A critical issue in loss prevention in security term paper

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

Loss prevention stands as a strong issue in studies pertaining to security maintenance. It is important to prevent problems involving the disappearance of important articles ranging from computer data to cargo contents to ensure proper transportation of private information. As an added insurance of securing exchange of articles in data and cargo formats, loss prevention is a crucial arena that requires constant improvements. Yet, to help identify the needed improvements, it is important to focus on a particular issue on loss prevention – the involvement of well-meaning factors as intrusions.

This study aims to identify instances in which well-meaning factors in security maintenance thrive. As previously stated in a frequent fashion, two

key areas of transportation security pertaining to well-meaning factors characterize the flow of this study – data and cargo. Data transportation raises strong issues on security, since several computer users from around the world entrust their private details to data-related mechanisms accessible via the Internet. Cargo transportation stands as an essential component of the globalized market, given that trading activities across all nations continue to grow in prominence. Verily, both data and cargo transportation face risks pertaining to loss, thus requiring intensive perusal of controversies on such matters for the sake of producing potential resolutions in the future.

Issues in Data Security

Millions of users transport data through the Internet every day, most of which consisting of private information essential for accessing personal profiles and transactions. Yet, the channels that hold data may become the subject of interference of well-meaning factors that may end up exposing confidential information to the public in several ways. Two concepts underline this concern – cloud computing issues and the well-meaning insider (Munir and Palaniappan, 2012; Wall, 2011).

Cloud Computing Issues

Access to data on the Internet has become more convenient due to the introduction of cloud computing. Through cloud computing, data has become more accessible in different gadgets through one source – the so-called “ cloud” server. Users only need to have access to the Internet from their preferred device so that they could view and download their files from the cloud computing services they are using. There is no restriction to the kinds

of files allowable for storage in the cloud server, as compatibility issues reside on the part of gadgets in use. However, convenience in access through cloud computing has found notable compromises found on the server side. Ultimately, information technology specialists have great control over cloud servers, making those susceptible to human error in several ways. Deliberate means cause some security breaches in cloud servers, while some happen accidentally. Unintentional lapses happen mostly due to shortcomings related to maintenance efforts on cloud servers, which could eventually pave way to possible breaches of privacy through exposure of confidential data to the public. Data security, in that sense, thus have problems in terms of cloud computing. Current infrastructures of cloud computing services have yet to incorporate more solid measures on how to eliminate potential lapses in maintaining cloud servers. The imminent danger of wider accessibility provided by cloud computing could take the problem of unauthorized private data exposure to a higher degree (Munir and Palaniappan, 2012).

Well-Meaning Insider

Information technology specialists have the primary objective of keeping data security mechanisms in place, whether within a small workplace or a large corporate setup that serves clients. While some information technology specialists may fail on that objective, it does not mean that their failure automatically roots from malicious intentions. In that case, an insider that fails to protect data security either could have malicious intents or acted in a well-meaning nature (Wall, 2013).

A well-meaning insider in a group of information technology specialists working for an organization does not have malicious intent in his failure to observe his duty to protect the integrity of the servers. Negligence and unawareness on dangerous consequences usually cause the actions of a well-meaning insider. There are five categories classifying well-meaning insiders according to Wall (2013): the underminers, overly-ambitious employees, socially engineered employees, data leakers and data spillers. Underminers. Information technology specialists called “ underminers” prefer to take on procedures they think would make their work easier without minding the harmful consequences on security. An underminer, for instance, use easy codes for passwords and neglect the use of additional security layers due to the tedious nature of the work involved (Wall, 2013). Overly-Ambitious Employees. Organizational goals serve as the basis of many information technology specialists, depending on the nature of their organization. However, some information technology specialists think they have better ideas other than those stated in the organizational goals they are bound to observe, making them “ overly-ambitious employees”. Failure to observe organizational goals usually lead to security risks (Wall, 2013). Socially-Engineered Employees. Not all information technology specialists end up in well-paying positions. Low compensation, in that sense, leads to vulnerability to outsiders willing to pay large sums of money in exchange of the malicious intent to reveal confidential data. Socially-engineered employees usually involve information technology specialists receiving low compensation who give in to bribes from malicious outsiders (Wall, 2013) Data Leakers. Information technology specialists hold access to confidential

information. Yet, some may have ethical or self-centered purposes for revealing data that should not tread on the public realm. Thus, “ data leakers” pertain to information technology specialists driven by public or self-interests who go against their duties through revealing confidential information to effective communication channels, particularly social media (Wall, 2013)

Data Spillers. Any information technology specialist becomes a data spiller if he ends up handling information carelessly. Losing company laptops, failing to delete data on confidential hard disks and leaving information on unsecured public channels are some lapses associated with data spillers (Wall, 2013).

Issues in Cargo Security

Loss prevention greatly treads on tangible instances, particularly in terms of cargo transportation. Given the contemporary globalized capitalist setting, cargo transportation continues as a flourishing activity between nations involved in the global market trade. At the same time, the trend of migration also necessitates activities that involve bringing tangible articles by air, land or sea from one place to another. However, the problem with cargo transportation lies within the fact that transportation channels do not have the guarantee of security. In other words, many instances could affect cargo transportation due to the growing complexity of its nature (Skorna and Fleisch, 2012).

Global distribution of cargo does not just go through a one-step process that enables transportation from one place to another. Each process in goods

distribution has meticulous steps ensuring two things: that the superb quality of cargo will remain and transportation delays would not occur. However, the present problem in that case lies on the transparency of the conditions surrounding cargo distribution. Clearly, there is not just one organization involved in any cargo transportation process, since such varies on arrival and destination places. Lack of efficient communication between cargo transportation organizations tends to harbor lack of transparency. In return, actors in cargo transportation tend to take the process for granted, to the peril of those supposed to benefit from cargo transportation. Such could result to damage or loss of articles in transportation. For cases of loss, cargo might end up in the hands of unauthorized markets running against domestic and international commercial laws or malicious figures that would benefit from any confidential information involved (Skorna and Fleisch, 2012).

Conclusion

Data and cargo security are two compelling issues in loss prevention, given the globalized nature of the status quo. For globalization to work efficiently, actors should work on preventing losses in terms of data and cargo. Confidential information and personal or commercial articles should fall under the protection of more efficient processes to enable protection against perils on loss such as exposure of confidential information and displacement of cargo to other areas. While this study does not purport to provide concrete proposals, the literature used aims to encourage future recommendatory studies on the matter.

References

Munir, K., and Palaniappan, K (2012). Security threats/attacks present in cloud environment. IJCSNS International Journal of Computer Science and Network Security, 12 (12), 107-114

Skorna, A., and Fleisch, E. (2012). Loss prevention in transportation to ensure product quality: Insights from the cargo insurance sector. In J. Frick and B. Laugen. (Eds.), Advances in production management systems. Value networks: Innovation, technologies, and management (148-156). Germany: Springer Berlin Heidelberg.

Wall, D. (2013). Enemies within: Redefining the insider threat in organizational security policy. Security Journal, 26, 107-124.

.