Introduction

In this collaborative discussion, I will be highlighting the legal, ethical and social concerns from the Malware case study (ACM, 2018).

The case study focuses on Rouge Services, a fictitious company that provided web hosting services to cyber criminals until they were forcibly taken offline by a cyber-attack.

BSC Code of Conduct Violations

The BCS Code of Conduct (BCS, 2022) is a set of key principles for ensuring the integrity of IT professionals. There are 4 key principles of the BSC code of conduct; the first one is related to public interest, the second one is related to professional competence and integrity, the third one is related to duty to authority and the final one is related to duty to profession.

Rouge Services violated the public interest principle as they showed no regard for the privacy or security of others when they refused to do anything to stop cyber criminals from hosting malware on their services. Their inaction could be interpreted as a human rights violation as the right to privacy is a fundamental human right in over 185 countries (European Data Protection Supervisor, 2024).

Rouge Services violated the principle related to integrity as their inaction and lack of cooperation with governmental agencies caused harm to the victims of the cyber-attacks carried out by their users.

Rouge Services violated the duty to relevant authority principle by failing to take any form of responsibility for the cyber-attacks after they were made aware of them. In most jurisdictions, Rouge Services would be considered complicit in their users' crimes and could even be incarcerated.

ACM Code of Ethics Violations

The ACM Code of Ethics and Professional Conduct (ACM, 2021) outlines a series of ethical principles, professional responsibilities and professional leadership principles that computing professionals must abide by.

The general ethical principles related to avoiding harm and the quality of life of all peoples (principles 1.1 and 1.2) were violated by Rouge Services as by allowing cybercriminals to host malicious software they facilitated the harm caused by their clients.

The professional responsibilities related to the public good (principles 2.8 and 3.1) were violated by Rouge Services as they were aware their services were being used by cybercriminals for criminal activity and took no action thereby failing to consider the public good.

Conclusion

Whilst Rouge Services' actions weren't technically illegal in their jurisdiction it was most certainly unethical as they didn't consider the harm, they did to others by allowing their users to carry out cyber-attacks. Additionally, the lack of cooperation with governmental agencies and the steps said governmental agencies had to take to resolve the situation suggests a company that is only concerned with its profits.

References

ACM. (2018) Code of Ethics Case Studies. Available from: **https://www.acm.org/code-of-ethics/case-studies** [Accessed 29 October 2024].

ACM. (2021) ACM Code of Ethics and Professional Conduct. Available from: **https://www.acm.org** [Accessed 29 October 2024].

BCS. (2022) BCS Code of Conduct. Available from: **https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf** [Accessed 28 October 2024]

European Data Protection Supervisor (2024) Data Protection. Available from: **https://www.edps.europa.eu/data-protection/data-protection_en** [Accessed 29 October 2024]