Prioritizing computer security controls for home users

Justin Fanelli Corresp., Equal first author, [1] , **John Waxler** Equal first author, [2]

[1] Marymount University, ARLINGTON, VA, United States
[2] School of Engineering and Applied Science, George Washington University, Washington, District of Columbia (DC), United States

Corresponding Author: Justin Fanelli
Email address: justin.fanelli@marymount.edu

Hundreds of thousands of home users are victimized by cyber-attacks every year. Most experts agree that average home users are not doing enough to protect their computers and their information from cyber-attacks. Improperly managed home computers can lead to individuals losing data, systems performing slowly, loss of identity, and ransom payments; en masse attacks can act in concert to infect personal computers in business and government. Currently, home users receive conflicting guidance for a complicated terrain, often in the form of anecdotal 'Top 10' lists, that is not appropriate for their specific needs, and in many instances, users ignore all guidance. Often, these popular 'Top 10' lists appear to be based solely on opinion. Ultimately, we asked ourselves the following: how can we provide home users with better guidance for determining and applying appropriate security controls that meet their needs and can be verified by the cyber security community? In this paper, we propose a methodology for determining and prioritizing the most appropriate security controls for home computing. Using Multi Criteria Decision Making (MCDM) and subject matter expertise, we identify, analyze and prioritize security controls used by government and industry to determine which controls can substantively improve home computing security. We apply our methodology using examples to demonstrate its benefits.

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

Prioritizing Computer Security Controls for Home Users

John Waxler[1], Justin Fanelli[2]

[1] College of Engineering, George Washington University, Washington, DC, USA
[2] School of Business and Technology, Marymount University, Arlington, VA, USA

Corresponding Author:
Justin Fanelli[2]
719 N Abingdon St Arlington VA 22203
Email address: justin.fanelli@marymount.edu

Abstract

Hundreds of thousands of home users are victimized by cyber-attacks every year. Most experts agree that average home users are not doing enough to protect their computers and their information from cyber-attacks. Improperly managed home computers can lead to individuals losing data, systems performing slowly, loss of identity, and ransom payments; en masse attacks can act in concert to infect personal computers in business and government. Currently, home users receive conflicting guidance for a complicated terrain, often in the form of anecdotal 'Top 10' lists, that is not appropriate for their specific needs, and in many instances, users ignore all guidance. Often, these popular 'Top 10' lists appear to be based solely on opinion. Ultimately, we asked ourselves the following: how can we provide home users with better guidance for determining and applying appropriate security controls that meet their needs and can be verified by the cyber security community? In this paper, we propose a methodology for determining and prioritizing the most appropriate security controls for home computing. Using Multi Criteria Decision Making (MCDM) and subject matter expertise, we identify, analyze and prioritize security controls used by government and industry to determine which controls can substantively improve home computing security. We apply our methodology using examples to demonstrate its benefits.

Introduction

There are ~4.07 billion home users with computers connected to the Internet world wide. (Internetlivestats, 2018) Home users rely on their computers to store and process personal, sentimental and financial data, which makes them targets for cyber criminals. As an example, one of the largest growing attacks against home users is tech support scams. "In the latest twist, tech support scammers were found using the Nuclear exploit kit to drop ransomware onto intended victims' computers." (Symantec Corportation, 2016) This attack encrypts users' data, eliminating access to their files. The victim then receives a pop-up from an organization impersonating an antivirus company. The pop-up claims that the target has been infected by a virus and that to retrieve the data, the target can pay for the virus to be removed. Little does the victim know, the person offering the fix is also the person that performed the attack.

- -

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

To aid home users in protecting themselves from cyber criminals, a number of conflicting resources have been created. These resources are often presented in what we call a 'Top 10' approach. This approach often provides clear, actionable, and time-conscious steps that home users can take to increase their computer's security in the form of a top 10 list. However, these lists rarely follow a systematic approach and even less frequently agree with or complement each other, making it hard for users to know which list is the right one to follow. Additionally, the lists do not provide a clear description of how they were generated, making them impossible to verify.

On the other end of the spectrum, cyber security professionals provide large organizations with detailed security frameworks backed by robust methodologies. These frameworks guide organizations in securing their information systems. However, their greater value lies in the methodology they present, which allows them to adapt their cyber security posture based on emerging threats. While invaluable to large enterprises, these frameworks are too complex, expensive and time consuming for the typical home user to understand, much less implement.

The goal of our effort is to bridge the gap between these two extremes. To achieve this, we present a hybrid solution that utilizes a robust methodology similar to the big business approach to produce a prioritized list modeled after top 10 lists. Our methodology was derived from a well-known cyber security framework (Risk Management Framework), a well-known system engineering technique (Multi Criteria Decision Making), and subject matter expertise. The results were then validated with a sensitivity analysis. We have defined a standard methodology based on systems engineering and cyber security standards that can improve the advice given to home users in securing their computers. We demonstrate the methodology step by step, including results, analysis and critique.

The remaining six major sections of this paper are as follows: the second section is background. It briefly covers the resources available for home users versus business users to access cyber security information. It speaks to the security frameworks available to big business and summarizes the value of Multi Criteria Decision Making (MCDM) and why we chose Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) as our MCDM methodology. The third section details our methodology and focuses on the inputs TOPSIS requires along with how TOPSIS is performed. The fourth section presents TOPSIS's results. The fifth section is the sensitivity analysis, where we test the stability of our results by creating variations in input and measuring the changes they cause to the original results. The sixth section provides discussion on some of the paper's limitations and opportunities for future work. The seventh section is our conclusion.

Materials & Methods

Background

This section presents background knowledge on MCDM and why TOPSIS was selected for this study. It then provides a brief overview of what top 10 lists and large security frameworks currently offer. This includes the selection of Risk Management Framework (RMF) as our source of security controls. Lastly, it presents an opportunity for improvement by using a hybrid approach.

Current State

We are not aware of past research that claims to provide home users a prioritized list of security controls through a transparent methodology. However, we will provide a brief discussion of available cyber security advice. We break this advice into two categories: the top 10 approach and the Big Business approach. Additionally, we found one paper that contains a call for action, "Our results suggest a need for extensive research and discussion to define and prioritize general security advice for non-expert users." (Reeder, Consolvo, & Ion, 2017) Our paper is a start to answering this call.

Top 10 Approach

Home users who want to secure their computers often look at magazines or websites that provide a top 10 list for securing their computers. The top 10 lists appeal to home users because they are usually simple, targeted to that audience and readily accessible. These lists generally do not provide a strong rationale for the actions they recommend, and almost never include the methodology on how the list was generated or prioritized. For example, the Massachusetts Institute of Technology (MIT) provides *Top Ten Safe Computer Tips* on their website. (Massachusetts Institute of Technology, 2017) It provides a limited rationale on why each tip is important but provides no methodology on how its list was generated. This leaves cyber security experts and home users with no way to validate the list provided, or any way of distinguishing one list from another. This begs the question of whether implementing such a list is an efficient use of resources. Without a methodology, there is no way to update these lists as cyber threats change.

Big Business's Approach

Large businesses often leverage entire frameworks to assess and then address their cyber security risks. These frameworks often require large teams to implement. These teams consist of training professionals, policy makers, system administrators, validators, and others. The benefit to these approaches is that they have been vetted by many cyber security professionals and they lay out in detail how they should be executed. These frameworks walk large organizations through assessing/reassessing their needs, laying out a strategy to address their needs, implementing their plan, and evaluating if their needs have been met. The problem for home users is that these frameworks were not created with them in mind. They are too lengthy and technical for anyone to complete by themselves. As an example, to implement RMF, you need to look at three primary documents: Federal Information Processing Standards (FIPS) 199 (13 pages), the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 (462 pages), and NIST Special Publication 800-37 Revision 1 (102 pages). (NIST, 2016) This does not include other referenced documents or supplementary material that is required to understand and support these three main documents. If a home user undertook reading these three documents, at over 500 pages, they may have a better understanding of security, but they would still have no idea what to do on their home systems.

We considered three major cyber security frameworks as the source for our security controls: NIST's Risk Management Framework (RMF), the International Organization for Standardization (ISO) / the International Electrotechnical Commission (IEC) 27001, and the European Telecommunications Standards Institute (ESTI) Cyber Security Standards. These frameworks all have similar advantages and disadvantages.

Ultimately, we selected NIST's RMF as the source of our security controls. RMF was selected because it is comprehensive, industry recognized where the research was performed, freely available and familiar to the researchers. RMF is a process for applying controls that leverage many existing NIST documents and standards. RMF "…provides an effective framework for selecting the appropriate security controls for an information system---the security controls necessary to protect individuals and the operations and assets of the organization." (NIST, 2016) For a brief comparison between RMF, 27001, and Cyber Security Standards, see Table 1.

Multi-criteria Decision Making

MCDM is a systems engineering technique that helps decision makers to make evidence-based choices when presented with multiple alternatives and multiple evaluation criteria. To choose a useful MCDM technique, we must consider our problem, our criteria, the available data, the relationships among the criteria, and the desired output.

According to Guitouni and Martel, "Despite the development of a large number of refined multicriterion decision aid (MCDA) methods, none can be considered as the `super method' appropriate to all decision-making situations." (Guitouni & Martel, 1998) (Note: The terms MCDM and MCDA are often used interchangeably.) Guitouni and Martel set forth seven guidelines in selecting a MCDM methodology.

Guitiouni and Martel broke the MCDM they examined into four categories: single synthesizing criterion, outranking, interactive, and mixed. Single synthesizing criterion methods provide an aggregation function to represent the decision maker's preference. Single synthesizing criteria methods were the focus for this paper because the results are easy to explain and are well suited for robust analysis.

Guitouni and Martel's MCDM Methodology Selection Guidelines:

> Guideline G1: Determine the stakeholders of the decision process. If there are many decision makers (judges), one should think about group decision making methods or group decision support systems (GDSS).
>
> Guideline G2: Consider the DM (Decision Maker) `cognition' (DM way of thinking) when choosing a particular preference elucidation mode. If he is more comfortable with pairwise comparisons, why use tradeoffs and vice versa?
>
> Guideline G3: Determine the decision problematic pursued by the DM. If the DM wants to get a ranking of alternatives, then a ranking method is appropriate, and so on.
>
> Guideline G4: Choose the multicriterion aggregation procedure (MCAP) that can properly handle the input information available and for which the DM can easily provide the required information; the quality and the quantities of the information are major factors in the choice of the method.
>
> Guideline G5: The compensation degree of the MCAP method is an important aspect to consider and to explain to the DM. If he refuses any compensation, then many MCAP will not be considered.

Guideline G6: The fundamental hypotheses of the method are to be met (verified); otherwise, one should choose another method.

Guideline G7: The decision support system coming with the method is an important aspect to be considered when the time comes to choose a MCDA method.

(Guitouni & Martel, 1998)

Guitouni and Martel go on to classify a number of popular MCDM according to guidelines two to six. A comprehensive discussion is outside the scope of this paper; however, the chart and explanation in Table 2 show the important values that led to the selection of TOPSIS as this paper's MCDM tool of choice.

1. TOPSIS employs a straightforward decision-making methodology (direct rating method). Guideline 2
    - This was preferred because it is easily applied and works well with a large number of alternatives.
2. TOPSIS was designed to answer the choice problematic; however, it is also well sorted to answer the ranking problematic. Guideline 3
    - Our goal is to rank the controls and TOPSIS fits this need well.
3. The input is cardinal and deterministic. Guideline 4
    - This fits well with our data gathering methodology and the direct scoring used on our alternatives.
4. TOPSIS allows for compensation. Guideline 5
    - We do not have required scores for any of our attributes.
5. Each attribute has monotonically increasing or decreasing utility (Yoon & Hwang, 1981) Guideline 6
    - This is required to use TOPSIS and is met by our selected attributes.

(Guitouni & Martel, 1998)

For more information on the criteria and values, see *Tentative Guidelines to Help Choosing an Appropriate MCDA Method* by Guitouni and Martel.

In broad terms, TOPSIS is an MCDM technique that seeks the best alternative by measuring the distance of existing alternatives from a hypothetical ideal solution and a hypothetical negative ideal solution, also called an anti-ideal solution. More detail on how TOPSIS performs appears in section 3.2, Perform TOPSIS.

Methodology

In this section, we lay out our methodology. This includes tailoring the list of security controls provided by RMF, setting up TOPSIS's inputs, and performing TOPSIS. To create this top 10 list, we followed the steps below.

1. Down Select and Tailor Security Controls
2. Identify TOPSIS Inputs
    2.1. Identify Criteria
    2.2. Rate Security Controls using Expert Elicitation
    2.3. Establish Criteria Weights
3. Perform TOPSIS Calculations

Down Select and Tailor Security Controls

One of the advantages that RMF offers is that it has over 200 controls, which provide guidance on how to address many security short comings. However, many of the controls are not applicable to home users. For example, RMF has a control entitled "Separation of Duties" that describes how roles such as configuration management, testing, and security configuration should be performed by different individuals. Many homes don't have four people, much less four people that can be assigned to these functions. If there is one person even performing these duties on a perfunctory level, they are doing a better job than most at keeping their systems secure.

To address this, three cyber security subject matter experts (SMEs) combed RMF's controls to down select controls applicable to home users. Because these controls are worded to focus on large government organizations, some tailoring was required to word them appropriately for home users. A large number of the controls could be applicable to home users in certain situations. However, for the sake of being concise and clearly demonstrating our methodology the experts focused on sixteen controls that were highly applicable to home users and were likely to be implementable. This down selection is not meant to be authoritative but is meant to provide the basis for a manageable example that is relatively easy to discuss.

When considering which controls should be included in this paper the SMEs considered:

1. Does this control apply to the home environment? (Some controls assume specific hardware or software is being used that is not often present in the home environment, for example, controls that assume servers are present.)
2. Does it make sense for a home user to implement this control? (Some controls assume the environment is a large organization and do not make sense for an organization the size of a family, for example, controls talking about separation of duties.)
3. Does the control remediate a threat that is present to home users?

To validate the selected controls against question three, the SMEs created a list of common cyber security threats that face home users. The threats used were identified by the SMEs, journal articles (Teymourlouei, 2015), and websites (Grimes, 2017) (Symantec, 2017) (Zaharia, 2015). Once created, the SMEs mapped the threats to the sixteen controls. If the control remediated that threat, it was marked as Maj, a major remediation, or as Min, a minor remediation. When a control was marked as a major remediation, it was judged to significantly decrease the chance of that threat being successful. When a control was marked as a minor remediation, it was judged to slightly decrease the chance of that threat being successfully exploited or to only protect against that threat in specific cases. Table 3 shows the remediation matrix that was generated by our three SMEs.

The goal of this mapping was to show that if the sixteen selected security controls are implemented successfully, then the most common threats to home users would be mitigated. As shown in the chart, every security control remediated at least two common threats, and all threats had at least one major remediation within the 16 controls. This leads us to the next section, where we identify the inputs to TOPSIS.

Identify TOPSIS Inputs

To complete TOPSIS, alternatives and criteria must be identified. Once this is complete, each alternative must be given a weight, and each alternative must be scored against each criterion. We have already discussed how we identified our alternatives. Our alternatives are the sixteen security controls we selected from RMF: Session Lock, Information Sharing, Account Management, System Acquisition, Media Protection, Security Awareness Training, Contingency

Planning, Risk Assessment, Configuration Settings, System Maintenance Policy and Procedures, Wireless Access, Audit and Accountability, Transmission Confidentiality and Integrity, Configuration Management, Malicious Code Protection, and Boundary Protection. We now identify the criteria we used to score the alternatives.

To select the appropriate criteria, it is important to consider the value of the controls being implemented along with the costs of implementation. This is the main idea of risk management, identifying to what extent risk should be mitigated when considering value and cost. In the case of security control implementation, the risk being managed is the threat to the home computer.

Criteria Selection

In TOPSIS, each alternative is scored against each criterion. For the results of TOPSIS to have value, the criteria that have an impact on our problem and stakeholders must be selected.

In this paper, we examined five criteria: two for measuring value and three for measuring cost.

We identified the value of each control based on:

1. Impact to security if this control is not implemented
    - This is important because our goal is to increase security. If implementing the control is not increasing security, there is no reason to implement it.
2. Length of time before this condition is exploited (if control is not implemented)
    - If your computer is unlikely to suffer ill effects in the next 100 years, it is unlikely that the risk is worth mitigating. However, if you expect the risk to be realized by the end of the day, you would probably want to take care of it immediately.

We identified the cost of implementing each control:

1. Time to implement a control
    - Time to implement the control is the major upfront cost a home user realizes when implementing security controls. Home users are unlikely to want to spend 100 hours to protect $50. However, they may want to spend 5 minutes to protect $50.
2. Time to maintain a control
    - This is the major recurring cost a home user suffers when implementing security controls. Some controls require weekly patching and others are set and forget. Many users are more willing to configure set and forget controls but do not keep up to date with ones that require regular maintenance.
3. Risk of Implementing a control
    - Some security controls have a risk associated with them. For example, if you put passwords on your computer and forget your password you lose access to your computer. In some cases, the risk of implementing a control offsets some of the value that control brings.

In short, we call these criteria Security Impact, Time to Exploit, Time to Implement, Time to Maintain, and Risk of Implementation. Notably, financial cost is missing from this list. Upon reviewing all our controls, we determined that there are free options available for home users to implement each control, and therefore elected to omit financial cost from our analysis.

Security Impact and Time to Exploit were clear choices for identifying the value of each control. As stated, the point of implementing security controls is risk reduction. Risk is often defined as Impact multiplied by Likelihood, where likelihood is the inverse of time to occur or in our case exploit. (OWASP, 2017)

The costs were identified by asking security experts, surveying websites, and talking to end users. Generally, users' biggest complaints are their time related to security and the adverse impact of implementing security (less user-friendly system).

Now that we have identified our controls and criteria, we need to score our controls with respect to our identified criteria.

Rate Security Controls using Expert Elicitation

There are many ways to score criteria. Generally, the best methods rely on objective data. In the case of security impact, this may require mapping all known attacks back to where a security control could prevent them, scoring the security impact of each attack and then determining a composite score for the control. These data do not exist and would be extremely difficult to generate. For this reason, we turned to Expert Elicitation (EE).

"Expert elicitation refers to a systematic approach to synthesize subjective judgments of experts on a subject where there is uncertainty due to insufficient data, when such data is unattainable because of physical constraints or lack of resources." (Slottje, Sluijs, & Knol, 2008) We lacked sufficient data for security value, time to exploit, time to implement, time to maintain and risk of implementation of each control, in other words, our criteria. For this reason, we created an online survey to ask security experts how they would score our criteria based on their experience.

Below are the questions we asked about each control in our online survey:

1) What is the likely impact to security if this control is not implemented?
2) How long does it take before this condition is likely to be exploited?
3) How much time actively working on the system does it take to implement this control (assuming you have the required expertise)? Actively working on the system refers to the time spent at a keyboard but not the time waiting for a download to complete or an installation to finish. Implement refers to initial implementation and not maintenance time.
4) How much time actively working on the system does it take to maintain this control (assuming you have the required expertise) per month?
5) What is the risk of implementing this control? (Example: If you implement passwords, you could lose your password and suffer a loss of availability.)

Survey

Our survey consisted of five questions for each of sixteen security controls, for a total of 80 questions. Additionally, space was given by each control for the participant to leave comments. The survey also included three additional questions about the participant's background in cyber security. The operational environment for the questions provided in this survey is the home use environment. This is described in detail in the introduction to the survey. It opens with, "The purpose of this study is to use TOPSIS, a multi criteria decision making method, to prioritize security controls for home users."

Participants

A total of 25 participants began the survey; however, six never completed it. Of the 19 remaining participants, 15 were included in the final TOPSIS analysis. Two of the participants were excluded from the final results because their responses in the free text field of the survey indicated they misunderstood the scope of the survey. Another was excluded because a large number of free text answers stated "it depends," but did not state on what their responses depended. One participant's survey response was excluded from the final results because the participant indicated that he had no cyber security experience or training. The participants whose survey results were included in the final results all self-identified as experts, had at least eight years of experience, and had either a relevant degree or professional certification in cyber security.

Delivery Mechanism

Participants were solicited via email to participate in the survey. The email provided a brief overview of the survey's purpose and a link to the website where the survey was hosted on surveyexpression.com. The website included a consent form and the survey questions. All surveys were completed anonymously. The survey and solicitation methodology went through the George Washington University's (GWU's) Office of Human Research Review Board and was deemed exempt (Study No: 011645 Study Title: Using Multi Criteria Decision Making for Security Control Selection in Risk Management Framework). Participants were selected for solicitation through the professional and academic connections of the authors.

Establish Criteria Weights

We have now provided our alternatives and scored our alternatives on our five criteria. Before we can perform TOPSIS, we also need to weight the relative importance of each criterion. Weights represent the importance of each criterion and are determined by the needs and desires of the home user. This should be determined by how they use their computers and how they view the importance of the confidentiality, integrity and availability of their computers as well as the information they contain and process. Each person's use, preference, and environment impact what criteria are most important to them. In this paper, we chose weights that reflected the priorities of a notional security conscious home owner. By adjusting these weights, new results can be calculated based on new preferences.

We will refer to our notional home owner as Bob. Bob and his family use their computers for online purchases and banking. Bob's children use their computers to access social media and school work. Bob is aware of growing security risks to his family's data and wants to secure their computers. He acts as the de facto security and IT specialist with some reliance on advice from friends and family. Additionally, as most people, he has limited time to devote to developing and maintaining a secure system.

Bob weights both security impact and time to exploit fairly high, showing his concern for security. Bob doesn't rate time to implement very high because he doesn't mind spending some time up front to secure his computers; however, he does rate time to maintain high because he doesn't want to spend much time revisiting security on a regular basis. We have identified our MCDM approach, defined our alternatives, established our criteria, and described our weights. We can now perform TOPSIS to generate our results.

Perform TOPSIS

Now that we have determined our criteria's weights and determined our alternatives' scores, we can use TOPSIS to rank our alternatives. TOPSIS seeks the best alternative by measuring the distance of existing alternatives from a hypothetical ideal solution and a hypothetical negative ideal solution, also called an anti-ideal solution. TOPSIS defines the ideal solution as an alternative with the best attributes of all alternatives. The negative ideal solution has the worst attributes of all alternatives. TOPSIS identifies the best solution by computing a combination of the closest alternative to the ideal solution and furthest alternative from the negative ideal. The following steps describe the calculations used when performing TOPSIS:

1. Populate a matrix with the alternatives, one to m, down the side. In our case, the matrix is populated with one to sixteen, representing our security controls. Populate the matrix with the scoring criteria, one to n, along the top. This is from one to five in our case, representing our five scoring criteria. Populate the bottom of the matrix with the weights for the columns' respective criteria. Finally, populate the rest of the matrix with the applicable scores X_{11} to X_{mn}.
2. Calculate the normalized decision matrix using the formula below, where r_{ij} represents the normalized value. This serves to transform the various criteria with their unique units into dimensionless quantity.

$$\boldsymbol{r_{ij}} = \frac{\boldsymbol{x_{ij}}}{\sqrt{\sum_{\boldsymbol{i=1}}^{\boldsymbol{m}} \boldsymbol{x_{ij}^2}}}, \boldsymbol{j = 1,2,\dots,n, i = 1,2,\dots,m}.$$

3. Calculate the weighted normalized matrix (V) by multiplying each attribute by its weight.

$$V = \begin{bmatrix} v_{11} \cdots & v_{1j} \cdots & v_{1n} \\ \vdots & \vdots & \vdots \\ v_{i1} \cdots & v_{ij} \cdots & v_{in} \\ \vdots & \vdots & \vdots \\ v_{m1} \cdots & v_{mj} \cdots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 v_{11} \cdots & w_j v_{1j} \cdots & w_n v_{1n} \\ \vdots & \vdots & \vdots \\ w_1 v_{i1} \cdots & w_j v_{ij} \cdots & w_n v_{in} \\ \vdots & \vdots & \vdots \\ w_1 v_{m1} \cdots & w_j v_{mj} \cdots & w_n v_{mn} \end{bmatrix}$$

where $\boldsymbol{w_j} = \frac{W_j}{\sqrt{\sum_{\boldsymbol{j=1}}^{\boldsymbol{n}} W_j}}, \boldsymbol{j = 1,2,\dots,n}.\ so\ that$

$$\sum_{\boldsymbol{j=1}}^{\boldsymbol{n}} W_j = 1\ and\ W_j\ is\ the\ oringal\ wight\ given\ to\ the\ indicator\ v_j, j = 1,2\dots,n.$$

4. Determine the positive ideal solution (A^+) and the negative solution (A^-). The 'best' solution as identified from TOPSIS is the closest to the ideal solution (a theoretical solution that has the best attributes of all identified solutions) and furthest from the negative ideal solution (a theoretical solution that has the worst attributes of all identified solutions). This is done using the following formulas:

$$A^+ = \left\{ \left(max_{V_{ij}} | j \in J_+ \right), \left(min_{V_{ij}} | j \in J_- \right) \right\} | i = 1,2,\dots m\} = \{v_1^+, v_2^+, \dots, v_j^+, \dots, v_n^+\}$$

$$A^- = \left\{ \left(min_{V_{ij}} | j \in J_+ \right), \left(max_{V_{ij}} | j \in J_- \right) \right\} | i = 1,2,\dots m\} = \{v_1^-, v_2^-, \dots, v_j^-, \dots, v_n^-\}$$

where $J_+ = \{j = 1,2,\dots,n | j\ associtated\ with\ benefit\ criteria\}$

$J_- = \{j = 1,2,\dots,n | j\ associtated\ with\ loss\ criteria\}$

5. Calculate the distance of each alternative from the positive (S_i^+) and negative ideal (S_i^-) solutions.

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^+ \right)^2},\ i = 1,2,\dots,m,$$

$$S_i^- = \sqrt{\sum_{j=1}^{n}\left(v_{ij} - v_j^-\right)^2},\ i = 1,2,\ldots,m.$$

6. Calculate the relative closeness to the idea solution(C_i^*). As C_i^* approaches 1, it approaches the ideal solution, and when it approaches 0, it approaches the negative solution.

$$C_i^* = \frac{S_i^-}{(S_i^+ + S_i^-)}, 0 < C_i^* < 1, i = 1,2,\ldots,m$$

7. Rank the alternatives. Those with the highest C_i^* are the most favorable and ranked the highest.

Once all of our data are put through TOPSIS, our calculations are complete, and our results are revealed.

Results

With TOPSIS complete, each alternative receives a score. The highest scored alternative is given rank 1; this means that it is the control that should be implemented first. The lowest ranked control is given rank sixteen and is the control that should be implemented last. After calculating the cumulative floating average, we realized that the rank was not stable, meaning that the rank was likely to change if new data were added. This is discussed in more detail in the next section, Sensitivity Analysis. To address this, we introduced preference bands grouping similarly scored alternatives together. Table 6 shows the results including control, rank, score, and preference band.

When a control has a different rank but the same preference band as another control, there is not a major difference and they are considered of equal value. It should be emphasized that one should implement all security controls of the first preference band before moving to the second and subsequent preference bands.

Remember, our goal is to make a prioritized top 10 list. Home users are used to lists that are actually 10 items long and are more likely to implement the security controls if there is not an overwhelming number. Ultimately, our top 10 list of security controls has become a top 11 and is as follows (listed in order of rank):

Session Lock, Information Sharing, Account Management, System Acquisition, Media Protection, Security Awareness Training, Contingency Planning, Risk Assessment, Configuration Settings, System Maintenance Policy and Procedures, and Wireless Access.

We chose to include 11 controls in our list because we want to include all the controls from our top three bands. As we stated, controls within the same band should be given equal importance, so it makes more sense to recommend implementing an additional control rather than splitting a band.

After our results were computed, we re-examined Table 3 and asked ourselves what happens if we drop Audit and Accountability, Transmission Confidentiality and Integrity, Configuration Management, Malicious Code Protection, and Boundary Protection, the security controls that didn't make our list. All of the threats we identified still have a major remediation except Distributed Denial of Service (DDoS)/DoS attack. It is interesting to note that DDoS attacks are usually thought to target large organizations; however, DDoS attacks are of growing concern to

PC gamers. (Incapsula, 2017) That being said, 11 of 16 controls providing major remediation for 17 of 18 threats provides a lot of value and reduces the workload of the home user.

Before moving on, we compared our top 11 list to three other lists of security advice for home users provided by four websites. First, we compared our threats to MIT's *Top Ten Safe Computer Tips* to compare a list to a reputable source. We found that MIT's tips provided major remediations for 15 of the 18 threats we identified. They did not fully address DDoS/Dos Attacks, Shoulder Surfing, or Key Logger (Hardware). (Massachusetts Institute of Technology, 2017)

We then performed a google search, "how to increase my home computer security", and compared the top three results that had ~10 items recommended. This excluded the second hit, *5 Ways to Increase Computer Security* by pctechguide.com. Vipreantivirus.com, hit one, quotes the source of its list as The Department of Homeland Security's United States Computer Emergency Readiness Team, and Us-cert.gov, hit 3, provides the same list. These lists have 9 pieces of advice and address 13 of the 18 threats we identified. They miss Environment, Physical Theft, Hardware Failure / Error, Software Failure / Error, and Key Logger (Hardware). (VIPRE, 2017) (US-CERT, 2017) The control they seem to be lacking most is Contingency Planning, which for home users is primarily backups. Finally, we compared our results to thetechrepublic.com, hit 4. Thetechrepublic.com provided 10 pieces of advice that addressed 6 of our 18 threats. It included advice such as use Linux and do not use Internet Explorer. (Wallen, 2017) This may enhance security but also may be outside of the scope of what many home users are willing to do. This validation provided further evidence that not all 'Top 10' lists provide the same quality of advice.

Additionally, we do not have a complete rationale or methodology regarding how these lists were developed. We know they consider the impact to security, but did they consider anything else? The comparison above is done solely on threat remediation as a measurement of security impact because that is all we can ascertain that the other lists address. Remember, we consider security impact, time to exploit, time to implement, time to maintain, and risk of implementation and provide our methodology. This means that our list is replicable, updatable, and seeks to provide advice that minimizes the burden on the home user.

After computing TOPSIS's results, it is important to perform sensitivity analysis to evaluate the stability of your results and account for imprecise input. (Triantaphyllou & Sánchez, 1997) "Often, data in multi-criteria decision making (MCDM) problems are imprecise and changeable. Therefore, an important step in many applications of MCDM is to perform a sensitivity analysis on the input data." (Triantaphyllou & Sánchez, 1997) Sensitivity Analysis (SA) is conducted when using MCDM techniques in order to show their robustness and the effect of minor changes of inputs on the results. (Pannell, 1997) In this paper, we discuss two types of sensitivity analysis. One is cumulative floating average, where we show the change in results as additional surveys are added, thus showing the change to the results as the values of our alternative's criteria change. Second, we perform sensitivity analysis by incrementing the weights of each of the criteria. "Most [MCDM] methods require definitions of quantitative weights for the criteria and this information is often difficult to obtain: the definition of weights itself is not very precise, nor are the values given by a decision-maker." (MARESCHAL, 1988) Because we cannot be confident that the decision maker has provided precise weights, it is important to evaluate the changes to the weights do to the results. If there is no change or the change is minor, we have greater confidence in the results.

Cumulative Floating Average

Figure 1 shows the cumulative floating average of the survey results. The x-axis represents additional survey responses being added. The y-axis represents TOPSIS rank. Value one on the x-axis shows the ranks provided by TOPSIS for the first survey. Value two on the x-axis shows the results provided by TOPSIS for the average of the first two surveys. Value three shows the results provided by TOPSIS for the average of the first three surveys. This continues until the x-axis reaches the value 15, which shows the average of all 15 survey results.
Generally, when sufficient data are present, the results will converge. Convergence means that as additional survey data (the input) are added, the rank of the alternatives (the output) will stay the same. In Figure 1, that is not the case. The graph above shows that the results are beginning to converge; however, they do not fully converge. Often when this is the case, it is simply a matter of gathering more data; however, it is unlikely that slightly more data will cause the results to converge in this case. This is because there are very small differences between many of the alternatives. Configuration Settings (rank 9) and System Maintenance Policy and Planning (rank 10) differ by less than .0001. A large number of other consecutive ranks differ by less than .01. To address this issue, preference bands were created, as shown in Table 6 and as shown in Figure 2.
The graph below is similar to the graph above; however, the y-axis represents preference instead of rank. The 16 alternatives were grouped into six preference bands. The preference groups were created by grouping alternatives with similar TOPSIS scores. When an alternative differed from the following alternative by less than .025, they were given the same preference. This led to similar alternatives being grouped together. Alternatives with the same preference are scored close enough that the order in which they are implemented is not important.
The preference graph above shows convergence by survey 12. This means that when adding surveys 13 through 15, the preference of an alternative didn't change. This is the desired result and shows that our preferences have stabilized.

Sensitivity Analysis by Varying Weight

"Sensitivity analysis (SA) is the study of how the uncertainty in the output of a model (numerical or otherwise) can be apportioned to different sources of uncertainty in the model input." (Saltelli, 2002) One of the inputs to our model was the weights provided in Table 4. It is important to understand if a slight change in weight has a large impact on the final results. Some variation is expected; however, if a large change in the output occurs after a minor change in the input, there may be an issue with the model.
In our sensitivity analysis, we examined each of our five attributes independently by increasing the weight of the attribute in 1% increments until a total of a 5% increase was reached. We also looked at what would happen if the weight was increased by 10%.

Security Impact

When the weight of Security Impact was increased, there was not much change in the preference of our alternatives. There was no change until we increased the weight from .25 to .30. At .30, Wireless Access changes from preference three to four, and Audit and Accountability changes from four to three. More changes occur when the weight increases to .35. It is interesting to note that the top and bottom rated alternatives do not change.

Exploitation Time

Security Impact is the attribute that causes the most change to our results. When its weight is increased from .20 to .24, changes begin to occur. Larger changes occur at weights of .25 and .30. This analysis is the only time that Session Lock moved out of preference one; however, it only moved one preference band to preference two.

Implementation Time

As the weight of implementation time is increased from .15 to .25, the preference of our alternatives did not change at all.

Maintenance Time

The weight of maintenance time is also slow to affect the preference of the results. There is no change in results until we jump from .25 to .35. At .35, System Maintenance Policy and Procedures moves to preference 4, and Transmission Confidentiality and Integrity moves to preference 3.

Adverse Impact

There is not much change when the weighting of adverse impact changes. The first change occurs when the weight of adverse impact is changed from .15 to .20. Another small change occurs when the weight is increased to .35. As was the case previously, these changes tend to occur in the middle of our preference range—not at the top or bottom.

Summary of Sensitivity Analysis by Varying Weights

After varying the weights of each criteria, we did not notice any surprising or concerning patterns. Minor variations in the weights did not cause major variation in the outputs. No changes occurred until there was at least a 4% increase in the weight of an attribute. This occurred when varying Exploitation Time. All other attributes did not cause a change until there was at least a 5% increase. This shows that minor variations in the decision maker's or user's priorities will not cause large changes in the results. Large changes will have a significant impact; however, this is expected and desired. If the decision maker has vastly different desires, the results and list of security controls should change to meet those desires.

In TOPSIS, there is concern that minor changes in the input could cause major changes in the output. If this happens, there is reason to question the validity of the results. Since our results are stable, we can feel confident that our results are accurate.

Discussion

We have presented a transparent methodology that can be verified by other cyber security experts, and we demonstrated this methodology by ranking sixteen tailored RMF security controls that are applicable to home users. This allows future researchers and cyber security experts to examine, analyze, and improve our methodology. Our approach presents a significant step forward in rigorously justifying and prioritizing security controls for the home user. However, our research is not without shortcomings.

We only ranked sixteen security controls of RMF's more than 200. We did this in part because our scope is home users and in part so the demonstration performed in this paper was concise. In the future, all controls that have even a small chance of being implemented by home users should be scored. If the larger community of cyber security experts agrees that a control is not very valuable, they will rank it near the bottom of the list and won't recommend it for implementation. Additionally, when this list is presented to a home user, a description of how to implement each control should be included.

In the future, this work can be expanded to examine other computer environments, including microbusinesses, large organizations, academic environments, and even government facilities. This would include applying EE to all of NIST security controls that apply to the organization of interest. Additionally, the survey would need to be updated in order to include questions tailored to the needs of the organization being examined. Once data was gathered, a tool could be developed to allow the company to set targets based on its needs and to provide a recommended order for implementing security controls. Our prioritized controls would fit well within RMF, giving organizations a transparent, quantitative, and robust methodology to complete security control selection and prioritization.

In this paper, weights were determined through a notational user. Additionally, only a single weight was varied at a time through sensitivity analysis. In the future, other sets of weights could be analyzed and sensitivity could be analyzed by simultaneously varying the weights of multiple criteria.

Last, when a large number of results are presented by TOPSIS, it is not unusual for some of the results to clump together. In this paper, we addressed clumping with preference bands. These bands were created by using heuristics to group similarly scored solutions. However, in the future, these bands could be created using a more quantitative method.

Conclusions

We presented a transparent methodology to generate a list of security controls for home users and described how and why this methodology was created.

In the background, we

1. Identify an Appropriate MCDM Technique – TOPSIS was selected
2. Identify a Base Set of Security Controls – RMF's Controls were identified

In the methodology, we

3. Down Select and Tailor Security Controls
4. Identify TOPSIS Inputs
   4.1. Identify Criteria
   4.2. Rate Security Controls using Expert Elicitation
   4.3. Establish Criteria Weights
5. Perform TOPSIS

In the results and data analysis section, we

6. Present the Results
7. Perform Sensitivity Analysis

We presented the results of our example as a top 11 list. This list considers the security impact, time to exploit, time to implement, time to maintain, and risk of implementation for each control. The major benefit of the methodology we present is that it can be scrutinized, verified, and updated as cyber threats change. It is a strategy the cyber community can further develop and discuss to ensure that they give home users (and other non-experts) accurate, well-thought out and efficient security advice, similar to that enjoyed by big business.

Acknowledgements

A special thank you to family, advisors, friends and participants who have supported this investigation and have looked forward to this sharing of its findings.

References

ESTI. (2017, September 19). *cyber-security*. Retrieved from etsi.org: http://www.etsi.org/technologies-clusters/technologies/cyber-security

Grimes, R. A. (2017, August 21). *The 5 cyber attacks you're most likely to face*. Retrieved from csoonline.com: https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html

Guitouni, A., & Martel, J.-M. (1998). Tentative Guidlines to Help Choosing an Approriate MCDA Method. *European Journal of Operational Research*.

Incapsula. (2017, September 27). *Protecting Gamers: Answering Your Questions About Stopping DoS and DDoS Attacks*. Retrieved from incapsula.com: https://www.incapsula.com/blog/protecting-gamers-from-dos-ddos-attacks.html

Internetlivestats. (2017, August 26). *Internetlivestats*. Retrieved from internet-users: http://www.internetlivestats.com/internet-users/

ISO. (2017, September 19). *ISO/IEC 27000 family - Information security management systems*. Retrieved from iso.org: https://www.iso.org/isoiec-27001-information-security.html

MARESCHAL, B. (1988). Weight stability intervals in multicriteria decision aid. *European Journal of Operational Research*, 54-64.

Massachusetts Institute of Technology. (2017, August 8). *Top Ten Safe Computing Tips*. Retrieved from mit.edu: https://ist.mit.edu/security/tips

NIST. (2016, 1 25). *http://csrc.nist.gov/*. Retrieved from groups/SMA/fisma/framework.html: http://csrc.nist.gov/groups/SMA/fisma/framework.html

OWASP. (2017, September 27). *OWASP Risk Rating Methodology*. Retrieved from OWASP.org: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Pannell, D. J. (1997). Sensitivity analysis of normative economic models: theoretical framework and practical strategies. *Agricultural Economics*, 139-152 .

Reeder, R. W., Consolvo, S., & Ion, I. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users. *IEEE Security & Privacy*.

Saltelli, A. (2002). Sensitivity Analysis for Importance Assessment. *Risk Analysis*, 579-590.

Slottje, P., Sluijs, J. v., & Knol, A. (2008). *Expert Elicitation: Methodological suggestions for its use in environmental health impact assessments* . National Institute for Public Health and the Environment Centre for Environmental Health Research .

Symantec. (2017, September 9). *The 11 most common computer security threats*. Retrieved from symantec-norton.com: http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

Symantec Corportation. (2016). *Internet Security Threat ReportInternet Report.* Mountain View, CA: Symantec Corportation.

Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*. Retrieved from http://waset.org/publications/10000665/quick-reference-cyber-attacks-awareness-and-prevention-method-for-home-users

Triantaphyllou, E., & Sánchez, A. (1997). A Ssensitivity Analysis Approach For Some Deterministic MultiCriteria Decision Making Methods. *Decision Sciences*, 151-194.

US-CERT. (2017, September 27). *Security Tip (ST15-003)*. Retrieved from us-cert.gov: https://www.us-cert.gov/ncas/tips/ST15-003

VIPRE. (2017, september 27). *9 Ways to Improve the Security of Your Home Computer*. Retrieved from vipreantivirus.com: https://blog.vipreantivirus.com/security-tips/9-ways-to-improve-the-security-of-your-home-computer/

Wallen, J. (2017, Sepetember 27). *10 things you can do to improve network and PC security*. Retrieved from thetechrepublic.com: http://www.techrepublic.com/blog/10-things/10-things-you-can-do-to-improve-network-and-pc-security/

Yoon, & Hwang. (1981). *Multiple Attribute Decision Making-Methods and Applications A State-of-the-Art Survey.* Berlin, Germany: Springer-Verlag.

Zaharia, A. (2015, November 11). *Keep My Computer Safe from Cyber Threats that Target Home Users*. Retrieved from heimdalsecurity.com: https://heimdalsecurity.com/blog/keep-my-computer-safe-from-cyber-threats-that-target-home-users/

Table 1 (on next page)

List of relevant security frameworks

Framework	Freely Available	Comprehensive	Industry Recognized
NIST RMF (NIST, 2016)	Yes	Yes	In United States
ISO/IEC 27001 (ISO, 2017)	No	Yes	Yes
ESTI Cyber Security Standards (ESTI, 2017)	Yes	Yes	In Europe

Table 1 - Security Frameworks

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

Table 2 (on next page)

Key TOPSIS selection criteria

Guideline	1	2	3	4	5	6	7
		Straightforward Total preorder	Ranking	Cardinal	Absolute Totally	Monotonic	N/A

Table 2 - TOPSIS Selection Criteria

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

Table 3(on next page)

Control-to-Threat Mapping

Controls \ Threats	Social Engineering	Malware/Adware Automated	Malware/Adware User Action	Password Attacks	DDoS / DoS Attacks#	Man in the Middle	Eavesdropping	Session Hijacking	SPAM	Environment (power loss,etc.)	Physical Theft	Hardware failure / error	Software failure/error	User Error	Shoulder Surfing	Snooping (without hacking)	Keystroke Logger Software	Key Logger Hardware
Session Lock			Min											Min		Maj	Maj	
Information Sharing	Min															Min		
Account Management		Min	Maj								Maj			Maj		Maj	Maj	
System Acquisition												Min	Min					
Media Protection											Maj					Min		
Security Awareness Training	Maj		Maj	Maj		Maj		Maj	Maj					Maj	Maj		Min	Min
Contingency Planning										Maj	Maj	Maj	Maj					
Risk Assessment										Min	Min							
Configuration Settings				Maj					Min	Maj	Maj	Min	Min					Maj
System Maintenance Policy and Procedures		Maj	Min			Maj	Min					Min	Min	Min			Min	
Wireless Access					Min		Maj											
Audit and Accountability			Min											Min			Min	Maj
Transmission Confidentiality and Integrity						Maj	Maj	Maj										
Configuration Management		Min	Min			Min	Min							Min			Min	Maj
Malicious Code Protection		Maj	Maj			Min	Min							Min			Maj	
Boundary Protection		Maj	Min		Maj	Min	Min		Min									

Table 1 - Control to Threat Mapping

Table 4(on next page)

Home User Criteria Weights

Criteria	*Weight*
Security Impact	.25
Time to Exploit	.2
Time to Implement	.15
Time to Maintain	.25
Risk of Implementation	.15

Table 1 - Home Owner Criteria Weights

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

Table 5 (on next page)

Notional TOPSIS Matrix

Criterion Titles	Criterion 1	Criterion 2	• • •	Criterion n
Alternative 1	X_{11}	X_{12}	• • •	X_{1n}
Alternative 2	X_{21}	X_{22}	• • •	X_{2n}
• • •	• • •	• • •	• • •	• • •
Alternative m	X_{m1}	X_{m2}	• • •	X_{mn}
Criterion Weights	W_1	W_2	• • •	W_n

Table 1 - Notional TOPSIS Matrix

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

Table 6 (on next page)

Ranked List of Alternative Approaches

Control	Rank	TOPSIS Score	Preference Band
Session Lock	Rank 1	0.678900129	Preference 1
Information Sharing	Rank 2	0.557860567	Preference 2
Account Management	Rank 3	0.541394122	Preference 2
System Acquisition	Rank 4	0.517944871	Preference 2
Media Protection	Rank 5	0.46340047	Preference 3
Security Awareness Training	Rank 6	0.455556353	Preference 3
Contingency Planning	Rank 7	0.453121506	Preference 3
Risk Assessment	Rank 8	0.446371585	Preference 3
Configuration Settings	Rank 9	0.427878107	Preference 3
System Maintenance Policy and Procedures	Rank 10	0.427806016	Preference 3
Wireless Access	Rank 11	0.414003266	Preference 3
Audit and Accountability	Rank 12	0.375586409	Preference 4
Transmission Confidentiality and Integrity	Rank 13	0.366434466	Preference 4
Configuration Management	Rank 14	0.352386874	Preference 4
Malicious Code Protection	Rank 15	0.232172916	Preference 5
Boundary Protection	Rank 16	0.122421284	Preference 6

Table 1 - Ranked Alternatives

Figure 1 (on next page)

Cumulative Floating Point Average By Alternative

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.27540v1 | CC BY 4.0 Open Access | rec: 15 Feb 2019, publ: 15 Feb 2019

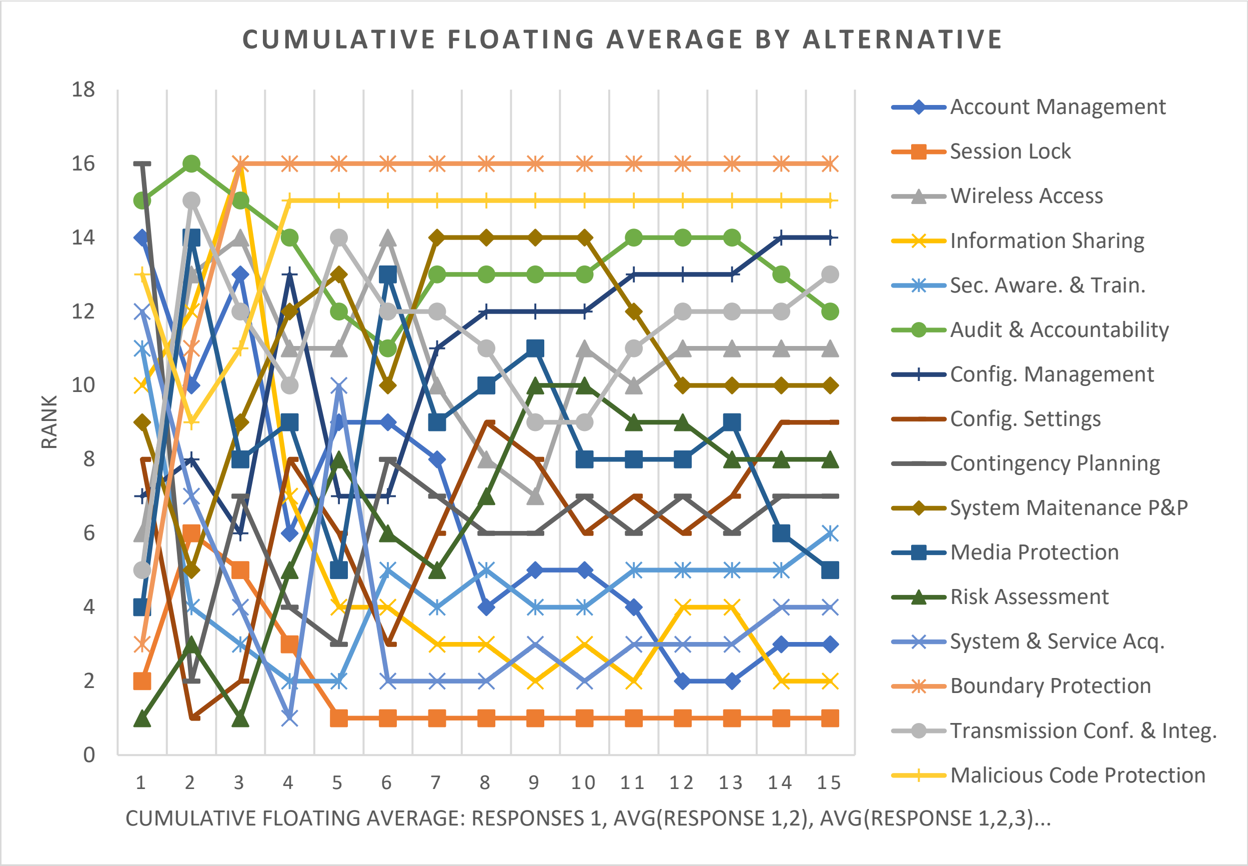

Figure 1 - Cumulative Floating Average by Alternative

Figure 2 (on next page)

Cumulative Floating Average by Group Preference

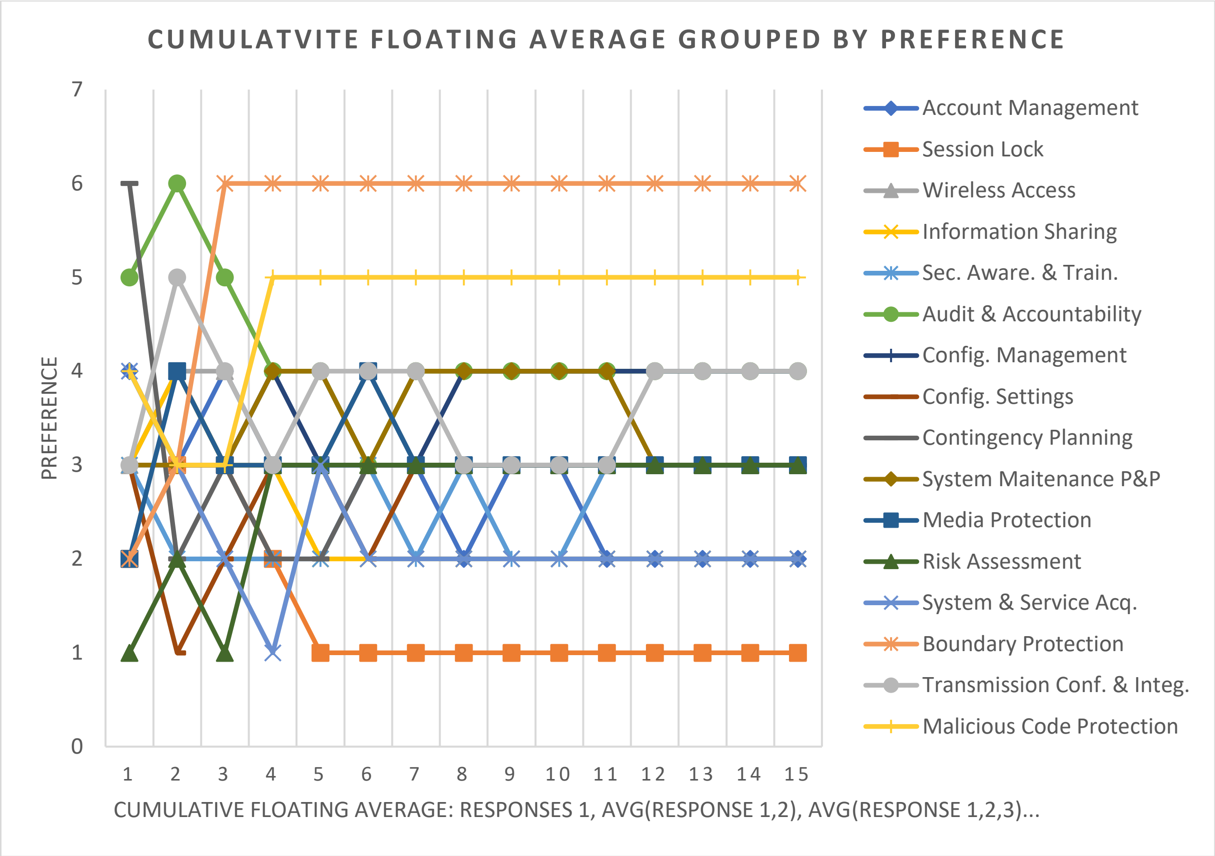

Figure 1 - Cumulative Floating Average by Preference