Honors Capstone Reflective Critique

Grant McDonel

November 30, 2023

Introduction

Researching and writing my Honors Capstone Project was one of the best experiences I have had as a Radford University student. Having the opportunity to do research on a topic relating to my field was not only a privilege, but also quite fulfilling and very helpful for the process of my development into a professional in the field of cybersecurity. My project, "A Policy Solution for Protecting PII on the RU Cloud", led me to do deep research into state, national, and international data privacy laws, corporate policies protecting against legal liability, and several US civil court cases relating to breaches in data privacy. The proposal I introduced in this project was that smaller institutions who make use of cloud-based data storage via large cloud service providers (CSPs) should create their own institution-level policies to help protect their own personally identifiable information (PII) which is stored and curated by CSPs. These policies would serve to protect those smaller institutions in the event of any legal litigation that may occur as a result of a data breach against a CSP that exposes that PII, bringing harm to the institution whose PII was exposed. In this reflective essay, I will discuss some of the strengths and weaknesses of my capstone project, as well as some additional research that I would have done to strengthen the weaker portions of the project.

Strengths

I will begin by analyzing the stronger points of my capstone project. The most well-researched portion of the project was that of corporate safe harbor policies, annual SEC Form 10-K reports created by large CSPs, as well as federal and international laws relating to cloud security. Showcasing how these CSPs use safe harbor policies and other regulations to avoid legal action resulting from data breaches that exposed their customers' PII, I made a strong case revealing the background of why the policy-based solution I proposed was important. I discussed how many CSPs' main concern is becoming subject to civil or criminal liability that would result in reputational damage, and how compliance with newer cloud regulations set by various governments impedes their commercial operations. These regulations, such as the EU's General Data Protection Regulation (GDPR) and several US state-level data privacy laws, were the foundation to this project, as my ultimate vision is to see these governments enacting new laws in the future that elevate the legal standing of cloud users. Doing so would allow those users to have a greater chance of winning civil suits against CSPs that did not ensure proper protection of their customers' PII.

Another subject I researched quite extensively was US case law relating to breaches in PII stored by CSPs. Most of these cases were class-action lawsuits brought up by customers whose personal data was lost, stolen, or tampered with as a result of a cyber attack against their respective CSP. Unfortunately for those customers, the CSPs would win these cases much more often due to the corporate policies and business strategies I mentioned earlier, as well as some legal precedents that tipped the scales in favor of the defending corporations. One of these precedents, known as “injury-in-fact”, first appeared in the 2009 US Supreme Court case Kerchner v. Obama, a case that had nothing to do with cloud security, but that influenced several class-action lawsuits brought against CSPs in the years following its conclusion. Injury-in-fact makes it so that the plaintiffs of these data breach cases are required to provide concrete evidence that the theft of their personal data caused them either direct or “certainly impending” harm, which can be quite difficult for the plaintiffs of a class-action suit to provide as the average cloud user does not spend much of their time closely monitoring how their PII is being handled. The background I created for this project from gathering research on court cases, regulations, and policies formed a strong foundation for the policy proposal that I made in the latter section of my research paper.

Weaknesses

Now that I have discussed the strengths of my Honors Capstone Project, I will also analyze some of the weaknesses in my proposal that I have noted since the project’s completion. One missing piece of information that I wish I had discussed more in the original project was that I focused so much on creating a brand-new solution to this problem, that I did not do any research into an already-existing solution to the problem. My proposal was that smaller institutions should create data privacy policies to protect themselves in civil court against CSPs, but the already-existing solution to this problem is that many institutions simply invest in cybersecurity insurance to protect themselves from losing large amounts of data and money following a breach on their CSP. The insurance solution is easier to implement, as it is an established concept that institutions would find easier to understand and fit into their budgets. Policy solutions often take much longer to put into place and require lawyers and policy specialists to be involved to ensure everything is done correctly and legally throughout the process. If I were to continue working on my capstone project, I would open an entirely new avenue of research about cybersecurity insurance, and likely add a new section to the paper comparing the advantages and disadvantages of my new idea against the established idea of cybersecurity insurance.

There is also a complication involved with the policy solution I proposed which I mentioned in my research paper, but into which I should have put much more research and discussion. That complication is the fact that a CSP would not be very willing to accept the implementation of a policy created by one of their own customers that actively works against their own interests. To reconcile this issue, business negotiations between the institution creating the policy and the CSP would need to be opened, and those negotiations would likely be quite complex, time-consuming, and expensive. I would need to do more research into the processes behind business negotiations and figure out a potential line of arguments to convince CSPs to agree to the implementation of a cloud security policy like the one I proposed. Additionally, I did not go very deep into the policymaking process itself, so more research would definitely be needed there as well.

Conclusion

Overall, I think the research I did for this capstone project provided me with a strong foundation for my proposed solution, but the solution itself could have used more development and research to sound fully convincing. In this essay, I identified the strengths and weaknesses in my project, as well as the topics of research that would be required to bolster my argument for an institution-based policy solution for cloud security. I would like to thank the Radford University Honors College for providing its students with the opportunity to conduct research projects that are significant to their respective fields of study. It was a privilege to be given the proper resources and guidance for doing undergraduate research at a level of innovation that cannot be found at many other universities.