbers and expiration dates, with no evidence of other personal information such as names, addresses or PIN numbers being stolen\textsuperscript{40}. As this occurred so close to the data breach with Target at the end of 2013, it definitely caused some concern for customers wanting to use their debit and credit cards at stores, whether they are large or small. Michaels had suspicions of the data breach in January 2014, however the announcement to confirm the breach came out in April 2014\textsuperscript{41}. Further, Michaels stated that the security breach was an attack by criminals that were using highly sophisticated malware\textsuperscript{42}. This demonstrates the importance of companies having AntiVirus and AntiSpyware in their systems and ensuring they continuously monitor their systems for any suspicions of breaches into the system. As Michaels is such a large consumer store, this shows that companies containing large amounts of personal customer data need to ensure they take extra cautions in protecting this confidential information as it can lead to more severe consequences, such as future loss of sales and a damaged reputation, as mentioned earlier.

Conclusion
Overall, information leakage and data loss prevention are both areas of concern for anyone in any industry as well as on an individual level. In this report, the roles of C-Suite executives and professional accountants were focused on to provide some specific insight as to how these individuals are impacted by information leakage and how they can prevent the issue from occurring in the future. It provided awareness regarding the state of information leakage today and helpful tools that may be used to prevent any loss of data as a result of information leakage. Finally, it presented issues that exist today that affect multiple people around the world. From the results of the research in this report, it is evident that information leakage is an issue that all

\textsuperscript{40} Ibid
\textsuperscript{41} Ibid
\textsuperscript{42} Ibid
employees at all levels of an organization should be aware of, including those individuals that are external resources to the company, such as an auditor or consultant. Also, there are multiple information leakage controls and data prevention tools that can be implemented in order to protect the confidential information within a company. The first step in protecting important information is to ensure everyone is aware of information leakage and then educate them in preventing the loss of data to ensure continued future success for any type of company.
Appendices

Appendix 1

**Year: 2008**

<table>
<thead>
<tr>
<th>Media/Route</th>
<th>2008 Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>8.1%</td>
</tr>
<tr>
<td>FTP</td>
<td>0.0%</td>
</tr>
<tr>
<td>PC</td>
<td>7.3%</td>
</tr>
<tr>
<td>Removable recording media (USB drive, etc.)</td>
<td>9.9%</td>
</tr>
<tr>
<td>Web • Net</td>
<td>11.7%</td>
</tr>
<tr>
<td>Uncertain</td>
<td>0.7%</td>
</tr>
<tr>
<td>Others</td>
<td>6.5%</td>
</tr>
<tr>
<td>Paper medium</td>
<td>55.9%</td>
</tr>
<tr>
<td>Removable recording media (USB drive, etc.)</td>
<td>10.5%</td>
</tr>
<tr>
<td>Email</td>
<td>1.1%</td>
</tr>
<tr>
<td>PC</td>
<td>2.7%</td>
</tr>
<tr>
<td>Others</td>
<td>0.3%</td>
</tr>
<tr>
<td>Paper medium</td>
<td>59.5%</td>
</tr>
</tbody>
</table>

**Ratios of different media/routes for information leakage (number of cases)**

The media for information leakage with the most number of cases is "paper medium." The main causes of this leakage are "handling error," "management error," and "loss or misplacement."

**Ratios of different media/routes for information leakage (number of people)**

Since eleven cases of large-scale incidents (involving over 100,000 people) concerning paper occurred, this number represents over half (59.5%) of all the cases.


Works Cited


Gordon, Peter. Data Leakage - Threats and Mitigation. SANS Institute InfoSec Reading Room, Oct. 2007. PDF.


*Internal Control - Integrated Framework.* N.p.: Committee of Sponsoring Organizations of the Treadway Commission. PDF.


