RMPP - Collaborative Learning Discussion 1

Codes of Ethics and Professional Conduct

Initial Post

I have chosen the “Malware Disruption” case as an example of how both the ACM Codes of Ethics (CoE) and the BCS Code of Conduct (CoC) are impacted by the described incident.

The case study involves Rogue Services, a web hosting service which advertises uptime and continuous delivery indifferent to the client’s use case. This guarantee was leveraged by several malicious actors, who used Rogue’s services to host botnets, issue spam and other fraudulent services, and delivered corrupted advertisements that carried payloads to exploit browser vulnerabilities (ACM Ethics, N.D.).

By allowing the hosting of malicious activities, Rogue Services has violated several principles of both the ACM CoE and the BCS CoC, which are highlighted in the following table:

ACM Code	BCS Code	Identified Issues
Principle 1.1: Contribute to society and human wellbeing, acknowledging that all people are stakeholders in computing. **Principle 1.2:** Avoid harm. Within ACM’s CoE, "harm" means negative consequences, especially when those consequences are significant and unjust.	**Duty to the Profession:** Accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute; **Professional Competence and Integrity:** Avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction;	Rogue facilitated harm caused by their clients by allowing for the hosting of malicious software.
Principle 2.8: Access computing and communication resources only when authorized or when compelled by the public good.	**Duty to Relevant Authority:** Seek to avoid any situation that may give rise to a conflict of interest between you and your relevant authority;	Rogue was aware that its web servers were hosting activities that caused infections and accessed systems without authorization.
Principle 3.1: Ensure that the public good is the central concern during all professional computing work.	**Public Interest:** You shall have due regard for public health, privacy, security and wellbeing of others and the environment;	With its actions, Rogue did not ensure that the public good was the central concern of its operations.

Rogue was based in a country that did not have adequate laws in place to prohibit such services. Therefore, on a national level, there was no intervention on the hoster’s operations. However, a collective of security vendors and government organizations forcibly took Rogue’s servers offline by using a computer worm.

Principle 1.2 of the ACM CoE states that harm should be avoided, however, when intentional harm is necessary, the responsible parties need to ensure that it is ethically justified and that all harm is kept to a minimum. The worm was contained to only Rogue’s network and created with the specific intent to take

Rogue's systems offline, a service that was harmful and malicious in nature, and therefore is consistent with the obligations highlighted within the principle (ACM, 2018).

List of References

ACM Ethics (2018) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 11 March 2022].

ACM Ethics (N.D.) Case: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption/ [Accessed 11 March 2022].

BCS (2021) Code of Conduct for BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 11 March 2022].

Summary Post

Hi Laura,

Thank you for replying to my post and asking justified and important questions.

I fully agree; in an ideal scenario, there should be a follow-up facilitated by the governments involved with the take-down of Rogue's servers. An implementation of a nationwide framework and relevant regulations would help prevent similar cases from occurring in the future. Else, other hosting providers may just emerge and replace Rogue's services due to the lack of consequences from within their national jurisdiction.

However, often nation-state threat actors are found to be behind malicious acts. These actors either work for a government directly to disrupt or compromise foreign governments and authorities, or are indirectly supported by their governments and do not face repercussions for their actions (Edgar & Manz, 2017). An example of such an actor is the Nobelium group, a Russian nation-state actor, that was found to be behind the prominent SolarWinds hack in 2020 (Barr, 2021). In such cases, it might not always be possible to foster a debate or cooperate with the country where illegitimate services are hosted from or where specific threats originate from.

In conclusion, I believe we all agree that the reaction that was highlighted in the Rogue Services case study should neither be the first nor main tool to be utilised to mitigate such a situation. Instead, stakeholders should aim toward working together with the source nation to achieve a sustainable and viable long-term solution.

List of References

Barr, L. (2021) Russian nation-state actor behind SolarWinds cyberattack at it again: Microsoft. *ABC News.* Available from: https://abcnews.go.com/Politics/russian-nation-state-actor-solarwinds-cyberattack-microsoft/story?id=80771329 [Accessed 28 March 2022].

Edgar, T. & Manz, D. (2017) *Research Methods for Cyber Security*. Syngress, pp.177-192.

Peer Response #1

Hello Man Sze,

Thanks for your interesting and informative post on the Abusive Workplace Behaviour case study. You have summarised the issues well. In addition to the important issues you have identified already, regarding Max's and Jean's conduct, it is important to also highlight that the organisation they are working for is at fault.

It is the duty of any organisation's HR department to implement clear processes and communication channels for employees to reach out to when facing workplace abuse. For the UK specifically, workplace harassment and abuse fall under the Equality Act (UK Legislation, 2010) and it is important for Diane's employers to have a grievance procedure in place. As highlighted in the UK government's workplace bullying and harassment guidelines (2021), it is the employer's responsibility to prevent any harassment suffered by their employees as they are the liable party.

If such procedures and ethical standards were communicated and reinforced throughout the organisation, perhaps Max would not have the freedom to behave as erratically as he did due to eventual consequences.

List of References

UK Government (2021) Workplace bullying and harassment. Available from: https://www.gov.uk/workplace-bullying-and-harassment [Accessed 18th March 2022].

UK Legislation (2010) Equality Act 2010. Available from: https://www.legislation.gov.uk/ukpga/2010/15/contents [Accessed 18th March 2022].

Peer Response #2

Hi Shiraj,

Thank you for the informative and insightful post about the dark user experience (UX) patterns case study. You have summed up the issues very well and I agree with your analysis.

It is interesting to note that even large corporations utilise dark UX patterns to their benefit, often neglecting user rights through misleading design choices. One such example would be the case of Facebook hindering users to decline cookie collection requests as opposed to accepting them. This particular case is very similar to the identified issue of "Dark UX patterns harm users by leading them down unwanted paths" above. Although Facebook provides a button to accept cookies instantly, it does not provide an immediate option that allows the user to simply decline them. This leads the user to accept the cookies due to the UX being designed deceivingly on purpose.

CNIL (2022), the French National Commission for Computing and Liberties, reports that the company has been fined 60 million euros after an online investigation identified that this implementation violated the French Data Protection Act.

Reference

CNIL (2022) Cookies: FACEBOOK IRELAND LIMITED fined 60 million euros. Available from: https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros [Accessed 18th March 2022].