Executive Summary

The purpose of this paper is to identify the need of businesses to recognize the risk associated with data collection and data breaches for both their customers and employees. Additionally, it is the responsibility of businesses to ensure their employees are properly trained to handle collected personal data and to react in the event of a data breach. This stance is supported by the concept of corporate social responsibility, which is a business model that allows businesses to be held accountable. Employees who are required to use certain communication technologies at work should be allowed the same protections regarding cybersecurity as the customers who use their services.

Communication technologies have become the standard forms of communication in businesses, especially as more companies go digital with a growing portion of employees working remotely. When using communication methods online, however, the ethics surrounding user safety and the security of personal data are called into question. Employees regularly send and receive sensitive information about projects, themselves, customers, and even other employees via the internet using tools such as e-mail, online databases, and online client portals. There is no single organization or type of business that will be investigated, as many modern businesses rely heavily on communication technology. It is up to the business to create a culture of digital security and encouraging good practices.

It was found that the best way for businesses to combat data breaches and other cyber-attacks is to promote a corporate culture that embraces the vales of cybersecurity. This can be done by ensuring adequate resources are invested into cybersecurity efforts and providing comprehensive cybersecurity training to employees. Through this training program, employees would be equipped to recognize threats to personal data or cybersecurity and understand what

they should do in the event of a cyber-attack or data breach. The skill level of each employee should be assessed to identify areas for improvement. The cybersecurity knowledge of each employee should also be tested periodically to further gauge their skills.

Abstract

The purpose of this paper is to identify key areas around corporate cybersecurity for both employees and clients. As communication technology has developed and expanded, the threat of data breaches and other cybercrimes has also advanced. Using published sources, including peer reviewed journal articles, published frameworks, and web-based articles, information regarding cybersecurity and corporate social responsibility has been gathered and analyzed to determine the best way for businesses to ensure the safety and security of their employees and customers alike. Businesses are able to achieve this through adopting a corporate culture that values cybersecurity and providing an employee training program to recognize threats and identify the proper response in the event of a cyber-attack.

Key terms: cybersecurity, data breach, corporate social responsibility, communication technology

Introduction

Over the last few years, there has been rapid development and advancement in communication technologies. These technologies have become the standard forms of communication in businesses, especially as we have seen more companies go digital with a growing portion of employees working remotely. When using communication methods online, however, the ethics surrounding user safety and the security of their data are called into question. Cybercrimes in the US alone cost companies an average of $15.4 million a year with an estimated 160 cyberattacks per week (WSU Online, 2020). Whether property was stolen, trade secrets were exposed, or customer data leaked, data breaches cost organizations more than just monetary losses. Data breaches often tarnish the reputation of the organization that experienced the cybercrime.

This paper will explore the ethical violations that are associated with data sharing via communication technologies in a business setting. Examples of such violations include the misuse of personal information, lack of oversight or regulation, and lack of accountability or disclosures about how collected data will be used. Additionally, it will look at the responsibility organizations have to protect employees and their data while performing their daily work obligations. Any organization that deals with the collection or storage of personal information of customers, employees, or both via communication technology has a responsibility to ensure the safety of its users and the security of their data.

Corporate social responsibility is a business model that allows a company to be socially accountable to itself, its stakeholders, and the public. It is based on the expectation that firms, corporations, industries, companies, and businesses do more than just make economic contributions to society. The way companies adopt policies, manage information security, and respond to threats can often shape normal business functions and regular daily life. While corporate social responsibility is a voluntary commitment, it pushes businesses to support company values while promoting positive social changes (Tsiakis, 2009). As a part of corporate social responsibility, businesses must exercise caution when collecting and using data of both their customers and their employees. This includes businesses of all types, such a doctor's office e-mailing a patient file to another office, an accounting team that stores payroll information in an online data base, or a human resources (HR) department sharing files about a particular incident.

This paper will include a detailed background information section to understand the scope and context of the issue at hand, provide supporting evidence from published literature to further the context, and propose possible solutions to the problem. The background information will provide context as to what constitutes a data breach and why businesses should be responsible for data protection. The supporting evidence is drawn from peer reviewed journal articles and manuscripts related to the subject matter. Lastly, this paper will provide realistic solutions regarding cybersecurity.

Background and Problem

As businesses continue to develop and expand, especially as more companies go digital with a growing portion of employees working remotely, they increasingly rely on communication technologies to communicate with employees, clients, and other stakeholders. When using communication methods online, however, the ethics surrounding user safety and the security of their data are called into question. The first issue is what data is being collected and how it will be used. While individuals are willingly sharing personal data, they may not fully understand how their data will be used and shared or be fully educated of the associated risk (Beardsley et al., 2019). Businesses need to disclose this information to clients and employees.

The main information and communication technology used at work is still by and large e-mail and phone. Other popular technologies used in the workplace are online chat, video conferencing, shared calendars, and collaborative documents. While these technologies are useful in providing an efficient way for businesses to communicate internally to employees or externally to clients, they are also sharing sensitive information. This brings up another issue, which is that while there are regulations to control consumer information misuse, these regulations often protect data after it has been collected. This can be referred to as an “information externality” meaning the use and misuse of information often effects consumers in ways that are not necessarily revealed to them before the data is collected (Cassidy & Chae, 2006). Data can be better protected using property and liability regulations in addition to privacy regulations and holding businesses accountable for how data is handled.

Data breaches, which occur when information is taken or stolen without the knowledge or authorization of the owner, have been identified as one of the biggest issues for businesses (Ayyagari, 2012). Organizations heavily rely on information systems to interact with stakeholders and perform general business operations. Businesses could face fines, legal action, expenditure, and loss of customer trust should a data breach occur. A data breach is constituted by the unauthorized access, destruction or alteration of personal data. This generally occurs when information is taken from a system without the knowledge or authorization of the system owner. While we generally associate cyber-attacks with anonymous hackers online, data breaches can also be caused by a “human factor.” An employee could unintentionally leak information though password sharing, phishing emails, and mishandled hard copies.

Proposed Solution

Digital security risk management involves general skills, responsibility and liability, human rights and fundamental values, and co-operation from stakeholders to be effective. Operational principles are focused on the implementation of digital security risk management in organizations. Security measures should be appropriate to and commensurate with the scale of the risk. Digital security is dynamic; it has constantly evolving threats and vulnerabilities (OECD, 2022). To implement an effective digital security strategy, sufficient resources need to be allocated. Each individual business needs to create a culture of digital security and encouraging good practices to prevent security risks.

Regarding privacy online, a lack of experiences using online services that collect and use consumer data, lack of user-friendly privacy controls, and the complexity of privacy notices contribute to users' vulnerable while online. In a work setting, it is the responsibility of employers to ensure adequate training of employees with online services they are required to use so that employees feel secure and comfortable. Employees need this understanding to ensure that they are properly handling the data of clients, as well as their own personal data. Consumers often have concerns when giving personal data to businesses because they are no longer in control of it, which often leads to concerns about the safety of their information and feelings of vulnerability data leaks or unauthorized access (Chen et al., 2023).

The main solution is to create a culture of corporate social responsibility and provide cybersecurity awareness training. This type of training allows employees to understand the importance of cybersecurity and identify potential threats. Additionally, this training will teach employees what to do should an attack take place. There are several key items to address with this training. Employees should be informed of how to make strong and unique passwords. Employees should know how to identify a phishing attack, which is typically a fraudulent email impersonating a known sender in an attempt to gain passwords or other personal information. Employees should only download company approved software on work devices, as downloading unauthorized and unlicensed applications may introduce malware. Employees should also be taught to simply store computers and other work devices in a secure location when not in use.

Employee awareness is beneficial as it minimizes risks and enables employees to protect themselves and the business. Digital security risk management involves general skill, responsibility and liability, human rights and fundamental values, and co-operation from stakeholders to be effective (OECD, 2022). Businesses are able to test the effectiveness of their cybersecurity training in multiple ways. First, managers should identify skill gaps, which are deficiencies caused by lack of skills or knowledge, and their root causes to help employees improve their skills (Purohit, 2022). Second, employees should have their knowledge of cybersecurity issues tested though comprehension quizzes. Additionally, businesses can use cyberattack simulation software to gauge the skills of employees. Testing employees' cybersecurity skills is a great way for businesses to gauge their efforts on cybersecurity. It is the responsibility of businesses to create a culture of digital security by providing the training and resources necessary for cybersecurity.

Conclusion

It is the responsibility of businesses to educate its employees to recognize cybersecurity threats and understand how to respond accordingly. Cybersecurity training is part of a business's corporate social responsibility to protect its employees and customers. Creating a corporate culture that values cybersecurity will empower employees to protect both the clients' data as well as their own. Any organization that deals with the collection or storage of personal information of customers, employees, or both via communication technology has a responsibility to ensure the safety of its users and the security of their data.

References

Ayyagari. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, *8*(2), 33–56. https://doi.org/10.1080/15536548.2012.10845654

Beardsley, M., Santos, P., Hernández, L. D., & Michos, K. (2019). Ethics in educational technology research: Informing participants on data sharing risks. *British Journal of Educational Technology*, *50*(3), 1019–1034. https://doiorg.ezproxy.bellevue.edu/10.1111/bjet.12781

Cassidy, C. & Chae, B. (2006). Consumer information use and misuse in electronic business: An alternative to privacy regulation. *Information Systems Management*, *23*(3), 75–87. https://doi.org/10.1201/1078.10580530/46108.23.3.20060601/93709.8

Chen, S. J., Tran, K. T., Xia, Z. R., Waseem, D., Zhang, J. A., & Potdar, B. (2023). The double-edged effects of data privacy practices on customer responses. *International Journal of Information Management*, *69*. https://doi.org/10.1016/j.ijinfomgt.2022.102600

Chen, & Rea, A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control Techniques. *The Journal of Computer Information Systems*, *44*(4), 85–92. https://doi.org/10.1080/08874417.2004.11647599

D’Cruz, P., Du, S., Noronha, E., Parboteeah, K. P., Trittin-Ulbrich, H., & Whelan, G. (2022). Technology, megatrends and work: Thoughts on the future of business ethics. *Journal of Business Ethics*, *180*(3), 879–902. https://doi-org.ezproxy.bellevue.edu/10.1007/s10551-022-05240-9

Derbeck, D. W. (2017). Cybersecurity, Encryption, and Corporate Social Responsibility. *Georgetown Journal of International Affairs*, *18*(3), 105–111. https://doi.org/10.1353/gia.2017.0042

Findlay, P. & McKinlay, A. (2003). Surveillance, electronic communications technologies and regulation. *Industrial Relations Journal*, *34*(4), 305–318. https://doi.org/10.1111/1468-2338.00277

Giannoumis, G. (2016). Framing the universal design of information and communication technology: An interdisciplinary model for research and practice. *Studies in Health Technology and Informatics*, *229*, 492–505. https://doi.org/10.3233/978-1-61499-684-2-492

Maeng, D. M. & Nedovic-Budic, Z. (2004). Chicago and Seoul: a comparative study of the impact of information and communications technologies on urban land use and regulation. *The Journal of Urban Technology, 11*(2), 61–92. https://doi.org/10.1080/10630730412331297314

OCED. (2019, September). *Challenges to consumer policy in the digital age*. Tokushima; OECD.

OECD. (2022). *OECD policy framework on digital security*. Paris; OECD Publishing.

Purohit, A. (2022, April 27). *How to measure the effectiveness of your cyber security training*. DeltaNet. Retrieved February 18, 2023, from https://www.delta-net.com/blog/how-to-measure-the-effectiveness-of-your-cyber-security-training/

Sarabi, Naghizadeh, P., Liu, Y., & Liu, M. (2016). Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity (Oxford)*, *2*(1), 15–28. https://doi.org/10.1093/cybsec/tyw004

Stahl, B. C., Timmermans, J., & Flick, C. (2017). Ethics of emerging information and communication technologies: on the implementation of responsible research and innovation. *Science & Public Policy (SPP)*, *44*(3), 369–381. https://doi-org.ezproxy.bellevue.edu/10.1093/scipol/scw069

Tsiakis, T. (2009). Contribution of corporate social responsibility to information security management. *Information Security Technical Report*, *14*(4), 217–222. https://doi.org/10.1016/j.istr.2010.05.001

WSU Online. (2020, June 8). *Why every business leader should care about cybersecurity*. Retrieved January 22, 2023, from WSU Online MBA.