ETHICAL ISSUES RELATING TO CYBERSECURITY IN AUSTRALIAN SME

ACCG8086

STANLEY ONYEDIKA EPUNA
Student ID: 45731365

Stanley Onyedika Epuna

Introduction

Cybersecurity is an important factor in risk management, governance, and the compliance of organizational computing systems.

The SMEs in Australia are progressively becoming a hub where cyber-attackers infest.

In the economic development of a nation, A SME plays a vital role (Wong &Aspinwall, 2004) through their involvement in the Australian supply chain.

The SME is an attractive sector that brings attention to the governments. In Australia, the SME consist of 95% of businesses and 70% being employees. This gives an increase to Gross Domestic Product (GDP) of 57%.

In Australia there are three types of SMEs; the micro-ones which have less than 4 employees, small businesses with less than 20 employees, then the medium business with less than 100 employees (ABS, 2012).

In a recent survey conducted in Australia and New Zealand SMEs, there is a shortage of cybersecurity management resources especially in cybersecurity skills for workers and also timing and budget (Symantec 2009). National culture influences the organizational culture in a country and this ought to apply to SMEs. Links have been drawn between national culture and organizational culture (Van Muijen and Koopman 1994). National culture influences an individual in making a decision (Vitell, Nwachukwu and Barnes 1993). This culture should be applicable to SMEs which lack the skills to make a cybersecurity decision.

Research is indeed needed to enable efficient security culture on Australian SMEs. This research would assist in leveraging the gap and offer assistance to SMEs.

This report is a detailed summary of the cyber ethical issues faced in Australia SMEs, the analysis of the cyber ethical issues and challenges faced in the Australia SME, how COBIT could help support organization ethics process around Australia SMEs, and in what manner the ACM code of ethics would provide guidelines in dealing with cyber ethics around cybersecurity in Australia SMEs.

Ethical dilemma relating to cybersecurity in Australia SMEs and how emerging technology support the digital economy.

Due to the lack of ethical behaviors, SMEs can face several vulnerabilities. For instance, lack of competence can make any organization vulnerable to social engineering attacks like phishing. If an employee is not competent enough to differentiate a legitimate business email from a phishing email, it puts an organization at risk. Furthermore, the lack of concern for professional development and to update one’s knowledge can lead to a lack of awareness of current cyber threats such as DDoS (Distributed Denial of Service), Social Engineering, hacktivism, and Credential harvesting malware (ACSC, 2017). This means that employees do not practice due diligence, and this could lead to a multitude of financial and legal risks.

Emerging technologies that support the digital economy

Artificial Intelligence (AI)

Emerging technologies like Artificial Intelligence (AI) would be helpful in the digital economy concerning cybersecurity. AI would help to detect attacks and protect against data breaches. Cyber-attacks are targeted at computer networks of businesses, to address this difficulty, AI technique is introduced. With the help of AI techniques, cybersecurity practices are becoming useful. Attacks like multi-step and Zero-day are so common in networks, with machine learning these attacks could be tracked and removed. Machine learning can also be referred to as artificial intelligence. Machine learning has some features in it which helps in the detection of such attack, example includes sequence tracking, behavioral anomalies. Research has been done on both Machine Learning and statistical analysis to track attacks that are difficult to identify (Parrend et al., 2018).

Blockchain

Blockchain is a great advantage to the digital market in terms of security and also useful for financial purposes. Blockchain would be of great help to companies by securing computer devices, internet data, and services from cyber-attacks. The benefit of using blockchain is that it's impossible to crack the codes and cryptographical keys because blockchain combines the users and computer devices that are anonymous. Users and devices can be authenticated without providing important information with the use of blockchain technology in businesses. Blockchain takes full responsibility for shielding the information from attacks.
(Farion, 2019)
With the use of blockchain, companies could be able to defend themselves against computer hackers. Nowadays, financial institutions are now implementing blockchain technology into their system to reduce cyber fraud and risks. NASDAQ stock market has announced plans to include blockchain leger in their business to boost equity (Singh & Singh, 2016). Blockchain technology is rising to be the most powerful and reliable technology for cybersecurity.

Also, these digital technologies are not limited to just technology alone, they do add importance to the growth of the economy.

In businesses, these emerging technologies could potentially make work more efficient, help improve the needs of the customer.

Agriculture:

Agriculture is one of the most popular industries, being among the oldest. The farmers are gearing for more technologies to improve efficiency in the farmland. for example, high-tech equipment with GPS-guided tractors is being used in the Australian farming industry. This helps the farmers to be more productive, saving costs on chemicals. In the future, different technologies will join hands to assist the farmers in making decisions like fertilizing, planting, and crop watering. These different technologies include satellite technology and drones (Hall, 2017).

Manufacturing

Manufacturers in Australia are using modernized technologies for their processes and systems. Technology is becoming an essential part of doing business, through artificial intelligence, robotics to some advanced software/hardware like 3D print. This technology should help Australian manufacturers in the future. With the use of 3D printers, sensors implementation using IoT, and component design using cloud-based tools, this will help ensure the highest quality of service and demand.

Health

There as so many openings that emerging technologies implemented in the health sector (Shrapnel, n.d), (Australian Government, 2018). Software built by CSRIO to manage patient flows are being used in the hospitals now, remote areas are now gaining access to this product and services through digital channels. Robot equipment is used by healthcare professionals to improve surgery, radiographers are using this equipment to identify irregularities in their scans. There are now devices that monitor heart rate and blood pressure which helps in saving lives and improving health. Soon there would be further improvements in the health sector which would help in getting a solution for individual needs.

Anaslyze the particular cybersecurity ethical issues and challenges around Cybersecurity in Australia SMEs

Internal Attacks

This is a security threat in an organization that is being launched by an insider in the company. It normally involves a past employee or former employee who has a link to confidential information or has access to the computer network of the establishment and misuses it. (add reference). Their motivation sometimes steers up from malice. An employee could view gossip against him or her as social injustice and might want to retaliate to the opposition party by causing harm to the computer network. The pressure created around workplace competition could be because of social undermining behaviors (Lee et al., 2013). employees competing in the office is a result of social injustice (Lee et al., 2013). The insiders who have access to the information of the organization pose a huge risk to the employers. Employees who are facing financial issues could use office computers to commit fraud. Also, other employees who are motivated by revenge, that is the technical employees. Use their ability to damage the employer's network (Moore et al, 2008).

Wireless internet vulnerabilities

Small businesses like the ones in the hospital sector offer free wireless connections to the public to gain customers. Other companies which use Wireless local area networks could accidentally open their connection or maybe use vulnerable authentication. Problems involving wireless connection include a man in the middle attack, session hijacking, and Distributed Denial of Service attack (DDoS). Users that connect to this wireless network are at great danger of having their information stolen, making their account vulnerable to the outside world. This attack happens when the cookies which are meant to authenticate the user gets intercepted by the attacker so that he or she could impersonate the account of the user (Dacosta et al. 2011).

Another example is the man in the middle attack, in this report, traffic between a browser and the website gets intercepted by a middleman (an attacker) over an unencrypted connection. It happens when the browser thinks the proxy of the attacker is the genuine website thereby making the website validate the browser. The proxy then goes on to read the password and alter the transmitted data.

Compromised websites

Some web servers could be compromised to host illegal materials without the site owner knowing (Moore, Clayton & Anderson 2009). 92 Australians arrested in 2008 as a result of them accessing child porn images that were being hosted on some hacked sites (Hutchings, 2012). These compromised servers distribute software that is malicious to the visitors on the site, this is called a drive-by download. (Egele et al. 2009). A business that has a compromised website could harm the company in different ways. Reputation could be lost due to the lack of integrity of the website contents. These websites could be added to the blacklist search engine which will limit users from searching for business-related products and services because a warning will be shown to the users stating the website might be harmful. These websites could also be blocked by internet filters especially if those websites were hosting illicit content like child exploitation information (EFA 2010). If the business advertises or performs trading online, the penalties could be much. An average of 2% of small businesses that experienced cybersecurity attacks had issues with their web applications. It was a result of malicious attacks on the business website. Although the percentage is low compared to other cyber-attacks, this event might be higher if the business is not conscious that its website has been attacked.

Denial of service is another type of attack where the hacker floods the network by sending lots of traffic, making the website to become inaccessible to genuine users (Ianelli & Hackworth 2005). 4% of businesses that had a cyber-attack in 2006-2007 fell under a Dos attack. This attack is normally launched for extortion or revenge.

Lack of employee training/cybersecurity investment

In large enterprise organizations, awareness of cyber threat and risk is being critically studied which brings about investment in their IT infrastructures. But the SMEs still have little awareness about cyber threats and their risks (put reference).

In developed countries, SMEs have little knowledge of cybersecurity, control measures, and security technologies and they often forget to create a security policy or a risk assessment (Dojkovski et al, 2007). It could be that the SMEs lack knowledge or have fewer funds or also, lack awareness on security matters on how to train and educate employees (Furnell et al, 2005). According to reports being published, the SME owners do not support allocating budget or time to information security, therefore this impacts the degree of awareness of security and their technologies.

Employees who browse the internet on non-business-related tasks invites the presence of malicious attacks like malware, phishing attacks, trojan, spyware and even Distributed denial of service attack (DDoS). This reckless act on the employee could cause a huge problem to the organization.

Malware attacks carried out on the email system are a result of the employee not well trained on risks.

How COBIT 2019 can be useful in supporting organization cyber ethics processes around Australia SMEs

Kim and Scheller-Wolf (2019) contrasted the increasing productivity of the firm using technology and upholding the stakeholder’s interests. COBIT 2019 framework was developed to harmonize between ethics and technology disruption.

The Information System Audit and Control Association (2019) states that the objective of the Enterprise Governance of Information Technology (EGIT) system is to mollify stakeholder's needs by creating and protecting the organization's business values using Information Technology. COBIT 2019 framework has suitable objectives which enlighten how governance and management objectives add to the stakeholder needs. This can be expressed in three ways; Firstly, these goals started from the stakeholder's needs elevating to top-priority goals of the enterprise. This enterprise goal falls to align with the goals of the organization. Thirdly, the organization's goals now cascade to the governance and management objectives of the company (De et al, 2020).

The EGIT structure was made from interrelated components. individually and collectively connection improved the happenings of the EIGT. Evaluation of these components can only happen if the EGIT system has achieved the governance and management objectives. the governance components can be summed up into eight groups which are: organizational structure, processes, competence and people, flow and information items, culture, skills, ethics and behavior, policies, and procedures. Due to the nature of this report, the sole focus would be on policies, Culture and behavior, Ethics, framework principle, and it are components (ISACA, 2019).

SMEs that put emerging technologies like cybersecurity should state their frameworks, policies, and principles that ought to rule the affairs of these technologies to mirror the behavior, ethics, and culture of the organization. (De et al, 2020).

These behavioral ethics and culture components of the government aim to provide expected results on the organization's behavior, ethics, and culture. This will enhance the governance and management objective. Ethics means decisions we take or make. culture also influences the organization's ethics. So, it's fair to say ethics should belong to the category of enablers (ISACA, 2018).

The standards and principle in which businesses operates are as a result of organizational ethics. COBIT 2019 framework is made flexible and adaptive to business, this framework is developed by ISACA to integrate with other cybersecurity standards and frameworks such as IS0 27001 standards and NIST framework. COBIT also works with a professional code of ethics and code of conduct.

SMEs rolling out these cybersecurity technologies and framework should ensure that it aligns with Australia computer society code of conduct which includes honesty, the primacy of public interest, competence, professionalism.

The extent to which the ACM code of ethics provides guidelines in dealing with cyber ethics around cybersecurity in Australian SMEs.

Association for Computing Machinery (ACM) was founded in 1992. This code of ethics helps as an ethical guide for professionals in IT, students, influencers, and also individuals who are involved in computing to impact and influence lives positively. ACM Code of ethics helps in remediating and settling violations of rules and regulations in computing technology. This ethics contains responsibilities and principles which help in the best interest of the public. (ACM, 2018).

Brinkman et al (2016) said that the ACM ethical code emphasizes the IT professional's meaningful contributions to the relevant stakeholder's well-being who are at receiving end of the programs. All actions taken from the computing expertise should be an improvement to mankind, just as the technologies in computing should not cause any harm to the end-users who might even be ignorant of such consequences. Another aspect in the ACM code of conduct also states the need for Information technology to humans, it also places a caution that computing technologies should be rigorously accessed so as not to bring harm and danger to the health of the users, also not to bring danger to the user's privacy and safety both in the short and long term.

ACM Code of ethics warns against well-intended actions which may lead to harm. Those responsible should ease the harm, that is if the harm is accidental. If the harm is intentional, those responsible for it should make sure the harm is morally acceptable. The IT professionals in the organization ought not to harm others directly or indirectly. For example, the IT professionals have a responsibility to report risks that might cause hard in the organization. Leaders ought to lead by example by mitigating risks, else suitable measures would be taking that will not be favorable for them, like "blowing the whistle" to reduce likely harm (ACM, 2018).

A section of the code of ethics states the value of being trustworthy, honest, fair, and equal in the organization. It states the need to be in an environment that honors the virtues and principles of the enterprise (Ron et al, 1993).

The computing professional should be always transparent in all endeavors. He or she should disclose the limitations, system capabilities, or potential problems if summoned up by the employers. Fabricating information or accepting bribes from sources outside the company to leak or share information violates the code of ethics. These professionals should always say the truth about their qualifications and their inability to complete a task due to incompetence. The IT professionals in these SMEs must not misinterpret the policy of the organization. Authority must be given to the IT professionals before they speak concerning an issue.

It is stated in the ACM ethics code, these IT professionals must be trustworthy, therefore should provide credible evaluations and judgment to clients, employers, employees, the public, and the users. They ought to be careful when identifying and lessening risks in the office systems. Reassessment of risks should be done frequently by the IT professional because the computing systems evolve and because future risk cannot be predicted.

The IT professionals need to share technical knowledge with other employees and employers in the organization. He or she must promote awareness of computing techniques and terminologies, educate others about cyber risks and threats that could occur anytime. Communication between the employees and the IT professional should be respectful, clear, and welcoming. They should always address inaccurate information concerning computing or technology (ACM, 2018).

According to Section 2.8 in the ACM code of ethics, the IT professional does not have any right to access another employee's computer system except under exceptional circumstances where the professional wants to stop a malicious attack on a system. Extra safety measures ought to be taken in order not to harm others. Individuals have the right to restrict these IT professionals in their computing systems if it falls in the company code of ethics (ACM, 2018).

The computing future hangs on ethical and technical excellence. These IT professionals should abide by the code and ethics and find ways to improve them. Action should always be taken by these experts when resolving ethical problems, they have known about. IT experts should politely express their worry to the party involved in the violation of the code (ACM, 2018).

Reflection of a proper organizational response in dealing with cyber-security ethical issues.

The Cyber-attack dilemma could be handled if certain principles were put in place and kept. I will be talking about three case studies that reflect the ethical decision of organizations in response to cyber-attacks and also some wrong decisions made by two parties.

Uber had a breach in 2015 where hackers stole 57 million customers and driver personal information details. During that time of the incident, Uber was bargaining with U.S regulators over a privacy violation that happened earlier. Uber negotiated with the attacker to delete the files stolen from them. Uber paid the attacker $100,000 to keep their mouth shut. Unfortunately for the company, the hack was later leaked a year after the hack happened on various media. Not until the cyber-attack was revealed to the press, uber did not disclose the breach to its customer's riders and the press. The CISO in charge of the case Joe Sullivan and his deputy were fired for mismanaging the attack. Uber was later fined $148M for failing to notify the drivers of the hack.

The Uber breach and its cyber ethics failure in reporting the incident to the victims and the regulatory authority is an example of what can occur if the organizational behavior is not regulated by good ethics.

Yahoo was said to agree with Verizon when it highlighted the data breach that happened three times in the space of one year (2013-2014) which affected over a billion users. The data breach was revealed after the acquisition deal it had with Verizon. The deal was over $4 Billion. After Yahoo revealed the breach to the public, their net worth was cut down by $352M. Yahoo was investigated by the Security and Exchange Commission (SEC) for failing to notify the victims of the cyber-attack earlier than now and also for violating SEC rules by not providing substantial documents relating to the data attack that occurred. The company, Yahoo continues to be liable for debts that are incurred from the regulatory body.

The fines incurred on Yahoo was as a result of a lack of cyberethics from the organization board. This is an example of an organization that lacks ethical principles.

On the other side of this case study, the Australian Red Cross was attacked online whereby 550,000 blood donor personal details including their Sexual history were collected. This data was later published on an online platform by some third-party contractors.

After the cyber-attack that happened to the Australian Red Cross, the organization immediately disclosed it to the donors affected and the Australian government, which is the Computer Emergency Response Team (CERT). due to the swift response of the Red cross, it avoided high fines due to the breach. The commissioner of the Australia Information Commission, Timothy Pilgrim commended their fast response in reporting the breach. The kind act of the Red Cross in providing for the donors increased their reputation and trust in being clear and transparent within Australia.

The above case study examples emphasize the need for an incident response team that will hold the core values of the organization. Trust should be established between the customers and the organization.

A quality incident framework should be implemented to align with the purpose and core values of the establishment. It ought to balance best practices and organizational risk in a clear manner that meets the business and regulatory requirements, also ensuring its leaders can properly access the information.

Conclusion

In summary, cybersecurity and ethics go together. The SMEs must always stick to fulfilling their integrity and values. The staff should be monitored to keep the value at all times. There should be transparency and honesty to the customers when dealing with their information. The detailed report above shows what harm could occur when the organization does not abide by cyber ethics. The data and information of the company should be a priority in cyber/ethical decision making.

Some steps should be taken to reduce and mitigate risk in the establishment:

- Organizations should consider and identify their biggest treasure and assets and find critical ways to secure them. It’s difficult to protect all data files in the network at all times, also there is always a limit to their security budget. So, the identification of these assets will help enable you to implement security measures where it matters.
- Investment should be made in regards to Cyber Security. Training on cyber matters should be made available to the staff in the establishment. Most cyber-attacks in the company are a result of human error, which includes downloading malware through an email message or clicking a phishing link. Risk awareness is important because it is a cheap method of mitigating risk.
- It’s important to keep a backup of all your important files in case there is a ransomware attack. Ransomware is an attack that illustrates the computer system and blocks access from users accessing data files till the money is transferred to the attacker. Most times the enemy demands that the transfer is sent to a bitcoin account to avoid contact tracing. It is a risk because the company does not know if the attacker will keep to their word. There is no guarantee that the data being encrypted will be unlocked to the user.
- Multi-factor encryption is needed in the organization because theft of user credentials can harm the company’s network system. This encryption technique requires a user

password and another form of protection like an iris scanner, fingerprint reader, or a security key (Universal 2nd factor) to be able to safeguard the information of the users or the organization. With multi-factor authentication, it’s difficult for attackers to gain permission to the network and also user credentials because they have to prove they have entry to the second authentication method.

An organization which trains their staffs and invest finances in cybersecurity have sound ideas of making ethical decisions that will help strengthen their network, also, reduce the chance of susceptible attack. Consumers place trust as the number one factor in dealing with a business. After how the Australia Red Cross tackled the cyber-attack that was placed on them, the bar is set high for other companies to follow.

Reference

Daud, S. and Yusoff, W.F.W., 2010. Knowledge management and firm performance in SMEs: The role of social capital as a mediating variable. *Asian Academy of Management Journal*, *15*(2).

Symantec Corporation, *Symantec Survey Reveals More than Half of Small and Midsized Businesses in Australia and New Zealand Experience Security Breaches*, media release, Symantec Corporation, 12 May 2009, p.1.

Van Muijen, J.J. and Koopman, P.L., 1994. The influence of national culture on organizational culture: A comparative study between 10 countries. *European Journal of Work and Organizational Psychology*, *4*(4), pp.367-380.

Vitell, S.J., Nwachukwu, S.L. and Barnes, J.H., 1993. The effects of culture on ethical decision-making: An application of Hofstede's typology. *Journal of business Ethics*, *12*(10), pp.753-760.

Navarro, J., Deruyver, A. and Parrend, P., 2018. A systematic survey on multi-step attack detection. *Computers & Security*, *76*, pp.214-249.0

Farion, A., Dluhopolskyi, O., Banakh, S., Moskaliuk, N., Farion, M. and Ivashuk, Y., 2019, June. Using blockchain technology for boost cyber security. In *2019 9th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 452-455). IEEE.

Australian Government, 2018. *Australian Government - Department of Industry, Science, Energy and resources: Stepping into global markets.* [Online]
Available at: https://www.industry.gov.au/data-and-publications/stepping-into-global-markets

Hall, M., 2017. *Australian Government (Australian Trade and Investment Commission): Case Study - Using the internet of things to increase global food production.* [Online]
Available at: https://www.austrade.gov.au/agriculture40/case-studies/using-the-internet-of-things-to-increase-global-food-production

Shrapnel, W., n.d. *Export Finance Australia Report 2018-2019: Case Study (HeliMods).* [Online]
Available at: https://www.transparency.gov.au/annual-reports/reporting-year/2018-2019-23

Lee, Y.K.B.G., 2013. An analysis for the mediating effect of organizational justice on the performance in the virtual organization. *International journal of software engineering and its applications*, *7*(1), pp.201-210.

Moore, A.P., Cappelli, D.M. and Trzeciak, R.F., 2008. The “big picture” of insider IT sabotage across US critical infrastructures. In *Insider Attack and Cyber Security* (pp. 17-52). Springer, Boston, MA.

Dacosta, I., Chakradeo, S., Ahamad, M. and Traynor, P., 2011. *One-time cookies: Preventing session hijacking attacks with disposable credentials*. Georgia Institute of Technology.

Moore, T., Clayton, R. and Anderson, R., 2009. The economics of online crime. *Journal of Economic Perspectives*, *23*(3), pp.3-20.

Hutchings, A., 2012. Computer security threats faced by small businesses in Australia. *Trends and issues in crime and criminal justice*, (433), pp.1-6.

Egele, M., Wurzinger, P., Kruegel, C. and Kirda, E., 2009, July. Defending browsers against drive-by downloads: Mitigating heap-spraying code injection attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 88-106). Springer, Berlin, Heidelberg.

Hackworth, A. and Ianelli, N., 2005. Botnets as a vehicle for online crime. *Baltimore, USA, December*.

Dojkovski, S., Lichtenstein, S. and Warren, M.J., 2007. Fostering information security culture in small and medium size enterprises: an interpretive study in Australia.

Furnell, S.M. & Clarke, N.L. (2005) Organisational Security Culture: Embedding Security Awareness, Education and Training, in Proceedings of the 4th World Conference on Information Security Education (WISE 2005), Moscow, 67-74.

Kim, T., and Scheller-Wolf, W. (2019) 'Technological Unemployment, Meaning in Life, Purpose of Business, and the Future of Stakeholders'. Journal of Business Ethics, 160(2), 319-337.

De, S., Grembergen, V., Wim, Joshi, Anant, Huygh, Tim. (2020). *Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations.* Management for Professionals (3)

ISACA (2011) *Information Ethics.* Available at: http://www.isacajournal-digital.org/isacajournal/2012vol5?article_id=1077871&pg=NaN#pgNaN (Accessed 23 May 2021)

ACM. (2018). ACM code of ethics and professional conduct. Available at: https://www.acm.org/code-of-ethics. (Accessed 3 June 2020)

ACM Code of Ethics and Professional Conduct' (1992) *Communications of the ACM*, 35(5), pp. 94–99. doi: 10.1145/129875.129885.