507-11 William Carson Cr.
Toronto, Ontario
M2P 2G1
(416) 224-0057
hmkim@yorku.ca
www.yorku.ca/hmkim

Henry M. Kim, Ph.D.
Associate Professor
Schulich School of Business
York University

Risk Analysis of Traditional, Internet, and other Types of Voting Alternatives for Town of Markham

A Study Prepared for the Chief Electoral Officer, Town of Markham

June 23, 2005

I. Executive Summary

In this study, a risk analysis of various voting alternatives for the Town of Markham was performed. The alternatives analyzed were the following: 1) Poll voting only; 2) One step Internet voting + poll voting; 3) Two step Internet voting + poll voting; and 4) Mail-in voting only. Telephone voting alternative was not analyzed in detail because it just is not user-friendly enough to be used for the voter population of Markham. 45 different risk threats were identified. For each threat, the likelihoods of occurrence as well as recovery from the threat was estimated and then multiplied against a weighted estimation of the impact of the threat on election integrity, vote-ability, confidentiality of voter information, and public trust. For each threat, a risk score was then calculated. Some threats were associated with only one or some of the alternatives, so different total risk scores resulted for each alternative.

The poll only alternative was always the least risky alternative. In the most reasonable risk scenario, the poll only alternative was followed by the Internet 2 step, then Internet 1 step, and trailed by mail-in. Additionally, it was found that the threats with the greatest scores were associated with the mail system and with those representing Town of Markham, including ES&S, ITS, town officials and poll workers. Moreover only about 1/3 of the overall threat scores were associated with deliberate threats; the remaining 2/3, with accidental threats. The three threats with the largest risk scores were: 1) completed ballots mailed out in time for the mail-in only alternative are received after vote tabulation because of Canada Post mishandling; 2) mail theft of notification cards, which provide the opportunity to directly vote in the mail-in and Internet one step alternatives; and 3) denial-of-service attacks for the Internet alternatives.

Under an alternate, still-reasonable scenario in which the scale of damage of a mail thief stealing notification cards was assumed much higher, the Internet 1 step alternative was by far the most risky. Under another, still-reasonable scenario in which the likelihood of mail-in ballots arriving late was assumed lower, the mail-in alternative became a less risky alternative than the Internet alternatives. What these results outline is that the risk scores are very sensitive to assumptions made about the vulnerability of the mail system, *not the Internet*. Especially in light of the fact that the Internet voting was successfully carried out by ES&S and the Town of Markham in 2003, the choice of the alternative chosen depends really on asking pointed questions about some unknowns of the mail system, and not so much on Internet threats.

If those who would have otherwise been subversive decide not to steal notification cards and vote on-line because they fears getting caught in the act, then the Internet one step is not significantly more risky than the two step. If Canada Post can guarantee extremely high (around 99.99%) delivery within an acceptable time window, then the mail only alternative is superior to Internet alternatives. However under risk averse scenarios dictated by principles described as “err on the side of caution” and “maintain control,” Internet two step alternative is always the second best alternative next to poll only voting.

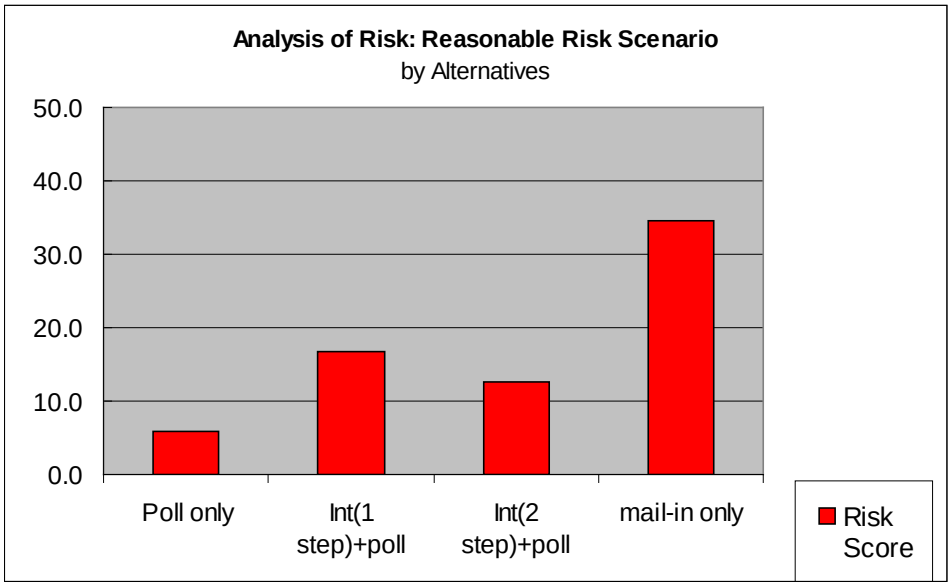
Table of Contents

II. Commentary

The Town of Markham successfully conducted Internet voting as an adjunct to traditional poll voting in 2003. The particular mode of Internet voting adopted in 2003 entailed a two step process (1st in which the potential voter registered to vote specifically online, and 2nd in which the vote is cast online). For the impending election in 2006, the Town of Markham is considering leveraging the successes of 2003 by adopting other modes of voting, which would make voting even more accessible and increase voter participation. Though the benefits of these voting alternatives are well-understood and it is reasonable to objectively compare them, the same cannot be said about evaluating the risks of these alternatives. In fact, research conducted for this study yielded very little in the way of existing methodologies that could be used to compare alternatives so that it is possible to compare "apples to apples" in terms of risk analysis. Therefore the first part of this study entailed extending existing risk analysis methodology, OCTAVE, to compare the different alternatives. The results from the application of this methodology are discussed herein.

In this study, four alternatives are compared: 1) Traditional poll voting only (with advanced polling); 2) 1 step Internet voting + polling; 3) 2 step Internet voting + polling; and 4) mail-in only. As well, though telephone voting was considered, this alternative is not analyzed in detail. Telephone is a medium that is inappropriate for use in terms of user friendliness given the characteristics of Town of Markham elections. One, use of telephone is inherently serial. If there are several candidates for various positions, plus instructions and security verifications that are needed, it may take more than five minutes to vote. Voters may not have patience to go through what they consider to be an ordeal. Two, as studies of telephone based customer services have outlined, these systems are notoriously unforgiving of customer errors and have a tendency to frustrate customers. Three, people for whom English is a second language are better readers than listeners, and given Markham's diverse population, other modes are definitely better at reaching this segment of the population.

The following chart shows the key result of the analysis:



This aggregates the finding that for the most reasonable assumptions about the risks of different alternatives—there are 45 threats for which the likelihood of occurrence and effects on election integrity, vote-ability, voter confidentiality, and public trust—have some risk factor above 0. The poll only alternative is clearly the least risky alternative. It is obviously superior to the Internet alternatives since these alternatives inherently include poll voting risks as well as Internet-only risks. The mail-in only alternative is also clearly the most risky alternative.

Some aspects of these results are striking insofar as they may be considered somewhat unexpected.

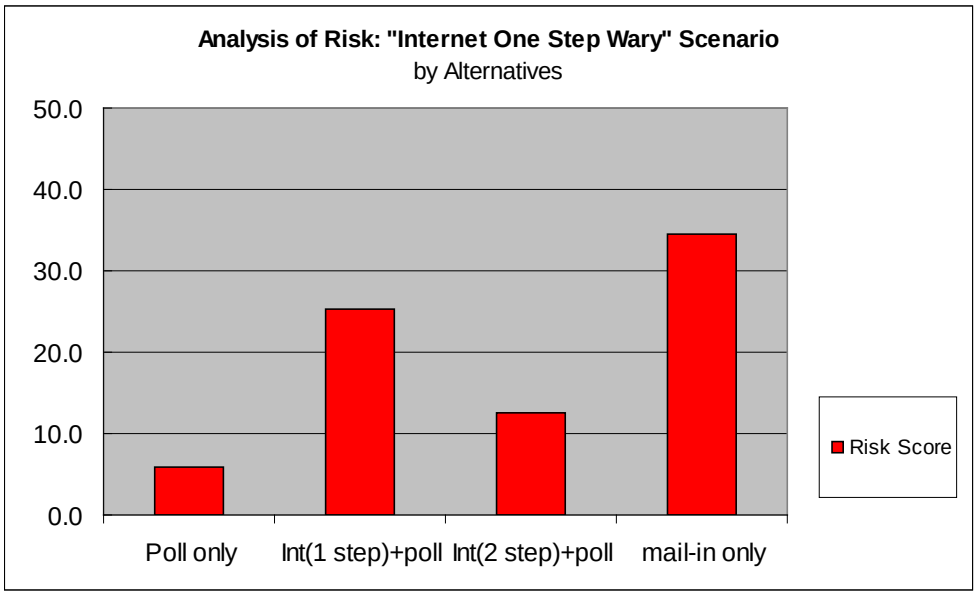
Why isn't the difference between one and two step Internet voting more pronounced?

This is because for the most part both alternatives share the same threats such as bugs and denial-of-service attacks with identical risk scores. However the one risk that can be expected to be higher with the one step versus the two step is the threat that notification cards mailed from the Town of Markham is stolen. In the one step alternative, the thief can then take the cards and cast a vote for each of the cards. In the two step, even if the thief registers to vote for each of the cards, s/he must then check each of the mailboxes to again steal the second notification cards that are needed in order to vote.

At first glance then, the risk score for this threat should be significantly higher for the one step alternative than the two step. This is true as the risk score (2.43) for one step is nearly 10 times the score for two step (0.27). In fact, the difference in this score accounts for about ½ of the

difference in total risk scores between the two alternatives. However some may argue that the risk score differences due to mail theft should be even more profound. To counter this argument it can be put forth that though the threat of a mail thief seems quite high, the likelihood of someone actually going through and casting a false ballot is rather low. Why is this so? Studies show that people commit Internet crimes because they believe they will not get caught and will not be prosecuted even if caught, and because they feel detached from the crime as it involves minimal physical movement and hence is more convenient. For the mail thief to cast a false vote online, they must physically steal—which means that they know that they can get caught because someone or some camera may see their theft—and they must pre-meditate actions both physically and "virtually." On top of that, if the thievery is identified before the actual election day, the Town of Markham does have the last resort option to annul the results of Internet voting altogether and count only the poll voting. For these reasons, the likelihood and the effect of this threat is not as profound as in first glace.

Having said that, under a more "One step Internet wary" scenario in which the scale of damage of mail theft is higher, the overall risk score for one step versus two step goes from 16.7 versus 12.5 in the most reasonable scenario to 25.4 versus 12.5.



What this sensitivity analysis demonstrates is that there is a distinct difference between one and two step alternatives, but the difference only becomes profound under a more "One step Internet wary" scenario in which the psychological factor of lack of control is manifested. Though the protection of the Website and databases is under the control of Town of Markham (ES&S, ITS, and other Town officials are classified as "Town of Markham"), what happens when notification

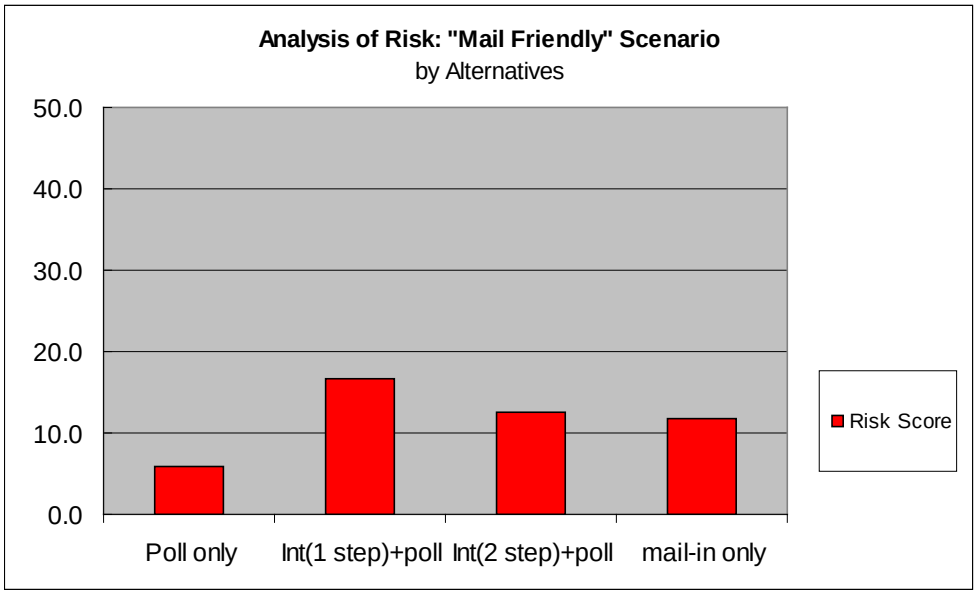
cards are left to Canada Post mailpersons or left in mailboxes is beyond the Town's control. If a key principle for conducting the election is to "err on the side of caution" and "maintain control," then the two step alternative is a distinctively more reasonable one to adopt.

Why Is the Mail-In Alternatively So Much More Risky?

One salient feature of the mail-in alternative is that there is no election day poll voting to serve as a means of recovery. Also unlike Internet and poll voting alternatives, this alternative cedes a lot of control to Canada Post. What this means is that a threat as seemingly innocuous as Canada Post not delivering a few mailed-in votes on-time cannot be recovered from and the Town of Markham is limited in what it can do to eliminate or even heavily mitigate this possibility. That is, there is a reasonable large likelihood that at least one voter who observed all the rules and voted in good faith may not get his/her vote counted. Note the following threats with the highest scores under the most reasonable risk scenario:

Alternative	Scenario	Likelihood	Possibility of Recovery	Scaled Risk of Threat
4-mail-in only	Mail-in ballot mailed at right time arrives in ToM too late.	7.5000%	25%	25.31
4-mail-in only	Notification card mailed from ToM stolen	0.7500%	25%	5.16
2-Int(one)+poll	Denial-of-service attack	0.0750%	90%	4.97
3-Int(two)+poll	Denial-of-service attack	0.0750%	90%	4.97
2-Int(one)+poll	Mishaps by ITM in testing or operation resulting in Website going down	0.0075%	90%	4.19
3-Int(two)+poll	Mishaps by ITM in testing or operation resulting in Website going down	0.0075%	90%	4.13
1-Poll only	Access to polls delayed because of poll worker oversight	0.7500%	99%	4.05
2-Int(one)+poll	Notification card mailed from ToM stolen	0.7500%	25%	2.43
				.....
				69.67

The mail-in delay threat contributes 36% (25.31/69.67) of all the risk scores for all the alternatives! **The threat of mail-in votes not being counted is extremely sensitive to assumptions about likelihood of its occurrence!** In the most reasonable scenario, the likelihood of occurrence is set at 7.5%. If the likelihood is changed to a more "relaxed" 0.75% under a more "mail friendly" scenario, the risk scores for all alternatives look completely different and make the mail-in alternative slightly more risky that the poll only alternative, and more attractive than the Internet alternatives.



Let's say that integrity of mail-in voting is eroded if 10 mail-in ballots arrive too late for counting even though they were mailed-in before a postmark date. Say further that 40,000 vote, and 25% or 10,000 vote within two days of the postmark date. Say that the Town of Markham sets the tabulation date as five business days after the postmark date. It should be posed to Canada Post then whether they can deliver mail from Markham to Markham within 7 days 99.9% of the time (10 late ballots out of 10,000), or 99.99% (1 late ballot out of 10,000) of the time. If Canada Post's confidence level is the latter, the risks of mail-in is similar to poll only; if it is the former, then mail-in is even more risky than the Internet alternatives.

What this means is that a large consideration in deciding whether to conduct mail-in only voting depends on factors such as Canada Post's capability to deliver *all* mail on time, the willingness for the Town of Markham to have a longer time window between the final postmark date and the date at which the votes are tabulated, and willingness of the Town to pay a premium for Canada Post to treat mail-in votes as a priority letters.

Why Aren't the Risk Scores for the Internet Alternatives Even Higher?

The study's methodology quantifies risk as likelihood of threat x effect of threat being realized. As much as it is reasonable to objectively express the threat, it is not easy to come upon a number that accurately represents the likelihood of a threat occurring. For example, should the likelihood of a successful denial-of-service attack that renders Internet voting as disastrous be represented as 0.01%, 0.1%, 1%, or some other probability? The strongest statement that can be made is that the likelihood of occurrence is extremely low, but that the effect of a threat can still

be catastrophic. Therefore though the risk scores of various Internet threats such as denial-of-service and bugs is very low, it does not mean that they should be ignored altogether. On the flip side, studies show that people tend to subjectively judge those alternatives that are not within their control or level of comfort to be more risky. The low scores attached to the Internet threats mitigate this biased subjectivity.

By using this methodology, it has been shown that Internet based threats that have been sensationalized in the popular press may occur in the context of this election. These threats are:

- **Denial-of-service attacks**: Numerous "unassuming" computers on the Internet are instructed to bombard a Website with frivolous messages, effectively shutting down the Website as it tries to respond to these messages at the expense of serving other, valid requests. The ES&S solution has hidden and/or dynamic addresses that cannot be so easily "pinned down" for an attack
- **Hackers gaining access to electors list or voting results**: The likelihood of this occurrence is extremely low because the electors list database is securely protected and kept off-line from the Internet by ES&S so that a connection to it really cannot be made. The voting results are protected even more so, employing sophisticated biometric encryption and security techniques.
- **Website defacing**: A hacker breaks into the Website and essentially uses the Website to paint his/her graffiti. ES&S's solution is quite robust against intrusions of this kind.
- **Phishing**: Con artists exploit the opportunity of an election to send email or mail to potential voters asking to vote at a false site. The voters are then asked to provide private information, which then can be used by con artists for acts like identity theft.
- **Spyware**: Shared computers at public places like libraries where voters may vote online are particularly vulnerable to spyware, which are stealth software the may log keystrokes and keep track of which Websites were visited, or hijack the browser. The election may present an opportunity for con artists to again exploit people's expectations about the election for getting them to download and use spyware.

What studies show is that often the true vulnerability is not in gaining virtual access, but rather in using classical means to infiltrate within a firewall or line of defense and then gaining access. This is called "social engineering." An example is a hacker who calls an unsuspecting employee pretending to be a IT person and then gets the employee's user name and password. The hacker then has much easier access to assets that s/he wants to violate. There definitely is a possibility that a hacker may try to "social engineer" access by conning ES&S or ITS staff. This is a successful, albeit "low-tech," means of hacking in.

What is instructive in the context of this study is that the "low-tech" threats are in fact the significant ones, and the sensationalized threats mentioned above pale in comparison in terms of

vulnerabilities. The two biggest threats of Internet voting are mail theft of notification cards and family members coercing another as the latter votes online. These threats definitely are “low-tech.” The bottom line is that the vulnerabilities of the Internet alternatives are in fact very similar to the vulnerabilities of the “low-tech” alternatives of polling only or mail-in only. If ES&S and ITS hadn’t succeeded in running an Internet election in 2003, the fidelity of the ES&S solution could be further questioned, and then it could be argued that there is a significant “high-tech” vulnerability to the Internet alternatives. As it is, the ES&S solution was carefully vetted and tested in 2003. Therefore in the end, the significant threats on all alternatives is of the low-tech kind, which explains why the risk scores of Internet alternatives is not substantially higher than on other alternatives.

III. Methodology – Threat Profiles

The basic framework used in this study to organize threat profiles of different voting alternatives is the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Method from the CERT Coordination Center® at Carnegie-Mellon University[1].

What Is OCTAVE?[2]

Information systems are essential to most organizations today. However, many organizations form protection strategies by focusing solely on infrastructure weaknesses; they fail to establish the effect on their most important information assets. This leads to a gap between the organization's operational and information technology (IT) requirements, placing the assets at risk.

The first step in managing information security risk is to understand what your risks are. Once you have identified your risks, you can build mitigation plans to address those risks. The OCTAVE Method enables you to do this, and that is why a simplified variant of the OCTAVE Method is being used for this study.

The OCTAVE Method is an information security risk evaluation that is comprehensive, systematic, and context driven. By following the OCTAVE Method, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology (IT) assets.

The phases of the OCTAVE Method are the following:

- **Phase 1: Build Asset-Based Threat Profiles** – This is an organizational evaluation. Staff members within the organization identify important information assets, the threats to those assets, and the security requirements of the assets. They determine what the organization is currently doing to protect its information assets (protection strategy practices) and identify weaknesses in organizational policies and practice (organizational vulnerabilities).
- **Phase 2: Identify Infrastructure Vulnerabilities** – This is an evaluation of the information infrastructure. The key operational components of the information technology infrastructure are identified based on the information gathered during Phase

[1] OCTAVE Information Security Risk Evaluation (http://www.cert.org/octave/), Accessed: June 2005, Last Modified: August 23, 2003.
[2] The following descriptions are modified from material available in the Website addressed above.

1 and then examined for weaknesses (technology vulnerabilities) that can lead to unauthorized action.

- **Phase 3: Develop Security Strategy and Plans** – Risks are analyzed in this phase. The information generated by the organizational and information infrastructure evaluations (Phases 1 and 2) are analyzed to identify risks to the organization and to evaluate the risks based on their impact to the organization's mission. In addition, a protection strategy for the organization and mitigation plans addressing the highest priority risks are developed.

For the purposes of this study, only the first phase of building asset-based threat profiles has been performed. Though progressing through to the other phases of the Method is encouraged, doing so is beyond the scope of this study.

Threat Profile

A key aspect of the OCTAVE Method is the identification and analysis of threats to the organization's assets. A threat is an indication of a potential undesirable event. It refers to a situation in which a person could do something undesirable (an attacker initiating a denial-of-service attack against an organization's email server) or a natural occurrence could cause an undesirable outcome (a fire damaging an organization's information technology hardware). Threats consist of the following properties:

- asset – something of value to the organization (information in electronic or physical form, information systems, a group of people with unique expertise)
- actor – who or what may violate the security requirements (confidentiality, integrity, availability) of an asset. Actors can be from inside or outside the organization.
- motive (optional) – indication of whether the actor's intentions are deliberate or accidental
- access (optional) – how the asset will be accessed by the actor (network access, physical access)
- outcome – the immediate result of violating the security requirements of an asset (disclosure, modification, destruction, loss, interruption)

In the OCTAVE Method, the analysis team creates threat scenarios based on known sources of threat and typical threat outcomes. The resulting outcome or effect of these threat scenarios typically falls into these categories:

- disclosure or viewing of sensitive information
- modification of important or sensitive information
- destruction or loss of important information, hardware, or software

- interruption of access to important information, software, applications, or services

Elements of Threat Profile for Voting

What the OCTAVE Method does not specifically allow for is the specification of alternatives. Since the alternatives are essentially means by which voters *access* the opportunity to vote, what is called access in OCTAVE is called Alternatives in this study. The Alternatives studied are the following, and what is common to all alternatives is that notification cards with voter address information as well as information about candidates for whom the voter would vote are mailed.

- **Polling only**. This is the traditional mode of voting at the polls only. The voter takes the notification cards to the polls and votes. Even those that did not receive the notification cards or did not bring them to the polls can vote as long as they clearly demonstrate their eligibility to the poll workers. This alternative also considers the inclusion of advanced polling.
- **Internet Voting (2 step) + polling**. This is the mode of Internet voting that was employed in 2003. The first step in this alternative entails the voter following directions that accompany the notification cards to access the Website to verify eligibility and provide a secret question and answer. The second step then entails the receipt of another ID via mail. Once this ID is provided along with the answer to the voter's personal question, the voter then votes on-line. Once a cut-off date has passed, voters can only vote at the polls and not on-line.
- **Internet Voting (1 step) + polling**. In this Internet voting mode, the voter follows directions that accompany the notification cards and once his/her eligibility is verified online, then votes. There is no additional step as in above. Similar to above, the voter cannot vote online after a cut-off date and can only vote at the polls.
- **Mail-in only**. In this alternative, there is no voting at the polls. Instead, the voter follows directions accompanying the notification cards and fills out a ballot and mails that in.

As for assets, there are really three different types:

- **Electors list**: For the polling alternative, there is one master copy that is kept on a database within the Town of Markham offices and updated until just before the day of polling. The poll workers are then provided with subsets of the master list that applies for their wards. As for the Internet alternatives, a copy of the electors list database for Internet voting is securely stored; the vendor—ES&S in the last election—is responsible for the database's security. After the cut-off date for Internet voting, the master copy at Town of Markham offices is updated with data on who voted via the

Internet. As for the mail-in alternative, the electors list is a master list that gets updated periodically as the votes come in.

- **Unmarked Ballots**: In this study, this is a catch-all term to describe those "things" that give a voter the opportunity to vote, and hence can be threatened. For the polling alternative, not only are these actual ballots that are given out at the polls, but they encompass notification cards that are sent out. For mail-in, the ballots are sent out with the notification cards. In addition, for the Internet alternatives, the Website itself can also be considered "unmarked ballots" since it and its screens provide the opportunity to vote.
- **Completed Ballots**: For the poll and mail only alternatives, these are the actual physical ballots that are then tabulated. For the Internet alternatives, they are the records of voting that are kept in a secure database.

Though not an asset per se, there are a handful of credible threats that may be associated with tabulation. However it turns out that the effects of delays or challenges to manual tabulation are very minimal, and with heightened security measures and virtual audit trails, the likelihood of threat being realized for Internet alternatives is also nearly 0. Therefore the tabulation activity is not considered something that would be critically threatened.

An obvious question then is this. Why have different types of assets been aggregated under just three types? The answer is that it is important to be able to compare "apples to apples." So even though electors lists may be kept as physical lists or as database records, or unmarked ballots may refer to physical ballots or the Website itself, it is possible to say that the threat to unmarked ballots, for example, of the polling alternative is lower (or higher) and than the threat of the mail-in alternative, even if what constitutes unmarked ballots differs between alternatives.

So far alternatives then can be assessed with respect to one property, assets. According to OCTAVE, another key property to describe threats is actor, and for this study, there are four types of actors.

- **Town of Markham**: These are all those that somehow represent the Town of Markham. For the polling alternative, that includes officials who work for the Town as well as poll workers. For mail-in, that means just Town officials. For the Internet alternatives, that means not just officials including IT&S, and but also the software vendor, who is very likely to be ES&S.
- **People of Markham**: These represent the voters and their families, and the candidates, their staff, and supporters.
- **Internet**: Anyone who poses a threat using the Internet, and who cannot be considered Town of Markham or People of Markham. Generally, these people do not have a vested

interest in the outcome of the election. Rather they make seek to subvert the election to make a political statement or for thrill seeking (e.g. hackers).

- **Mail**: Chiefly this is Canada Post. However in a similar vein to above, people who seek to subvert the election by exploiting the mail system and who are neither Town or People of Markham can be considered here.

Two other properties are self-explanatory for this study: intent and outcome. As recommended by OCTAVE, intent can be **accidental** or **deliberate**, and outcome can be **disclosure**, **modification**, **destruction or loss**, or **interruption of access**. Included in this study, though not stated in OCTAVE is scale. This is how far reaching the threat can be. Threats can be of **large scale**, **small scale**, or **very small scale**.

Therefore it is possible to characterize one threat according to these properties. For instance, here is the general description of one threat:

- Alternative: Poll Only
- Asset: Unmarked Ballot
- Actor: People of Markham
- Intent: Deliberate
- Outcome: Disclosure
- Scale: Very Small Scale

The most reasonable and applicable description of this threat to is that of ineligible voters who, possibly sponsored by some candidate's supporters, try to get a ballot to vote at the polls.

In this study, there are 4 alternatives, 3 assets, 4 actors, 2 intentions, 4 outcomes, and 3 scales. That means that there potentially 4x3x4x2x4x3 = 1152 threats. However the vast majority of these threat profiles have no real world meaning (e.g. anything with Poll only Alternative and Internet as the Actor) or have likelihood of occurrence that is basically 0 (e.g. an Internet alternative, Town of Markham as the actor, deliberate Intent, and threat of large scale). In the former example, someone using the Internet is not going to threaten poll voting, and in the latter example, no one at IT&S nor ES&S is likely to sabotage Internet voting so that the effect is of large scale.

As a matter of fact then, only 45 credible threats have been identified in this study.

Finally according to OCTAVE, each threat has an effect on the availability, integrity, and confidentiality vis-à-vis the threatened asset. For this study, these effects have the following interpretations:

- Integrity - the authenticity, accuracy, and completeness of an asset. In this study, this refers to **Election Integrity**: What is the effect on the extent to which the results of the election are accepted if the threat is realized?
- Availability - when or how often an asset must be present or ready for use. In this study, this refers to **Vote-ability**: What is the effect on the capability of a voter to cast a vote if the threat is realized?
- Confidentiality - the need to keep proprietary, sensitive, or personal information private and inaccessible to anyone who is not authorized to see it. In this study, this refers to **Confidentiality**: What is the effect on the confidentiality of voters or potential voters if the threat is realized?
- Public Trust. What is the effect on the public trust of the election process if the threat is realized? In this study, this refers to **Public Trust**. Though not included in OCTAVE, this effect is included for the study, since public opinion of how the election is conducted is very important when novel voting alternatives are employed.

IV. Methodology – Risk Analysis

More on Threat Profile

	What?	What We call it?	What we are considering
Threat type			
	Election alternative to consider	Alternative	polling only, polling+Internet voting 1 step, polling+Internet voting 2-step, mail-in only, Internet voting 1-step only, Internet voting 2-step only
	Asset that is threatened	Asset	elector's list, unmarked ballots, completed ballots, tabulation system
	What is the scale of the threat--large or small	Scale	large-scale, small-scale
	Who is threatening the asset	Actor	Town of Markham (workers representing ToM), People of Markham (voters and their friends/family, councillors and those helping them), Mail (Canada Post), Internet (anyone else who poses a threat by using the Internet)
	Their motives	Motives	Deliberate, Accidental
	Outcome of their access attempts	Outcomes	Disclosure (someone does damage by disclosing the asset to others), Modify (someone modifies the asset so that its use could potentially produce inconsistent, inaccurate, or questionable results), Loss/Destruction (someone loses or destroys some part or all of the asset), Access Interrupted (someone interrupts authorized access to the asset for short or long periods of time)
Threat profile			
	Example of how threat could be realized	Example	
	Likelihood that threat is realized	Likelihood	0%, Extremely Low (EL), Very Very Low, Very Low (VL), Low (L), Medium (M), High (H)
	Possibility of recovery after threat	Recovery Possibility	Low (L), Medium (M), High (H), 100%
Damage profile if ToM does rcover from threat			
	Damage to election integrity	Effect on Integrity	0, L, M, H
	What's the effect on capability to cast a vote	Effect on Voteability	0, L, M, H

	What's the likelihood that it violated voter's confidentiality	Effect on Confidentiality	0, L, M, H
	What's the effect on public trust if they found out	Effect on Public Trust	0, L, M, H
Damage profile if ToM <u>does not</u> recover from threat			
	Damage to election integrity	Effect on Integrity NR	0, L, M, H
	What's the effect on capability to cast a vote	Effect on Voteability NR	0, L, M, H
	What's the likelihood that it violated voter's confidentiality	Effect on Confidentiality NR	0, L, M, H
	What's the effect on public trust if they found out	Effect on Public Trust NR	0, L, M, H

How Risk Factors Are Calculated

# of total voters	# of Int(1) voters	# of int(2) voters
42,198	11,708	7210

Risk Profile	**Reasonable Risk**	**Risk Tolerant**	**Risk Averse**
1	1	2	3
	10	**15**	**5**
Likelihood	**Probabilities**	**Probabilities**	**Probabilities**
0	0.000%	0.0000%	0.000%
1-Extremely L	0.001%	0.0001%	0.024%
2-Very Very L	0.008%	0.0015%	0.120%
3-Very L	0.075%	0.0222%	0.600%
4-L	0.750%	0.3333%	3.000%
5-M	7.500%	5.0000%	15.000%
6-H	75.000%	75.0000%	75.000%
Factors	**Importance**	**Importance**	**Importance**
Integrity	50%	50%	50%
Voteability	20%	20%	20%
Confidentiality	10%	10%	10%
Public Trust	20%	20%	20%
	100%	100%	100%
Factor Effects	**2 Weights**	**2 Weights**	**2 Weights**
0	0.00	-	0.00

1-L	2.50	2.50	2.50
2-M	5.00	5.00	5.00
3-H	10.00	10.00	10.00
Recovery	**Probabilities**	**Probabilities**	**Probabilities**
1-L	0.25	25%	25%
2-M	0.75	75%	75%
3-H	0.9	90%	90%
5-100%	1	100%	100%
4-Very H	0.99	99%	99%
Scale	**5 Weights**	**5 Weights**	**5 Weights**
1-Large-Scale	5.00	5.00	5.00
2-Small-Scale	1.00	1.00	1.00
3-V-Small-Scale	0.20	0.20	0.20

EXAMPLE - as applied to the reasonable risk scenario

ID	Asset	Actor	Motive	Outcome	Alternative	Scale	Likelihood
012021	0-Various	1-ToM	2-Accidental	0-Various	2-Int(one)+poll	1-Large-Scale	3-Very L

Recovery	IntegrityEffect	voteabilityEffect	ConfidentialityEffect	PublicTrustEffect	IntegrityNR	VoteabilityNR	ConfidentialityNR
3-H	0	1-L	0	1-L	2-M	2-M	1-L

PublicTrustEffectNR	Scenario
3-H	Bugs with the ES&S product

Weight if you <u>don't</u> recover from threat = Importance of each factor x Effect is you don't recover
= Integrity Weight x IntegrityEffectNR + Voteability Weight x VoteabilityEffectNR + Confidentiality Weight x ConfidentialityEffectNR + Public Trust Weight x PublicTrustEffectNR

Integrity Weight	IntegrityNR	Voteability Weight	VoteabilityNR	Confidentiality Weight	ConfidentialityNR	Public Tust Weight	PublicTrustEffectNR
50%	2-M = 5.00	20%	2-M = 5.00	10%	1-L = 2.50	20%	3-H = 10.00

Weight if you don't recover from threat = (50% x 5.00) + (20% x 5.00) + (10% x 2.50) + (20% x 10.00)
= <u>5.75</u>

Weighted if you <u>do</u> recover from threat = Importance of each factor x Effect if you do recover
= Integrity Weight x IntegrityEffect + Voteability Weight x VoteabilityEffect + Confidentiality Weight x ConfidentialityEffect +
Public Trust Weight x PublicTrustEffect

Integrity Weight	IntegrityEffect	voteabilityEffect	Voteability	Confidentiality Weight	ConfidentialityEffect	PublicTrust Weight	PublicTrustEffect
50%	0 = 0.00	20%	1-L = 2.50	10%	0 = 0.00	20%	1-L = 2.50

Weight if you don't recover from threat = (50% x 0.00) + (20% x 2.50) + (10% x 0.00) + (20% x 2.50)
= <u>1.00</u>

Weight of threat = Likelihood of non-recovery x Weight if you don't recover from threat + Likelihood of recovery x Weight if you recover from threat

Recovery	<u>Likelihood of recovery</u>	<u>Likelihood of non-recovery</u>
3-H		

= 0.90 = 0.90 = 1 - 0.90 = 0.10

Weight of threat = (0.10 x 5.75) + (0.90 x 1.00) = 1.475

Risk Factor = Weight of threat x likelihood of threat x effect of scale x 1000

Scale	Likelihood
1-Large-Scale	3-Very L
=5.00	=0.075%

Risk Factor = 1.475 x 5.00 x 0.075% x 1000

= 5.53125

This is one of the risks of Internet voting only!
However this risk holds only for the percentage of voters who vote online. This risk must be added to the risks that exist at the polls since the alternative is Internet + polling.

A poll risk that is similar in type to this Internet voting risk is the risk at the polls of accidental spoilage or disclosure
Risk Factor for this risk = 0.3375

Risk Factor for Internet Alternatives

= Risk Factor for Internet Voting x Probabilty of Internet Voting + Risk Factor for Poll Voting of similar risk

Results - 2003	# of total voters	# of Int(1) voters	# of int(2) voters
	42,198	11,708	7210

Probability of Internet Voting (1 step) = 11,708 / 42,198 = 0.2775

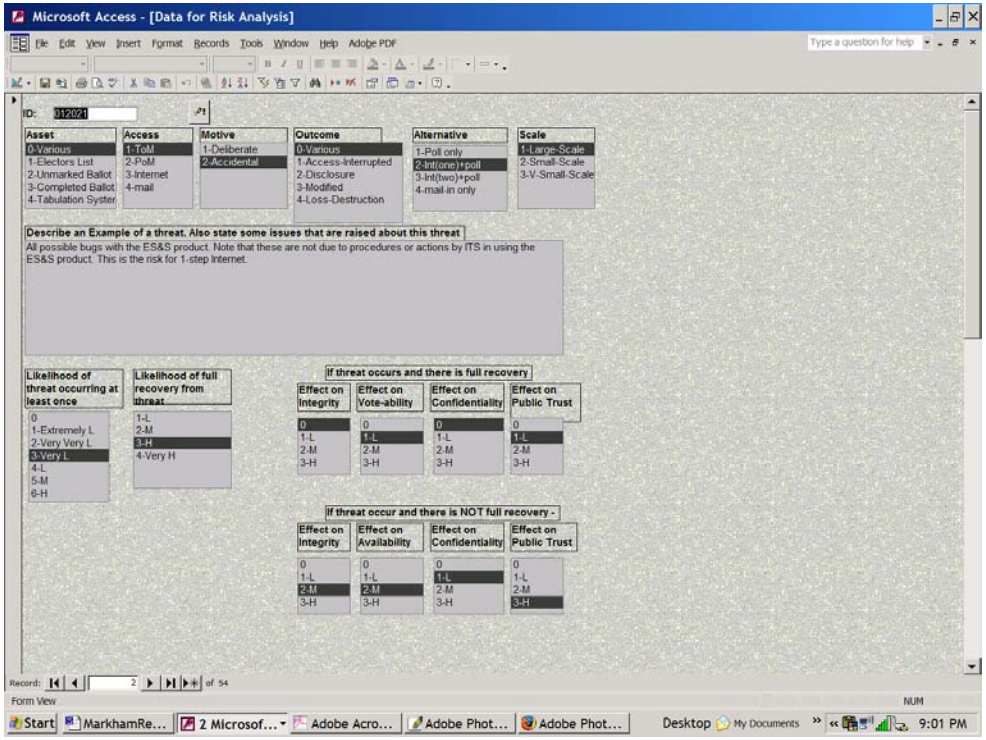
Risk Factor for this Internet Voting Risk = 5.53125 x 0.2775 + 0.3375 = 1.8722

Alternative	Total
1-Poll only	5.91125625
4-mail-in only	34.498125

2-Int(one)+poll	16.73074966
3-Int(two)+poll	12.5319817
Grand Total	69.67211261

For the Reasonable Risk Scenario, the sum of all Risk Factors for 1step Internet+poll = **16.7307**

V. Data


Microsoft Access - [Data for Risk Analysis]
File Edit View Insert Format Records Tools Window Help Adobe PDF
ID: 312021
Asset
0-Various
1-Electors List
2-Unmarked Ballot
3-Completed Ballot
4-Tabulation Syster
Access
1-ToM
2-PoM
3-Internet
4-mail
Motive
1-Deliberate
2-Accidental
Outcome
0-Various
1-Access-Interrupted
2-Disclosure
3-Modified
4-Loss-Destruction
Alternative
1-Poll only
2-Int(one)+poll
3-Int(two)+poll
4-mail-in only
Scale
1-Large-Scale
2-Small-Scale
3-V-Small-Scale
Describe an Example of a threat. Also state some issues that are raised about this threat
All possible bugs with the ES&S product. Note that these are not due to procedures or actions by ITS in using the ES&S product. This is the risk for 1-step Internet.
Likelihood of threat occurring at least once
0
1-Extremely L
2-Very Very L
3-Very L
4-L
5-M
6-H
Likelihood of full recovery from threat
1-L
2-M
3-H
4-Very H
If threat occurs and there is full recovery
Effect on Integrity
Effect on Vote-ability
Effect on Confidentiality
Effect on Public Trust
0
1-L
2-M
3-H
If threat occur and there is NOT full recovery -
Effect on Integrity
Effect on Availability
Effect on Confidentiality
Effect on Public Trust
Record: 2 of 54
Form View
NUM
Start
MarkhamRe...
2 Microsof...
Adobe Acro...
Adobe Phot...
Adobe Phot...
Desktop
My Documents
9:01 PM

ID	Asset	Actor	Motive	Outcome	Alternative	Scale	Likelihood	Recovery	Integrity Effect	voteability Effect	Confidentiality Effect	Public Trust Effect	Integrity NR	Voteability NR	Confidentiality NR	Public Trust Effect NR	Scenario
012012	0-Various	1-ToM	2-Accidental	0-Various	1-Poll only	2-Small-Scale	3-Very L	3-H	0	0	0	0	2-M	2-M	0	2-M	Accidental poll error resulting in spoilage or disclosure
012021	0-Various	1-ToM	2-Accidental	0-Various	2-Int(one)+poll	1-Large-Scale	3-Very L	3-H	0	1-L	0	1-L	2-M	2-M	1-L	3-H	Bugs with the ES&S product
012031	0-Various	1-ToM	2-Accidental	0-Various	3-Int(two)+poll	1-Large-Scale	3-Very L	3-H	0	1-L	0	1-L	2-M	2-M	1-L	3-H	Bugs with the ES&S product
012112	0-Various	1-ToM	2-Accidental	1-Access-Interrupted	1-Poll only	2-Small-Scale	4-L	4-Very H	0	1-L	0	0	2-M	2-M	0	2-M	Access to polls delayed because of poll worker oversight
012121	0-Various	1-ToM	2-Accidental	1-Access-Interrupted	2-Int(one)+poll	1-Large-Scale	2-Very Very L	3-H	0	1-L	0	1-L	1-L	2-M	0	3-H	Mishaps by ITM in testing or operation resulting in Website going down
012131	0-Various	1-ToM	2-Accidental	1-Access-Interrupted	3-Int(two)+poll	1-Large-Scale	2-Very Very L	3-H	0	1-L	0	1-L	1-L	2-M	0	3-H	Mishaps by ITM in testing or operation resulting in Website going down
031121	0-Various	3-Internet	1-Deliberate	1-Access-Interrupted	2-Int(one)+poll	1-Large-Scale	3-Very L	3-H	0	1-L	0	1-L	1-L	2-M	0	3-H	Denial-of-service attack
031131	0-Various	3-Internet	1-Deliberate	1-Access-Interrupted	3-Int(two)+poll	1-Large-Scale	3-Very L	3-H	0	1-L	0	1-L	1-L	2-M	0	3-H	Denial-of-service attack
131021	1-Electors List	3-Internet	1-Deliberate	0-Various	2-Int(one)+poll	1-Large-Scale	1-Extremely L	2-M	1-L	1-L	2-M	2-M	2-M	2-M	3-H	3-H	Hacker accessing electors list
131031	1-Electors List	3-Internet	1-Deliberate	0-Various	3-Int(two)+poll	1-Large-Scale	1-Extremely L	2-M	1-L	1-L	2-M	2-M	2-M	2-M	3-H	3-H	Hacker accessing electors list

212311	2-Unmarked Ballot	1-ToM	2-Accidental	3-Modified	1-Poll only	1-Large-Scale	2-Very Very L	2-M	1-L	1-L	0	1-L	2-M	2-M	0	2-M	Mistake at ToM in preparing mail out and wrong package mailed out
212321	2-Unmarked Ballot	1-ToM	2-Accidental	3-Modified	2-Int(one)+poll	1-Large-Scale	2-Very Very L	2-M	1-L	1-L	0	1-L	2-M	2-M	0	2-M	Mistake at ToM in preparing mail out and wrong package mailed out
212331	2-Unmarked Ballot	1-ToM	2-Accidental	3-Modified	3-Int(two)+poll	1-Large-Scale	2-Very Very L	2-M	1-L	1-L	0	1-L	2-M	2-M	0	2-M	Mistake at ToM in preparing mail out and wrong package mailed out
212341	2-Unmarked Ballot	1-ToM	2-Accidental	3-Modified	4-mail-in only	1-Large-Scale	2-Very Very L	2-M	1-L	1-L	0	1-L	3-H	3-H	0	3-H	Mistake at ToM in preparing mail out and wrong package mailed out
221112	2-Unmarked Ballot	2-PoM	1-Deliberate	1-Access-Interrupted	1-Poll only	2-Small-Scale	2-Very Very L	4-Very H	0	1-L	0	0	2-M	2-M	0	2-M	Protests at polls delaying voting
221123	2-Unmarked Ballot	2-PoM	1-Deliberate	1-Access-Interrupted	2-Int(one)+poll	3-V-Small-Scale	0	4-Very H	0	0	0	0	0	0	0	0	
221133	2-Unmarked Ballot	2-PoM	1-Deliberate	1-Access-Interrupted	3-Int(two)+poll	3-V-Small-Scale	0	4-Very H	0	0	0	0	0	0	0	0	
221213	2-Unmarked Ballot	2-PoM	1-Deliberate	2-Disclosure	1-Poll only	3-V-Small-Scale	2-Very Very L	1-L	1-L	0	0	1-L	2-M	0	0	2-M	People trying to vote at polls though they don't live in Markham
221223	2-Unmarked Ballot	2-PoM	1-Deliberate	2-Disclosure	2-Int(one)+poll	3-V-Small-Scale	2-Very Very L	1-L	0	1-L	1-L	1-L	2-M	2-M	2-M	2-M	People Internet voting using a notification card that's not theirs
221233	2-Unmarked Ballot	2-PoM	1-Deliberate	2-Disclosure	3-Int(two)+poll	3-V-Small-Scale	1-Extremely L	1-L	0	1-L	1-L	1-L	2-M	2-M	2-M	2-M	People Internet voting using a notification card that's not theirs

221243	2-Unmarked Ballot	2-PoM	1-Deliberate	2-Disclosure	4-mail-in only	3-V-Small-Scale	2-Very Very L	2-M	0	1-L	1-L	1-L	2-M	2-M	2-M	2-M	People voting by mail using a notification card that's not theirs
231222	2-Unmarked Ballot	3-Internet	1-Deliberate	2-Disclosure	2-Int(one)+poll	2-Small-Scale	1-Extremely L	1-L	1-L	1-L	0	2-M	3-H	2-M	0	3-H	Hackers giving free access to vote
231232	2-Unmarked Ballot	3-Internet	1-Deliberate	2-Disclosure	3-Int(two)+poll	2-Small-Scale	1-Extremely L	1-L	1-L	1-L	0	2-M	3-H	2-M	0	3-H	Hackers giving free access to vote
231321	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	2-Int(one)+poll	1-Large-Scale	1-Extremely L	3-H	0	1-L	0	3-H	0	2-M	0	3-H	Website defacing
231322	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	2-Int(one)+poll	2-Small-Scale	1-Extremely L	2-M	0	0	1-L	1-L	2-M	2-M	3-H	3-H	Phishing
231323	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	2-Int(one)+poll	3-V-Small-Scale	1-Extremely L	2-M	0	0	1-L	1-L	0	0	3-H	3-H	Spyware
231331	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	3-Int(two)+poll	1-Large-Scale	1-Extremely L	3-H	0	1-L	0	3-H	0	2-M	0	3-H	Website defacing
231332	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	3-Int(two)+poll	2-Small-Scale	1-Extremely L	3-H	0	0	1-L	1-L	2-M	2-M	3-H	3-H	Phishing
231333	2-Unmarked Ballot	3-Internet	1-Deliberate	3-Modified	3-Int(two)+poll	3-V-Small-Scale	1-Extremely L	3-H	0	0	1-L	1-L	0	0	3-H	3-H	Spyware

241013	2-Unmarked Ballot	4-mail	1-Deliberate	0-Various	1-Poll only	2-Small-Scale	3-Very L	3-H	0	1-L	1-L	1-L	2-M	2-M	3-H	3-H	Notification card mailed from ToM stolen
241023	2-Unmarked Ballot	4-mail	1-Deliberate	0-Various	2-Int(one)+poll	3-V-Small-Scale	4-L	1-L	0	1-L	1-L	1-L	2-M	2-M	3-H	3-H	Notification card mailed from ToM stolen
241033	2-Unmarked Ballot	4-mail	1-Deliberate	0-Various	3-Int(two)+poll	3-V-Small-Scale	1-Extremely L	4-Very H	0	1-L	1-L	1-L	2-M	2-M	3-H	3-H	Notification card mailed from ToM stolen
241043	2-Unmarked Ballot	4-mail	1-Deliberate	0-Various	4-mail-in only	3-V-Small-Scale	4-L	2-M	0	1-L	1-L	1-L	3-H	3-H	3-H	3-H	Notification card mailed from ToM stolen
242012	2-Unmarked Ballot	4-mail	2-Accidental	0-Various	1-Poll only	2-Small-Scale	2-Very Very L	3-H	0	1-L	1-L	1-L	1-L	2-M	2-M	2-M	Inaccurate mailings (e.g. wrong ballots) or mailman error
242022	2-Unmarked Ballot	4-mail	2-Accidental	0-Various	2-Int(one)+poll	2-Small-Scale	2-Very Very L	3-H	0	1-L	1-L	1-L	1-L	2-M	2-M	2-M	Inaccurate mailings (e.g. wrong ballots) or mailman error
242032	2-Unmarked Ballot	4-mail	2-Accidental	0-Various	3-Int(two)+poll	2-Small-Scale	2-Very Very L	4-Very H	0	1-L	1-L	1-L	1-L	2-M	2-M	2-M	Inaccurate mailings (e.g. wrong ballots) or mailman error
242042	2-Unmarked Ballot	4-mail	2-Accidental	0-Various	4-mail-in only	2-Small-Scale	2-Very Very L	3-H	1-L	1-L	1-L	1-L	2-M	2-M	2-M	3-H	Inaccurate mailings (e.g. wrong ballots) or mailman error
312012	3-Completed Ballot	1-ToM	2-Accidental	0-Various	1-Poll only	2-Small-Scale	1-Extremely L	4-Very H	0	0	0	1-L	1-L	0	0	2-M	Completed ballots disclosed
312021	3-Completed Ballot	1-ToM	2-Accidental	0-Various	2-Int(one)+poll	1-Large-Scale	1-Extremely L	3-H	1-L	0	0	2-M	2-M	0	0	3-H	Access to Internet voting results is delayed because of ES&S or ITM accident

312031	3-Completed Ballot	1-ToM	2-Accidental	0-Various	3-Int(two)+poll	1-Large-Scale	1-Extremely L	3-H	1-L	0	0	2-M	2-M	0	0	3-H	Access to Internet voting results is delayed because of ES&S or ITM accident
312042	3-Completed Ballot	1-ToM	2-Accidental	0-Various	4-mail-in only	2-Small-Scale	2-Very Very L	2-M	1-L	0	0	0	1-L	0	0	1-L	Acccess to completed mail-in ballots interrupted or are disclosed to those unauthorized
321222	3-Completed Ballot	2-PoM	1-Deliberate	2-Disclosure	2-Int(one)+poll	2-Small-Scale	3-Very L	1-L	1-L	0	0	0	1-L	0	0	2-M	Coercion to vote a certain way
321232	3-Completed Ballot	2-PoM	1-Deliberate	2-Disclosure	3-Int(two)+poll	2-Small-Scale	2-Very Very L	1-L	1-L	0	0	0	1-L	0	0	2-M	Coercion to vote a certain way
321242	3-Completed Ballot	2-PoM	1-Deliberate	2-Disclosure	4-mail-in only	2-Small-Scale	3-Very L	1-L	1-L	0	0	0	2-M	0	0	2-M	Coercion to vote a certain way
331021	3-Completed Ballot	3-Internet	1-Deliberate	0-Various	2-Int(one)+poll	1-Large-Scale	1-Extremely L	2-M	1-L	1-L	0	2-M	2-M	2-M	0	3-H	Hacker gains access to Internet voting results
331031	3-Completed Ballot	3-Internet	1-Deliberate	0-Various	3-Int(two)+poll	1-Large-Scale	1-Extremely L	2-M	1-L	1-L	0	2-M	2-M	2-M	0	3-H	Hacker gains access to Internet voting results
342143	3-Completed Ballot	4-mail	2-Accidental	1-Access-Interrupted	4-mail-in only	3-V-Small-Scale	5-M	1-L	0	0	0	0	1-L	1-L	0	1-L	Mail-in ballot mailed at right time arrives in ToM too late.

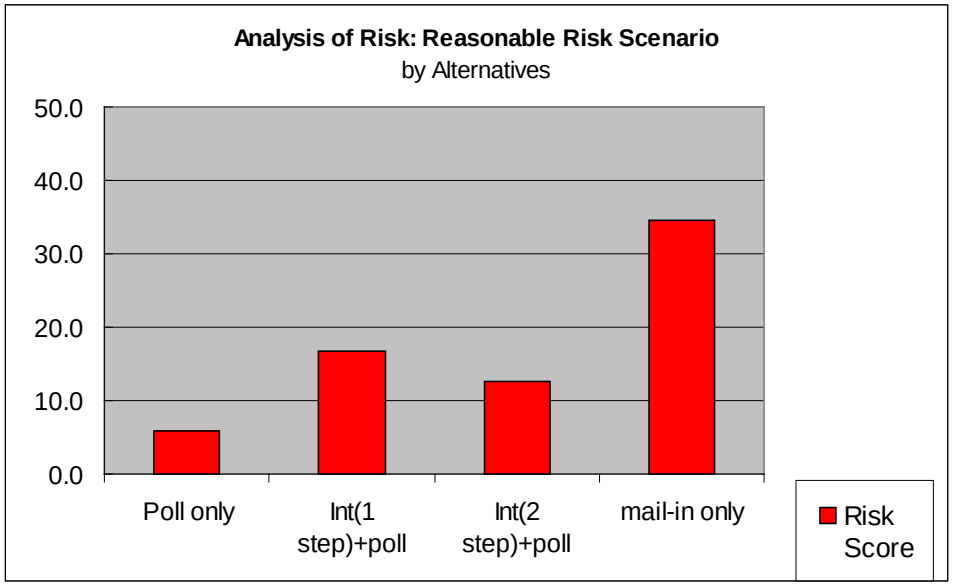
VI. Results

The analysis of results is done for three different profiles of risk-taking: 1) reasonable risk scenario; 2) risk tolerant scenario; and 3) risk averse scenario.

Reasonable Risk Scenario

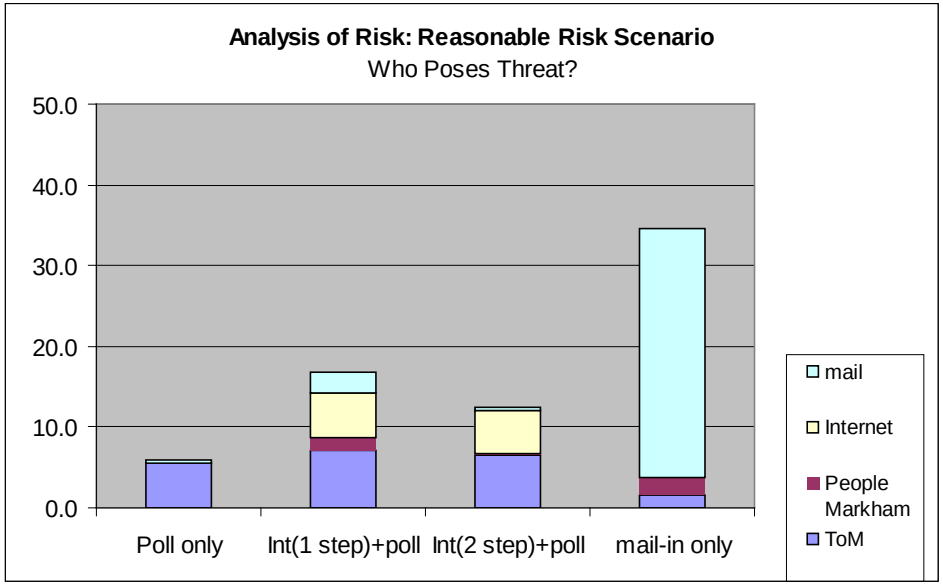
Analysis of Risk: Reasonable Risk Scenario

Alternative	Scaled Score
Poll only	5.9
Int(1 step)+poll	16.7
Int(2 step)+poll	12.5
mail-in only	34.5
	69.7



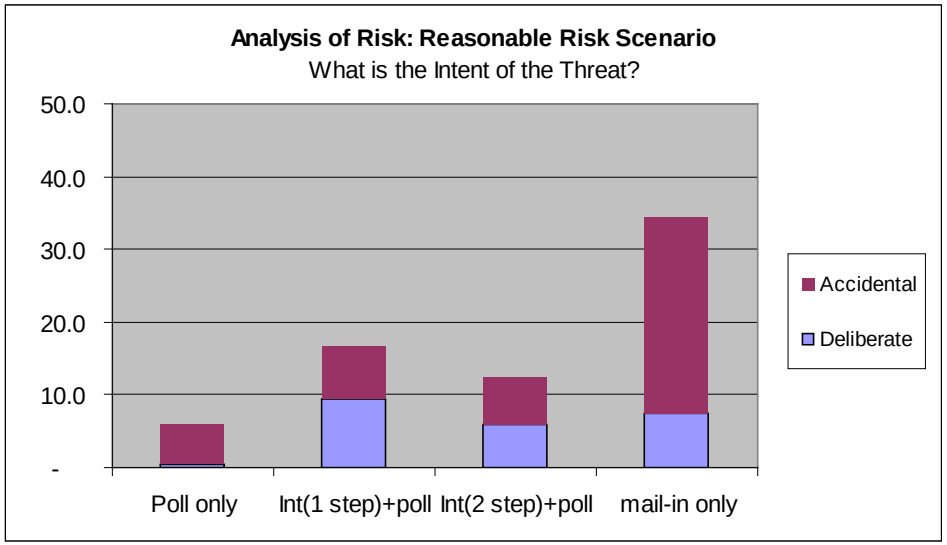
Who Poses Threats? - Reasonable Risk Scenario

Alternative	Town of Markham & poll workers	People of Markham (voters, people helping with campaigns)	Others exploiting the Internet	Those who have access to the mail system	Total
Poll only	5.4	0.1	0.0	0.4	5.9
Int(1 step)+poll	7.1	1.6	5.4	2.6	16.7
Int(2 step)+poll	6.5	0.2	5.4	0.4	12.5
mail-in only	1.6	2.2	0.0	30.7	34.5
Total	20.7	4.2	10.8	34.0	69.7



What is the intent of the the Threat? - Reasonable Risk Scenario

Alternative	Deliberate	Accidental	Total
Poll only	0.4	5.6	5.9
Int(1 step)+poll	9.4	7.3	16.7
Int(2 step)+poll	5.9	6.6	12.5
mail-in only	7.4	27.1	34.5
Total	23.1	46.6	69.7



What are the Threats? - Reasonable Risk Scenario

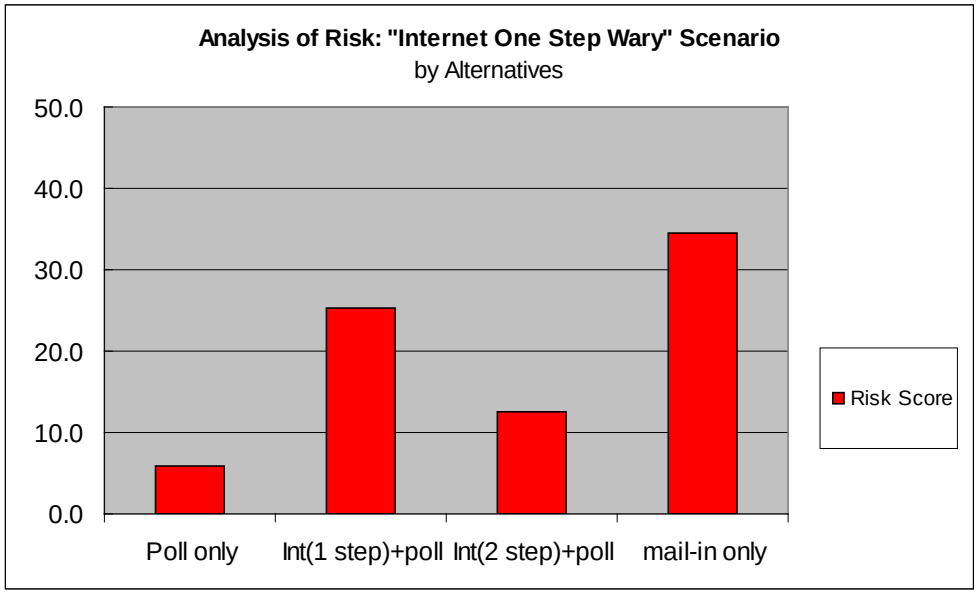
Rank	ID	Alternative	Scenario	Likelihood	Possibility of Recovery	Risk of Threat
1	342143	4-mail-in only	Mail-in ballot mailed at right time arrives in ToM too late.	7.5000%	25%	25.31
2	241043	4-mail-in only	Notification card mailed from ToM stolen	0.7500%	25%	5.16
3	031121	2-Int(one)+poll	Denial-of-service attack	0.0750%	90%	4.97
4	031131	3-Int(two)+poll	Denial-of-service attack	0.0750%	90%	4.97
5	012121	2-Int(one)+poll	Mishaps by ITM in testing or operation resulting in Website going down	0.0075%	90%	4.19
6	012131	3-Int(two)+poll	Mishaps by ITM in testing or operation resulting in Website going down	0.0075%	90%	4.13
7	012112	1-Poll only	Access to polls delayed because of poll worker oversight	0.7500%	99%	4.05
8	241023	2-Int(one)+poll	Notification card mailed from ToM stolen	0.7500%	25%	2.43
9	321242	4-mail-in only	Coercion to vote a certain way	0.0750%	25%	2.20
10	012021	2-Int(one)+poll	Bugs with the ES&S product	0.0750%	90%	1.87
11	321222	2-Int(one)+poll	Coercion to vote a certain way	0.0750%	25%	1.50
12	212341	4-mail-in only	Mistake at ToM in preparing mail out and wrong package mailed out	0.0075%	75%	1.48
13	012031	3-Int(two)+poll	Bugs with the ES&S product	0.0750%	90%	1.28
14	212311	1-Poll only	Mistake at ToM in preparing mail out and wrong package mailed out	0.0075%	75%	1.05
15	212321	2-Int(one)+poll	Mistake at ToM in preparing mail out and wrong package mailed out	0.0075%	75%	1.05
16	212331	3-Int(two)+poll	Mistake at ToM in preparing mail out and wrong package mailed out	0.0075%	75%	1.05
17	012012	1-Poll only	Accidental poll error resulting in spoilage or disclosure	0.0750%	90%	0.34
18	241033	3-Int(two)+poll	Notification card mailed from ToM stolen	0.0008%	99%	0.27
19	241013	1-Poll only	Notification card mailed from ToM stolen	0.0750%	90%	0.27
20	242042	4-mail-in only	Inaccurate mailings (e.g. wrong ballots) or mailman error	0.0075%	90%	0.21
21	131021	2-Int(one)+poll	Hacker accessing electors list	0.0008%	75%	0.15
22	131031	3-Int(two)+poll	Hacker accessing electors list	0.0008%	75%	0.15
23	321232	3-Int(two)+poll	Coercion to vote a certain way	0.0075%	25%	0.15
24	242022	2-Int(one)+poll	Inaccurate mailings (e.g. wrong ballots) or mailman error	0.0075%	90%	0.14
25	331021	2-Int(one)+poll	Hacker gains access to Internet voting results	0.0008%	75%	0.13

26	331031	3-Int(two)+poll	Hacker gains access to Internet voting results	0.0008%	75%	0.13
27	242032	3-Int(two)+poll	Inaccurate mailings (e.g. wrong ballots) or mailman error	0.0075%	99%	0.13
28	242012	1-Poll only	Inaccurate mailings (e.g. wrong ballots) or mailman error	0.0075%	90%	0.11
29	312042	4-mail-in only	Acccess to completed mail-in ballots interrupted or are disclosed to those unauthorized	0.0075%	75%	0.10
30	231321	2-Int(one)+poll	Website defacing	0.0008%	90%	0.10
31	231331	3-Int(two)+poll	Website defacing	0.0008%	90%	0.10
32	221223	2-Int(one)+poll	People Internet voting using a notification card that's not theirs	0.0075%	25%	0.06
33	231222	2-Int(one)+poll	Hackers giving free access to vote	0.0008%	25%	0.05
34	231232	3-Int(two)+poll	Hackers giving free access to vote	0.0008%	25%	0.05
35	221233	3-Int(two)+poll	People Internet voting using a notification card that's not theirs	0.0008%	25%	0.05
36	221213	1-Poll only	People trying to vote at polls though they don't live in Markham	0.0075%	25%	0.05
37	221112	1-Poll only	Protests at polls delaying voting	0.0075%	99%	0.04
38	221123	2-Int(one)+poll		0.0000%	99%	0.04
39	221133	3-Int(two)+poll		0.0000%	99%	0.04
40	221243	4-mail-in only	People voting by mail using a notification card that's not theirs	0.0075%	75%	0.03
41	312021	2-Int(one)+poll	Access to Internet voting results is delayed because of ES&S or ITM accident	0.0008%	90%	0.03
42	312031	3-Int(two)+poll	Access to Internet voting results is delayed because of ES&S or ITM accident	0.0008%	90%	0.02
43	231322	2-Int(one)+poll	Phishing	0.0008%	75%	0.02
44	231332	3-Int(two)+poll	Phishing	0.0008%	90%	0.01
45	312012	1-Poll only	Completed ballots disclosed	0.0008%	99%	0.00
46	231323	2-Int(one)+poll	Spyware	0.0008%	75%	0.00
47	231333	3-Int(two)+poll	Spyware	0.0008%	90%	0.00
						69.67

“Internet One Step Wary” Scenario

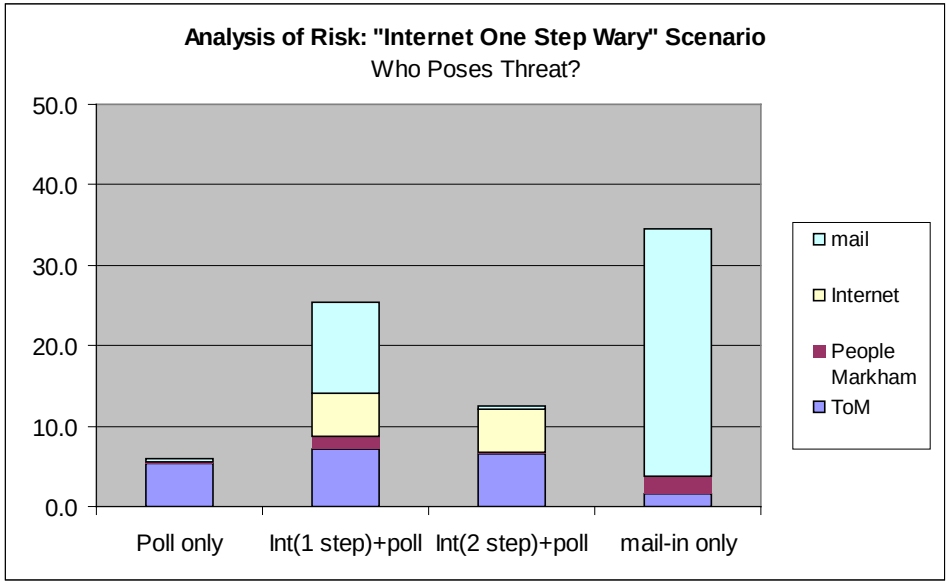
Analysis of Risk: "Internet One Step Wary" Scenario

Alternative	Risk Score
Poll only	5.9
Int(1 step)+poll	25.4
Int(2 step)+poll	12.5
mail-in only	34.5
	78.3



Who Poses Threats? - "Internet One Step Wary" Scenario

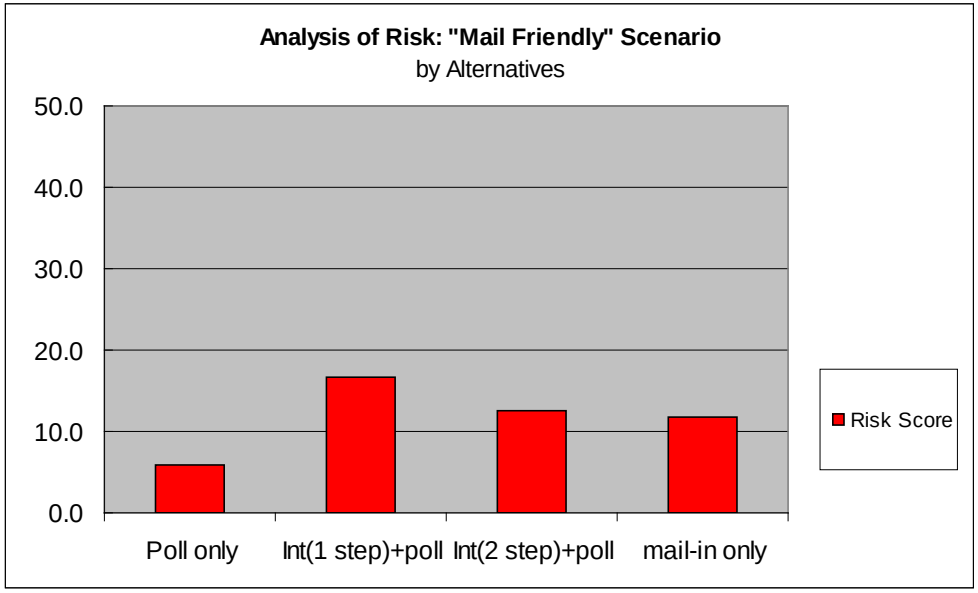
Alternative	Town of Markham & poll workers	People of Markham (voters, people helping with campaigns)	Others exploiting the Internet	Those who have access to the mail system	Total
Poll only	5.4	0.1	0.0	0.4	5.9
Int(1 step)+poll	7.1	1.6	5.4	11.2	25.4
Int(2 step)+poll	6.5	0.2	5.4	0.4	12.5
mail-in only	1.6	2.2	0.0	30.7	34.5
Total	20.7	4.2	10.8	42.7	78.3



“Mail Friendly” Scenario

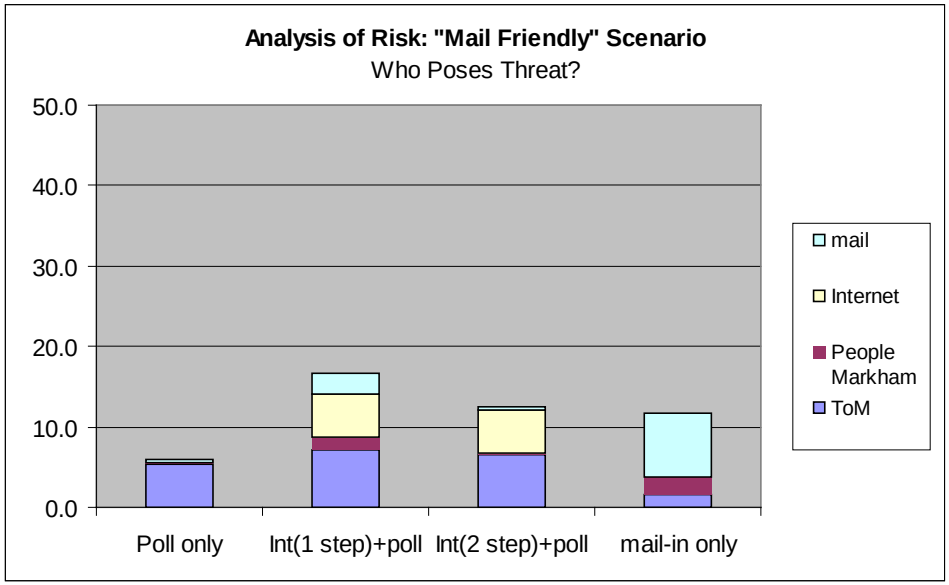
Analysis of Risk: "Mail Friendly" Scenario

Alternative	Risk Score
Poll only	5.9
Int(1 step)+poll	16.7
Int(2 step)+poll	12.5
mail-in only	11.7
	46.9



Who Poses Threats? - "Mail Friendly" Scenario

Alternative	Town of Markham & poll workers	People of Markham (voters, people helping with campaigns)	Others exploiting the Internet	Those who have access to the mail system	Total
Poll only	5.4	0.1	0.0	0.4	5.9
Int(1 step)+poll	7.1	1.6	5.4	2.6	16.7
Int(2 step)+poll	6.5	0.2	5.4	0.4	12.5
mail-in only	1.6	2.2	0.0	7.9	11.7
Total	19.1	1.9	10.8	3.3	46.9

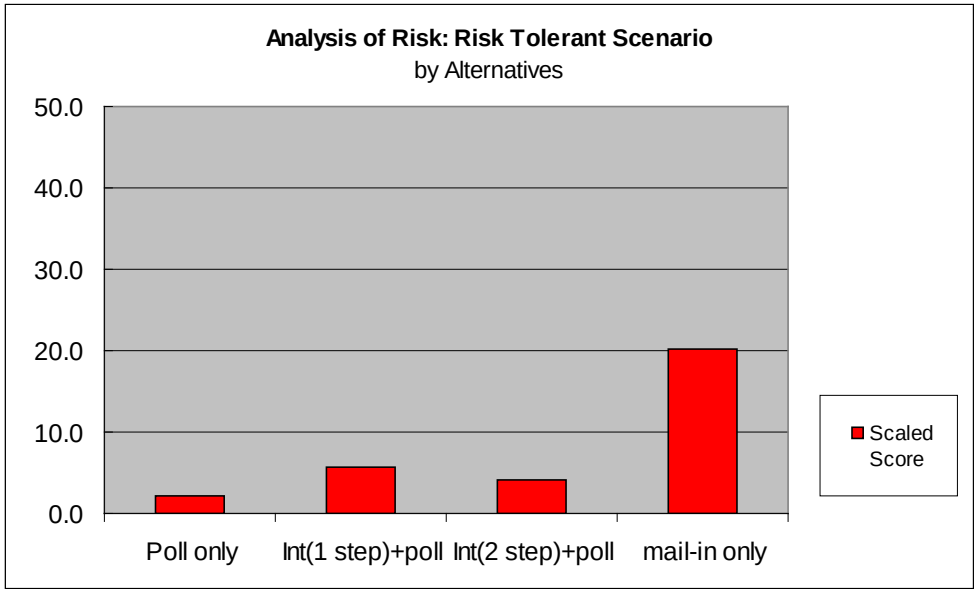


Risk Tolerant Scenario

This is a scenario in which the likelihood of threats is set lower, relative to the reasonable risk scenario, for all threats.

Analysis of Risk: Risk Tolerant Scenario

Alternative	Scaled Score
Poll only	2.2
Int(1 step)+poll	5.7
Int(2 step)+poll	4.1
mail-in only	20.2
	32.2



Risk Averse Scenario

This is a scenario in which the likelihood of threats is set higher, relative to the reasonable risk scenario, for all threats.

Analysis of Risk: Risk Averse Scenario

Alternative	Scaled Score
Poll only	41.2
Int(1 step)+poll	131.9
Int(2 step)+poll	107.1
mail-in only	118.1
	398.4