Picture credit: Getty

DEMOCRACY IN PERIL

Thomas Richards *reports on the potential security issues that could throw the upcoming US Election into chaos*

In November, the world will watch with great anticipation as millions of US citizens assemble at the polls once again – or at least figuratively. The US electoral system, already riddled with complexities, has had another challenge thrown in the mix following the outbreak of COVID-19. Leaders have had to adapt and make impromptu decisions, resulting in political ramifications as well as logistical ones.

Indeed, the chaos that seized the primaries offers a glimpse into the complications provoked by this unprecedented pandemic. Wisconsin, for instance, witnessed a temporary stalemate between Democratic governor and Republican legislature over calls for a postponement. When the election was scheduled to proceed at the last minute, on 7 April, Americans had to make a tough choice between protecting their physical health or exercising their right to vote.

In New York, where votes have historically been cast almost exclusively in person, the atypical spate of absentee ballots left two congressional races undecided more than six weeks post the election day.

Ransomware attacks remain a very real and highly likely threat

In Georgia, some absentee ballots failed to reach citizens and those who showed up to the polls faced long lines caused by a shortage of poll workers and technical issues. No primary was left intact, and this only goes to show that elections are a fragile infrastructure that necessitate meticulous planning and action taken well in advance. Having undergone this 'trial run' of sorts, the country has had a bit of time, though not much, to consider the best course of action in the lead up to the November general election.

A number of voting alternatives have been offered, with some advocates championing the employment of online voting. Delaware, New Jersey and West Virginia are among a few states that have dabbled with the idea, piloting a digital voting system through the company Democracy Live.

An issue that arises is vote tampering. Voting over the internet essentially opens a gateway for cybercriminals, both state-sponsored and fortune-seeking, to infiltrate the system and manipulate votes. For instance, downloadable PDF ballots could be picked up 'en-route', and edited as it is submitted.

Worse still, due to the anonymity of voting, it would be impossible to check that the vote has been transmitted correctly. In this way, a secure online voting system demands end-to-end encryption. With encryption, the data is made unintelligible to everyone but the sender and the recipient. Unfortunately, such technology has yet to be developed and tested on scale in the US. It is no wonder then that the federal government has issued a warning against such 'high-risk activity'.

Mobile voting also presents comparable risks. In fact, on top of having to ensure the secure transit of a vote through the internet, voters would need to confirm that their devices are not already compromised. The US still has a way to go before achieving such a feat. Both online and mobile voting require significant time and resources to become viable and secure options for the US.

This leaves us with mail-in voting. Despite President Trump's attempts to invalidate the use of mail-in voting, claiming without reasonable evidence that it is susceptible to fraud, it is in fact the most feasible option for the US today. Mail-in voting is based on a pre-existing system of absentee balloting, which has been demonstrated to work effectively. The majority of states have opted to enable mail-in voting for the November election in varying degrees.

As for electronic voting machines that are used for casting votes in-person at polling places, there are concerns about whether the vote is counted or could somehow be manipulated. Most of these concerns could be alleviated by more understanding of how these systems work. While the majority of these systems aren't connected to the internet, and poll workers would likely notice someone attempting to tamper with the devices, municipalities and state governments still need to do their part to ensure they are tested, secured and deployed correctly.

For one, they should not be using devices that are out of support from a vendor or run unsupported operating systems. Legacy systems should be depreciated and replaced with more modern ones, which also come with better security enhancements. All poll workers should be trained on how to properly deploy these systems and protocols to follow if they find someone tampering with or attempting to remove a voting machine.

In the 2016 elections, we learned of Russian cyber intruders targeting voter databases and software systems. In 2019, we saw a sharp rise in ransomware attacks on local and state governments from Louisiana to Texas, Mississippi City to Baltimore. Regrettably, this only makes the threat of a ransomware attack in the upcoming election a very real and likely possibility. What's more, the threat is exacerbated by the fact that most election officials, on local, state and federal levels, are enduring considerable strains to their staffing and budget.

ONLINE AND MOBILE VOTING REQUIRE SIGNIFICANT TIME AND RESOURCES TO BE VIABLE

The demographic that typically assists in maintaining the smooth running of the polls tend to be retired and of an older generation. Indeed, in a survey held by the US Election Assistance Commission, of the 917,694 poll workers who worked during the 2016 election, 59 percent were 61 or older. This group of workers also happen to be most vulnerable to the virus, resulting in many renouncing their post in the upcoming election.

With few staff on board to help, those who have stayed behind are expected to work overtime. The fatigue this engenders can easily cloud their judgement when faced with a phishing email – one of the most common means of entry in a cyberattack. Humans can certainly be a weak link in the security life cycle; cybercriminals know this and are quick to exploit it.

The government does offer some free cybersecurity services and courses to boost the cybersecurity awareness of poll workers. More recently, an initiative instigated by the University of Chicago has also put local election officials in contact with cybersecurity experts who can offer advice. While both useful endeavours, the lack of funding will only continue to impede any lasting fixes. Without the funds, the right resources and technology cannot be allocated to address concerns. Without the means to deploy advanced anti-malware technology or an instrument to audit for vulnerabilities, the system remains exposed to the delight of cybercriminals.

The evident target for hackers are the voter registration databases (VRDBs); yet, these do not appear to be adequately safeguarded either. Just last year in July 2019, it was found that 10,000 electoral jurisdictions were using Windows 7 or an older operating system. This is concerning because these operating systems have since stopped receiving technical support from Microsoft, including 'patches' for vulnerabilities.

Another study, by Recorded Future, highlighted the lack of transparency on vulnerability reporting by election software vendors. Without transparency, the individuals liable to keeping the VRDBs safe are left in the dark.

Moreover, these databases are often administered by tools such as Remote Desktop Protocol and Citrix, both of which have become a common exploit for actors utilising ransomware. The widespread cyberattacks on Australian infrastructure deployed by way of a vulnerability in Citrix products is a clear demonstration of this. In fact, they have quickly become the most popular entry point in attacks, even overtaking phishing. Such developments need to be incorporated in cybersecurity awareness training.

An attack on VRDBs could have sensitive data exfiltrated and held for ransom or sold on the Dark Web – not only throwing the elections into disarray, but potentially reaping millions of dollars in the process. A ransomware attack could also disrupt vote-tallying. And for those pushing forward with in-person voting, an attack could impede officials from authenticating a voter's identity and eligibility.

> ELECTIONS ARE A FRAGILE INFRASTRUCTURE THAT NECESSITATE METICULOUS PLANNING AND ACTION

Nevertheless, more devastating than these disruptions is the doubt that such attacks would cast over the election's legitimacy, and of those yet to come. Cyberattacks do not necessarily have to occur in one, explosive hit – they can be a means of silently and steadily chipping away at the foundations of trust through disinformation. Alas, a ransomware attack, regardless of its true impact, can be leveraged as part of such a campaign.

Since voting machines are owned and managed at the local district level, and aren't involved in interstate commerce, the Computer Fraud and Abuse Act (CFAA) didn't cover unauthorised access to voting machines. With passage of the Defending the Integrity of Voting Systems Act, the CFAA was amended meaning that unauthorised access to local voting machines used in Federal elections will become subject to CFAA. Unfortunately, the CFAA isn't without controversy as it doesn't define "unauthorised access". Clarification of this situation is currently before the US Supreme Court where the outcome could have a significant impact on how cybersecurity research is conducted, and the scope of what research is permissible.

MAINTAINING INTEGRITY

Voting is fundamental to our democracy and way of life. Should this be manipulated by way of a cyberattack, ransomware attack or any type of malware that affects computer networks or the networks of infrastructure providers, could result in the integrity of the votes being called into question.

As the general election draws closer, electoral officials need to work alongside experts to educate anyone from the public and private sector involved in the elections. They need to be made aware of the latest threats, in order to appropriately deal with them ●

Thomas Richards, is an associate principal consultant at Synopsys. His primary areas of expertise include Red Teaming and Mobile Security. He is an Offensive Security Certified Professional (OSCP) and a member of The Open Organization of Lockpickers (TOOOL).

The evident targets for hackers are the voter registration databases