Protecting Employee Data in a Global Corporation

Ashley Hall and Dr. H. Anna Yu

Department of Computer Science
North Carolina A&T State University

Abstract
The purpose of this case study is to enhance the information assurance curriculum by providing conceptual information that is relevant and parallel to the material that is learned in the classroom. The learning goals of this case study are for the student to be able to understand why protecting employee data is essential, differences in protecting employee data globally versus protecting employee data nationally, approaches to protect employee data, and effects of improper employee data protection. Real world global employee data protection cases are presented.

1. Introduction

What information should an employer store about an employee of a corporation? What employee information should be released to a third party? How would an employee react to information being released to someone they did not want to have that information? These are questions that have to be considered by a corporation when they ask employees for information and store that information.

An employee's privacy can be violated by having information given to a corporation released to parties who are not authorized to have the information. There have been several cases where an employee's information has been released mistakenly and several cases where information was purposely released. Though information about protecting employee data has been discovered, many corporations continue to fail at protecting employee data.

This case study will help students understand techniques of protecting employee data, the difference in protecting employee data in a global organization versus a national organization, approaches to protecting employee data, and the effects of improper employee data protection. This case study includes learning objectives, discussion questions, and real world cases to help students understand related topics.

2. Protecting Employee Data in a Global Corporation

Protecting employee data is detrimental to ensuring each employee's information is safe guarded and making sure employees' privacy is not violated. Employee data is protected by only allowing the proper parties to view certain information. Many corporations use human resource software platforms, including databases which hold employee data. This data may be very diverse, from an employee's age to an employee's favorite color. Regardless of what the data is, each employee data field may be important for different reasons.

2.1 Protecting a Global Corporation's Data in General

When protecting employee data, employee consent, data loss prevention, and the difference in laws among different legislations should be taken into consideration. Data loss prevention

(DLP) is an issue all corporations must consider whether they have employees in one nation or many nations. With the growth of the internet and ways information can be transported electronically, data loss has become a major issue among corporations' security and privacy measures. Many times it may be much easier to lose data electronically than to protect it. Companies may lose data as it is in motion (such as in an email) or as it is at rest (such as in a database). The more dangerous is the loss of data as it is in motion, as many mistakes can be made and much damage can be caused in little time [1].

Though many companies educate their employees on the importance of retaining confidential information and DLP, there are still possibilities for information to be released intentionally and mistakenly. There are several ways confidential information can be leaked via the internet including email, websites, instant messaging, and ftp. It has been suggested that companies use content scanning mechanisms and encryption to prevent confidential information from being released. Companies should monitor communications to external destinations, encrypt confidential email, secure partner communications, enforce acceptable use policies, and give consequences for violating privacy and confidential information policies [1].

In addition to making sure data is not lost, corporations must also make sure they are legally storing data. Because of this need, employee consent forms and privacy policies are vital. A privacy policy is a document where employees consent to the ways a corporation may gather, use, disclose, and manage their information. The contents of a privacy policy are usually created based on several local, national, and/or international regulatory mandates. This privacy policy is pertinent to making sure an employee has been informed and agrees to how their personal information is stored and used.

IBM is a global technology corporation which aims to protect its employees, customers, and business partners personal data through its privacy policy. The privacy policy helps to ensure fair and proper practices for collecting, disclosing, storing, accessing, transferring, or any processing of personal data. The general principles in the privacy policy are fairness, purpose, accuracy, disclosure, security, and access. Through the fairness principle, IBM aims to process personal information fairly. The purpose principle states that IBM only collects personal information which is relevant and necessary. Accuracy shows IBM vows to keep personal information accurate, complete and up to date. Disclosure gives employees assurance that their personal information will only be available in the appropriate circumstances. Through the access principle, states that their employees, and other individuals whose information is kept, will have access to the information being stored by the corporation [2].

2.2 Regulatory Mandates

Different legislations may have different laws and different corporations may have to abide by special regulations depending on the type of information they store and use. Regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the European Union's Data Protection Directive, require companies to protect private and personally-identifiable information which is any information that can be used to uniquely identify, locate, or get in contact with a person. The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for

enhancing payment account data security. The regulation was developed by several credit card companies, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help in ensuring data is consistent and secure globally. The European Union's Data Protection Directive is a regulation which sets legal standards for processing personal data and protecting privacy. The regulation applies to countries in the European Union (EU) and countries communicating data with the EU. The European Union has some mandates and restrictions on the collection and storage of personal information that are stricter than the U. S. restrictions [1].

Regulations, such as HIPAA can affect data in transit and data at rest. HIPAA requires the health care industry to handle information with certain restrictions, and directly affects the operation of messaging systems. Corporations have to make sure email messages containing HIPAA protected health information are properly secured and senders and recipients are properly verified and authenticated. They also have to ensure messages contained on email servers are protected. Corporations do not have to worry about using specific technology as long as they comply with the mandates. Most corporations find it helpful to pay close attention to authentication, encryption, content filtering, hardened message server software and archiving when complying with HIPAA requirements [1]. Regulatory mandates can become a headache to a corporation as there may be a wide variety of regulations and many mandates to follow. Though these mandates can be time consuming and may feel tedious to a corporation, they help to ensure that a corporation's employee information is kept private.

2.3. Techniques for Protecting Employee Data

When protecting employee data globally, the transferring of data physically as well as electronically or virtually must be considered. As time goes by and electronic communication technology moves forward, the separation of physical and electronic data transfer is slimming.

Two common techniques used to negotiate agreements for the proper handling of employee data by companies based in the United States are model contracts and the United States Department of Commerce's Safe Harbor. A model contract is an agreement between a data exporter and a data importer which covers aspects important to both communicators regarding transporting data. This means a corporation in the U.S. would have to have a contract for each of the nations to which it sends and receives data. Model contracts are usually better for small to medium sized companies which do not have employees or partners in many countries. In larger companies which may have employees or partners in several nations, model contracts are not as practical as there is more data being communicated. In larger companies, model contracts are thought to be expensive and difficult partly due to having to amend several contracts too often [3].

The Safe Harbor program is used mostly by large corporations. The Safe Harbor contains seven principles which are notice, choice, onward transfer, access, security, data integrity, and enforcement. Notice deals with the notification of individuals about how their information may be stored and/or used by the corporation. Choice gives individuals the choice to opt out of disclosing their information to a third party or the use of their information for a purpose other than the reason it was originally collected. Onward transfer involves ensuring third parties receiving information also abide by the rules of the Data Protection Directive. Access makes

sure individuals are able to access the information given to their employers. Security requires a corporation to make sure an individual's personal information is protected from being lost, altered, deleted or misused. Data integrity requires an organization to make sure that personal information is relevant. Enforcement makes sure that complaints are investigated, Safe Harbor verification procedures have been followed, and consequences for not complying with principles have been enforced [4].

To qualify for the Safe Harbor, an organization has to develop a self-regulatory privacy policy that follows Safe Harbor rules or be a part of a self-regulatory privacy program that follows Safe Harbor rules. The corporation must submit a letter of self certification to the Department of Commerce annually that it adheres to the requirements of the Safe Harbor. The corporation is also required to have a privacy policy that states that it abides by the principles of the Safe Harbor [4].

3. Protecting Employee Data Globally vs. Nationally

Making sure an employee's information is only released to the correct parties is not the only concern of protecting employee data. A corporation also has to make sure they are only storing data that can be lawfully kept. This is where knowing the laws of different legislations and following them all simultaneously can be difficult.

Protecting employee data can be a difficult task in a national corporation, let alone a global corporation. With a national corporation, a corporation must be certain to only store or share certain information about an employee according to the national laws. A corporation with employees in multiple countries has to be certain that this is done with respect to the laws of multiple countries at once. This can be a very difficult task as countries have very different laws and approaches to protecting employee data.

European Union's initial Data Protection Directive was issued in October 1998. The European Union has 27 member states. The directive prohibited the transfer of any personal data that did not meet specific criteria which was explained in the directive to or from its member states. The European Union is considered to have some of the stricter mandates and relies heavily on legislation for the protection of personal data [4].

To comply with the more strict policies of the European Union, the United States Department of Commerce created the Safe Harbor framework, which was approved by the European Union in 2000. The Safe Harbor framework was created to help ensure that companies communicating personal information with nations of the European Union are abiding by the policies of the European Union's Data Protection Directive. Corporations are not required to be Safe Harbor certified but there are several benefits if a corporation chooses to join. These benefits include waiving of or automatic approval of requirements for prior approval of data transfers. Abiding by the rules of the Safe Harbor also saves time and money as companies often do not have to create separate data protection agreements with each country in the EU [4].

4. Effects of Improper Global Employee Data Protection

Improper protection of employee data can cause damage to both the employee and the corporation. Many times improper protection can lead to legal action against a corporation, which can in turn bring less productivity and loss in profit for a period of time.

One of the most damaging ways an employee's privacy can be violated is when employee data is leaked to one or more parties in which the employee did not consent to. Corporations can face several negative effects if employee information is leaked. Corporations may have to face bad publicity, may face fines and/or other legal actions, and as a result of other effects may lose profit.

If an employer is a member of the United States' Safe Harbor, the corporation's failure to protect an employee's personal information may result in action by state or federal government depending on the business sector. The Federal Trade Commission, which provides enforcement for many corporations, may impose a fine of up to $12,000 per day if a certified corporation's failure to follow the Safe Harbor principles is found to be deception or misrepresentation. If a corporation consistently fails to follow the principles, they may no longer be a part of the Safe Harbor program. The Department of Commerce will then in turn publicly indicate when a corporation is no longer Safe Harbor assured [4].

5. Real World Global Employee Data Protection Cases

5.1. Shell Oil's Global Data Privacy Practices

Shell Oil is a group of global energy and petroleum companies. It has about 101,000 employees in over 90 countries. The company was ranked number 1 of the Fortune 500 companies in 2009. Shell's core values are honesty, integrity, and respect which help to form the Shell General Business Principles. Though Shell is a large corporation with a good business strategy, its protection of employee data has recently come under fire [6].

As recent as on February 12, 2010, it was reported that 170,000 Shell Oil employees contact information had been sent to environmental and human rights groups. This information, which had been kept in an unencrypted corporation database, was sent along with a cover note which explained the reasons the information had been leaked. The cover note explained that the email containing the database and the cover note had been allegedly sent by several Shell Oil employees who were upset about the corporation's harmful actions done in Nigeria [7]. This leak did not contain a large quantity of information about each employee but it did give many employees' phone numbers away without any consent.

5.2. Hewlett Packard's Global Data Privacy Practices

Hewlett Packard (HP) is one of the world's largest information technology companies. HP's headquarters is in Palo Alto, California. The corporation has about 304, 000 employees across the world. It operates in over 170 countries. Through its Global Citizenship, the corporation vows to focus its energies and expertise on human rights and labor practices, environmental sustainability, social investment, privacy, ethics, and compliance [7].

HP states “Protecting customer and employee personal data promotes trust and loyalty and strengthens the HP brand”. The corporation is charged with covering job applications, personnel files, performance evaluations, medical records, and other documents containing varying data. Any employee who has access to their human resources database is required to complete privacy training. The corporation’s privacy policy was created to comply with four different regulations, the Fair Information Practices, Organization for Economic Cooperation and Development Principles, Global Business Dialogue on Electronic Commerce guidelines, and the Safe Harbor Agreement. HP was the first Fortune 50 company to self-certify with the Safe Harbor program [8]. Though HP is a large corporation, its dedication to protecting employee data has prevented mishaps, such as major leaks of employee data.

6. Conclusion

To fully understand how to approach protecting employee data in a corporation, one must first understand how any important data within a corporation is kept private. Although regulatory mandates can seem overwhelming at times for corporations, regulations help to ensure that an employee’s information is handled properly. Having a good data loss prevention plan as well as only storing data that can be legally stored by the regulations that apply are both important in protecting employee data. Joining programs such as the Safe Harbor, not only gives other nations’ companies assurance that information is being handled correctly, but also gives employees a sense of safety when it comes to their private information.

References

[1] Cisco Systems, Inc., “Data loss prevention best practices: managing sensitive data in the enterprise,” 2000-2007. http://www.ironport.com/pdf/ironport_dlp_booklet.pdf. [Accessed: Mar. 15, 2010]

[2] IBM, “IBM policies,” http://www.ibm.com/ibm/responsibility/policy7.shtml. [Accessed: Apr. 5, 2010].

[3] B. Roberts, **“**Protecting employee data globally: knowing the rules can help employers safeguard employee privacy and still keep data flowing,” HR Magazine, FindArticles.com, 2008. http://findarticles.com/p/articles/mi_m3495/is_5_53/ai_n25432215/. [Accessed: Apr. 1, 2010].

[4] Export.gov, “Safe Harbor Overview,*”* Washington, DC: U.S. Government Office, 2006. http://www.export.gov/safeharbor/eg_main_018236.asp. [Accessed: Mar. 20, 2010].

[5] “Shell at a Glance,” http://www.shell.com/home/content/aboutshell/at_a_glance/. [Accessed: Apr. 1, 2010].

[6] T. Wilson, “Shell employee directory leaked, allegedly by activist workers,” 2010. http://www.darkreading.com/database_security/security/client/showArticle.jhtml?articleID=222900239. [Accessed: Apr. 2, 2010].

[7] Hewlett-Packard Development Corporation, “HP Fast Facts,” 2009. http://www.hp.com/hpinfo/newsroom/facts.html. [Accessed: Apr. 2, 2010].

[8] Hewlett Packard Development Corporation, “Respecting Privacy at HP,” 2004. http://www.hp.com/hpinfo/globalcitizenship/privacy/privacy_2p_r3.pdf. [Accessed: Apr. 2, 2010].