Collaborative Discussion 1 - Codes of Ethics and Professional Conduct

Word Count ≈ 750

Initial post –

Hello,

My chosen case study was 'Malware Disruption,' which delves into the unethical practices of a company known as Rogue Services. This company offered "cheap, guaranteed uptime, no matter what" for website facilitation, a service that might seem appealing to legitimate businesses and consumers looking for reliable and affordable web hosting (Association for Computing Machinery N.D.). However, this seemingly beneficial service also attracted spammers, hackers, and other malicious actors who exploited the platform to disseminate harmful content. Specifically, these bad actors used Rogue Services to host corrupted advertisements that infected personal machines with ransomware. The situation highlighted in this case study illustrates a significant ethical breach, particularly in relation to the ACM Code of Ethics and Professional Conduct.

Knowing that their platform could be, and indeed was, used to distribute ransomware, Rogue Services failed to uphold key ethical standards set out by the ACM. The company's actions, or rather inactions, violated several core principles of the ACM Code, particularly those related to Professional Leadership Principles and the mandate that 'the public good must be the central concern during all professional computing work' (Association for Computing Machinery 2018). By allowing their services to be used in such a harmful way, they neglected their duty to protect the public, instead prioritizing profit over ethical responsibility. Moreover, the use of ransomware on their platform put the personal data of countless individuals at risk, directly conflicting with the General Data Protection Regulation (GDPR) established in Europe (European Union 2016). This regulation was designed to ensure the protection of personal data and privacy, and Rogue Services' facilitation of ransomware attacks represented a gross disregard for these critical legal and ethical obligations. Ultimately, Rogue Services failed to prioritise public interest, choosing instead to profit from activities that were not only unethical but also illegal.

Looking to the future, the implementation and spread of ransomware are likely to increase, particularly with the ongoing advancements in financial technologies such as cryptocurrency. Cryptocurrencies provide a layer of anonymity that is highly attractive to cybercriminals, making it easier for them to demand and receive ransom payments without being traced. As Upadhyaya and Jain (2016) pointed out, the explosive growth of the internet has paved the way for an increase in cyber-attacks, with Cryptolocker ransomware becoming increasingly common. This type of ransomware works by encrypting the data of individuals, rendering it inaccessible until the victim pays a ransom to receive the decryption key. Typically, the demanded payment is in cryptocurrency, further complicating efforts to track and apprehend the criminals involved. The trend towards more sophisticated and widespread use of ransomware poses a growing threat to data security and privacy, underscoring the need for stronger cybersecurity measures and ethical standards in the technology industry.

References –

- Association for Computing Machinery (N.D.) Case: Malware Disruption. ACM Code of Ethics. Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed: 11th August 2024].
- Association for Computing Machinery (2018) ACM Code of Ethics and Professional Conduct. Available from: https://ethics.acm.org/ [Accessed: 11th August 2024].
- European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed: 11th August 2024].
- Upadhyaya, R. and Jain, A., (2016) Cyber ethics and cyber-crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 143-148). IEEE.

Peer responses –

by Rocio Altair Perez Liou - Saturday, 17 August 2024, 3:03 PM

Your analysis of the "Malware Disruption" case study effectively highlights the ethical and legal breaches committed by Rogue Services. the company clearly violated the ACM's ethical guidelines, because they knowingly allowed their platform to be exploited for distributing ransomware, particularly the principle that the public good must be the central concern in all computing work. Your emphasis on the company's failure to protect users and their data underscores the critical importance of ethical responsibility in technology.

The comparison to GDPR is particularly relevant, as it highlights the legal implications of Rogue Services' actions. Facilitating ransomware attacks not only breached ethical standards but also contravened GDPR, which mandates the protection of personal data. This serves as a stark reminder that ethical lapses in technology can have severe legal consequences.

Furthermore, your discussion on the future risks posed by ransomware, especially with the rise of cryptocurrency, is insightful. It illustrates the evolving nature of cyber threats and the need for continuous advancement in both cybersecurity measures and ethical standards within the industry. The citation of Upadhyaya and Jain (2016) adds depth to your argument by connecting the growth of the internet and cryptocurrency to the increasing prevalence of cyber-attacks, including ransomware.

Overall, your analysis is thorough, well-referenced, and provides a strong critique of the ethical and legal failures in the case study.

by Syed Imran Ali - Wednesday, 21 August 2024, 3:46 AM

Hi Chris,

Your analysis of the “Malware Disruption” case study effectively highlights the significant ethical breaches committed by Rogue Services. You astutely identify how the company’s failure to uphold the ACM Code of Ethics directly contributed to the harmful spread of ransomware. By emphasizing the importance of the public good in professional computing work, you underscore a fundamental ethical responsibility that Rogue Services neglected in favor of profit.

Your exploration of the implications of these unethical practices, particularly in relation to GDPR and the future landscape of cybersecurity, adds a critical dimension to the discussion. The connection you draw between the increasing sophistication of ransomware and the anonymity provided by cryptocurrencies like Bitcoin is particularly insightful. This point not only underscores the evolving nature of cyber threats but also highlights the ongoing need for enhanced cybersecurity measures and stricter adherence to ethical standards in the tech industry.

Additionally, your reference to the GDPR is crucial in illustrating the legal ramifications of such ethical lapses. This serves as a potent reminder of the broader consequences that unethical behavior can have, both legally and socially. Overall, your analysis is comprehensive and well-articulated, effectively linking ethical theory with real-world implications.

It might also be valuable to consider how companies like Rogue Services could implement better ethical oversight or governance structures to prevent such breaches. Encouraging a proactive rather than reactive approach to ethics in technology could be a way forward in mitigating the risks you've outlined.

Summary Post

To conclude, the decision by Rogue Services to ignore or even facilitate the spread of harmful malware to users represents a significant breach of ethical standards and a violation of the General Data Protection Regulation (GDPR). By failing to prevent or mitigate the distribution of malware, Rogue Services not only compromised the security and privacy of countless users but also violated fundamental principles of data protection and user safety. As noted by Rocio, while the legal implications of such actions are substantial, they have not been sufficient to act as a deterrent for similar behaviour by other organisations. This suggests that the current regulatory framework and penalties, such as fines or legal action, may not be severe enough to discourage companies from prioritising profit over ethical conduct and compliance with data protection laws. To address this gap, it may be necessary to impose more stringent punishments and higher fines to ensure that companies are more vigilant in safeguarding personal data and upholding ethical standards.

My other peer, Syed, mentions the importance to ensure that personal data protection remains a priority for professionals, and adopting a proactive rather than a reactive approach. This involves not only complying with legal requirements but also fostering a culture of data protection awareness and ethical responsibility within organisations. Ongoing training and education on the importance of personal data protection can empower professionals to recognise the value of safeguarding user information, thereby helping to create a positive working environment that prioritises ethical practices over mere profit maximization. By understanding the significance of protecting personal data, professionals can better appreciate the impact of their actions on consumers and the broader digital environment. Ultimately, cultivating an ethical mindset and proactive stance on data protection can help prevent future breaches and build greater trust with customers and stakeholders, something that Rogue Services failed to do.