Title: “Managing Subjectivity in Qualitative Risk Assessment of Communication Networks Using a Modified Delphi Approach”

Topic Area: Telecommunications Security & Critical Infrastructure / Network Security

Authors: Kevin Shaffer, Fort Hays State University

Kevin Shaffer is an associate professor in the Department of Information Networking and Telecommunications with instructional responsibilities in data communication theory and advanced networking.

Email Address: kshaffer@fhsu.edu

Phone: 785-628-4484

Fax: 785-628-4098

Publication Preference: Abstract and Full Paper
Abstract
Security assessments for communication networks play an important risk management role because they allow risks to be prioritized for mitigation or risk acceptance. Qualitative risk assessments that involve intangible elements require the subjective judgment of the security analyst completing the risk assessment and this may lead to low confidence in the results due to a perception that evaluations will vary, depending upon the analyst or security group completing the assessment. One approach to handling the variability of subjective evaluation is to seek consensus from a group of knowledgeable stakeholders or experts. One formal approach to developing consensus of expert opinion or expert evaluations is the Delphi method. Delphi studies are more common in economic forecasting or health care studies, but are applicable to many fields where intangible elements must be considered in forming expert opinion. A modified Delphi method involving two Delphi exercises is integrated with the ETSI's TIPHON risk assessment methodology to provide a formalized qualitative assessment procedure that should reduce variability and improve confidence in the risk assessment of telecommunications networks. A brief case implementing the proposed methodology is described and implications are considered. The paper concludes with opportunities for further study in this area.
Introduction

Risk assessment can be viewed as an attempt at forecasting harm so that measures can be taken to reduce potential damages. Predicting the future is a subjective process and without a formalized process, results can vary. Some formalized methods of forecasting reduce the variability of evaluations by building consensus from multiple experts. Delphi methods are one such formal method. An approach for using Delphi methodology in information systems security risk assessment is described in this paper. The following section notes some issues with the subjective nature of qualitative risk assessments and identifies Delphi methodology as one approach to solving this issue. The remaining sections of this paper introduce an application of the Delphi method to a risk assessment method proposed by the European Telecommunications Standards Institute. The sections describe a multi-step process that can be used to develop consensus in threat identification and the inputs that determine risk products for each threat.

Subjectivity

When reliable data concerning information system security threats and system costs are not available, security analysts can make use of qualitative risk assessment methods to determine relative levels of risks to a system (GAO 1999). Many researchers note that qualitative risk assessment methods are subjective (Baskerville 1993; Hamdi and Boudriga 2003; Hoo 2000; Stonebumer et al. 2001). This is because qualitative risk assessments rely on subjective evaluations of the intangible risk characteristics, such as threat likelihood and impact severity (Stonebumer et al.). Subjective evaluations depend upon the person or group conducting the assessment, leading to variability in the results. The consequence is that qualitative risk assessment results are open to controversy (Hoo). One method of dealing with the variability of subjective evaluations is the use of a Delphi model (or Delphi technique) to evaluate the
subjective elements. Delphi models are useful in subjective analysis, especially when the subjective inputs become the dominating parameters (Linstone and Turoff 2002). Because some qualitative risk assessment methods rely heavily on subjective inputs (ETSI 2003; Stonebumer et al.), they appear to be good candidates for the application of Delphi techniques.

The aim of this paper is to propose a risk assessment method that makes use of formal Delphi techniques during the subjective evaluation processes found within qualitative risk assessments. Delphi techniques could be applied to many different risk assessment methodologies, in which subjectivity seems to be inherent (Freeman et al. 1997), but the proposal here is to apply the technique to the risk assessment methodology identified by the European Telecommunications Standards Institute (ETSI) for the TIPHON communications architecture (ETSI 2003). ETSI's TIPHON risk assessment methodology, hereafter referred to as TRAM, is a qualitative risk assessment method that requires the identification of threats to a system and then the determination of the likelihood and impact severity of each threat. Delphi techniques can be used as a method of identifying the system threats for TRAM as well as evaluating the likelihood and impact severity of each threat. Once these characteristics are assessed, risks can be calculated following the TRAM formula and the risks can be reviewed using TRAM's recommendations.

The TRAM Approach to Risk Assessment

The European Telecommunications Standards Institute specifies the use of a simplified qualitative risk assessment (TRAM) for TIPHON systems in technical specification ETSI TS 102 165-1 (ETSI 2003). While the specification makes no reference to TRAM's historical development, the specification is similar to the risk assessment method specified by the National
Institute of Standards and Technology in special publication 800-30 (Stonebumer et al. 2001, chap. 3).

TRAM first specifies that security threats be identified for the subject system. After threats are identified a security analyst evaluates each one to determine the threat’s likelihood and impact severity. This determination considers the cost and motivation of a threat source along with the difficulty of exploiting vulnerabilities (including countermeasures). TRAM does not specify that vulnerabilities be identified for specific threats separately from an evaluation of likelihood in contrast to the NIST approach. A security analyst considering all aspects of difficulty, cost, and motivation makes a subjective decision and assigns a numeric value for the likelihood of occurrence to each threat. Likelihood values of 1 for unlikely, 2 for possible and 3 for likely may be assigned. TRAM provides guidance for making subjective evaluations of likelihood as follows (ETSI 2003):

- **Unlikely** (1) – Attackers would need to solve very strong technical difficulties to perform the threat or motivation to perform the threat is very low.

- **Possible** (2) – Attackers have access to technical solutions and would be expected to be reasonably motivated to perform the threat.

- **Likely** (3) – Attackers would experience no technical difficulties and would be expected to be highly motivated to perform the threat

After assigning numeric values for the likelihood of each threat, an analyst will consider the impact level of each threat. This is done in a similar manner, with the analyst assigning numeric values of 1, 2 or 3 for the impact, following TRAM’s guidance (ETSI 2003):

- **Low impact** (1) – The system provider or user is not harmed very strongly, the possible damage is low.

- **Medium impact** (2) – The system provider or user might experience a loss of service or damage to interests.
• *High impact* (3) – The system provider or user might experience great loss to core business functions or experience outages for extended periods of time.

After the likelihood and impact of each threat is assigned, a security analyst calculates a numeric value representing risk for each threat. TRAM identifies the mathematical product of likelihood and impact as the measure of risk for each threat, \( \text{risk} = \text{likelihood} \times \text{impact} \). The risk product formula is identical to the method presented by NIST (Stonebumer et al. 2001).

TRAM ranks the risk of each threat by the risk product. A threat with a risk product of 1, 2 or 3 is identified as a minor risk. A major risk is represented by a threat with a risk product of 4 and a risk product of either 6 or 9 would identify a critical risk (the products, 5, 7 and 8 are not possible). TRAM recommends that critical risks be attended to as quickly as possible because the threats are likely to cause significant harm. TRAM also recommends that major risks be handled in a timely manner. Minor risks do not require additional countermeasures because they have little to no impact or because attackers have no motivation to perform the threat. These recommendations are similar to other qualitative methods (Barbeau 2005; Stonebumer et al. 2001).

**The Delphi Methodology**

The Delphi methodology originated within the RAND research organization in the 1950s (Linstone and Turoff 2002) in an effort to obtain a reliable consensus of expert opinion (Dalkey and Helmer 1963). Delphi methods became popular for expert forecasting (Boehm 1981) and more recently in generating expert consensus in healthcare research (Jenkins and Smith 1994; Katcher et al. 2006; Sharkey and Sharples 2001; Sindhu et al. 1997). Using Delphi techniques, a panel of experts can work together to formulate a consensus on subjective questions. A typical Delphi exercise might follow these steps (adapted from Boehm 1981):
1. Facilitator calls a group meeting with panelists to characterize question to be evaluated, hold an introductory discussion, and distribute surveys.

2. Panelists complete their surveys privately and anonymously return them to facilitator.

3. Facilitator collates and distributes results to panelists.

4. Facilitator holds another discussion meeting and then distributes new surveys.

5. Steps 2, 3, and 4 are repeated until the panel reaches consensus.

Several points can be made concerning the process noted above. First, where questions are not overly complex, two or three rounds are typically sufficient to reach an acceptable level of consensus with groups of 3 to 12 panelists (Linstone and Turoff 2002; Sindhu et al. 1997). Second, review and adjustment of opinion in multiple rounds is accomplished more easily outside of the group discussion, when submissions are anonymous (Linstone and Turoff; Sharkey and Sharples 2001). Finally, care should be exercised in conducting a Delphi exercise: The facilitator should carefully manage the pace of the process to limit the fatigue of panelists (Linstone and Turoff; Sharkey and Sharples); use care to create an organized, precise survey instrument (Linstone and Turoff); encourage consistent panel membership for all rounds (Sindhu et al.); and provide participants opportunities to clarify their responses (Sindhu et al.).

**Using a Delphi Exercise in TRAM**

Within TRAM, the determination of threats, likelihood and impact, are good candidates for the application of a Delphi methodology. Because threats must be identified first, two Delphi exercises should be conducted, following the generalized procedures listed earlier. The first exercise should identify, through consensus, a list of legitimate threats and descriptions for each threat. In this exercise, the panel should determine all potential threats that jeopardize any vulnerability of the target system. If a known list of threats is available, it should be used as a seed for the first round. Otherwise panelists can simply be asked to generate a list of threats from
scratch during the first round. Rounds continue until the panel is satisfied it has characterized the threats to the system.

A new Delphi exercise follows to evaluate the likelihood and impact of each threat. During the exercise, panelists should provide their comments describing why they have made specific numeric assignments for each attribute. The comments are important for resolving potential conflicts and for allowing further rounds to reach consensus. Again, rounds repeat until the panel is satisfied it has reached consensus.

**Difficulty Reaching Consensus**

There is a possibility that, after several rounds, consensus might not be reached during the first or second Delphi exercises. If consensus cannot be reached concerning one or more threats during the first exercise, the facilitator can recommend that a questioned threat be included in the final threat list so that its risk can be considered during risk analysis. If during the second exercise, panelists cannot reach consensus on the severity of a threat's likelihood or impact, the facilitator may recommend that the higher value be used, noting that it would be preferred to overrate a risk than to underrate it.

**Completing the Assessment**

After the Delphi exercises are completed, determining risks, their likelihoods and impacts, risk products may be calculated following the TRAM formula. Evaluating the risks can be completed according to the recommendations in TRAM, with risk products of 1-3 being considered minor risks, products equal to 4 being major risks, and products of 6 or 9 being critical risks. TRAM recommends interpreting the risks as follows (ETSI 2003):

- Critical risks (6 or 9) -- Threats causing critical risks are a high priority. They should be addressed as quickly as possible.
• Major risks (4) -- Threats causing major risks are serious and should be handled without significant delay.

• Minor risks (1, 2 or 3) -- Threats causing minor risks have no primary need for additional countermeasures, but they should be re-evaluated periodically.

Assessment Process

The following steps were followed to conduct the risk assessment. First, assets were identified and the boundaries of the system to be evaluated were defined (following Stonebumer et al. 2001) by three panelists, members of the IT staff in charge of the wireless network. Then, potential threats were identified by panelists during a single Delphi round starting with a preliminary list of potential threats (collected from Barbeau 2005; European Telecommunications Standards Institute 2003). The three panelists then participated in two Delphi rounds to reach consensus on the likelihood and impact of the identified threats, during which numeric values for likelihood and impact were assigned to each threat. Finally, risk measures were calculated using the risk product formula to rank and prioritize the risks.

Identifying Threats

Seven general threat areas identified and used in TRAM (European Telecommunications Standards Institute 2003) and repeated by Barbeau (2005) were considered for three functional areas of the University wireless networking system to generate a preliminary list of potential threats. The functional areas considered were radio communications interface security, physical security, and managerial operations security. Upon completion of the Delphi round, the final list consisted of six air interface threats, ten physical threats, and four managerial operations threats. The identified threats generally agree with a list of security threats for 802.11 networks reported by Karygiannis and Owens (2002).

Assessment Results
Tabulated risk results are presented in Appendix A, which lists likelihood, impact and the resulting risk metric for each threat. Results should be viewed with some caution because the assessment of likelihood and impact are subjective. Further, none of the participants in the discussion had prior experience conducting a risk assessment. Overall the assessment produced 15 minor risks and 5 major risks. The wireless networking staff and the researcher did not feel any likely threats would have a medium or higher impact, nor did they believe any possible threats would have a high impact. Such combinations would have resulted in a critical threat in need of immediate attention.

**Minor Risks**

Twelve risks were considered minor. There are two characteristics of the multiple-AP system at the University that limit the impact of these threats.

- If an AP fails mechanically, is disconnected, damaged, stolen or encounters a denial of service attack, other APs can still provide service to users because service areas overlap. It is likely that users will not be aware the system is encountering any problems.

- The rotation of WEP keys and the requirement for re-authentication sets a high technical barrier for eavesdropping, masquerading as a client or the intentional corruption of data. This is the source of a network availability concern noted below, however.

The three remaining minor risks were related to the management configuration devices (MXs): mechanical failure of an MX, a management configuration error, and software vulnerabilities of an MX. Management servers can be taken off line without affecting the wireless network operation. Further, they use a firmware based proprietary operating system that presents a technically high barrier to intrusion and that requires firmware updates to make changes to the operating system. Configuration errors that cause outages on the network can be
fixed quickly, because all APs can be returned to a prior working configuration simultaneously and remotely in a few minutes.

**Major Risks**

Five major risks were identified and these are described below. First, staff noted that two sections of the campus network had not been upgraded to support 802.1x authentication and thus would allow unauthorized access to the network. They did not feel any subsystems would be at increased risk but they were concerned that anonymous access to the network would allow consumption of all network capacity, limiting the usefulness of the entire wireless network for other users. Staff thought that even in this situation, they could identify and resolve the problem within a few minutes of discovering a performance problem. This threat was described as *possible* with a *medium impact*.

Second, a threat source could masquerade as an AP in an attempt to perform additional threats such as denial of service or eavesdropping. The campus wireless management system automatically monitors for rouge access points and sends disconnect signals to clients attempting to associate with rouge APs, preventing their use. However, staff noted that this was set to occur only if the APs were attempting to act as a middleman in the network, forwarding traffic on to the campus wireless network. It is therefore still possible for rouge APs to masquerade as the system if they did not pass traffic on to the system.

Third, wireless networking staff suggested that system-wide power failures would prevent the entire network from functioning because access-layer switches were not making use of uninterruptible power supplies (UPS). Network failure was considered a *medium impact* event and it was considered a *possible* event due to the frequency of inclement weather.
Fourth, staff rated themselves as unlikely to conduct any malicious activity affecting the network but conceded that this could have a high impact on the network. Ironically, if they did have this intention, they would not report it. The researcher found no reason to believe the staff members were intent on any malicious activity, either.

Fifth, the use of the 802.1x protocol for authentication with the rotation of WEP keys and re-authentication actually causes an unintentional denial of service that has been found to be a common problem for users. When some users’ laptops or PDAs are in sleep mode for longer than the key rotation time or the re-authentication time the user might have significant difficulty re-establishing connectivity with the network upon waking their device. Wireless networking staff members have not found feasible technical solutions to this issue, with the exception of abandoning 802.1x authentication and encryption. Losing access because of the dropped authentication was rated as a low impact event, but is it known to be a likely occurrence and is therefore a major risk to providing reliable services.

Lessons Learned from the Assessment

Several lessons can be learned from the risk assessment described above. First, the assignment of likelihood and impact was clearly subjective. While the wireless networking staff offered their honest opinions of the level of likelihood and impact of threats, they did not have high confidence that their appraisals were accurate. Only through general consensus building was any confidence built up that the appraisals might be believable. In part, this could be due to having no experience with risk assessments of any kind. One potential advantage of the subjective approach is that tacit knowledge from experience and general wisdom can be included in the decision making process. The approach allows for the inclusion of any concerns or countermeasures that may affect likelihood or impact. Another advantage of the process used for
this risk assessment is that the members of the wireless networking staff had a long careful discussion of potential threats to their network for the first time. The mere act of conducting the risk assessment, whether accurate or not, increases their understanding of security and the potential changes to risk levels associated with any change to the system, such as topology, equipment, policy or software changes.

**Limitations, Concerns, and Further Study**

A practitioner should be aware of a few limitations to and concerns with the approach identified here. First, this approach does not remove subjectivity; rather, it provides a more rigorous approach to making subjective evaluations. Subjectivity will be an inherent part of the final assessment. Second, the approach depends on a minimum number of panelists, at least three. Small organizations may be unable to fill a panel to conduct a Delphi exercise. In this instance, the analyst can simply proceed with TRAM as before, completing the assessment without using an expert panel. Third, discussion meetings during the Delphi exercises should focus on discordant opinion with a concentration on synthesizing consensus, but need not reach full consensus, something completed more easily through anonymous responses to a round’s survey. It is more difficult for a panelist to change a publicly stated opinion than an anonymous one. Finally, choosing a facilitator is critical to the success of the Delphi exercises. Experts should participate on the panel, rather than facilitate the process. This allows them to participate without undue influence on the process and prevents influence upon the collation of results.

Additional study in this area could investigate the relative changes in perceived subjectivity when comparing standard and Delphi approaches to risk assessment. Further study could also investigate whether Delphi methods would be beneficial when applied to more complex risk assessment methodologies. Other research could compare the different procedural
steps found in various modified versions of Delphi techniques (noted in Linstone and Turoff 2002).

**Conclusion**

This paper has presented some concerns with the subjective elements of qualitative risk assessments that may lead to controversial and variable results. A two-part Delphi approach has been proposed as a way to provide a more rigorous determination of the subjective elements in TRAM as applied to an 802.11 campus wireless network risk assessment. The Delphi approach described here should be applicable to the determination of intangible elements in other risk assessment methodologies if planned and managed carefully.
Appendix A

Table of Numeric Risk Assessment Results

<table>
<thead>
<tr>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio Communications Interface Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat source masquerading as a client</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Threat source masquerading as an AP</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Threat source gains unauthorized access to wireless network</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Threat source conducts successful eavesdropping of transmissions</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Natural loss or intentional corruption of data</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Denial of service by threat source</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Physical Network Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Theft of APs</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Theft of data center or wiring closet devices</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Mechanical Failure of AP</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Mechanical Failure of Access Switch or Cabling</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Mechanical Failure of MX</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Device vandalism</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Cable vandalism</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>AP vandalism</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Local power failure</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>System wide power failure</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Managerial Operations Security</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management configuration error</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Malicious activity by staff</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Software vulnerability on MX</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>dropping of authenticated access</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
References


European Telecommunications Standards Institute (2003), "Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; Protocol framework definition; Methods and protocols for security; Part 1: Threat analysis."


Katcher, M. L., A. N. Meister, C. A. Sorkness, A. G. Staresini, S. E. Pierce, B. M. Goodman, N. M. Peterson, P. M. Hatfield, and J. A. Schirmer (2006), "Use of the modified Delphi technique to


