Kush Patel

Sara Ghadami

CPSC 315

11/19/2024

Project 2

I'm implementing an ethical framework for a tech company called SecureNet Rescue, which is a cutting-edge cybersecurity firm dedicated to providing comprehensive digital security solutions for small to medium-sized enterprises across various industries. As cyber threats continue to evolve and become more sophisticated, SecureNet Rescue aims to empower organizations with the tools and knowledge necessary to protect their digital assets, ensure compliance, and maintain customer trust. SecureNet Rescue offers personalized security solutions tailored to the specific needs and risks of different industries and individual organizations. This includes conducting thorough risk assessments to identify vulnerabilities unique to each client. SecureNet Rescue aims to provide secure service to the client. The mission of the company is to create a safer online environment for those enterprises by delivering innovative, user-friendly cybersecurity solutions tailored to their specific needs. They want to educate our clients about potential threats and equip them with proactive measures to mitigate risks, ensuring their operations remain uninterrupted and their data remains secure. The company also has training programs for employees to educate them about cybersecurity best practices and how to recognize phishing attacks and other threats. It offers ongoing monitoring and support services to manage clients' cybersecurity infrastructure. SecureNet Rescue primarily targets small to medium-sized enterprises that may lack the resources or expertise to manage their cybersecurity effectively. These businesses span various sectors, including healthcare, finance, retail, and technology, all of which face unique cybersecurity challenges.

While I was developing an ethical framework, several ethical issues arrived during the development of the ethical framework. Key issues are Data Privacy in which Handling sensitive client data poses risks related to privacy and security breaches. Transparency in which Clients may not fully understand the risks or the measures implemented and must be aware of the extent of data collection and monitoring practices. Accountability, in which the workers who handle all the data must hold responsibility for their handling of the data and, and there could be potential misuse of cyber security tools used in the company .

We can address these ethical concerns that popped up during the framework. The company has many beliefs and guiding values like “Putting Privacy First”,”Being Transparent with Customers”, and “Proper Use of Tools”. There are so many issues in Data Privacy, like Handling sensitive client data poses risks related to privacy and security breaches. If a company handles sensitive client data it can be risky and could fall victim to data breaches. In “Cyber risk and cybersecurity: a systematic review of data availability”, it states “Besides cyberattacks, data breaches can also cause high costs. Under the General Data Protection Regulation (GDPR), companies are obliged to protect personal data and safeguard the data protection rights of all individuals in the EU area.”[3]. This quote explains that the client data could be exposed depending on how they handle the data. There are so many ways companies can ensure that client data isn’t exposed by like collect only necessary data, limit access to authorized personnel, implement strong encryption methods, regularly monitor for vulnerabilities, conduct employee training on data privacy, enforce robust password management practices, and comply with relevant data protection regulations like GDPR or CCPA, while also ensuring third-party vendors uphold the same security standards. By developing strong encryption methods with strong algorithms it’ll keep the data safe and secure.We also need to provide hashing in order to prove that there is a

digital signature, if there is a digital signature then it provides informed consent to the clients, and digital signatures build trust among clients with the company. In “5 Steps to Ensure Customer Data Protection and Privacy”, it talks about how companies can put strong measures in place like implement strict access controls, encryption, and regular audits to prevent unauthorized access to client information[4]. Adhere to data protection regulations and ensure clients are informed about data handling practices. The ethical theory involving data privacy is Deontological Ethics, in which individuals have a right to privacy, and data collectors have a duty to respect that right. For instance, companies should obtain informed consent before collecting personal data and be transparent about how that data will be used, regardless of the potential benefits. In “Linkedin”, it states “Deontology takes a hard look at the morality of what we do based on a set of rules, basically saying some things are just right or wrong, no matter what comes of them[7]. When we talk about cybersecurity, this means sticking to privacy laws like glue and treating the protection of personal data as a rule that can't be bent.”. This quote explains that's the essence of deontological ethics, which is a moral philosophy that emphasizes adherence to rules and duties rather than focusing solely on the outcomes of actions, this explains belief that violating privacy laws or ethical guidelines is always wrong, even if one might argue that doing so could lead to a perceived benefit .Many clients are also not aware of or fully understand the risks or the measures implemented, they are also unconscionable of the security measures that are put in place and they also must be aware of the extent of data collection and monitoring practices. The main issue regarding it is transparency. In “The Ethical Dilemmas of Cybersecurity: Balancing Privacy and Security” it states “Cybersecurity professionals and organizations are expected to be transparent about their methods, intentions, and the data they collect or access. This principle is crucial because it helps build trust among users and

stakeholders."[5]. This quote explains that we must build trust in which it helps establish trust between organizations and their users. When cybersecurity professionals openly communicate their methods and intentions, users are more likely to feel secure and confident in the organization's ability to protect their data. By being transparent about data collection and access methods, organizations enable users to make informed decisions about their privacy.Transparency fosters accountability. If organizations are clear about their practices, they are more likely to adhere to ethical standards and legal requirements. They need to be clear and explain their policies, their actions, and decisions to their customers in order to build trust which is known as Cybersecurity Transparency in Business as stated in "Blue Goat Cyber"[8]. Cybersecurity transparency in business is increasingly important for building trust, mitigating risk, and ensuring compliance. This all aligns with Deontological ethics in which the business has a duty to Protect and Inform their customers. Accountability in cybersecurity for businesses is essential for safeguarding data, maintaining trust, and managing legal and ethical obligations. In "Accountability in Cybersecurity: Save Money, Reduce Cyber Risk", it talks about how an organization must prevent the likelihood of a cyber attack to happen. If an attack does happen, the organization must then take every practical step to mitigate its impact on customers, partners, and employees. The company must communicate with all of its customers about the cyber attack, and the company usually doesn't communicate with their customers[9]. The lack of communication is one of those common problems and ethical issues that arise in a cybersecurity company. Accountability is aligned with Utilitarianism because it maximizes positive outcomes by preventing harm from breaches and ensuring the protection of all stakeholders' data. Utilitarianism is the belief of determining what is the best decision for everyone and by showing accountability, you are following the utilitarian belief in the company. Another ethical issue and

concern in the company is that there is so much misuse of cyber security tools and software in the company. Many cyber criminals who work in cyber security businesses misused many cyber security tools in an unethical manner. Criminals could be exploiting the tools used by security teams and because of this there is a higher chance a cyber attack would occur. In "How Criminals Abuse Common Security Tools – and Use Them Against You", it states "Criminals are exploiting the very tools used by security teams. Sophos researchers have recently observed an increase in attacks in which criminals target tools used by incident responders and penetration testers."[11]. This quote explains that cybercriminals are leveraging legitimate tools, those typically used by security teams for defensive or testing purposes to carry out attacks. Another concern is that employees in SecureNet Rescue could misuse the IT resources in many different ways. IT employees can misuse the IT resources which could include all the cyber security tools in many different ways such unauthorized file copying, downloading unauthorized software,using pentesting tools for fun rather than business purposes and using personal devices for business purposes as stated in "Security Threats in Employe Misuse of IT Resources". Using cyber security tools to stalk someone or get someone's personal information violates the social contract theory. Cybersecurity tools can monitor network activity, but using them to invade employee privacy without informed consent can lead to legal repercussions. In "Breaching the Contract" it explains that a company like SecureNet Rescue utilizes cybersecurity technologies in a way that violates the implied agreement with its customers and stakeholders to protect their data and privacy, and since it violates privacy it violates the social contract theory[12]. To guarantee ethical and responsible use of all developed or recommended tools and technologies, cybersecurity professionals should actively educate clients about the principles of ethical hacking, emphasizing the critical need for informed consent before conducting any penetration testing or vulnerability

assessments, clearly outlining the scope of the testing and potential impacts on their systems, as stated in “Unveiling the positives of ethical hacking”, we should educate everyone about when to use these cyber security tools, when it is appropriate to use these tools, and the effects of using these tools. One way for proper use is to implement Role-Based Access Control, Assign permissions based on job roles and responsibilities. Only employees who require access to sensitive cybersecurity tools should have it, limiting the potential for misuse by restricting access to essential personnel only. We can also set up Multi-Factor Authentication to access critical cybersecurity tools, adding a layer of security to prevent unauthorized access and making it harder for malicious actors to misuse these resources. The company should also regularly review logs and audit trails to detect unusual or unauthorized use of cybersecurity tools.

After implementing an ethical framework for a tech company called SecureNet Rescue, there were many positives about this company, while at the same time, there were many negatives that generated so many ethical issues and because of this we had to analyze many ethical theories like Deontology, Utilitarianism, and the Social Contract to help develop an ethical framework of the company. SecureNet Rescue aims to protect data, maintain network performance, prevent unauthorized access of resources, and mitigate risks for many companies around the world. Many companies can ask for SecureNet Rescue to implement strong security features for their companies, yet some of them are good, while some of them could cause many ethical concerns among individuals related to data privacy, lack of being informed, being accountable for any problems, and misuse of cyber security tools.

Sources

1. *Cybersecurity ethics grows in urgency as the digital landscape continues to Transform Society*. Cybersecurity Ethics: What Cyber Professionals Need to Know. (2023, August 21). https://www.augusta.edu/online/blog/cybersecurity-ethics/
2. Cybersecurity ethics: Everything you need to know. (n.d.). https://www.ollusa.edu/blog/cybersecurity-ethics.html#:~:text=What%20are%20the%20ethical%20considerations,measures%2C%20and%20responding%20to%20threats
3. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). *Cyber risk and cybersecurity: A systematic review of data availability*. The Geneva papers on risk and insurance. Issues and practice. https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/
4. *5 steps to ensure customer data protection and privacy*. Business Class: Trends and Insights | American Express. (n.d.). https://www.americanexpress.com/en-us/business/trends-and-insights/articles/7-steps-to-ensure-customer-data-privacy/#:~:text=By%20keeping%20employees%20informed%20and,of%20accidental%20breaches%20or%20leaks

5. Skillfloor. (2023, September 11). *The ethical dilemmas of cybersecurity: Balancing privacy and security*. Medium. https://skillfloor.medium.com/the-ethical-dilemmas-of-cybersecurity-balancing-privacy-and-security-318adcf949a3#:~:text=One%20of%20the%20foundational%20ethical,autonomy%20in%20the%20digital%20realm
6. Loi, M., & Christen, M. (1970, January 1). *Ethical frameworks for cybersecurity*. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-030-29053-5_4#:~:text=Principlism%20is%20a%20form%20of,no%20other%20prima%20facie%20duties
7. Koroma, M. (2024, March 5). *How do we balance the scales? navigating privacy, security, and Ethics in the Cyber Age*. LinkedIn. https://www.linkedin.com/pulse/how-do-we-balance-scales-navigating-privacy-security-ethics-koroma-4jwze/
8. *Moving towards Cybersecurity transparency*. Blue Goat Cyber. (2024, October 26). https://bluegoatcyber.com/blog/a-guide-to-cybersecurity-transparency/#:~:text=Transparency%20in%20cybersecurity%20is%20not,data%20is%20in%20safe%20hands
9. Accountability in cybersecurity: Save Money, reduce cyber risk. (n.d.-a). https://blogs.blackberry.com/en/2023/01/accountability-in-cybersecurity
10. Using utilitarian ethics to analyze the Equifax breach of 2017. (n.d.-e). https://libraetd.lib.virginia.edu/downloads/9p290b01g?filename=Gumabay_Ethan_STS_Research_Paper.pdf

11. *How criminals abuse common security tools – and use them against you*. CSO Online. (2021, May 13). https://www.csoonline.com/article/570735/how-criminals-abuse-common-security-tools-and-use-them-against-you.html#:~:text=Criminals%20are%20exploiting%20the%20very,you%20may%20need%20to%20investigate.%E2%80%9D

12. Full article: Breaching the contract? using social contract theory to explain individuals' online behavior to safeguard privacy. (n.d.-c). https://www.tandfonline.com/doi/full/10.1080/15213269.2019.1598434

13. *Security threats in employee misuse of IT resources*. Avasant. (2021, April 27). https://avasant.com/report/security-threats-in-employee-misuse-of-it-resources/#:~:text=Interestingly%2C%20the%2014%20categories%20of,or%20loss%20of%20system%20availability.