Defending Democracy: Cybersecurity in Elections

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Madeleine Ashby

Fall, 2022

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

Rosanne Vrugtman, Department of Computer Science

Defending Democracy: Cybersecurity in Elections

CS4991 Capstone Report, 2022

Madeleine Ashby
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
mra4t@virginia.edu

ABSTRACT
Starting with the recount in the 2001 Presidential Election and exacerbated by foreign interference in the 2016 Presidential Election, public trust in the United States electoral system is at an all-time low in 2022. In an effort to restore trust, the Virginia Department of Elections called for interns in Virginian universities to work with localities across the state in their cybersecurity and information technology departments to improve cybersecurity performance. This was achieved through a variety of means, all of which were intended to spread awareness of and eliminate both potential and actual vulnerabilities. The Virginia Department of Elections uses the Locality Election Security Standards (LESS) to measure localities' compliance with cybersecurity standards each year. Interns spent much of their time researching good cybersecurity practices and election administration in order to develop county-wide policies that established strategies for incident prevention and precedent for any future security incidents. This internship program ultimately achieved its goal of strengthening national security at the local level, as indicated by a far higher compliance score with LESS across the board. Future work would include further experience in the field for both interns and locality IT departments, and additional research into specific threats and vulnerabilities as technologies progress.

1. INTRODUCTION

Recently, the biggest contributor to accessible, democratic elections has been the advancement of voting technologies. However, the drawback to such rapid progress is that the machines are often deployed with insufficient testing, which renders them vulnerable to cyber-attacks, ultimately becoming a huge weakness to elections where they were supposed to be a strength.

2. RELATED WORKS

Agawu (2018) argues that Russian interference in the 2016 election was only the beginning, and that future elections may bring new adversaries—such as China or North Korea—with sophisticated (and superior) cyber operations. This discussion was incorporated into my internship project in that we explored both internal and external threats to the election system at the local level. This was mainly done by performing risk assessments to reveal new or unexpected threats and vulnerabilities.

Deluzio (2019) proposes four modifications to improve the current system, with particular emphasis on the relationship between election officials and vendors. Specifically, he recommends:

1. mandating patching and software updates for vendors to assure that vulnerabilities and weaknesses are addressed;
2. conducting security assessments and audits to ensure vendor compliance with regulations;
3. conducting regular penetration testing for continual vulnerability scans; and
4. normalizing transparency from vendors in their ownership and affiliation affecting their operations.

My internship project incorporated these ideas by writing them into relevant policies and plans by which the locality abides.

Fiddler (2017) argues that change must occur immediately. He further states that prioritizing cybersecurity at the international level will allow for harmonized policies addressing election cybersecurity, ultimately helping secure our elections. While we could not extend our influence into the international realm, we did open lines of communication with other localities in Virginia to promote unified cybersecurity policies.

3. PROJECT DESIGN

A thorough understanding of election infrastructure and locality deficiencies is necessary to understand the context of my work.

3.1 Review of Election Infrastructure

Fair and free elections are critical to the nation's democracy, and there are several components that make such elections possible. The Voter Registration Database (VRDB) is the foundation of the election system in Virginia, as it contains records of every registered voter in the state. This is important because the database is accessed by poll workers on Election Day to check voters in and ensure that they are actually registered to vote. The registration records are easily accessible via pollbooks, which can be paper or electronic. After being checked in, the voter will proceed to cast their vote; this can also be done on paper or electronically. Finally, the ballots are cast via some sort of ballot box, most frequently electronic scanners and tabulators. At the end of the night, the locality's General Registrar will record the final tally in an online statewide system called Integra.

Without proper precautions and mitigation, this process can fall victim to cyber threats. As a result, the Virginia Department of Elections created the Locality Election Security Standards (LESS). There are 22 specific standards, each of which consists of several categories and sub-standards. When fully met, these standards ensure secure elections. In March of every year, every locality must report their current state of compliance using Integra, and each locality's compliance is then measured by a score which indicates the total percentage of the standards that are currently being met.

3.2 Motivation

The Cybernavigator Internship Program partnered with 17 localities in Virginia who struggled with one or more of the following problems pertaining to LESS:

1. very little documentation of policy, if any;
2. a lack of knowledge of what to do in case of an incident;
3. a general lack of awareness of cybersecurity and its importance in all county departments; and
4. a shortage of trained employees to make the necessary changes.

All of these problems contribute to low compliance scores and thus serve as a weakness to election security.

3.3 Taking Action

To remedy these deficiencies, interns were paired with individual localities to better meet specific needs in order to raise compliance scores. My locality had a particularly low compliance score with LESS because they had no documentation of policy and, in some cases, no idea of what to do in case of emergency. Further, they lacked several tools necessary to provide a secure working environment. Thus, my team's goals for this summer were:

1. to create and document policies and plans outlined in LESS;
2. to increase physical security on-site through physical risk assessments; and
3. to provide security recommendations (tools, softwares, etc.) to enhance employees' security in their everyday operations.

To meet the first objective, my team created eight lengthy deliverables during the two month program: an Acceptable Use Policy; an Incident Response Plan; a Password Management Policy;

a Personnel Security Management Policy; a Non-Disclosure Agreement; an Access Control Policy; a Security Awareness and Training Policy; and a Continuity of Operations Plan. Each of these documents served a unique purpose in outlining non-negotiable rules regarding their respective LESS category and/or a plan of action in case of emergency.

To meet the second objective, I toured the facility extensively to perform a physical risk assessment. Specifically, I was assessing the server room, voting equipment storage room, and election office for physical threats to the wires and computers, voting machines, and paper files, respectively. Examples of potential threats include fire hazards, sprinklers over paper files and/or machines, and environments of extreme temperatures and humidity levels.

To meet the third objective, I documented areas of deficiency when developing policies and conducting my risk assessment. Toward the end of the program, I began to explore these pitfalls to better understand how to resolve them. From here, I was able to assess and evaluate potential solutions based on key considerations for each problem, and decide upon an optimal solution. In many cases, I had to consider cost and ease of use throughout the locality. For example, one large component that the locality lacked was a security awareness training program. I searched for a provider that would allow for easy online distribution, completion tracking, and comprehensive modules, and eventually settled on KnowBe4. Among many, other notable shortcomings included a lack of password management software and a lack of a virtual private network from which to access locality systems remotely.

3.4 Challenges

The most prominent challenge that my team repeatedly faced throughout the internship was the strong dependency on knowledge of the current state of the locality without being permanent or long-term employees. Moreover, a thorough lack of documentation proved difficult in that we had to start every task from scratch with very little guidance. However, we did want every policy and plan to accurately reflect any non-documented procedures that may have existed. Thus, a lot of time was required to explain the importance and purpose of each document to the locality supervisors in non-technical terms and fully understand how they wished to implement and adapt the policies to the locality.

4. RESULTS

Upon completion of this program, all of my team's documents were sent to the Board of Supervisors for approval, all of which have since been approved. As a result, my work has benefitted the elections office by increasing security measures and creating contingency plans. This is shown in the current LESS compliance score projection being double what it was in June. On a larger scale, my work has also benefited the entire locality in that security awareness is increasing. This is shown in the fact that the percentage of failed cyber threat tests is plummeting and all employees have completed their assigned security awareness onboarding training.

5. CONCLUSION

Understanding our election system and its vulnerabilities is crucial to ensure safe and secure elections in the future. In 2016, we saw evidence of foreign interference in our elections, and if we do not begin to take preventative and mitigative actions now, we will certainly see it again soon. The work done by Cybernavigator interns this summer was only the beginning, but has played a catalytic role in jumpstarting localities' cybersecurity policies, practices, and awareness that will boost LESS scores in years to come.

6. FUTURE WORK

Full compliance with LESS will guarantee a secure election system, but this goal is not immediately achievable without additional aid. Many localities (especially those in more rural areas) only have a handful of information

technology (IT) employees for the entire county – let alone the elections department – and lack funding to bring in external IT contractors. To ameliorate this problem, the Cybernavigators program should increase in size to better accommodate the needs of each locality. Not only would this allow for more interns to be assigned to each locality, but it would also allow for more localities to enter the program and receive the help they need.

Another way in which this work could be expanded upon would be for the Virginia Department of Elections to release smaller subsets of LESS each year that they feel are most necessary given the current state of election technology and perceived threats. Using the smaller set of standards would allow for a shorter mandated timeline to reach compliance through a minimized scope which maintains emphasis on the most vital aspects.

REFERENCES

[1] Agawu, E. A. (2018). The 2016 Election and the Response. *In How To Think About Election Cybersecurity: A Guide for Policymakers* (pp. 6–14). New America. http://www.jstor.org/stable/resrep17622.5

[2] Fidler, D. P. (2017). *Transforming Election Cybersecurity*. Council on Foreign Relations. http://www.jstor.org/stable/resrep29928

[3] Deluzio, C. (2019). *A Procurement Guide for Better Election Cybersecurity*. Brennan Center for Justice. http://www.jstor.org/stable/resrep28491