HighGrade Student

Heading is 2 lines maximum

CS 285 – 02 – Professor Potasznik, 5/17/2020

Title clearly stipulates Scenario and #

Scenario #2: Hacking the T

Introduction summarizes scenario without copy/ pasting it directly from the class site.

According to Scenario 2, three computer science juniors at MIT decided to spend their time exploring ways to apply the theoretical knowledge they gained from a cyber security class they took in the previous semester. Gaining inspiration from the old, automatic gates in Boston's subway stations, through which thousands of people walk in and out on their way to work (MBTA, 2020), the students decided to test just how strong the system was at reading the magnetic Charlie cards and ensuring each person is fairly charged. Eventually, they found a major security vulnerability that allowed them to bypass payment and potentially get free subway rides. Before the end of their winter break, they had organized the details of their exploit into both a paper and presentation and registered to present it at an IEEE computer conference later in the summer. Upon learning of this, the MBTA filed a lawsuit against the students, and the judge issued a court order preventing the students from discussing the issue publicly. Therefore, the students' presentation was cancelled, and they were forbidden from distributing their research. For the purposes of this paper, I will be assuming the role of one of the three students that exploited the MBTA's software and wrote a research paper about it. My colleagues and I are now debating whether we should circulate the works of our research online.

You may, but are not required to, add extra details like this to the scenario. Since these are fabricated, there's no citation needed.

If you choose to add real-world information outside of the scenario, it is cited in APA format in-line.

Thesis is extremely clear, identifying the exact decision to be made and the role from which you will make it.

Scenario Brainstorming

You may, but are not required to, use headings to differentiate sections of your paper.

Follow the 9.3.1 Methodology. Introduce each stakeholder, their rights, and how they may benefit or suffer from the current situation.

There are multiple parties involved in this situation, perhaps the clearest among them being the students themselves. Their discoveries come with huge potential for their future careers in software development and security and may pave a pathway for good positions in companies upon graduation. Additionally, as Americans, they have **the First Amendment right to free speech** and, therefore, to also share their discoveries if they desire—the exception being a court order or any form of law enforcement forbidding it, if there is a lawsuit or trial involved (Potasznik, Day 6). The court and law enforcement officials are, however, not above the law itself, and should be subject to scrutiny if their orders infringe upon the rights of any party as determined by pre-existing laws. Another clear stakeholder is the MBTA, which can be negatively affected by the students' discoveries via press coverage of their weak security system. Additionally, if the method the students used to hack the system is leaked, and the MBTA does not, or is unable to fix this vulnerability, some passengers may be able to get free rides, potentially reducing the MBTA's income. Of course, the MBTA has the right to be safe from hacking, as stated in the **CFAA, the Computer Fraud and Abuse Act**, which illegalizes computer access without authorization (Potasznik, Day 12)—an act that the students do not deny doing.

Class terms and legal considerations are defined and explained where applicable. Definitions are cited accordingly.

Class terms and legal considerations are defined and explained where applicable. Definitions are cited accordingly.

Continue the 9.3.1 Methodology. Introduce the next stakeholder, their rights, and how they may benefit or suffer from the current situation.

Other noteworthy stakeholders include the MBTA passengers and Massachusetts taxpayers. State taxes provide funding for the MBTA (Powers, 2013), so taxpayers have the right to be assured that the MBTA handles their software correctly and does not ignore anything that might suggest a major flaw in the system. If the MBTA has to raise its fares because of potential significant harm from the freeloaders, the honest passengers will be harmed while the others will continue to bypass payment. It is the right of the customers that the MBTA ensures that everyone pays fairly.

If you choose to add real-world information outside of the scenario, it is cited in APA format in-line.

Finally, MIT is also an involved entity in this case. Depending on how involved MIT was with the students' projects, it may be subject to liability. If MIT provided resources that the students used to hack the MBTA's software, it may be required to deal with lawyers and court questioning, similar to what happened with the Aaron Swartz case in the very same institute. Aaron Swartz used MIT's servers to access and distribute copyrighted articles from JSTOR, causing MIT to be in direct communication with them regarding the incident (Potasznik, Day 12). Additionally, in our case, MIT might also be subject to liability if a professor mentored the students for this, or if the students hacked the system as part of a class assignment.

Vague or missing information is identified as it arises.

You make assumptions to address the vague or missing information so you can analyze fully.

For the purposes of this project, I will assume that although the students may have learned coding and hacking skills from their classes, MIT, its faculty, staff, and utilities had no further use, involvement, endorsement, or encouragement for the students' actions, nor did the students incur any support from anyone affiliated with MIT. Assuming the role of a student, I can clarify another ambiguity of the scenario: what were the students' intentions, and by extension, what were the contents of the research paper? Did the students exploit the weak security system for personal use or the use of others, to take as many free rides as they like? Or was it in the hopes that the MBTA's security would improve, ensuring fair pay for all? And despite what their intentions may have been, what were the results of their hacking and the scale to which they bypassed subway payment? What were the costs incurred?

Vague or missing information is identified as it arises.

You make assumptions to address the vague or missing information so you can analyze fully.

As a participating student myself, I can assure that we only intended to explore the specifics of the MBTA's weak security so that the MBTA can take the right steps to correct itself. Moreover, our hacking was small-scale, and we only used it for the purpose

of clarifying the flaw in the system. In total, our activities amounted to no more than a few dozen dollars in bypassed fares. Our intentions are in fact reflected in our yet unpublished research paper, in which we not only detail the methods used to manipulate the system, but also outline detailed suggested steps on how to improve the vulnerabilities we found. We, in fact, consider our project to be a work of **hacktivism,** or hacking for a political cause (Potasznik, Day 12) —specifically with the hopes that the MBTA uses its funds more efficiently to provide a smoother, fairer transportation system. Since the system is partially funded by taxpayers, and by extension reflects political decisions, encouraging them in this way can be considered a political goal.

Anything used as a class term is in bold, fully defined, cited, & EXPLICITLY applied to the topic.

It is important to consider whether the MBTA addressed the security weaknesses after realizing that the students were able to bypass it—and also whether they had sufficient time to do so before the students would present their research. In order for we, the students, to fairly label ourselves as "**white-hat hackers**," hacking only for the common good and acting fairly with the party being hacked, we must fulfill **responsible disclosure,** ensuring that the MBTA would have adequate time to address the issue before we publicize it (Potasznik, Day 12). Because we, the students, did not yet publicize our research, and did not yet fully explain the method used to exploit the subway system, the MBTA may still have time to address it before the conference a few months away. In this scenario, I will assume that the students first contacted the MBTA regarding their vulnerability, warning them about the date of the conference a few months away so that they can work on fixing their security system before the exploitation method goes public. This may not be the best way to responsibly disclose the vulnerability—it is likely that the MBTA may need more time to address the issue. Nevertheless, I will

Terms and definitions that come from the same lecture can be combined into one sentence and cited together.

assume that the MBTA chose to pursue a lawsuit against the students before addressing their vulnerability.

Looking at the situation from the MBTA's perspective, since they do not immediately address the vulnerability and attempt to fix it, it is clear that they fear that the distribution of this research will cause several passengers to bypass payments. However, it is important to point out the ***post hoc ergo propter hoc*** fallacy—as it pertains to this case, if there is a way to bypass paying for the subway that surfaces after this research, it does not mean that this research is the cause for it (Potasnik, Day 3). Rather, the cause would be that the MBTA itself did not address their vulnerability or did not notice it before the students did. The students found the weakness, exploited it a few times to discover its cause and potential ways to fix it, and presented it to the MBTA as a warning before their publication later in the year.

You consider various points of view. Your own points and ideas are analyzed and synthesized, not simply mentioned or summarized. Various elements of different ideas are weighed against others.

Another issue to deliberate is the type of order issued by the court against the students. I will assume that it is specifically a gag order, which is typically issued before a trial to ensure that both parties have their right to a fair and impartial jury, without any biases due to discussions about the case from the press (Strickland, n.d.). Although the gag orders are typically issued pre-trial, they are sometimes used post-trials in an attempt to guard trade secrets, as it was in this case to protect the MBTA. The gag order has the potential of inducing a **chilling effect** on the students, or the restriction on the students' First Amendment Free Speech rights, preventing them from discussing their project in any forum and restricting the distribution of their research (Potasznik, Day 6). On the other hand, the gag order may potentially prove to have the opposite desired effect on the MBTA and the students. Instead of suppressing the students' research and hiding the

MBTA's flaw, the gag order might induce the **Streisand effect,** which is a phenomenon that amplifies a subject matter, exposing it to several more people, once it is attempted to be hidden or censored (Potasznik, Day 3). Since people are generally interested in cases that the government and/or private companies have tried to hide, the Streisand effect is highly likely in a case with clever students, a large network of conference-attending computing professionals, and heavy-handed courts.

Anything used as a class term is in bold, fully defined, cited, & EXPLICITLY applied to the topic.

The contents of this gag order are also important to consider—how much of their research are students not allowed to share? I will be assuming that the students were ordered not to present their findings at any conference, not to share their written research paper, and not to circulate anything involving the details of *how* they exploited the vulnerability. Essentially, they are not allowed to expose or teach anyone else how to bypass the subway payment system.

Option Analysis

You may, but are not required to, use headings to differentiate sections of your paper.

Once the situation at hand has been fully considered, you begin to weigh potential options for solving the problem, including how each option affects each stakeholder and categorizing it as ethically obligatory, acceptable, or prohibited.

The trial is over, and the students now face a choice: what should we do with our research paper? We have a few different options. One, we could disregard the court order and circulate the research online. On the other side of the spectrum, we could decide to completely obey the court order, put our research away, and never discuss it again. Or, we could choose not to distribute our research, but instead choose to publicize our actions—meaning, we could share that we found a vulnerability and show that we were able to bypass the MBTA system, without detailing *how* we did so. A last option would be for us to use their research to work with the MBTA to solve the issue before

publishing their research. I will now analyze each of these options in order to conclude which one is the most ethically correct.

Option 1: Circulating the Research Online

There are **3 things to consider before leaking any information: the type of material, the value to society, and the risks to society and involved individuals** (Potasznik, Day 7). The material in question is the entirety of a research paper whose authors were specifically ordered not to share it. The value to society might be greatly positive or negative. Positively, it would expose the MBTA and therefore put pressure on them to responsibly handle their systems' flaws and prevent possible fare by-passers from getting any more free rides. It could also serve as a warning for other transit systems in different cities to ensure they do not implement this flawed system. On the other hand, if the MBTA does not or is unable to address the issue, several more people might be able to exploit the subway fares, potentially causing significant damage to the MBTA's profits. Consequently, other honest passengers or taxpayers will not be given their due right to fair treatment and the assurance that the given prices are fair.

Consider how each option affects each stakeholder; categorize it as ethically obligatory, acceptable, or prohibited.

The students, as individuals, also face benefits or risks with this option. The most obvious risk, perhaps, is that they may face yet another lawsuit, and this time, since they disobeyed the gag order, they might face serious consequences, including high fines or even jailtime (Strickland, n.d.). On the other hand, some companies may be attracted to their resourcefulness and ingenuity in bypassing the system, and they may be recognized as smart and capable computer scientists, especially in the field of cybersecurity. This may eventually lead to them securing good jobs in the future.

Because of the risks to the MBTA and the students themselves through this option, I would label it as ethically prohibited. Despite the potentially promising recognition the students would receive, they would be harming themselves by directly disobeying a judge's order. They also might be unfairly publicizing the MBTA's issues without giving it adequate time to address them, forgoing any responsible disclosure necessary for ethical hacking.

Clearly justify your reasoning for the categorization you assigned.

Option 2: Keeping Quiet

By keeping quiet and never distributing any detail of their research again, the students would be safe from further lawsuits. Of course, they no longer have the chance of being recognized as capable hackers based on this particular incident, but there are other ways to achieve recognition for their skills if that was their main goal. There are larger risks that come with this option, the first being that the security weakness might remain, especially if the MBTA has no intention on fixing it. This way, others who might have found out about the vulnerability on their own might continue to exploit it for their own benefit, harming both the MBTA's profits and the consequences that come with it—higher prices for those that already pay fairly. Additionally, this option will allow the MBTA to get away with their security issue and it might cause them to believe they can hide their flaws without any accountability, which could open doors for future mistakes.

Consider how each option affects each stakeholder; categorize it as ethically obligatory, acceptable, or prohibited.

I would classify this option as ethically acceptable. The students face no harm from this, and anything that happens after this would be due to the MBTA's mistakes. The students would know of the issue, but having done their duty and alerted the MBTA to it, they are no longer responsible for the consequences of the vulnerability.

Clearly justify your reasoning for the categorization you assigned.

Option 3: Carefully Exposing the Vulnerability

This option would involve taking advantage of the Streisand effect. Instead of sharing their paper, or any details on how they exploited the MBTA's vulnerability, they could use online platforms to share that they found a vulnerability and that they are under a gag order suppressing them from sharing their research on it. They would not be directly disobeying the gag order, since they would not be teaching anyone how to exploit the flaw (based on my previous assumption). Rather, they would be highlighting the flaw in the subway system, the trial they went through, and the MBTA's desire to hide their mistakes. This might cause the case to get a lot of attention and put public pressure on the MBTA to address the issue without necessarily exposing how to bypass the fares. Still, there is no guarantee that the MBTA would be able to solve the issue, and it would not be utilizing the students' research which addressed how to solve the issue already. Because this option would result in low risk, high potential benefit, and would not require the students to disobey any orders, I would classify it as ethically acceptable.

Consider how each option affects each stakeholder; categorize it as ethically obligatory, acceptable, or prohibited.

Option 4: Collaboration

If the MBTA agrees to work with the students, the students could use their research to help fix the issue, and once it is fixed they could then share the details of the exploitation and solution in their research publication. This would abide by the ACM/IEEE Code of Ethics and would ensure responsible disclosure (Gotterbarn, 2001). This option has multiple benefits because it would not just expose the MBTA without helping—instead, the students clearly point out a flaw to the authority and work towards fixing it. The taxpayers and train riders benefit from improved security and accurate pricing. Additionally, the students would get the recognition as smart computer scientists

and would be able to publish their research. Due to the low risk of this option and the great benefit, I would classify it as ethically encouraged.

Based on your brainstorming and analysis, make a selection for a course of action. May be derived from one single option considered, or a blend of options.

Synthesis

The first two options—exposing the research or keeping quiet—are the most risky and the least fruitful, respectively. The first would involve not only disobeying an order but also not fulfilling responsible disclosure, potentially harming all stakeholders involved. The second would not produce desirable outcomes because there would be an unaddressed flaw and the students' research would not be utilized. The last two options are thus more desirable. If the MBTA agrees to work with the students, then Option 4 would be the best route. Working together towards fixing the issue would ensure that the vulnerability is solved, and also allow the students to share their research with the additional details on how they fixed the issue. It would not be ethically correct to use the Streisand effect of Option 3 to expose the MBTA if they have agreed to working with the students. However, if they do not decide to cooperate with the students, then Option 3 would be the best way of pressuring the MBTA to fix the vulnerability without teaching others how to exploit it and disobeying the gag order. So, in conclusion, if this were an ideal situation in which the MBTA was willing to cooperate, the option with the highest benefit to all parties would be the fourth, in which the students use their research and their skills to fix the issue they found in the first place. This would encourage unity and collaboration from both sides to the benefit of all, and each side would have something positive to gain.

Reference section follows APA formatting guidelines.

References

Gotterbarn, D, Miller, K, Rogerson, S, Barber, S, Barnes, P, Burnstein, I, Davis, M, El-Kadi, A, Fairweather, NB, Fulghum, M, Jayaram, N, Jewett, T, Kanko, M, Kallman, E, Langford, D, Little, J, Mechler, E, Norman, MJ, Phillips, D, Werth, LH. (2001). *Software Engineering Code of Ethics and Professional Practice*. Science and Engineering Ethics. 7. 231-238. 10.1007/s11948-001-0044-4.

MBTA "Ridership and Service Statistics: Thirteenth Edition 2010" (PDF). MBTA. July 2010. Retrieved May 14, 2020.

Potasznik, A. Fall 2019, CSIT285L. *Day 3 slides.* Retrieved from https://www.dropbox.com/s/fsh3cia5oh08z8o/Day%203.pdf?dl=0 on May 16, 2020.

Potasznik, A. Fall 2019, CSIT285L. *Day 6 slides*. Retrieved from https://cpb-us-w2.wpmucdn.com/blogs.umb.edu/dist/7/3673/files/2018/05/Day-6-1vk4u44.pdf on May 15, 2020.

Potasznik, A. Fall 2019, CSIT285L. *Day 7 slides*. Retrieved from https://www.dropbox.com/s/u5kosfb7zyp860y/Day%207.pptx?dl=0 on May 15, 2020.

Potasznik, A. Fall 2019, CSIT285L. *Day 12 slides*. Retrieved from https://cpb-us-w2.wpmucdn.com/blogs.umb.edu/dist/7/3673/files/2018/05/Day-12-2hrw1xg.pdf on May 15, 2020.

Powers, J. (July 28, 2013). "What you need to know about the state's new transportation law". *Boston Globe*. Retrieved August 28, 2013.

Strickland, R.A. N.d., The First Amendment Encyclopedia. *Gag Orders.* Retrieved from https://www.mtsu.edu/first-amendment/article/961/gag-orders on May 15, 2020.