This page will describe the details of risks osf electronic voting machines such as trust of software and hardware, the votes transit of the machines and anonymity issue etc.

Firstly, The voting programme of the machines could be exposed to the risk of cyber-attacks including malwares. It cannot be guaranteed that the security of the voting programme is 100% safe and unhackable. Hackers may be able to find the vulnerability of the system and it’s a huge problem since the result of the vote could be changed. The machines at the polling place could be under attack or manipulated by someone while they are unattended. For instance, a different programme can be installed on the machines and nobody finds out the difference. These risks may result in inoperativeness of the machines and the replacement of them could delay the voting speed. The transit of votes is one of the concerns since there are various ways for it. All the machines could be transported to the counting place but it is physically impossible. The votes of each machine can be downloaded to an USB stick and transported, but this way the data can be lost on the way of transit. The votes could be directly sent to the counting server through internet, however, this way the result may not be trusted as there is no proof that the correct votes have been sent. Also, it is more difficult to detect and identify the source of errors. It will be almost impossible for non-expert to figure out the problem and voters may need to wait until the experts arrive and fix the problem. The electronic voting system also costs much. The cost includes software updates, replacement of outdated voting machines, maintenance etc. According to Turquoise, B., & Lawrence, N.(2022), the replacement of old machines will cost at least millions of dollars.

The young generation may find it easy to vote with electronic voting machines, however, old generations may struggle with the new system. In addition, people in rural areas may need to travel a long distance to vote sine the machines require electricity. The public trust is also an issue since people do not have access to the ballot counting process and there is no visible or clear evidence to check if the votes have been correctly recorded or the total number of ballots. Moreover, the anonymity of voters cannot be guaranteed with electronic voting system. Voters have to enter their personal details to the system to verify themselves and this can cause serious problems such as privacy issues and it would be possible to find out who the voters voted for and it is obviously against the anonymity of the vote.

Reference

Matt, B., & David, W.(2007). Risks of E-voting. COMMUNICATION OF THE ACM. <https://people.eecs.berkeley.edu/~daw/papers/risks-cacm07.pdf>.

Gloria, L., & Nicole, E.(2007). Electronic Voting. <https://cs.stanford.edu/people/eroberts/cs201/projects/2006-07/electronic-voting/index.html>.

Turquoise, B., & Lawrence, N.(2022). Voting machines at risks in 2022. Brennan Centre. <https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-2022>.

E-Voting. (n.d). Ace, The Electoral Knowledge Network. https://aceproject.org/ace-en/focus/e-voting/benefits-risks-and-costs.