Group Project #1 Final Paper

Prepared for Information Assurance (INFO712)

Drexel University

March 17, 2019

Topic - Electronic Voting Systems

Members:
Kavya Kumar
Corey Mee
Albert Lin
Shubham Garg

Table of contents

Abstract

1. **Introduction**
2. **Research Methods**
3. **Traditional vs. E-Voting**
4. **Voting Perception**
5. **Policies and Standards**
6. **Advantages and Pros**
7. **Challenges and Cons**
8. **Risks**
9. **Results and Conclusion**
10. **Bibliography**

Abstract

1. Voting Perception

Voting with e-voting technologies is unfamiliar to many voters. When using newer technologies, voters would need to have a high degree of trust and willingness to take risks when using them. Voters' familiarity with the technology and sense of trust in it operating as expected would come together in forming individuals' attitudes and behaviors (Lippert & Ojumu, 2008, p. 63). If some individuals are interested in trying out the e-voting technology, then sooner or later, other people in their social groups would be willing to try it themselves (Lippert & Ojumu, 2008, p. 64). The extent to which individuals are open to trying out the newer e-voting technology can influence their willingness to vote electronically (Lippert & Ojumu, 2008, p. 65). People who have limited trust in the technology and intention to use it are often unwilling to vote electronically (Lippert & Ojumu, 2008, p. 69). Some individuals are vigilant in adopting the new voting technology (Lippert & Ojumu, 2008, p. 71).

The level of trust for constituents in the security of the electronic voting technology is a major consideration in their willingness to try voting electronically. Security issues that developers of the systems would need to address include invasion of privacy, misuse of voting records, or misrepresentation of voters' intentions as the electronic systems emerge. If voters trust the electronic voting systems to protect them from harm, then they would more likely consider them convenient, efficient, and accurate. Systems with very little or no history of errors or unauthorized disclosures would more easily be perceived as secure and favorable by voters (Lippert & Ojumu, 2008, p. 72). Security, accuracy, and privacy are all important issues for e-voting systems related to trust in the technology (Lippert & Ojumu, 2008, p. 74).

Voting is a process in which citizens choose whom they wish to represent and lead them. Many jurisdictions have been transitioning from paper ballots to electronic voting. However, electronic voting

carries several risks of vulnerabilities to attacks, compromising the security and integrity of the voting process. There is no consistent method across the United States or throughout Pennsylvania. Numerous resources were used to analyze electronic voting in the United States and Pennsylvania. Various traditional and electronic voting systems were discussed. Trust in newer technology influences voters' willingness to vote electronically. There are several requirements that electronic voting systems must satisfy to ensure security and integrity. Various advantages and disadvantages of electronic voting were analyzed. As technology continues to advance, security measures should also be updated to protect confidentiality and integrity of elections. There is still room for improvement in the voting policies and standards.

2. Introduction

Throughout history, elections have been held all over the world using various means and methods of voting in order to determine outcomes in a fair and democratic manner. From paper ballots to electronic voting, to the possibility of online voting in the future, the growth in the world of technology makes it more and more difficult to ensure that elections and the data collected on ballots is secure. In recent times, there has been fear that outside influences are having an effect on the outcome of elections, and some of the current means of voting have little to no defense against these kinds of attacks. In order for elections to be fair and democratic, there need to be policies and standards in place to help ensure that data is collected in a secure manner and that it is secure throughout the entire election process. Security from outside influences is imperative, and voters must feel that elections are fair and that the winners of the elections are an accurate reflection of the votes cast.

In the United States, standards and policies for voting are delegated to the state level. Rather than having one standard voting policy, each state creates its own legislation that dictates how elections are

carried out. From laws around registration to voter identification laws, the states decide the processes for each. This includes the actual voting methods, which also differ across state lines, and often times, they differ within the states themselves. While some larger jurisdictions use electronic voting systems, there are smaller jurisdictions still relying on paper ballots and sometimes counting these paper ballots by hand. Because of the lack of standardization, the ability to ensure that voting data is kept secure becomes increasingly more difficult. This can have a profound impact on voter confidence, and thus voting systems need to continue to improve and provide a level of trust for the voting population.

The goal of this report is to examine and analyze the current standards, policies, and securities of electronic voting systems in Pennsylvania. Once identified, an explanation of the pros and cons of these standards and policies will be provided in detail. The goal is to be able to conclude with recommendations for changes, improvements and standardizing policies.

3. Research Methods

Various academic publications have analyzed the security vulnerabilities in the electronic voting system. For this research project, several different research methods were utilized. First, many databases that are available through the Drexel Library were used in order to collect and analyze various recognized and legitimate journals related to the chosen topic. Also, search engines, such as Google, were utilized in order to find other scholarly and reputable resources to help better understand and analyze the electronic voting policies within the United States. Also, many government websites, along with those of other organizations, such as the National Conference of State Legislatures, were used to analyze the current policies in place for electronic voting systems. So far, resources have been found through various organizations' websites, which discuss both federal and state policies. Lastly, several cases, in which

current policies have failed, were found and analyzed. Then, suggestions for policy improvement will be made, while also applying course materials and teachings.

4. Traditional vs. E-Voting

In the United States, there is currently no standard voting method. The states have the right to choose the method or methods that they see fit and are responsible for enacting and enforcing these methods and policies. While many people initially thought the move towards electronic voting was the future, there has been a reemergence in paper ballot popularity. Because of this, as well as the responsibility being at the state level, there are several different voting methods currently in use in the United States. Discussed in this section will be the different types of voting methods along with the vulnerabilities of the older paper voting methods.

One voting method used in the United States is optical scan paper ballot systems. This system is paper-based, but electronic scanning devices are used to tabulate the votes after voters have marked their votes on paper ballots. The devices can be located at the voting site or ballots can be collected in a ballot box and tabulated at a central location. Two paper-based VVSs (voting verification systems) are direct VVSs, and end-to-end verifiable VVSs. Direct VVSs use paper ballots to allow individual and overall verification with paper audit trails. End-to-end VVSs generate a receipt for voters to take home and confirm that their votes were tallied accurately (Jardí-Cedó, Pujol-Ahulló, Castellà-Roca, & Viejo, 2012, p. 995).

Another voting method that combines both technology and paper ballots is the Ballot Marking Device. These devices allow voters to record their votes on an electronic screen, and once the voters are finished, they will print out paper ballots with their selections. The electronic machines can be tablets or

other types of screens, but votes are not saved to memory. These paper ballots are either hand counted, or like the previous method optical scan machines are used to count the ballots. The US voting system has been making a transition from punch cards and paper ballots, and first-generation voting systems to second-generation voting systems known as DRE (direct recording electric) systems (Epstein, 2007, p. 92).

Electronic-based VVSs include process separation-based VVSs, evidence-based VVSs, and end-to-end verifiable VVSs. Process-separation-based VVSs separate the generation and casting parts of the voting process. Evidence-based VVSs record actions of voters while casting their votes and they are invisible to the voters. Recorded actions are stored outside the voting terminal to ensure information integrity (Jardí-Cedó, Pujol-Ahulló, Castellà-Roca, & Viejo, 2012, p. 997). End-to-end verifiable VVSs encrypt votes and generate paper receipts to let voters confirm that their votes were counted in the tally process (Jardí-Cedó, Pujol-Ahulló, Castellà-Roca, & Viejo, 2012, p. 998).

The only fully electronic method used in the United States is the Direct-Recording Electronic voting machines which can be abbreviated as DRE. According to the NCSL, these machines are "designed to allow a direct vote on the machine by the manual touch of a screen, monitor, wheel, or other device"(Voting Equipment, 2018).. DRE machines record the votes and total the votes into a computer memory, thus there is no paper ballot. In some cases, these machines will provide a paper copy for the voter to review prior to casting their vote providing an extra layer of accuracy.

Lastly, in some cases states still use paper ballots that are counted by hand without the use of any technology. This is typically practiced in smaller jurisdictions, while in some cases it is only used to count absentee ballots and provisional ballots (Voting Equipment, 2018).

Traditional paper voting system had several vulnerabilities which was a motivation for electronic voting. For example, vulnerabilities associated with the punch card system and optical scan systems used in

the election process. There are two consequences namely undervote and overvote. In case of punch card system, undervote is when the holes are incompletely punched and overvote is when the voter punches too many hole. In later case, undervote is when the voters' marks are illegible and overvote is when the the voter makes too many marks. In all the above cases, it is not possible to identify the voters intent and the vote goes uncounted. Also, manual recounting can be used to consider the uncounted ballots, but it is tedious work. The consequences are referred to as error rates and from State of Florida's analysis in 2000 elections, the error rate for optical scan ballots was 5.68% and error rate for punch cards was 3.93%.

5. Policies and Standards

Voter Identification

Voting policies within the United States are enacted and enforced primarily at the state level, and because of this voter identification laws vary by state. As of February 11, 2019, there are a total of 35 states that enforce identification requirements for voters with 17 of those requiring photo identification (Voter identification laws by state, n.d.). The remaining 18 accept other forms of identification, which leaves 15 states that do not require identification. Pennsylvania falls into the category that does not require photo identification. However, legislators have been working to pass legislation that would require Pennsylvanian's to show photo identification at the polls. In 2012, Governor Tom Corbett signed into law a Voter ID Law which was challenged and later struck down in 2014 and thus was never fully enforced (Voting in Pennsylvania, n.d.).

Requirements

Essential requirements for voting process needs to satisfy every participant in the election, and so that they can sense it is fair. Ensuring each vote is recorded and counted truthfully. Verifying the data through the use of traceable information paths and keep track of the count regularly and individuals' records not mimicked. The most critical one is to guard the sites and voting machines against manipulation and interference on the voting data. One requirement of electronic voting system is secrecy and anonymity, in which no election official or third party should be able to find out how any individual voter voted. Election officials and members of the community should not have the capability to alter the results. The system should be equipped with the capability of confirming that all votes are tallied as each voter selected. The system should be simple and straightforward to be managed by poll workers who do not have technical expertise and with minimal training. It should also be usable by anyone in the general public, including those with disabilities and non-English speakers. The system should also be error-limiting by making it hard for voters to accidentally vote for two candidates in the same race. The voting equipment should also be a low cost for purchasing, maintaining and operating (Epstein, 2007, p. 92). There are several security requirements for the voting system to be efficient across the nation. It is the responsibility of the system developers to build the system that allows only eligible and authorized voters to cast the vote. Also, the link between the vote and the voter who casted it must remain private in the voting application. For this to be achieved, cryptographic techniques could be used in place. The integrity of the vote casted must be maintained, in other words, the vote casted must not be modified or deleted by third parties with malicious intent. Uniqueness plays an important role in a way that each voter casts only one vote, only one time. When thinking about the motivation for the electronic voting system, receipt freeness is one of the important aspect to consider. While the voting systems focus on this requirement, individual verifiability or

the ability to prove to the voters that their vote casted is same as what intended could be difficult. (Nguyen, & Dang, 2013)

Voting Methods

It has already been established that the United States does not have a standard voting method for the country as a whole, and that the states hold the responsibility for enacting and enforcing policies and standards surrounding voting methods. Consistent with the policies at the national level, Pennsylvania also does not have a standard method of voting statewide. The state has some jurisdictions using paper ballots and larger jurisdictions using Direct-Recording Electronic voting machines. However, the machines that are used in Pennsylvania do not provide a paper copy of votes which has recently been called out as a security issue by legislators although it has yet to be addressed. An update to the voting machines would cost taxpayers close to $125 million dollars with minimal support coming from the federal government(Scolforo, 2019).

6. Advantages and Pros

Ease of Use/Benefits

Remote voting or electronic voting makes the voting process more efficient, convenient and attractive. (Nguyen, & Dang, 2013). Electronic voting uses software and hardware to expedite the voting process by allowing individual voters to cast votes from either remote or poll-specific locations through computer information systems (Lippert & Ojumu, 2008, p. 57). Direct-recording electronic (DRE) voting machines with touchscreens systems are versatile and user-friendly voting systems. Ever since 2006, every

polling place was required to have at least one voting machine to be accessible to people with disabilities (Lippert & Ojumu, 2008, p. 60).

Voting Experience

Electronic voting can allow for voters to vote remotely, like using their personal devices, such as mobile phones or PCs (Birch, Cockshott, & Renaud, 2014, p. 187). HandiVote is an open-source voting system that allows voters to confirm that their votes are accurately recorded, without complex coding and decoding processes (Birch, Cockshott, & Renaud, 2014, p. 190). Handivote requires voters to register and assigns a unique voter number with an ID for the first digits and a random PIN for the remaining digits. After the registration period ends, unused voter IDs would be published and registered to make sure they are not used for registering fake votes. Voters would cast their votes by sending a text message that includes their full voter number and their votes. The votes would be counted electronically and published with their voter IDs minus PINs so that voters can confirm that their votes were counted properly. Any unused voter IDs would be published so that fake votes would likely be detected (Birch, Cockshott, & Renaud, 2014, pp. 191-192). Elections Systems & Software (ES&S) is a voting system with several components, including a direct recording election machine (DRE), real-time audit log printer (RTAL), personalized election ballot (PEB), and Compact Flash Card (CFC) (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1619). The DRE has a touchscreen on which individual voters cast votes. RTAL produces a paper audit trail. A PEB is inserted by a poll worker to load a ballot, it collects tabulated data and audit information, and the authenticity is checked by the DRE. A CFC is used to open and close polls and audits the data at the time of closing (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1620). The ES&S system is still subject to attacks by a variety of attackers, such as an outsider, voter, poll worker, or

election official. Some voters might walk away from a voting booth without confirming their votes; therefore, some attackers might change votes in favor of their preferred candidates. Some attackers may interfere with the voting process after voter finish casting their votes and change the selections (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1620). ASTRAL is a specification language designed for complex systems. It allows critical system requirements to be specified and ultimately proves that the system meets the requirements (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1623). RTAL prints when a voter selects or cancels a candidate, as well as beginning and summary information for each voting session (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1625). The DRE machine stores votes and automatically prevents overvotes, but not undervotes. After a ballot is loaded when inserting a PEB, it has to be removed safely by programming an operation for removal and putting it to sleep at the end (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1626). One CFC is used per machine and each one has a unique serial number. When the polls close, the CFC automatically has an audit file saved to it (Weldemariam, Kemmerer, & Villafiorita, 2011, p. 1629).

Counting and validating votes

Another advantage of electronic voting is that they can handle complex procedures and calculations and eliminate human error in the counting process (Birch, Cockshott, & Renaud, 2014, p. 188). With HandiVote, voters would cast their votes by sending a text message that includes their full voter number and their votes. The votes would be counted electronically and published with their voter IDs minus PINs so that voters can confirm that their votes were counted properly. Any unused voter IDs would be published so that fake votes would likely be detected (Birch, Cockshott, & Renaud, 2014, pp. 191-192).

Speed

In the real time, any system that processes a given input in less time is preferred. It is a tedious process to count the paper ballots casted by entire population of the state. By using electronic systems, it is possible to speed up the counting process and reduce the cost of paying the staff to count the votes manually. In electronic voting systems, only the absentee ballots are manually counted.

Low Cost

The total cost for the traditional voting system includes the cost of manual labor for various processes such as managing the ballot box, tangible resources like ballots and other voting essentials, physical space, ensuring the voter environment, setting up the voting ballots and recording with governance. Although the electronic voting includes the extra cost for software development and electronics used, it eliminates manual dependency in most process and uses electronic resources to achieve the same purpose.

Scalability

One consideration in electronic voting is that systems should be able to handle processing large populations of voters at the same time. The systems need to be able to sustain multiple votes since every individual voter casts his or her choices for both national and local representatives. The systems also need to be able to transmit the results in a timely and efficient manner (Lippert & Ojumu, 2008, p. 76).

7. Challenges and Cons

Privacy

As privacy was discussed, the use of hardware of tally server for better security was proposed. The major limitation of such a system is mobile agents because there are security issues and compliance issues

required for voting systems. After addressing those issues, remote e-voting should be as secure as current voting techniques while governments are transitioning to the cloud to leverage efficiency, transparency and accessibility advantages. Significant security issues are due to the original concept of operating a dedicated hardware server for validating and decryption. An important consideration in developing electronic voting technology is that the internet is not a secure tool. Information encryption to reduce the risk of data fraud and voter signature features to validate the votes are important features for e-voting to be successful (Lippert & Ojumu, 2008, p. 75).

Security: Hacking and Cyber Attacks

The attackers could exploit the vulnerability in the electronic voting software used in the voting terminals. Insider programmer attacks could be possible if the patch management and vulnerability assessment procedures for the software used are not effective. . Also, faulty software engineering practices like enabling programmer's ability to make undocumented alterations to the code can lead to third party codes to become a potential source of vulnerability. One such example is when the registered vote is not the same as the vote that is recorded in the system. That is, it is not possible to verify if the vote that is casted by the voter is same as the vote that is recorded in the system. This type of cyber attack is hard to identify without voter verification and audit trails. Verified voting is a non-profit organization that ensures that the voting systems used are auditable, in place and audits are conducted whenever required. Also, unauditable systems are eliminated and this would greatly contribute in preventing programmed insider attacks (VerifiedVoting.org).

Another important and most common form of attack is Denial-of-Service. In this type of attack, the hackers or the intruder need not gain confidential data or access any part of the voting system. They

prevent the legitimate voters from using the system by overloading the election web server and other system resources required for effective functioning of the voting system. With this rate of technological improvement, there are many variants in this type of attack. One such is called as Distributed Denial-of-Service attack, where the attackers perform the attack by using a network of computer devices to make the voting systems unavailable for the voters. Various devices are compromised by introducing a malware program designed to make the device obey the attacker's instructions and these devices are often referred as zombies or slaves (Jefferson, D., Rubin, A., Simons, B., Wagner, D., 2004).

Man-in-the-middle attacks can compromise the privacy of the voters by accessing the application data that is sent from the voting terminal to the voting server. Although the confidentiality of the information is compromised, integrity and the availability of the system is not usually affected in this type of attack. The man-in-the-middle could act as a SSL gateway and read all the voters' application data by decryption. It then encrypts and forwards the unaltered data to the voting server, which makes the identification of the attack more challenging. Voting machines and registration systems alone won't elections, commission report outline how state has to add security layer implemented by cybersecurity organizations, provide cybersecurity training for official elections and conduct cybersecurity assessments. To ensure that election officials respond and extensive contingency planning is done. (Jefferson, D., Rubin, A., Simons, B., Wagner, D., 2004)

Confidentiality

Another challenge is ensuring that the votes are cast and transmitted in a secure manner to those people in charge of counting them (Birch, Cockshott, & Renaud, 2014, p. 189). One concern of HandiVote is that the system might fail. Another concern is secrecy, especially with remote voting. If voters can cast

votes in an unmonitored and unrestricted environment, other people might see their votes and coerce them to vote a certain way or sell votes (Birch, Cockshott, & Renaud, 2014, pp. 192-193). The requirement of the private link between the voter and the vote casted is essential to protect the confidentiality of the vote. The use of authentication protocols in the network used between the client and server plays an important role in this context. Jefferson, D., Rubin, A., Simons, B., Wagner, D., (2004) have assessed the vulnerabilities in the voting system. One of them being lack of control of the voting environment. In this system, votes can cast their vote in their own computers or computers owned by third parties. In this case, it is possible for an attacker to pre-install a monitoring software to learn about the vote casted which results in the compromise of the vote confidentiality or to take complete control over the voting application. With the growth in technology, it is possible to build a vulnerability in the computer terminal used by the voter. Also it is important to note that the personal computers are not protected as much as the corporate ones. This gives more room for the attackers to intrude in the voting network. . (Jefferson, D., Rubin, A., Simons, B., Wagner, D., 2004). Overall evaluation in the aspect of security and privacy of the Sensus system, few assumptions the votes are not linked with the voter, and voting communications are anonymous, and voters' policy can only violate if voters allow someone to look over. Voters messages are encrypted cannot be decrypted without password/unique keys. In order to validate the voting system, mock exercises are conducted and confirm if vote counts are correct and voting is done effectively and efficiently.

Integrity and Auditing

A disadvantage of DREs is that there are no ballots, audit trails, or definitive assurances that votes are accurately recorded and processed, which is related to the issue of integrity. There are unclear standards for how to successfully execute the tasks for electronic polling. Even with internet voting, there

are still administrative costs of an election for purchasing and maintaining polling equipment (Lippert & Ojumu, 2008, p. 60).

A voting system should be tamper-resistant and inclusive so that the whole voting population can use it, regardless of age, technological competence, or disability. Insider attacks, network vulnerabilities, and challenges of auditing are challenges with the e-voting system. Correctness, robustness, and software security in a voting terminal are problems with e-voting (Lippert & Ojumu, 2008, p. 76). Printers can be added to voting machines so that a voter can print out his or her votes and double-check them before finalizing them. The paper can be retained at the poll for audits or recounts (Epstein, 2007, p. 95).

It's possible that there can be technical glitches that the system may not work and complete the electoral processes. Electric power supplies may be disrupted, polling stations might have dust and staff may not be well-trained in using the technology. Sometimes, voters' preferences are not recorded, counted, or reported properly. Electronic voting systems should include audit trails. Another challenge is ensuring that the votes are cast and transmitted in a secure manner to those people in charge of counting them (Birch, Cockshott, & Renaud, 2014, p. 189). Voters often don't trust voting systems and do not believe the team members who are involved in the electoral agencies which are voting system. Social personality and trust in internet-based voting adoption is decreasing every day. Government applications submitted through the web has introduced insightful engineering to frequent citizen's interactions with the government and have a meaningful impact of Internet-based voting.

Manipulation

One possible disadvantage is multiple voting, in which voters can create smart cards that are still valid, according to the DRE's requirements. To counteract this challenge, poll workers can be on the

lookout for suspicious activity. They can also compare the number of votes that were cast on DREs with the number of voters who signed in. The DRE can be programmed to require a specific code on a smart card to be considered authentic to make it harder for smart cards to be duplicated. The code should be changed every election. Cards should also have unique programs for each voter so that they cannot allow multiple use (Epstein, 2007, p. 94).

Another possible disadvantage is the introduction of a malicious code, which can change the votes from one candidate to another or make the DRE vulnerable to attacks. A removable memory card might be replaced with a different one that contains a malicious code. Poll workers can look for any voters replacing a memory card. Tamper-evident tape cannot be removed and replaced without detection because it usually has a serial number imprinted. It can provide evidence if a memory card has been replaced. Software can be designed better to prevent an executable code on a memory card from being loaded (Epstein, 2007, pp. 94-95).

Another possible disadvantage is accidental programming errors. Parallel testing involves casting test votes on a set of offline voting machines and comparing the results that they generate with the expected results. The DREs can also be tested during the logic and accuracy process and approval process. It is hard to achieve perfection with software, but these actions can reduce the risk and effect of errors (Epstein, 2007, p. 95).

Lack of Evidence

In traditional voting systems, the evidence that the voter has casted their vote was the receipts issued. As the receipt freeness concept emerged, there has been significant issues with respect to ensuring that the vote recorded is same as that intended by the voter. Due to the doubtful presidential election, voting

systems have been scrutinized by the public, and traditional methods are too complicated and challenging to use. As a privacy concern, the voting system should not expose any information except a total number of votes with segregation. Due to a sideband, internal and external communication within the system and determine the elections without breaking security. Significant challenges for designing an e-voting system are privacy, security, confidentiality and lack of evidence. Additionally, ease of use, low cost, speed and scalability are significant features to be included in the system.

8. Risks

More than 80% of voters in Pennsylvania use paperless electronic voting machines without audit trails (Deluzio, 2018). Older machines can be insecure, harder to maintain, and more likely to fail. Even though attacks or failures of a few individual machines may not have a major effect on national vote totals, voters can lose their confidence in voting with those machines. In very close contests, they can have a more significant effect (Brennan Center for Justice, n.d., p. 1). Failures and crashes can result in longer lines and lost votes. The hardware may be obsolete that it would be harder to find replacement parts. The software may also be obsolete that security patches would not be compatible, increasing the system's vulnerability to cyberattacks (Brennan Center for Justice, n.d., p. 2).

The Former U.S. Attorney David Hickton has said, it is estimated that 75 percent of Pennsylvania counties pay contractors to do some election-related work. (The Morning Call, 2019). It is very important to incorporate security policies and procedures among the contract employees to prevent any threat to the confidentiality and integrity of the information that is stored and transmitted in the voting environment. One such security process is by checking the background information of the contract employees.

9. Results and Conclusion

Through research, the current methods of voting both in the United States as a whole as well as Pennsylvania are shown to vary. Being that there are different methods of voting across the many jurisdictions, the ability to guarantee the security of voting data becomes difficult. Over time as technology continues to evolve, the standards policies and security measures surrounding this data must evolve as well. Prior to every election, there needs to be a review of these policies to ensure they are up to standards for the current period of time. With the increase in data breaches, it is imperative to ensure that everything is done to protect elections from such intrusions, and in the event, it does happen that there was preparations and plans on how to react.

In conclusion, through standardization of policies and security standards, at least through all jurisdictions through a given state, there is significantly less threat of intrusions in American elections. By using better DRE voting technology where paper copies are produced, this paper trail can help ensure that there is a backup in place given any breach of the network a jurisdiction keeps its electronic votes. Through standardizing voting methods, it will allow voters to become comfortable with the given voting method and can provide them with greater confidence that their votes are tallied correctly.

Overall, it can be concluded through research that many improvements can be made to the current voting policies and standards. As it currently stands, there are vulnerabilities, but through proper planning and with the given resources, it is reasonable to think of the possibility of being prepared for any possible intrusions.

Bibliography

Non-Academic

Brennan Center for Justice. (n.d.). Voting system security and reliability risks [PDF file]. Retrieved March 12, 2019 from https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf

Deluzio, C. (2018, September 27). Pennsylvania commission issues urgent call to replace vulnerable voting machines. Retrieved March 12, 2019 from

https://www.brennancenter.org/blog/pennsylvania-commission-issues-urgent-call-replace-vulnerable-voting-machines

Morning call. (2019). Pennsylvania voting systems at risk of cyber attack, says commission urging more security. Retrieved from https://www.mcall.com/news/nationworld/pennsylvania/mc-nws-election-vendors-cybersecurity-20181010-story.html

Scolforo, M. (2019, January 29). Report outlines way to make Pennsylvania voting more secure. Retrieved from https://www.apnews.com/204ff42a0d3340cdab56282e241fe378

Voting Equipment. (2018, August 20). Retrieved from http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

Voter identification laws by state. (n.d.). Retrieved March 11, 2019, from https://ballotpedia.org/Voter_identification_laws_by_state

Voting in Pennsylvania. (n.d.). Retrieved March 11, 2019, from https://ballotpedia.org/Voting_in_Pennsylvania

Academic

Armen, C., & Morelli, R. (2005). Teaching about the risks of electronic voting technology. SIGCSE Bull, 37(3), 227-231. DOI: https://doi-org.ezproxy2.library.drexel.edu/10.1145/1151954.1067508

Davtyan, S., Kiayias, A., Michel, L., Russell, A., & Shvartsman, A. A. 2012. Integrity of electronic voting systems: Fallacious use of cryptography. In Proceedings of the 27th Annual ACM Symposium on Applied Computing (SAC '12) (1486-1493). New York, NY, USA: ACM. DOI: https://doi-org.ezproxy2.li

Balzarotti, D., Banks, G., Cova, M., Felmetsger, V., Kemmerer, R., Robertson, W.,...Vigna, G. (2008). Are your votes really counted?: Testing the security of real-world electronic voting systems. In Proceedings of the 2008 international symposium on Software testing and analysis (ISSTA '08) (237-248). New York, NY, USA: ACM. DOI: https://doi.org/10.1145/1390630.1390660

Nguyen, T. A. T., & Dang, T. K. (2013). Enhanced security in internet voting protocol using blind signature and dynamic ballots. Electronic Commerce Research, 13(3), 257-272. doi:10.1007/s10660-013-9120-5

VerifiedVoting.org. (2019) Retrieved from https://www.verifiedvoting.org/about-vvo/

Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004). Analyzing internet voting security. Commun. ACM 47(10), 59-64. DOI: https://doi-org.ezproxy2.library.drexel.edu/10.1145/1022594.1022624

Jardí-Cedó, R., Pujol-Ahulló, J., Castellà-Roca, J., & Viejo, A. (2012). Study on poll-site voting and verification systems. Computers & Security, 31(8), 989-1010. Retrieved February 16, 2019 from https://doi-org.ezproxy2.library.drexel.edu/10.1016/j.cose.2012.08.001

Lippert, S. K., & Ojumu, E. B. (2008). Thinking outside of the ballot box: Examining public trust in e-voting technology. Journal of Organizational and End User Computing, 20(3), 57-80. Retrieved February 16, 2019 from http://dx.doi.org.ezproxy2.library.drexel.edu/10.4018/joeuc.2008070104

Weldemariam, K., Kemmerer, R. A., & Villafiorita, A. (2011). Formal analysis of an electronic voting system: An experience report. The Journal of Systems and Software, 84(10), 1618-1637. Retrieved February 16, 2019 from https://doi-org.ezproxy2.library.drexel.edu/10.1016/j.jss.2011.03.032

Birch, S., Cockshott, P., & Renaud, K. (2014). Putting electronic voting under the microscope. The Political Quarterly, 85(2), 187-194. Retrieved February 16, 2019 from https://doi-org.ezproxy2.library.drexel.edu/10.1111/1467-923X.12071

Epstein, J. (2007). Electronic voting. Computer, 40(8), 92-95. Retrieved February 16, 2019 from https://ieeexplore-ieee-org.ezproxy2.library.drexel.edu/document/4292024

Belton, M. G., Kortum, P., & Acemyan, C. (2015). How hard can it be to place a ballot into a ballot box? Usability of ballot boxes in tamper resistant voting systems. Journal of Usability Studies, 10(4), 129-139. Retrieved February 15, 2019 from https://dl-acm-org.ezproxy2.library.drexel.edu/citation.cfm?id=2817325.

Armen, C., & Morelli, R. (2005). E-voting and computer science. ACM SIGCSE Bulletin, 37(3), 227-231. Retrieved February 15, 2019, from https://dl-acm-org.ezproxy2.library.drexel.edu/citation.cfm?id=1067508

Pesado, P., Galdemea, N., Estrabou, C., Pousa, A., Rodriguez, I., Rodriguez Eguren S., . . . De Giusti, A. (n.d.). Experiences with electronic vote: Challenges and solutions. Proceedings of the 9th International

Conference on Theory and Practice of Electronic Governance, 406-407. Retrieved February 15, 2019, from https://dl-acm-org.ezproxy2.library.drexel.edu/citation.cfm?id=2910098

Burton, C., Culnane, C., & Schneider, S. (2016). VVote: Verifiable Electronic Voting in Practice. IEEE Security & Privacy, 14(4), 64-73. doi:10.1109/msp.2016.69

Everett, S. P., Greene, K. K., Byrne, M. D., Wallach, D. S., Derr, K., Sandler, D., & Torous, T. (2008). Electronic voting machines versus traditional methods. Proceeding of the Twenty-sixth Annual CHI Conference on Human Factors in Computing Systems - CHI 08, 883-892. doi:10.1145/1357054.1357195

J. Benaloh, D. Tuinstra, "Receipt-free secret-ballot elections", Proceedings of the Twenty-sixth Annual ACM Symposium on the Theory of Computing, pp. 544-553, 1994-May-23-25.

Secure Voting in the Cloud using homomorphic encryption and Mobile Agents
Mark A. Will, Ryan K. L. Ko, Silvino J. Schlickmann, "Anonymous Data Sharing Between Organisations with Elliptic Curve Cryptography", Trustcom/BigDataSE/ICESS 2017 IEEE

Challenges in Designing an Electronic Voting System B. Bederson, B. Lee, R. Sherman, P. Hernson, and R. Niemi.Electronic voting system usability issues. Proceedings of the SIGCHI conference on Human factors in computing systems.
Al-Ameen and Talab, 2013A. Al-Ameen, S.A. Talab The technical feasibility and security of e-voting International Arab Journal of Information Technology, 10 (4) (2013), pp. 397-404

Sahu, G P: A Literature Review and Classification of e-Governance Research (2008) proceeding of faculty development programme on management information systems at school of management studies Motilal Nehru National Institute of Technology Allahabad. July 14 to 26 ,2008, (95-103) https://www.csi-sigegov.org/egovernance_pdf