Rogue Services Ethical Case

Rogue Services offered web hosting services that it claimed would be cheap with guaranteed uptime no matter the situation. However, the case indicates Rogue encountered issues when some clients focused on spam and malware began to use its services (Case: Malware disruption, n.d.). They used Rogue's reliability guarantee to protect servers from efforts to take them down. The case demonstrates several ethical violations by Rogue. A key requirement of the British Computer Science Code of Conduct is the requirement to respect the individuals or organizations an entity works for by acting in their best interest (BCS Code of Conduct, n.d.). Since Rogue allowed clients who could cause harm to other service users to continue using its servers, the company acted unethically, exposing other users it worked for to the risk of cyber-attacks.

The Rogue Services case raises several legal and ethical issues for the company. One of the key legal issues is the company's responsibility in reporting the use of its services by cyber criminals. Article 3 of the Cybercrime Convention requires online service providers to report any intentional attempts to intercept without the right computer data (E4J university module series, 2019). Therefore, Rogue Services violated a key international law, highlighting a key legal issue. Besides, a significant portion of countries have regulations governing data protection and privacy, at least 71% (Data protection, n.d.). The actions of Rogue Services exposed its users to the risk of data breaches, highlighting a key legal issue.

Furthermore, the case highlights the impact of Rogue's behavior on different social issues. In particular, the case indicates the potential for malware to cause

reputational and economic harm. Data breaches can harm the reputation of online retailers as customers experience concern about the safety of their information held by a company (Davidoff, 2019). Thus, the Rogue case exposed users to social issues related to their reputation among customers. Finally, the problem had the potential for economic consequences due to cybercriminals using the information they obtain for fraudulent activities (Gottschalk & Hamerton, 2021). Accordingly, the case revealed the risk of another social issue arising from the likelihood of economic losses.

References

BCS Code of Conduct. (n.d.). British Computer Society. https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/

Case: Malware disruption. (n.d.). ACM Ethics. https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/

Data protection and privacy legislation worldwide. (n.d.). United Nations Conference on Trade and Development. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Davidoff, S. (2019). *Data breaches: Crisis and opportunity.* Pearson Education.

E4J university module series: Cybercrime. (2019). United Nations Office on Drugs and Crime. https://www.unodc.org/e4j/zh/cybercrime/module-2/key-issues/offences-against-the-confidentiality--integrity-and-availability-of-computer-data-and-systems.html

Gottschalk, P. & Hamerton, C. (2021). *White-collar crime online: Deviance, organizational behaviour and risk*. Springer.