**Initial Post - Institutional Affiliation**

With the continued use of information systems in organizations, it has become critical for them to pay attention to cybersecurity. According to IBM (n.d.), cybersecurity describes the efforts made to protect the sensitive information and crucial systems of organizations from digital attacks. The attacks rely mostly on the Internet that connects people across the world. As a result, cybersecurity has become a global issue affecting all types of businesses from SMEs to large multinational corporations. Firms have found it increasingly important to protect critical systems and sensitive data putting greater emphasis on cybersecurity. The following discussion provides an analysis of the importance for companies to invest in cybersecurity.

One of the most important reasons companies must invest in cybersecurity is due to the increasing adoption of technology. Modern enterprises use technology for a variety of purposes such as collecting and storing data. Bach, Celjo & Zoroja (2016) demonstrate the critical role technology plays in business intelligence by using the information they gather and store. Enterprises also utilize different devices in this data collection and analysis process. As a result, companies are facing a significant threat from the potential of cybercriminals using these technologies to facilitate attacks. For instance, cybercriminals can use networks and computers to install malicious programs to gather information or conduct surveillance on organizations. In this way, they conduct fraudulent activities such as stealing money from bank accounts or retrieving people’s personal information. Thus, organizations must invest in cybersecurity to prevent these problems from occurring.

Investment in cybersecurity is vital to boost the trust and confidence of clients or customers. The growth of e-commerce has seen companies shifting to the Internet to sell their products and services (Gray & Zappala, 2012). Companies collect considerable amounts of information related to their customers to facilitate the process of selling goods and services. For instance, they gather names and bank account details to process payments. They also gather addresses to deliver goods to customers. Cybercriminals are constantly seeking such information for different reasons, for instance, fraud. Thus, companies must protect the information to maintain the trust and confidence of customers. Abraham, Chatterjee & Sims (2019) stress the need to protect people's information to secure the reputation of organizations. Therefore, investing in cybersecurity is crucial to protect the information organizations have stored, uphold the trust and confidence of customers, and maintain the reputation of an enterprise.

Finally, companies must invest in cybersecurity to adhere to regulatory requirements. The growth of the Internet and its use for different purposes has resulted in companies holding significant amounts of information. As a result, governments have developed different laws to secure this information. For example, the HIPAA regulation requires health facilities to implement measures to secure patients' health records (Benitez & Malin, 2010). Hospitals that fail to observe this requirement are subject to lawsuits and the potential of being forced to pay fines. They can avoid such issues by investing in cybersecurity to reduce the potential of cybercriminals accessing systems and devices to gather patients’ data. Thus, organizations must invest in cybersecurity to avoid lawsuits and avoid the possibility of fines.

Cybersecurity is supposed to help companies to protect their sensitive information and critical systems. Without it, enterprises are at significant risk of becoming the targets of cybercriminals who use the information and systems for fraud. Furthermore, the failure to invest in cybersecurity jeopardizes the reputation of enterprises by reducing the trust and confidence of customers. Investing in cybersecurity is also crucial to enable firms to adhere to laws. Therefore, it is becoming increasingly important for companies to invest in cybersecurity. It will help to protect information and systems from the threat of cybercriminals who are increasingly using technology for fraudulent activities.

References

Abraham, C., Chatterjee, D. & Sims, R. (2019). Muddling through cybersecurity: Insights from the U.S. health industry. *Business Horizons, 62*(4), 539-548.

Bach, M., Celjo, A. & Zoroja, J. (2016). Technology acceptance model for business intelligence systems: Preliminary research. *Procedia Computer Science, 100*, 995-1001.

Benitez, K. & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association, 17*(2), 169-177.

Gray, C. & Zappala, S. (2012). *Impact of e-commerce on consumers and small firms*. Burlington, VT: Ashgate Publishing Company.

IBM. (n.d.). *What is cybersecurity?* Retrieved from https://www.ibm.com/topics/cybersecurity#:~:text=Cybersecurity%20is%20the%20practice%20of,sensitive%20information%20from%20digital%20attacks.&text=Security%20system%20complexity%2C%20created%20by,expertise%2C%20can%20amplify%20these%20costs.