

Ethics, Compliance Auditing, And Emerging Issues In Cyber Crime

Posted on September 16, 2018

Introduction

Innovation is the way in which humans create unique ideas to solve problems in society. Innovation is linked to technology, which has a major impact on society's way of life. Therefore, organizations are in a state of continual innovation or are able to take the risk of staying in the marketplace with their competitors who are keen on producing products and services innovatively. Generally, innovation is very significant for the progress of both companies and society at large. Hence, any innovation in technology, science, and other areas helps in solving the problems in society. However, new ideas and technologies present risks to the organization and the surrounding society. For instance, the proliferation of computers presents advantages and options to the average household and organization. Despite the advantages and the options brought by the technological innovation of computers, the innovation comes with risks, such as cybercrime, which has become a global risk.

Therefore, this paper will analyze cyber crimes as a technological global risk. First, the countries associated with the risk will be identified, and the effects of the risk on all the countries identified will be carried out. The role of ethical decision-making will be analyzed in an organization in regard to cyber crimes and the impact of business ethics on the stakeholders of the company. Moreover, this paper will analyze the importance of the creation of an ethics program in a business and why it is necessary to conduct training as well as engage in compliance auditing. Recommendations for a training plan for social responsibility and ethical considerations in relation to the major risk areas and the selected countries will be made. Finally, the description of the manner in which the compliance auditing will be carried out will be presented.

Cyber Crime As A Global Risk

Cybercrime is among the emerging risks globally due to the advancement in technology through innovations. The affordability and the rise in the use of computers have resulted in a rise in cybercrime globally. Another important technological advancement that goes hand in hand with computers is the internet. This is a global system made up of an interconnection of computer networks such as government networks and public, private, business, and academic networks, which are linked together for easier access to information. In fact, after the invention of computers, they were mainly used to connect academic and military networks. However, the advancement in computers and networking has led to the interconnection of every organization globally. As a result,

organizations have experienced both advantages and adverse effects in relation to ethical issues regarding the use of computers and the Internet. This is because the internet and the computer system have provided an opportunity for different cyber crimes to be performed by individuals and organizations (Grabosky, 2000).

Cybercrime is a crime committed via a computer and/or a network. Thus, a computer can be used to commit a cybercrime or can be the target of a crime. Cyber crimes are technological crimes committed by an individual or a group of individuals to cause mental or physical harm to other people. Some crimes can cause problems for an entire nation or several countries globally by threatening the nation's security. Some of the cyber crimes that can be perpetuated through the internet are hacking, infringement of copyright, financial theft, malware, denial of service attack, pornographic, extortion, computer fraud, altering or stealing data, espionage, identity theft, cyberbullying, hate crimes, cyberstalking and drug trafficking.

An extensive type of cybercrime is cyber warfare, which is carried out by super nations towards each other. Countries are now in a rush to develop abilities to carry out cyber wars or to protect themselves against any attacks. At the present moment, cyber warfare has not been controlled by any treaty or agreement between nations; it is controlled by the economic interdependence created by modern society. The nations such as the United States are more at risk from the cyber-attacks than the less developed nations. The less developed nations have weaker militaries, and a cyber attack on the developed nations would act as a weapon for attacking the developed nations. The areas in the superpower nations with inadequate protection are prone to cyber-attacks by the less advanced nations. Cyber attacks are less costly as compared to conventional weaponry which takes up too many resources as well as finances. Thus, cyber-attacks are a better option than modern weaponry, and they reduce the chances of being caught and eliminate the ramifications (Goud, n.d).

Countries Closely Associated With The Cyber Crime Risk

The preparedness for cyber attacks by countries is a significant issue. However, there are nations that are best prepared for the attacks while others are not. Some of those who are best prepared include Canada, the United States, Norway, Brazil, Estonia, Germany, Oman, Malaysia, and New Zealand. At the same time, the countries that could be most at risk of cyber-attacks include Belgium, Samoa, the Dominican Republic, China, Hong Kong, Afghanistan, South Africa, Tajikistan, and Australia (Goud, n.d). Therefore, the cyber superpowers have been able to respond to a number of attacks in the near future by threatening their cyber capabilities. However, the costs of cybercrime have affected most of these nations, making them lose billions to the crime, which can't be traced to an individual or a country (Breene, 2016).

A representation of the average cost in Million of US\$ of cybercrime in some countries as of August 2015

Role Of Ethical Decision Making In Relation To The Cyber Crimes

In regard to the statistics provided above, the US is currently leading in the highest costs of cyber attacks, while Russia has the lowest costs. Most organizations now belong to the global industry, and the greatest concern of management is the development and implementation of an ethical plan that would be helpful in dealing with the challenges of cyber attacks. Hence, the role of ethical decision-making in an organization must be implicit for ethical planning to be successful.

Ethical Issues In An Organization

An organization comes across many ethical issues in its operations. The ethical issues affect the company in one way or another. Companies should be very careful when dealing with other issues, such as financial growth and sales. They forget to deal with ethical issues in the organization (De Colle & Werhane, 2008). Some of the ethical issues that a company has to deal with in their operations include accounting fraud, bullying, corruption, conflict of interest, discrimination, fraud labor standards, violation of the rights to privacy, and many more crimes, including cyber crimes such as hacking to get the organizations information (Gonzalez-Pedron, 2015). Therefore, it is not easy for an organization to make ethical decisions. The decisions must be in accordance with the company's code of ethics and the ethical principles of each individual in the company. The ethical decision to be made in an organization should be based on moral reasoning, which would be helpful in presenting the best moral option to take in times of risk, such as cyberattacks.

Moral reasoning simply means that the people involved in decision-making are considerate of the right or wrong aspects of a decision. According to Archie et al.. (2014), moral character has a significant role in the determination of moral responsibility. Moreover, virtue ethics takes into account the moral character of an individual while making good decisions for an organization. A virtuous person has characteristics such as honesty, fairness, humility, and trustworthiness, which are important in identifying the ethical or right action to take in a situation (de Colle & Werhane, 2008).

Ethical decision-making requires the use of reasoning and logic in any situation. Therefore, the individual must be aware of the intentions of their actions, as well as the consequences and effects of the actions on others in the organization. For instance, an individual might use the computer in the office in the wrong way so as to prevent hurting other people or to prevent someone from harming others. These actions can also be for selfish reasons or for the good of the company against their competitors. Another example is stealing the rights and procedures of doing something from a rival company through the use of computer software or infecting their computers with a virus to beat rivals. In such circumstances, moral reasoning is very important in order to have the judgment of what is right and what is wrong. Moral reasoning requires the organization or the individual to analyze the situation and consider all factors that will affect a decision (De Colle & Werhane, 2008). Thus, an

individual or an organization will be better able to decide on pursuing what they deem right, as well as the flexibility and strength to uphold their moral principles (Gonzalez-Padron, 2015).

Importance Of Ethics On Stakeholders

A stakeholder is a party that is likely to be affected by an organization's decision. The stakeholders of a company can be employees, suppliers, creditors, customers, competitors, the government, and the surrounding community. Thus, any decision made by the company affects these stakeholders in one way or the other (De Colle & Werhane, 2008). An example is that of a company that was making a lot of losses due to competition and decided to use technology to control its production and service delivery. The decision was made in consideration of the stakes they had while staying put or making the changes. Not changing the system would disadvantage investors in terms of losses, and changing it would render most of the workforce jobless. The suppliers of some of their products would lose income opportunities. The surrounding community would lose opportunities that came with the company, such as job opportunities, or will have to deal with the challenges of technology, such as air and water pollution. Moreover, the change will impact the government in terms of revenues, and they will have to change regulations to deal with technology. However, the company has to decide which decision is most appropriate for all the stakeholders in such circumstances.

The code of ethics in a company is the guiding principle that helps in deciding what is right and what is wrong. The employees, suppliers, customers, and other stakeholders, such as the surrounding community of the company, are required to abide by these codes of ethics of the organization. In a company, there exist many decisions to be made, problems needing solutions, and other issues that need to be reviewed. Therefore, business ethics is very significant in the development of employee as well as customer loyalty. Loyalty to the company will avoid bad decision-making by the stakeholders of the company and, in the end, avoid a bad reputation for the company (Archie et al., 2014).

Importance Of Ethics Program, Training, And Compliance Audit

The time and resources spent on training workers will be a waste if those workers are lost through poor ethics. Thus, the workers, being the greatest assets of a company, should be ethical as they deal with the other stakeholders of the company, especially the customers. Hence, training employees on good ethics would help in the decision-making and the loyalty of both the employees and the customers of the organization. Training and retaining good employees in the company would build a good reputation for themselves, which will, in the end, attract investment opportunities (Boundless, 2015).

For an effective ethics program, some elements must be present. For instance, the ethics program must have a structure consisting of an ethics officer, along with the board of directors, to oversee the

program and maintain a reporting relationship within the program. Next, corporate standards must be established through the establishment of a code of conduct and consideration of the global impact of its implementation. The organization must then develop and execute a training plan. This should be followed by the creation of investigative procedures, which include ethical guidance, investigative processes, and a reporting mechanism. Finally, the organization must assess the effectiveness of the program through the assessment of ethical performance. This can be assessed by putting a metric system in place, which would help quantify the impact of the program on employees' behavior and limit misconduct (Gonzalez-Padron, 2015).

Training Plan

Goals And Objectives Of The Training Program

An ethics training program is important as it allows the organization to communicate with suppliers, employees, investors, and customers some important information. A successful training program has the capability of strengthening the relationships of stakeholders and the reputation of the company. An official ethics training program will avoid misunderstandings and confusion among the stakeholders in the organization as the same information is shared between them. Therefore, the objective of the training is to eliminate or reduce the conduct viewed as disorderly in the organization (Boundless, 2015).

Learning Methods

The training will involve placing the employees in various ethical scenarios through role-playing and question-and-answer sessions. They will then be provided with ethics handbooks for them to review and search for ethical issues and raise questions concerning the ethical issues found. The training will also present the way forward, what actions to take, or whom to notify or report in case the employees have any ethical concerns (Boundless, 2015).

Compliance Auditing

According to Julisch et al. (2005), a company needs to carry out a system and application audit to verify the appropriateness and effectiveness of the application and the systems. Thus, compliance should be measured by checking if there is adequate control, which will ensure timely, valid, and reliable processing of the secure input and output at all levels of the organization. An audit of the IT system in a company can be done through a technological innovation audit, which develops a risk profile for new and existing projects. Moreover, a comparison audit will be carried out to compare the company's innovative capabilities to those of its competitors. Lastly, the audit of the technological position will review the current technologies in the company and those that are needed (Goodman &

Lawless, 2010).

The first step will be planning for the audit, then analyzing and evaluating the results, followed by the testing and the evaluation of the results. Subsequently, reporting of the results will be performed, and finally, the follow-up of the report will be done to ensure compliance with the IT requirements (Robert, 2005). Consequently, the company will be in compliance with the laws and regulations of the industry in which they are operating. In addition, compliance is important for the organization's reputation and for saving the company from legal fees and other losses.

Conclusion

Cybercrime is among the emerging risks globally due to the advancement in technology through innovations. Some of those countries that are best prepared include Canada, the United States, Norway, Brazil, Estonia, Germany, Oman, Malaysia, and New Zealand. Those most at risk for cyber attacks include Belgium, Samoa, the Dominican Republic, China, Hong Kong, Afghanistan, South Africa, Tajikistan, and Australia. In this regard, the role of ethical decision-making is the development and implementation of an ethical plan that would be helpful in dealing with the challenges of cyber attacks. Minimization of the cyber attacks would be beneficial to the stakeholders of the company as the risk of doing business will be eliminated. Thus, an effective, ethical program will enhance decision-making and the loyalty of both the employees and the customers of the organization. Training and retaining good employees in the company would build a good reputation for themselves, which will, in the end, attract investment opportunities. A compliance audit will evaluate the appropriateness and effectiveness of the application and the systems in place for success in the industry.

References

- Archie, B. et al., (2014). Corporate Responsibility: The American Experience. *Administrative Science Quarterly*, 59(3)
- Boundless. (2015, June 27). Ethics Training: Boundless Management. Retrieved from <https://www.boundless.com/management/textbooks/boundless-management-textbook/ethics-in-business-13/ethics-an-overview-95/ethics-training-447-1833/>
- Breene, K. (2016, May 04). World Economic Forum. Who are the Cyberwar Superpowers? Retrieved from <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/>
- De Colle, S. Werhane, P.H. (2008). Moral Motivation Across Ethical Theories: What Can We Learn for Designing Corporate Ethics Programs? *Journal of Business Ethics*, 81(4), 751–764.
- Goodman, R.A. & Lawless, M.W. (1994). *Technology and Strategy: Conceptual Models and Diagnostics*. Oxford University Press: Oxford.

Grabosky, P. (2000). Computer Crime: A criminological Overview. Australian Institute of Criminology. Retrieved from

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.4660&rep=rep1&type=pdf&embedded=true>

Goud, N. (n.d). List of Countries which are most vulnerable to Cyber Attacks. Retrieved from

<https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/>

Gonzalez-Padron, T. (2015). Business ethics and social responsibility for managers. Retrieved from <https://content.ashford.edu/>

Julisch, K. et al., (2011). Compliance by Design – Bridging the Chasm between Auditors and IT Architects. *Computers & Security, Elsevier, 30* (6-7).

Robert, E.D. (2005). *IT Auditing: An Adaptive Process*. Mission Viejo: Pleier Corporation.