Dealing with Information Security and Privacy

I

Dennis Backherms
American Public University, USA

Kathleen Houlihan
Wilkes University, USA

INTRODUCTION

Technological developments continue to provide benefits to society by making rapid access to information cost effective and simple to obtain for the end-user. Unfortunately, easy access to information has complications that negatively impact personal privacy and security for individuals and for organizations. As technology becomes more pervasive it is important to understand how privacy and security can be compromised at the sake of progress.

According to Solove (2011), even when an individual has *nothing to hide*, it is troubling that a person's individual freedoms can be taken away just by walking down the street. Not only are surveillance cameras starting to track our every movement, social media allows almost instant access to information that formerly would not be accessible. There are no rules protecting the individual's right to privacy from government entities and organizations that collect information on citizens while in the public eye.

The collection of general information including the tracking of movements, combined with more specific information about the public allows for the development of profiles that eventually limit speech and limit freedom of individuals to freely associate with controversial groups (Doyle, 2012). Consequently, privacy should be addressed for the public specifically when individuals feel they have nothing to hide and as new devices are developed for the public privacy should be factor in the development. The information that is available on the Internet enhances the ability of organizations and hackers that later may compromise personal security for citizens.

For instance, consider the information that is available on Facebook, even though there are some security systems in place to protect the users, such as flagging content, users are not informed on how personal information is tracked, collected and disseminated to others in the network. Facebook potential grants access to friends but it also grants access of personal information to the world (Hull, Richter-Lipford, & Latulipe, 2011). Therefore, the Facebook user's information can be easily shared with third parties who have not been granted access to this information.

Since no information is available to the user explaining how the newsfeed function is shared with others, anyone who is a friend or an acquaintance may have access to these personal conversations that occur (Hull et al., 2011). In many cases the program interface extends information beyond the friendship circle. This design flaw confuses the user about who may have access to personal information; as evidenced by today's more complicated third-party privacy statements.

One way to determine the optimal investment level in security and privacy for an organization is to design a risk neutral situation. Organizational strategies can be developed based on the level of risk a company is willing to take based on the likelihood of certain outcomes. A risk neutral situation implies spending the least amount of money to protect the greatest amount of information that exists in the system and the likelihood of an attack happening. This is a difficult process to establish and it will vary based on the types of information available in the system. The costs associated with securing this information needs to be weighed carefully while providing the most secure system that is still profitable for the organization.

The most popular model, which uses risk neutral situation and is based on an economically based framework is called the Gordon-Loeb Model (2002). This model explains that the investment in security

DOI: 10.4018/978-1-4666-5888-2.ch421

should not exceed 37 percent of the expected breach loss because spending more than this percentage on a security breach does not make the organization any less vulnerable to attack. The model illustrates that organizations should make greatest investment in information sets with medium vulnerability rather than in areas of high vulnerability. Why?

Because in the areas of the highest vulnerability, the cost to protect the system would exceed the benefit to the organization. Given the example from above, securing the information with the credit card information makes the most sense because this is the most likely area where a breach may occur and installing a SSL certificate would suffice to secure the information rather than perhaps a finger print identification system which could be more costly.

It is also important to be able to assess and to mitigate risk whenever possible within the organization. Therefore, it is important to identify the areas of the system with the greatest probability of vulnerability and the *Accumulative Probability of Insecurity* (API) algorithm can be used to identify these areas in the system. This algorithm, based on threat flow models, help better determine the flow of attacks, most likely to occur, within an information system (Wang, Chen, Stirpe, & Hong, 2011). However, the complexity of all data centers in different organizations cannot be fully modeled.

Wang, Chen, Stirpe and Hong (2011) used the API and the *Optimal Security Investment* (OSI) algorithm, which is risk neutral based on the work of Gordon and Loeb, to calculate the information security investment for data centers based on a single threat to the system. The work on the data centers supports Gordon and Loeb's analysis that in areas where there are the highest threats to a security breach, seems like the less than optimal area of focusing when making the security investment. In the high vulnerability areas there are too many alternatives to how the breach can occur and therefore focusing on areas of medium vulnerability are recommended.

In addition to technological enhancements, organizations need to establish policies and laws that protect the individual citizens when business is conducted. Some examples of industries are regulated by the federal government in the United States are the healthcare sector, the financial sector, and educational sector. Each of these sectors and many others have specific laws and regulations that govern how consumer information is maintained, verified and shared.

BACKGROUND

Organizations that identify security and privacy in the organizational goals as part of the core values for the firm, will help to alleviate issues of human error in releasing secure information to the wrong parties which is one of the major risks organizations face. Employees are motivated to follow that culture that is identified by management as being appropriate for the firm. Therefore when leadership communicates the security goals and the risk associated with security breaches, then the IT managers have the opportunity to establish policies on how the employees and technology work together to control the specific security concerns for the organization. This process also creates trust that leads to coordination and cooperation by all employees within the organization around the security practices (Koskosas, Kakoulidis, & Siomos, 2011). When transparency exists surrounding the privacy and security process and the goals are clearly defined, this mindset helps protect the organization and the security of the organization's data.

When organizations fail to inform employees about security goals, some may feel that privacy and security are not a priority for the firm. In this case, the employee may develop apathy about the protection of data (Thomson, & van Niekerk, 2012). As explained in previous sections, a culture that establishes goals that include a security mantra are more effective in establishing pro-social behavior. If the culture does not include the organization's security goals, then the organization may be forced to manage fixes based on individual occurrences.

It is inefficient to manage individual instances of privacy and security breaches as the main method of security compliance. Overtime this process of individual case management will prove to be ineffective not only because the process will not be transformative for the organization, but because the data will most likely be unprotected by the majority of the employees because the information will be lacking for everyone. One person might be responsible for the breach but it will be the organization that is generally at fault for not making the environment conducive to security maintenance.

The situational aspects of security breaches can be lessened by providing information and by establishing a culture that supports security goals within the organization. However, there will be instances when security breaches need to be reviewed on a case-by-case basis. When these instances occur, the IT management should