University of Texas at Arlington

The Professional Ethics of Publishing Security Vulnerabilities

Landon Moon

Professional Practices: CSE-3314-002

Assignment #1

8 Sept. 2022

**Contents**

Introduction of the ethics scenario 3

Analysis of stakeholders and responsibilities 3

Real-life comparison 5

Conclusion 6

The Professional Ethics of Publishing Security Vulnerabilities

Throughout history, there have been multiple times where an issue is discovered in a system that if released to the public would cause even more damage. One scenario of this is that of a group of students who want to present a paper about a security vulnerability in a transit fare system. By determining the ethical impacts and responsibilities of this scenario, the students will be able to determine the best action to take for all parties involved.

The details of this scenario are given in chapter 9.3.5 of “A Gift of Fire 4th edition” where it states,

“Three MIT students planned to present a paper at a security conference describing security vulnerabilities in Boston’s transit fare system. At the request of the transit authority, a judge ordered the students to cancel the presentation and to not distribute their research. The students are debating whether they should circulate their paper on the Web. Imagine that you are one of the students.” (Baase 2019, 416).

In this scenario, we have a group of students who want to present their paper for a school project from MIT, but this paper would compromise the transit fare system if released to the public. The transit authority has taken a legal route to prevent the students from releasing their paper. If the students go against the judge’s order, the transit authority might file a lawsuit against them. This lawsuit may result in the students being fined, expelled, or possibly temporarily imprisoned. If the students don’t release their paper for their school project, they will receive a poor grade from their professor for not presenting anything at all.

In this case, there are four stakeholders, two primary and two secondary, that will be impacted by the student’s decision. The two primary stakeholders are the students and the transit authority because they are impacted directly by the students’ actions. If the paper becomes public, the transit system will have decreased profits because citizens will start using the vulnerability. This loss in profits can cause long-term damages to the transit system by causing employees to be laid off and delaying maintenance. The transit authority can sue the students for their damages because they went against the judge’s order. This lawsuit can result in financial compensation from the students and might cause the students to be expelled from MIT. Additionally, by releasing the paper the student has knowingly harmed the transit system when they could have found an alternative. While the students must deal with the legal ramifications, they must also deal with fact that they could have made a better decision. The two secondary stakeholders are MIT and the legal system. The lawsuit from the transit authority to the students might cause MIT might be held accountable for the students’ actions because it was a school project. MIT might be expected to cover some if not all of the financial cost of the lawsuit because the students were incentivized to release their paper. In between all these parties is the legal system who needs to make and enforce its decision on the situation. This can include a possible lawsuit from the transit authority or a possible compromise between all parties.

The two primary stakeholders have actions to take and have ethical, legal, and professional responsibilities for their actions. The students are the central actors in this scenario and have the primary ethical responsibility. Kaspersky, a cybersecurity provider, has multiple principles that apply to security vulnerability releases (Efremov et al. 2020). Primarily, these responsibilities are to “inform the affected party”, “coordinate efforts”, and “maintain confidentiality.” The students have an ethical responsibility to contact the transit authority about their discovery. Afterward, they should coordinate with the transit authority so both parties can agree on what to do. Then finally the students should keep their paper confidential until they can release it. The transit authority also has a responsibility to the students. Given that the students try to inform and coordinate with the transit authority, it is the transit authority’s responsibility to respond honestly and to consider the situation the students are in. Both the students and the transit authority have a responsibility of being honest, transparent, and careful when they communicate so they can come to a common ground.

For this scenario, the book states that “In the actual case, the transit authority requested a five-month ban to provide time for them to fix the problems. The judge dissolved the order after a week.” (Baase 2019, 417). Because the judge dissolved the order after a week, the students can freely release the security vulnerability damaging the transit fare system in the process. This outcome is not desirable because there are ethical responsibilities of both the students and the transit authorities that have not been considered, namely communication between them. Instead of simply releasing or withholding their paper, the students have the more ethical alternative to start a discussion with the transit authority. If both the students, and the transit authority can come to a common solution, then all stakeholders involved will benefit from this alternative.

A real-life scenario that had a similar outcome is that of the Citicorp Building. Due to neighboring buildings, the Citicorp building had to be built on “nine-story-high stilts” (Whitbeck 2006). The head engineer William LeMasurier accounted for cross-sectional winds but not for quartering winds. A student discovered this flaw and contacted LeMasurier about their research. LeMasurier found that strategic welds across the building could fix the structural vulnerability. The student and LeMasurier stayed quiet about the vulnerability until the welds could be made. Even the welding crews were “welding at night” to keep the vulnerability a secret (Whitbeck 2006). By communicating about the vulnerability and coming to an agreed plan, the student and LeMasurier did the right thing to fix the building. this is very similar to how our students and the transit authority should communicate and agree on a plan for the release of the security vulnerability.

In conclusion, both simple decisions the students could make would cause harm to one or more stakeholders in the situation. Instead, the students should decide to communicate with the transit authority so they can agree on a solution to the situation. This will most likely result in a temporary ban on the student’s paper with the understanding that they can present it later for full credit for their class. This way the students aren’t punished for being ethical in their decision and the transit system’s integrity isn’t damaged by the public’s knowledge of the security vulnerability.

References

Baase, Sara, and Timothy Henry. *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology*. 4th ed., Pearson, 2019.

Efremov, Andrey, et al. “Ethical Principles of Vulnerability Disclosure.” *Daily English Global Blogkasperskycom*, 18 May 2020, https://www.kaspersky.com/blog/vulnerability-disclosure-ethics/35581/.

Whitbeck, Caroline, and Eric Plosky. “William Lemessurier - the Fifty-Nine-Story Crisis: A Lesson in Professional Behavior.” *William LeMessurier - The Fifty-Nine-Story Crisis: A Lesson in Professional Behavior | Online Ethics*, 2006, https://onlineethics.org/cases/engineers-and-scientists-behaving-well/william-lemessurier-fifty-nine-story-crisis-lesson.

**CSE - 4314**

**Professional Practices**

**Academic Integrity**

**In order for your Assignment/Homework/Project to be accepted you must read the following, sign this form and attach it to your papers (as the last page of your assignment).**

**Academic Integrity:** Students enrolled in this course are expected to adhere to the UT Arlington Honor Code:

*I pledge, on my honor, to uphold UT Arlington’s tradition of academic integrity, a tradition that values hard work and honest effort in the pursuit of academic excellence.*

*I promise that I will submit only work that I personally create or contribute to group collaborations, and I will appropriately reference any work from other sources. I will follow the highest standards of integrity and uphold the spirit of the Honor Code.*

Student Signature: Landon Moon

Student Id Number: 1001906270

*Note: Must be read, signed and attached (stapled) as last page of homework or assignment. If it is a team assignment then all team members must read, sign and attach a single copy of the Academic Integrity form to the team’s paper as the last page. If not properly attached as last page a 2 point penalty will be assessed after grade assigned.*