

Case #	Threat	Vulnerability	Asset	Impact	Likelihood
1	Malicious Trustees	Collaborating trustees could leak the decryption key	The decryption key	In the upcoming election votes could be decrypted and linked back the submitter (CRITICAL)	This requires that a number of trustees equal or greater to the threshold to be malicious and collaborate (VERY LOW)
2	Malicious admin	The admin would be able to add any voter to the election	List of voters	The election is comprised as unelligible voters can be allowed to vote (HIGH)	The election admin should be chosen by careful consideration but it is a single point of failure but auditors can check for any noticable changes (Medium)
3	Malicious admin	The admin would be able to change the election configuration at any time	Election configuration	Unwanted adjustments to the settings could be made which could in worst case ruin the election (HIGH)	Single point of faliure but as the configuration is appended to the bulletin board everyone can validate they are correct (LOW)
4	Malware on Trustees PC	Collaborating trustees could leak the decryption key	The decryption key	In the upcoming election votes could be decrypted and linked back the submitter (CRITICAL)	This requires that a number of trustees equal or greater to the threshold to be infested and collaborate (VERY LOW)
5	Malware on election admin PC	The infested admin would be able to change the election configuration at any time	Election configuration	Unwanted adjustments to the settings could be made which could in worst case ruin the election (HIGH)	Single point of faliure but as the configuration is appended to the bulletin board everyone can validate they are correct (LOW)

				The election admin should be chosen by careful consideration but it is a single point of failure but auditors can check for any noticable changes (Medium)
6	Malware on election admin PC	The infested admin would be able to add any voter to the election	List of voters	The election is comprised as unelligble voters can be allowed to vote (HIGH)
7	Identity provider is unavalible	As identity provider is a third-party service we have no gurantees that it is avaliable	Identity provider	Depends on the identity provider but in most cases it would be very low as they would generally be avalible almost all of the time

Risk/damages Control recommendations

Diverse cast of trustees
should be chosen

Auditter & Careful
consideration whom the
admin should be

Careful consider whom
the admin should be

Trustees should have the
newest software updates
and know how to avoid
typical malware

Admin should have the
newest software updates
and know how to avoid
typical malware

Admin should have the
newest software updates
and know how to avoid
typical malware

Chose reliable identity
providers with very high
uptime