Bridge Rehabilitation/Replacement using Accelerated Bridge Construction Methods
(Technical Report)

Smart Security: effects and financial impact Charlottesville

(STS Research Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Miguel de Obaldia

Fall, 2019

Technical Project Team Members

Submitted By: Avery Davis, Beau Gutridge, Ben Redfern, Collin Shepard, Edler Saint-Jean, Jacob Hegemier, Miguel Ricardo de Obaldia, Sam Cave, Tommy Blankinship, Marc Michaud

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature _____ Date _____

Miguel de Obaldia

Approved _____ Date _____

Lindsay Ivey Burden, Department of Civil Engineering

Approved _____ Date _____

Sean Ferguson, Department of Engineering and Society

Prospectus

The Center of Strategic and Internal Studies (CSIS) published a report on the economic impact of cybercrime. They estimate that, worldwide, there were between 445 and 608 billion dollars spent on battling cybercrime on 2017. Dixon (2014) states “State and local government spending on information goods and services is projected to grow at a 3.3 percent rate between now and 2019, increasing to $70 billion from $60.4 billion over that period.” These numbers show how much cyber-attacks are affecting people on a daily basis and a lot of the people being impacted have no clue that they are at risk. Educating people about the existence of this threat could help them learn how to prevent exposing themselves to this type of problem. Not only individuals, but also entities and businesses who could be potential targets, so learning about this issue is important for everyone.

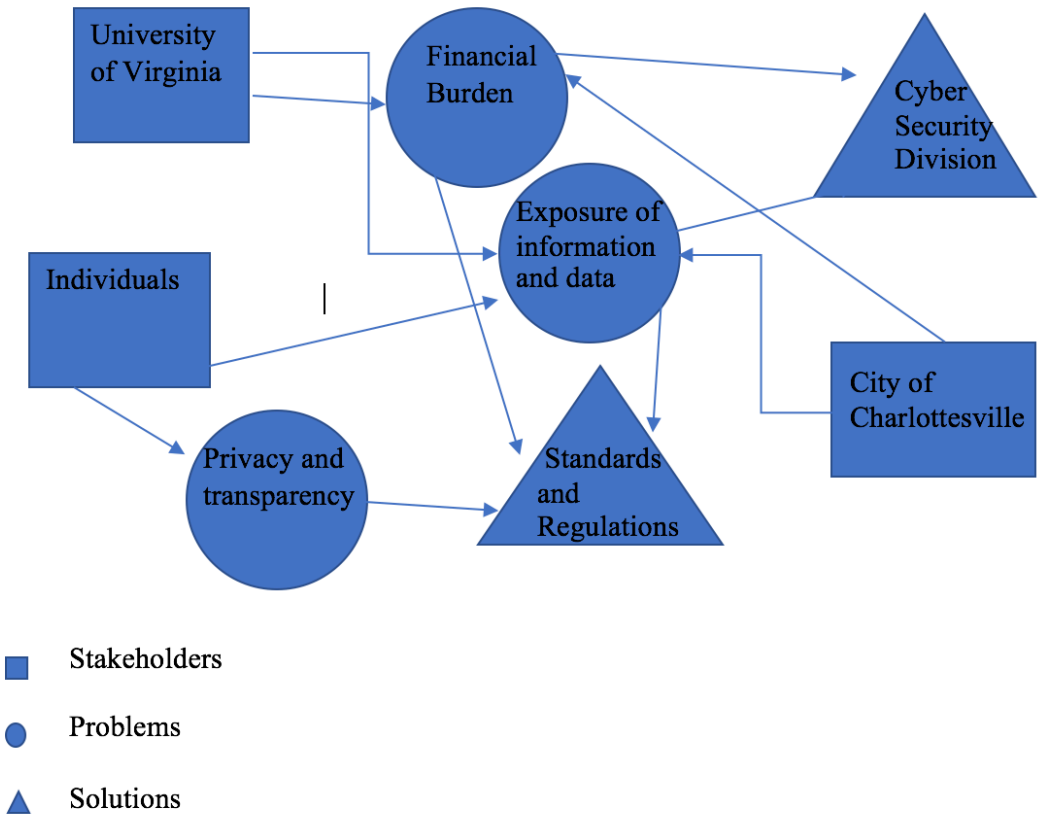
My research on the topic will be focused on information and solutions in the area of Charlottesville and the United States. The goal of my research is to find the different solutions being implemented by the city of Charlottesville to prevent exposure of its citizens’ information and use this information to look for other possible solutions and ways to manage the current situation. Although Charlottesville is a small city, earlier this year it was target of a cyber incident and government entities have been voicing their concern on the growing issue.

In September of this year, an email hack of a City Hall employee may have exposed the personal information of 10,700 utility billing customers. Right now, the government is in the process of notifying those affected and is trying to understand the ramifications of this attack.

NBC estimated that the city of Charlottesville spent $450,000 and Albemarle County spent $231,477.39 over the last five years battling cyber security. Although the numbers do not seem like a lot of money, the attacks keep becoming more and more frequent, meaning that the amount spent to protect the counties will be on the rise. Government officials have made statements talking about the matter, to let the citizens know it is an actual issue, and are taking advantage of this opportunity to provide training about the topic to employees, so that everyone is conscious about their part in avoiding future attacks.

Not only authorities have been aware of the issue, the University of Virginia has been silently working towards becoming less vulnerable to malware and hackers. Professor Yonghwi Kwon has been conducting research for the university on methods to protect and identify hackers and malware, and also doing research to build more reliable and safe networks. When he asked about the challenge of his research, he said: “Manually patching the vulnerabilities cannot keep up with the emerging cyber-attack trend. In the department of Computer Science at UVA, we are developing automated techniques that analyze insecure programs and make them secure.” Granting a professor’s research on this topic demonstrates the concern the university feels about the threat and the emphasis they are placing on trying to prevent exposure to future attacks. Kwon is working with professors from other universities to develop different platforms that not only identify intruders and malware, but also protect the content with firewall and VPNs to make it harder to access information.

It is clear that powerful entities and organizations inside the city of Charlottesville are conscious of the issue and are slowly working towards finding a long-lasting solution. As of today, the city of Charlottesville officials have not found an instant solution for this concern from a governmental standpoint but keep looking for answers. In the meanwhile, they are patching up their vulnerabilities by educating their employees and letting citizens now about the problem. To contribute with the city, the private sector is also looking for solutions. Last year, a company in Charlottesville called Mission Secure received $8 million worth of funding and their goal as a company is to help companies, entities, and individuals be more secure. Seeing how the government, the private sector, and an academic organization from the same city are all searching for answers on this issue shows how threatened the city feels about the risk.



The SCOT diagram above shows what I evaluated to be the most important stakeholders, problems, and solutions for Smart Security in the city of Charlottesville. I added UVA as one of my main stakeholders because the university is a very influential partner in the city. Noris, Mateczun, Joshi, & Finin, (2017) found "that local governments are under fairly constant cyberattack and are periodically breached. They are not especially well prepared to prevent cyberattacks or to recover when breached". Noris et al (2017) also states that the principal barriers to local cybersecurity are financial and organizations. In addition, Norris, Mateczun, Joshi, & Finin (2018) focus group of IT and cybersecurity officials noted that "local governments face several barriers in providing high levels of cybersecurity, including: insufficient funding and staffing; problems of governance; and insufficient or under-enforced cybersecurity policies." Charlottesville is not the exception. According to Noris et al (2018) "Participants suggested several ways to improve local government cybersecurity, including: vulnerability assessment, scanning and testing, cybersecurity insurance, improving end-user authentication and authorization, end-user training and control, control over the use of external devices, and improved governance methods, among others." As of today, the City of Charlottesville has no division or department that specializes in dealing with cyberattacks, hackers or malware. Having a committee of representatives from different entities (police, fire, utilities, City Hall), institutions (UVA), and the private sector that are committed to dealing with active threats and preventing futures attacks would be the most efficient way of pooling resources and finding solutions. This committee would also be responsible for issuing standards and regulations to help prevent exposure of data of companies and individuals. An example of these standards would be requiring VPN usage mandatory for public Wi-Fi service, to ensure users privacy and information security. Community involvement in the process of developing

the standards and regulations is of extreme importance, so the general public agrees and understands the purpose and extent of these policies.

Bibliography:

1. Lewis, James. “Economic Impact of Cybercrime - No Slowing Down.” Feb. 2018.
2. Mishal Alashari. “Accelerated Bridge Construction, A Better Approach to Bridge Construction?” Aug. 2016.
3. Tyree, Christopher. “UVA Computer Science Professor Brings the Skills of a Detective to Combat Cyber Attacks.” *University of Virginia School of Engineering and Applied Science*, Christopher Tyree, 17 Oct. 2019.
4. Mandell, Josh, et al. “Local Cyber Startup Backed by New $8 Million Investment • Charlottesville Tomorrow.” • *Charlottesville Tomorrow*.
5. Schroeder, Annie. “Charlottesville Officials Respond to Security Breach, Experts Offer Tips.” *WVIR NBC29 Charlottesville News, Sports, and Weather*.
6. Graff, Henry. “The Costs of Protecting Government Networks from Cyber Attacks.” *WVIR NBC29 Charlottesville News, Sports, and Weather*.
7. Craigen, Dan, et al. “Defining Cybersecurity.” *Technology Innovation Management Review*, vol. 4, no. 10, 2014, pp. 13–21., doi:10.22215/timreview835.
8. Norris, D. F., L. Mateczun, A. Joshi, and T. Finin. 2017. *Cybersecurity Challenges to American Local Governments: Results of a National Survey*. A paper presented at the 17th Conference on Digital Government. June 13–14, 2017. Lisbon, Portugal and printed in the conference proceedings.
9. Dixon, C. (2014, August 24). Deltek: State, local government IT spending increase is an opportunity for contractors. *The Washington Post*. Retrieved from https://www.washingtonpost.com/business/capitalbusiness/deltek-state-local-government-it-spending-increase-is-an-opportunity-for-contractors/2014/08/22/4f6f0834-288d-11e4-8593-da634b334390_story.html
10. **Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity**
    Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin
    Public Administration Review, 2019