Metrics-Based Assessment and Management of Digital Forensics Risk

M. Sahinoglu, S. Stockton, Scott Morton, Robert Barclay

Informatics Institute

Auburn University Montgomery

Abstract

Driven by the ubiquity of computers in modern life and the subsequent rise of cyber-criminality and cyber-terrorism in civilian and defense acquisition processes, Digital Forensics is an increasingly salient one. Though primarily located in the law enforcement community, Digital Forensics is increasingly practiced within the corporate world for legal and regulatory requirements such as Sarbanes-Oxley. Digital forensics risk essentially involves the assessment, acquisition, and examination of digital evidence in such a manner that legal standards of proof and admissibility are met. We will adopt a model of digital forensics risk that quantifies an investigator's experience with eight crucial aspects of the digital forensics process. This research adds the novel concept of quantifying through a designed Risk-O-Meter algorithm to calculate digital forensics risk indices. To accomplish this task, numerical and/or cognitive data was collected to supply the input parameters to calculate the quantitative risk index for the digital forensics process.

Two-line Summary

Digital Forensics risk (digital evidence assessment subject to legal standards) is quantified using a Risk-O-Meter algorithm for calculating risk indices.

Keywords

Digital Forensics, Risk Assessment and Management, Metrics, Cyber-Terrorism, Cyber-Criminality.

Body

Introduction

Digital Forensics is a topic that has been popularized by television programs such as *CSI*. Crime-solving glamour and drama aside, the reality of the digital forensics process is that it is a highly technical field that is dependent on the proper implementation of specific, well-accepted protocols and procedures. Inadequate forensic tools and technical examination, as well as lack of adherence to appropriate protocols and procedures can result in evidence that does not meet legal standards of proof and admissibility. Digital forensics risk arises, for example, when personnel lack the proper tools to conduct investigations, fail to process evidentiary data properly, or do not follow accepted protocols and procedures.

Assessing and quantifying digital forensics risk is the goal of this paper. To do so, a Digital Forensics Risk Meter based on a series of questions designed to assess personnel's perceptions of digital forensics risk will be utilized. Based on the responses, a digital forensics risk index will be calculated. Where this approach differs from others such as the ones in the US Department of Justice's *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (general guidelines and worksheets) (USDOJ, 2004), E*rror, Uncertainty, and Loss in Digital Evidence* (certainty levels) (Casey, 2002), *Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics* (suspicion levels) (Kim & In, 2008), *Two-Dimensional Evidence Reliability Amplification Process Model for*

Digital Forensics (evidence reliability) (Khatir, Hejazi, & Sneiders, 2008), or *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility* (checklist) (Jones & Valli, 2011), is that those approaches typically provide general guidance in the form of best practices, classification schemes, or at best a checklist for digital forensics procedures and do not provide quantitative tools (based on game theory) for risk management and mitigation. One approach that does employ quantification, *Metrics for Network Forensics Conviction Evidence*, is confined to network forensics, mostly measuring severity impact and does not provide mitigation advice (Amran, Phan, & Parish, 2009).

The Digital Forensics Risk Meter presented in this paper will provide objective, automated, dollar-based risk mitigation advice for interested parties such as investigators, administrators, and officers of the court to minimize digital forensics risk. See Figure 2’s advice column for sample mitigation advice generated from the respondent’s submitted inputs. This paper will not only present a quantitative model but also generate a prototype numerical index study that facilitates appropriate protocols and procedures, thus ensuring that legal standards of proof and admissibility are met.

Vulnerabilities, Threats

Based on industry best practices guidelines, such as the US Department of Justice’s *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, eight specific vulnerabilities are assessed: Protocols and

Procedures, Evidence Assessment, Evidence Acquisition, Evidence Examination, Documentation & Reporting, Digital Forensics Tools, Legal Aspects, and Victim Relations. Within each vulnerability category, questions pertain to specific threats and countermeasures. For example, within the Evidence Acquisition vulnerability, respondents are asked questions regarding Precautions, Protection, and Preservation threats and countermeasures. Within the Evidence Examination vulnerability, respondents are asked questions regarding Preparation, Physical Extraction, Logical Extraction, Timeframe Analysis, Data Hiding Analysis, Application/File Analysis, and Ownership/Possession threats and countermeasures. Within the Digital Forensics Tools vulnerability, respondents are asked questions regarding Hardware, Software, Training, and Funding threats and countermeasures. See Figure 1 below for the Digital Forensics Risk diagram detailing vulnerabilities and threats. The responses are then used to generate a quantitative digital forensics risk index.

Assessment Questions

Questions are designed to elicit responses regarding the perceived risk to proper digital forensics procedures, evidence handling/examination, admissibility, and other associated issues from particular threats, as well as the countermeasures the respondents may employ to counteract those threats. For example, in the Evidence Examination vulnerability, questions regarding the Data Hiding Analysis threat includes both threat and countermeasure question.

Threat questions would include:

- Do file headers not correspond to file extensions?
- Did the suspect encrypt or passwords protect data?
- Are hidden messages present?
- Are host-protected areas (HPAs) present?

While countermeasure questions would include:

- Did the examiner correlate file headers to the corresponding file extensions to identify any mismatches which may indicate that the user intentionally hid data?
- Did the examiner gain access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal the data from unauthorized users?
- Did the examiner conduct a thorough stenographic analysis?
- Did the examiner gain access to HPAs that may indicate an attempt to conceal data?

Sample vulnerability (Evidence Acquisition) assessment questions employed in the Digital Forensics Risk Meter are presented in Appendix A at the end of this paper.

Survey Notes, Risk Calculation & Mitigation

Essentially, the respondents are answering yes or no to these questions. These responses are used to calculate residual risk. Using a game-theoretical mathematical approach, the calculated risk index is used to generate an optimization or lowering of risk to desired levels (Sahinoglu, 2007). Further, mitigation advice will be generated to show interested parties such as investigators, administrators, and officers of the court in what areas the risk can be reduced to optimized or desired levels such as from 45.8% to 35.8% as shown in the screenshot representing the median response from the study participants (Sahinoglu, Cueva-Parra, & Ang, 2012). See Figure 2 for a screenshot of the Median Digital Forensics Risk Meter Results Table displaying threat, countermeasure, and residual risk indices; optimization options; as well as risk mitigation advice. For this study, a random sample of 27 respondents was taken and their residual risk results are tabulated and presented in Appendix B at the end of this paper.

The survey used in this research paper for the assessment showed the complexity of the field, as one realizes digital forensics encompasses tools, procedures, specific training, budget, and trial. Digital Forensics has two crucial phases. The first phase involves all the forensics involved with the collection of data, while the second phase involves defending the data collected, the means by which is was collected, and chain of custody applied from the original collection until court.

The initial goal was to obtain survey input from local city leaders. Although individuals from the Governor's Office, Montgomery Police Department, and District Attorney's office were willing to assist, our short time frame and their busy schedule prevented their office from providing input to the digital forensics survey.

Fortunately, the authors had contacts at some law enforcement offices and they agreed to make personnel available for the survey and eventual follow up. Ultimately, three law enforcement offices and one special investigation/training organization participated and provided valuable input.

Our first objective was to explain the purpose of the survey and the potential value the combined results could offer each of the offices. At each location, participants ranged from investigators, initial responders, digital forensics specialists, and legal experts, i.e. District Attorney Office personnel.

The range of expertise of the participants was invaluable, as each provided insight into an aspect of the survey that is often unique to a position within a department. Because of this range of expertise, the authors believe they were able to capture the three main components of the survey portion of the RoM. Perspectives from collection of evidence, packaging of evidence for trial, and presentation of evidence at trial activities were all given. Although the special investigation/training organization had much less participants, they did offer a unique perspective, as they represented an organization that focuses on training digital forensics experts for the military.

The results were then run for each participant, determining the Initial Repair Cost to Mitigate. This was determined by using a Criticality of 1.0, Equipment Cost of $0.0, and a Production Cost of $1,000. The Median of all results was determined and then optimized through the RoM to determine the best “bang for the buck” that would reduce the participant’s Total Residual Risk by 10 percent. The initial Total Residual Risk for the median participant was 45.8% with an Expected Cost of Loss (ECL) of $458.34. Once optimized, the Total Risk was reduced to 35.8% and the ECL was reduced by $100 to a total ECL of $358.34 as seen in Figure 2 below. The first optimized solution was to increase the countermeasure (CM) capacity for the Threat “Examiner Notes” for the Vulnerability “Documentation and Reporting” from 45.00% to 72.17% for an improvement of 27.17%. The second optimized solution was to increase the CM capacity for Threat “Victim Rights and Support” for the Vulnerability of “Victim Relations” from 72.50% to 99.92% for an improvement of 27.42%.

In addition to determining the Overall Median and optimizing it, the Median for each organization was determined. The optimization for each organization (except organization 4 with an even number of participants) was run and the results discussed with the point of contact for that organization.

In each case, the representative seemed impressed with the results and noted the results for possible future implementation. One organization actually commented that they had already begun looking into increases in at least one countermeasure that was identified by the optimization. Clearly, this validated the tool and its usefulness in their eyes.

Conclusions & Discussion

The Digital Forensics Risk Meter breaks new ground in that it provides a quantitative assessment of risk to the user as well as recommendations for mitigating that risk. As such, it will be a highly useful tool to interested parties such as investigators, administrators, and officers of the court seeking to minimize/mitigate digital forensics risk. Future work will involve the addition of Cloud Computing concerns such as service provider cooperation and data accessibility as well as the incorporation of new questions so as to better refine user responses and subsequent calculation of risk and mitigation recommendations. Minimization/ mitigation of digital forensics risk, will greatly facilitate the success of digital forensics investigations, ensuring that legal standards of proof and admissibility are ultimately met. The Digital Forensics Risk Meter tool and its future refinement provide the means to identify areas where risk can be minimized as well as providing the objective, dollar-based mitigation advice to do so. Figures 3 to 5 follow for the other median outcomes for each group.

Reference List

Amran, A. R., Phan, R. C. W., & Parish, D. J. (2009). *Metrics for Network Forensics Conviction Evidence*, IEEE .

Casey, E. (2002). Error, Uncertainty, and Loss in Digital Evidence, *International Journal of Digital Evidence*, Summer 2002 https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

Jones, A. & Valli, C. (2011). *Building a Digital Forensic Laboratory: Establishing and Managing a Successful Facility*, Butterworth-Heinemann.

Khatir, M., Hejazi, S. M., & Sneiders, E. (2008). Two-Dimensional Evidence Reliability Amplification Process Model for Digital Forensics, Third International Annual Workshop on Digital Forensics and Incident Analysis, IEEE.

Kim, D. H., & In, H. P. (2008). Cyber Criminal Activity Analysis Models using Markov Chain for Digital Forensics, 2008 International Conference on Information Security and Assurance, IEEE.

Sahinoglu, M. (2007). *Trustworthy Computing*, Hoboken NJ: John Wiley.

Sahinoglu, M., Cueva-Parra, L., & Ang , D. (2012) Game-theoretic computing in risk analysis, *WIREs Comput. Stat*, doi: 10.1002/wics, 1205. http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931

US Department of Justice. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Figures

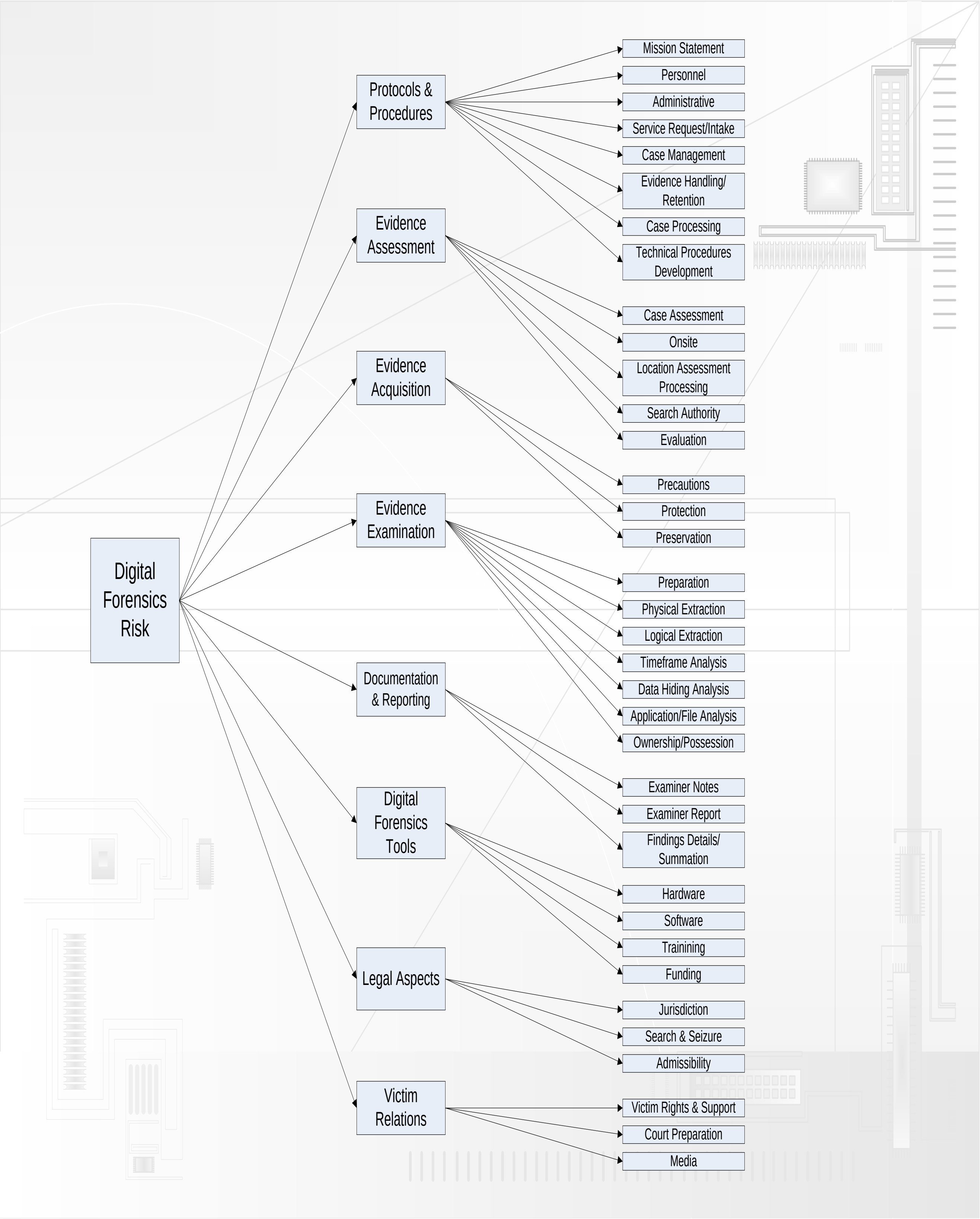
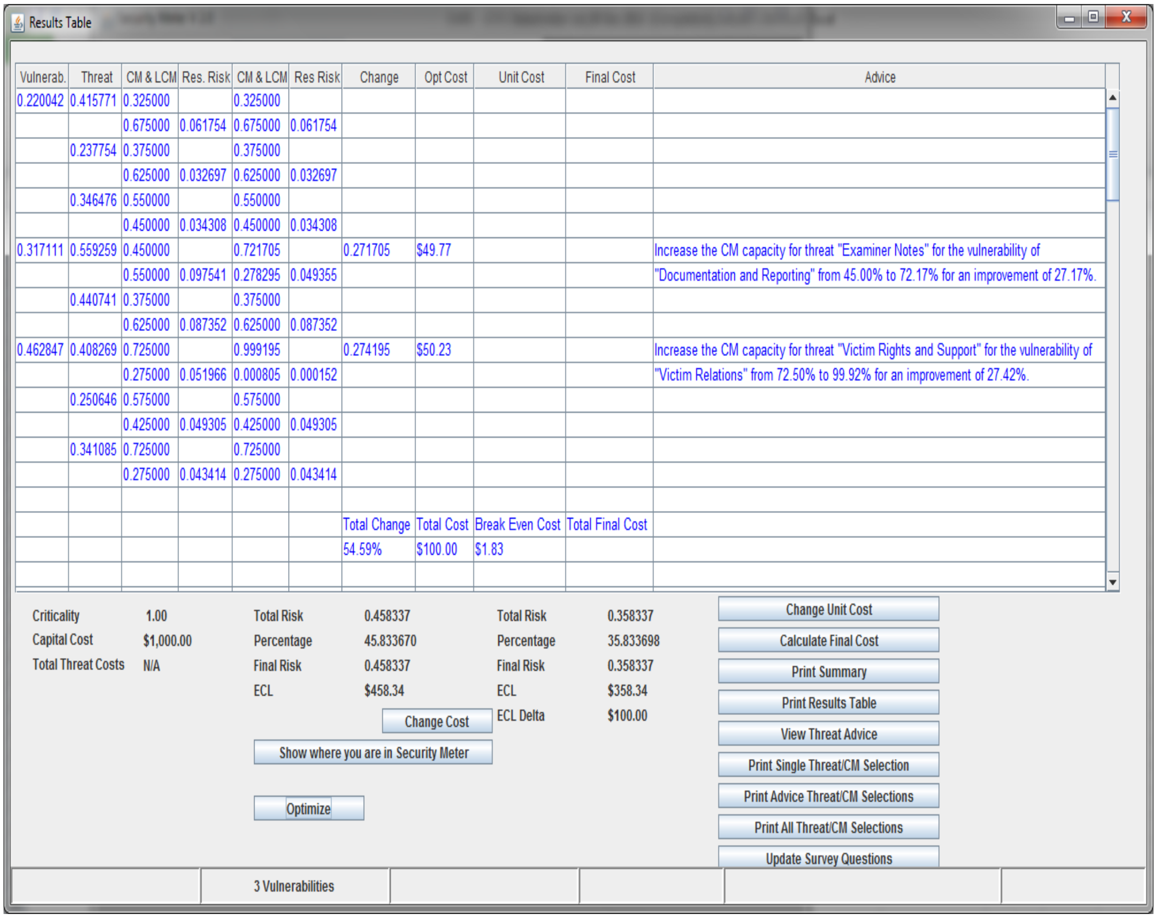


Figure 1: Digital Forensics Risk Diagram



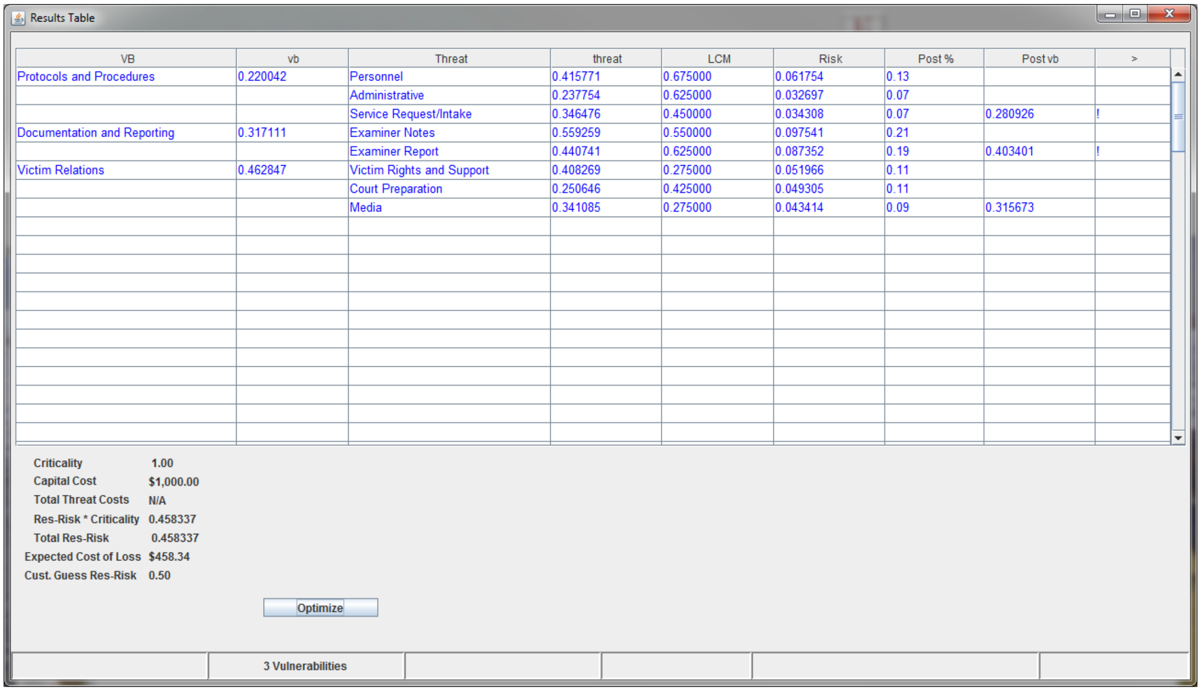
Vulnerab.	Threat	CM & LCM	Res. Risk	CM & LCM	Res Risk	Change	Opt Cost	Unit Cost	Final Cost	Advice
0.220042	0.415771	0.325000		0.325000						
		0.675000	0.061754	0.675000	0.061754					
	0.237754	0.375000		0.375000						
		0.625000	0.032697	0.625000	0.032697					
	0.346476	0.550000		0.550000						
		0.450000	0.034308	0.450000	0.034308					
0.317111	0.559259	0.450000		0.721705		0.271705	$49.77			Increase the CM capacity for threat "Examiner Notes" for the vulnerability of
		0.550000	0.097541	0.278295	0.049355					"Documentation and Reporting" from 45.00% to 72.17% for an improvement of 27.17%.
	0.440741	0.375000		0.375000						
		0.625000	0.087352	0.625000	0.087352					
0.462847	0.408269	0.725000		0.999195		0.274195	$50.23			Increase the CM capacity for threat "Victim Rights and Support" for the vulnerability of
		0.275000	0.051966	0.000805	0.000152					"Victim Relations" from 72.50% to 99.92% for an improvement of 27.42%.
	0.250646	0.575000		0.575000						
		0.425000	0.049305	0.425000	0.049305					
	0.341085	0.725000		0.725000						
		0.275000	0.043414	0.275000	0.043414					
						Total Change	Total Cost	Break Even Cost	Total Final Cost	
						54.59%	$100.00	$1.83		

Criticality	1.00	Total Risk	0.458337	Total Risk	0.358337
Capital Cost	$1,000.00	Percentage	45.833670	Percentage	35.833698
Total Threat Costs	N/A	Final Risk	0.458337	Final Risk	0.358337
		ECL	$458.34	ECL	$358.34
				ECL Delta	$100.00

3 Vulnerabilities

Change Cost
Show where you are in Security Meter
Optimize
Change Unit Cost
Calculate Final Cost
Print Summary
Print Results Table
View Threat Advice
Print Single Threat/CM Selection
Print Advice Threat/CM Selections
Print All Threat/CM Selections
Update Survey Questions

Figure 2: Median Digital Forensics Risk Meter Results Table

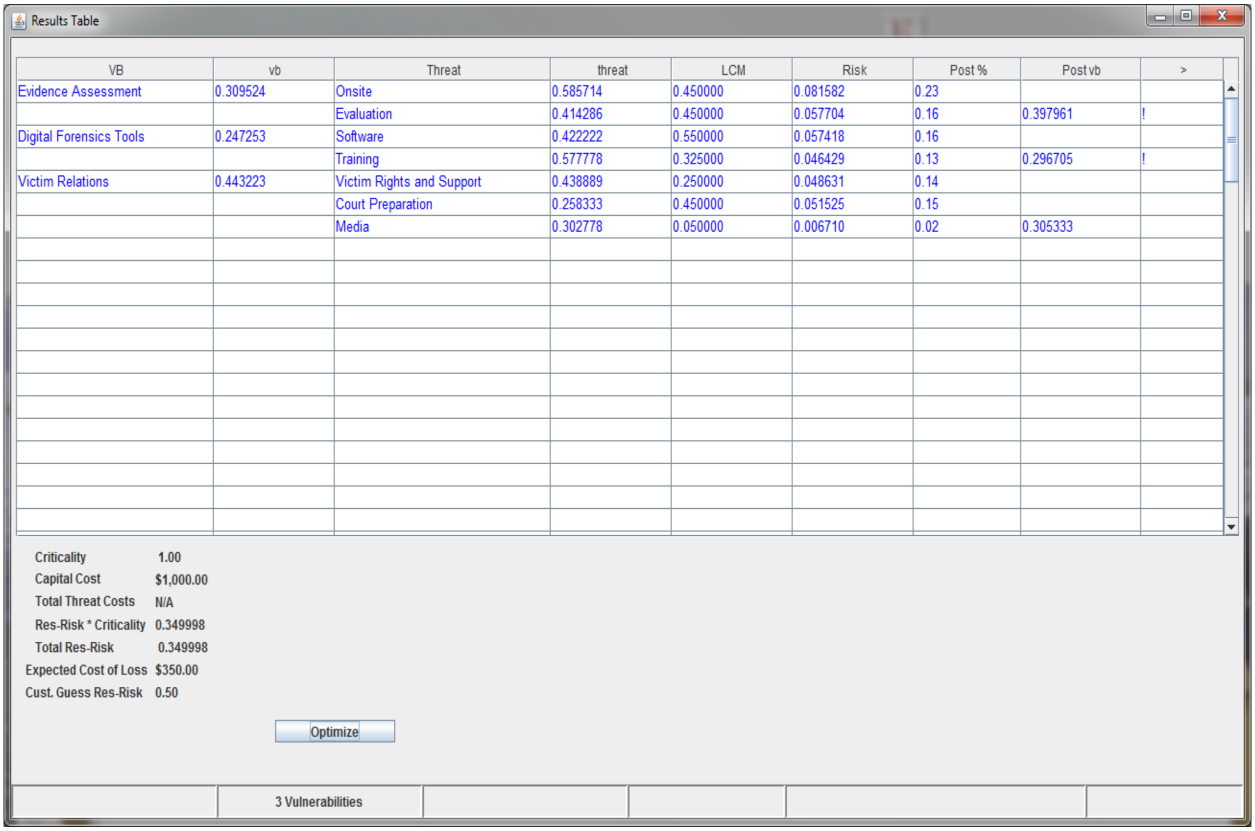


VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Protocols and Procedures	0.220042	Personnel	0.415771	0.675000	0.061754	0.13		
		Administrative	0.237754	0.625000	0.032697	0.07		
		Service Request/Intake	0.346476	0.450000	0.034308	0.07	0.280926	!
Documentation and Reporting	0.317111	Examiner Notes	0.559259	0.550000	0.097541	0.21		
		Examiner Report	0.440741	0.625000	0.087352	0.19	0.403401	!
Victim Relations	0.462847	Victim Rights and Support	0.408269	0.275000	0.051966	0.11		
		Court Preparation	0.250646	0.425000	0.049305	0.11		
		Media	0.341085	0.275000	0.043414	0.09	0.315673	

Criticality	1.00
Capital Cost	$1,000.00
Total Threat Costs	N/A
Res-Risk * Criticality	0.458337
Total Res-Risk	0.458337
Expected Cost of Loss	$458.34
Cust. Guess Res-Risk	0.50

3 Vulnerabilities

Figure 3. ECSO8: 14th Ranked overall Median Survey Taker's Original Survey Outcome

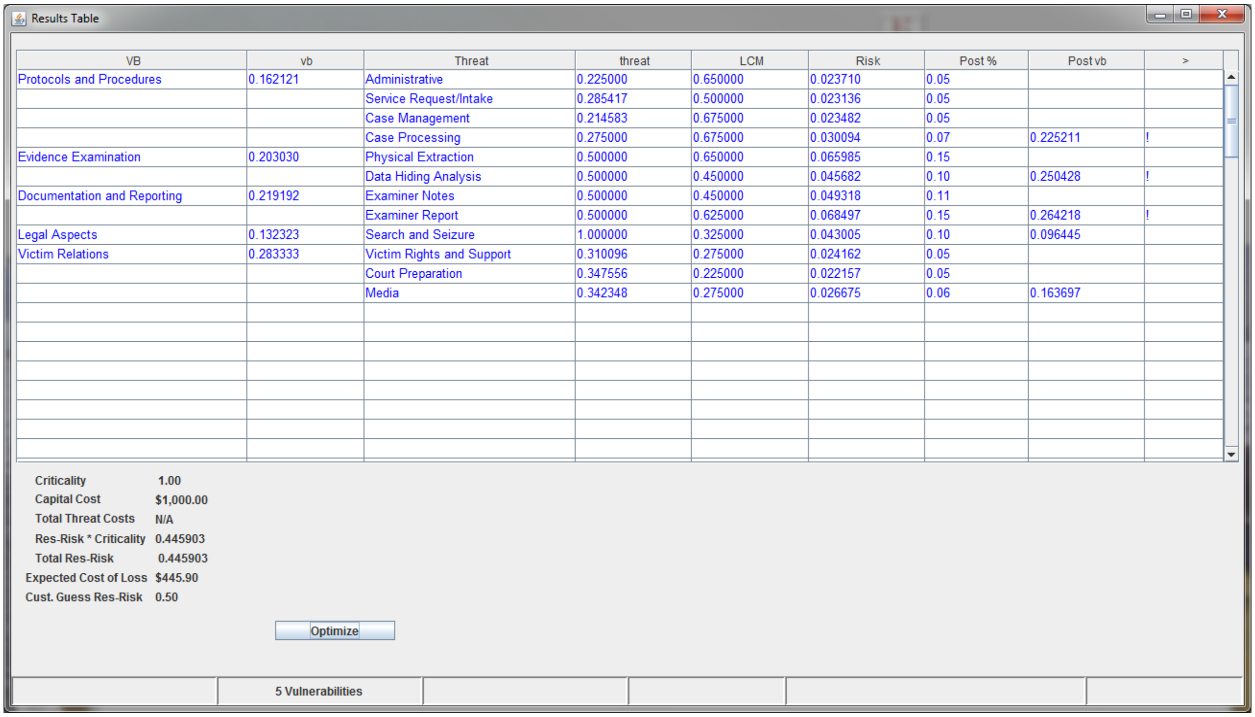


VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Evidence Assessment	0.309524	Onsite	0.585714	0.450000	0.081582	0.23		
		Evaluation	0.414286	0.450000	0.057704	0.16	0.397961	!
Digital Forensics Tools	0.247253	Software	0.422222	0.550000	0.057418	0.16		
		Training	0.577778	0.325000	0.046429	0.13	0.296705	!
Victim Relations	0.443223	Victim Rights and Support	0.438889	0.250000	0.048631	0.14		
		Court Preparation	0.258333	0.450000	0.051525	0.15		
		Media	0.302778	0.050000	0.006710	0.02	0.305333	

Criticality	1.00
Capital Cost	$1,000.00
Total Threat Costs	N/A
Res-Risk * Criticality	0.349998
Total Res-Risk	0.349998
Expected Cost of Loss	$350.00
Cust. Guess Res-Risk	0.50

3 Vulnerabilities

Figure 4. OPD1: Group Median Survey Taker's Original Survey Outcome



VB	vb	Threat	threat	LCM	Risk	Post %	Post vb	>
Protocols and Procedures	0.162121	Administrative	0.225000	0.650000	0.023710	0.05		
		Service Request/Intake	0.285417	0.500000	0.023136	0.05		
		Case Management	0.214583	0.675000	0.023482	0.05		
		Case Processing	0.275000	0.675000	0.030094	0.07	0.225211	!
Evidence Examination	0.203030	Physical Extraction	0.500000	0.650000	0.065985	0.15		
		Data Hiding Analysis	0.500000	0.450000	0.045682	0.10	0.250428	!
Documentation and Reporting	0.219192	Examiner Notes	0.500000	0.450000	0.049318	0.11		
		Examiner Report	0.500000	0.625000	0.068497	0.15	0.264218	!
Legal Aspects	0.132323	Search and Seizure	1.000000	0.325000	0.043005	0.10	0.096445	
Victim Relations	0.283333	Victim Rights and Support	0.310096	0.275000	0.024162	0.05		
		Court Preparation	0.347556	0.225000	0.022157	0.05		
		Media	0.342348	0.275000	0.026675	0.06	0.163697	

Criticality	1.00
Capital Cost	$1,000.00
Total Threat Costs	N/A
Res-Risk * Criticality	0.445903
Total Res-Risk	0.445903
Expected Cost of Loss	$445.90
Cust. Guess Res-Risk	0.50

5 Vulnerabilities

Figure 5. AUPD5: Group Median Survey Taker's Original Survey Outcome

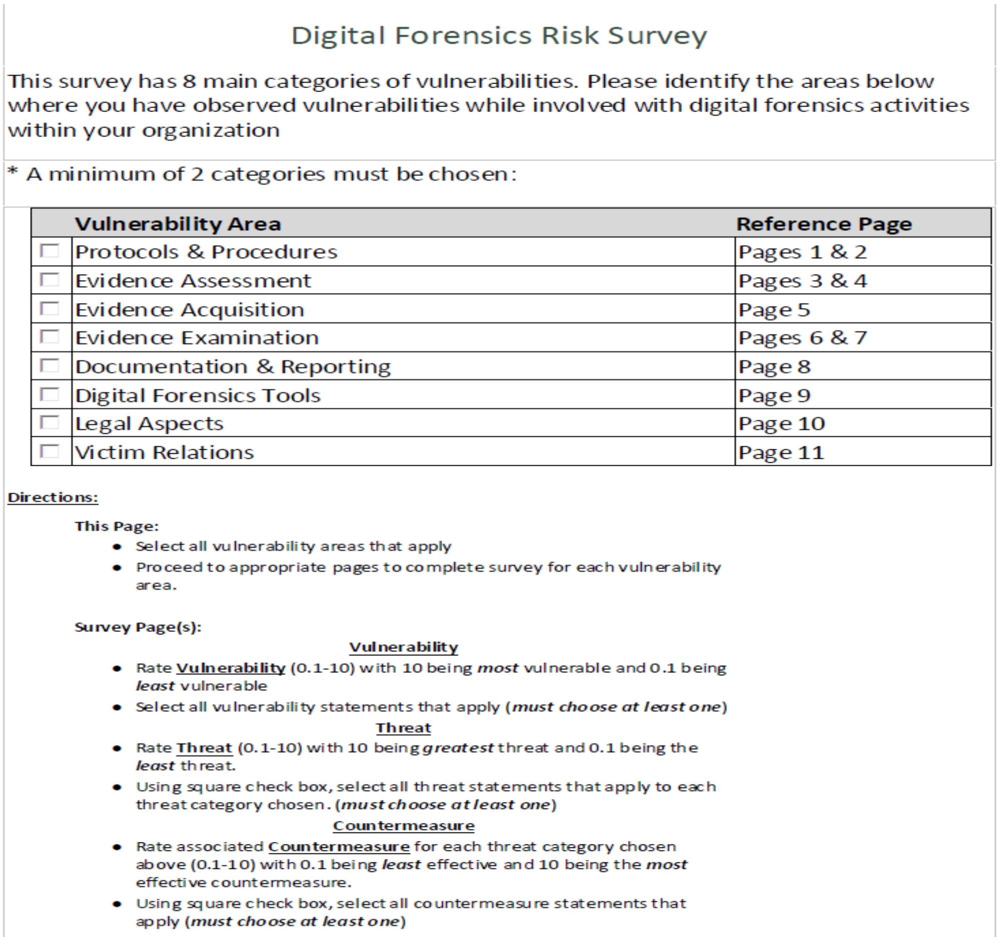
Appendix A

Sample Vulnerability (Evidence Acquisition) Assessment Questions (in XML format) and Survey Question Template

```
<survey>
 <vulnerability title="Evidence Acquisition" level="0">
<vQuestion> Are special precautions not taken to preserve digital evidence? </vQuestion>
<vQuestion> Was write protection not utilized to preserve and protect original evidence? </vQuestion>
<vQuestion> Was digital evidence not secured in accordance with departmental guidelines? </vQuestion>
<vQuestion> Was speed the primary concern when it came to acquiring digital evidence? </vQuestion>

<threat title = "Precautions" >
<tQuestion> Was evidence on storage devices destroyed or altered? </tQuestion>
<tQuestion> Was equipment damaged by static electricity and magnetic fields? </tQuestion>
<tQuestion> Was the original internal configuration of storage devices and hardware unnoted? </tQuestion>
<tQuestion> Were investigators unable to provide drive attributes? </tQuestion>

<threat title = "Protection" >
<tQuestion> Was CMOS/BIOS information and not captured? </tQuestion>
<tQuestion> Was the computer’s functionality and the forensic boot disk not tested? </tQuestion>
<tQuestion> Did the forensic boot disk not boot? </tQuestion>
<tQuestion> Did the investigators not collect drive configuration information from the CMOS/BIOS?
</tQuestion>
-----------------------------------
<threat title = "Preservation" >
<tQuestion> Did the investigators not perform the acquisition using the examiner’s system? </tQuestion>
<tQuestion> Was a RAID present in the subject system? </tQuestion>
<tQuestion> Was host-specific data not captured? </tQuestion>
<tQuestion> Was successful acquisition not verified? </tQuestion>
………………………………………
</threat>
</vulnerability>
</survey
```



Digital Forensics Risk Survey

This survey has 8 main categories of vulnerabilities. Please identify the areas below where you have observed vulnerabilities while involved with digital forensics activities within your organization

* A minimum of 2 categories must be chosen:

	Vulnerability Area	Reference Page
□	Protocols & Procedures	Pages 1 & 2
□	Evidence Assessment	Pages 3 & 4
□	Evidence Acquisition	Page 5
□	Evidence Examination	Pages 6 & 7
□	Documentation & Reporting	Page 8
□	Digital Forensics Tools	Page 9
□	Legal Aspects	Page 10
□	Victim Relations	Page 11

Directions:

This Page:

- Select all vulnerability areas that apply
- Proceed to appropriate pages to complete survey for each vulnerability area.

Survey Page(s):

Vulnerability

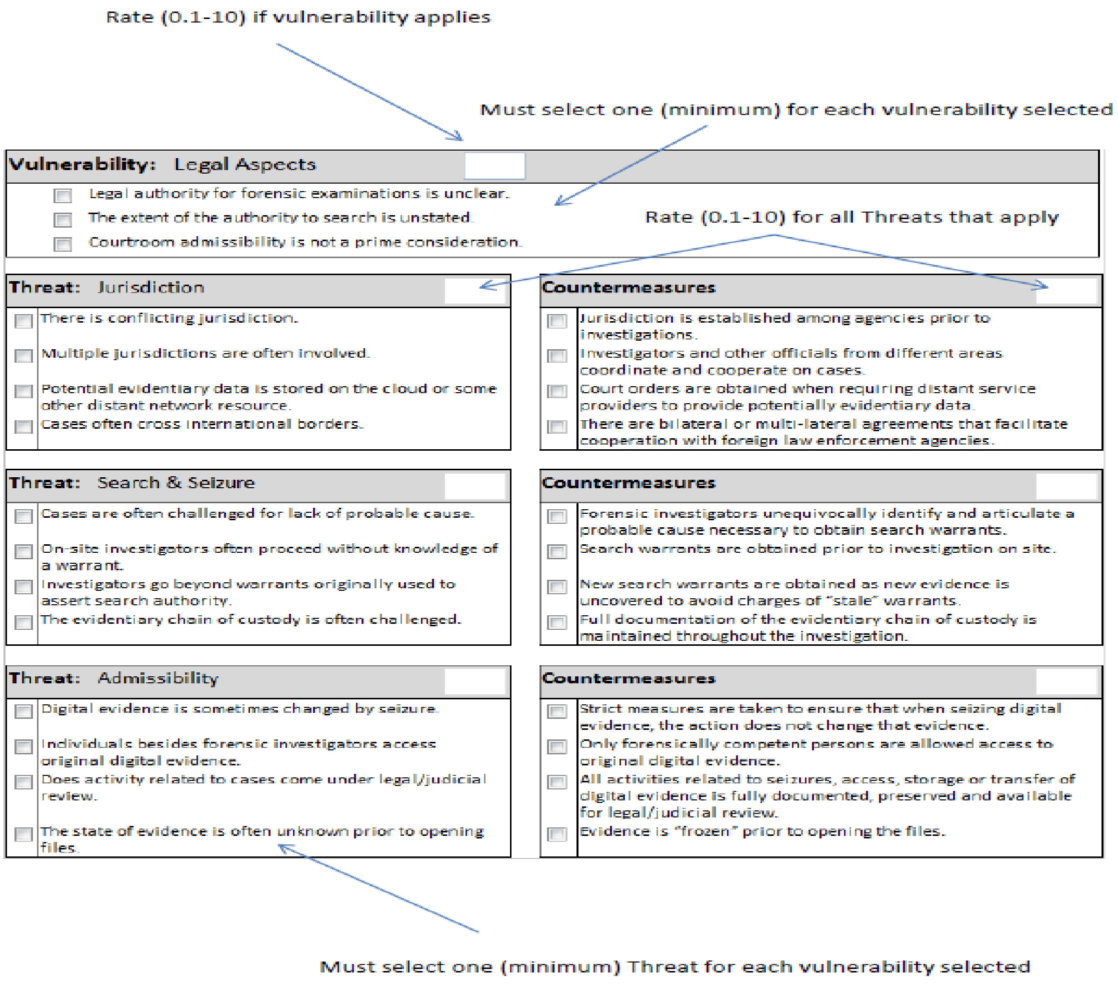
- Rate **Vulnerability** (0.1-10) with 10 being ***most*** vulnerable and 0.1 being ***least*** vulnerable
- Select all vulnerability statements that apply (***must choose at least one***)

Threat

- Rate **Threat** (0.1-10) with 10 being ***greatest*** threat and 0.1 being the ***least*** threat.
- Using square check box, select all threat statements that apply to each threat category chosen. (***must choose at least one***)

Countermeasure

- Rate associated **Countermeasure** for each threat category chosen above (0.1-10) with 0.1 being ***least*** effective and 10 being the ***most*** effective countermeasure.
- Using square check box, select all countermeasure statements that apply (***must choose at least one***)



Rate (0.1-10) if vulnerability applies

Must select one (minimum) for each vulnerability selected

Vulnerability: Legal Aspects

□ Legal authority for forensic examinations is unclear.

□ The extent of the authority to search is unstated.

□ Courtroom admissibility is not a prime consideration.

Rate (0.1-10) for all Threats that apply

Threat: Jurisdiction	**Countermeasures**
□ There is conflicting jurisdiction.	□ Jurisdiction is established among agencies prior to investigations.
□ Multiple jurisdictions are often involved.	□ Investigators and other officials from different areas coordinate and cooperate on cases.
□ Potential evidentiary data is stored on the cloud or some other distant network resource.	□ Court orders are obtained when requiring distant service providers to provide potentially evidentiary data.
□ Cases often cross international borders.	□ There are bilateral or multi-lateral agreements that facilitate cooperation with foreign law enforcement agencies.

Threat: Search & Seizure	**Countermeasures**
□ Cases are often challenged for lack of probable cause.	□ Forensic investigators unequivocally identify and articulate a probable cause necessary to obtain search warrants.
□ On-site investigators often proceed without knowledge of a warrant.	□ Search warrants are obtained prior to investigation on site.
□ Investigators go beyond warrants originally used to assert search authority.	□ New search warrants are obtained as new evidence is uncovered to avoid charges of "stale" warrants.
□ The evidentiary chain of custody is often challenged.	□ Full documentation of the evidentiary chain of custody is maintained throughout the investigation.

Threat: Admissibility	**Countermeasures**
□ Digital evidence is sometimes changed by seizure.	□ Strict measures are taken to ensure that when seizing digital evidence, the action does not change that evidence.
□ Individuals besides forensic investigators access original digital evidence.	□ Only forensically competent persons are allowed access to original digital evidence.
□ Does activity related to cases come under legal/judicial review.	□ All activities related to seizures, access, storage or transfer of digital evidence is fully documented, preserved and available for legal/judicial review.
□ The state of evidence is often unknown prior to opening files.	□ Evidence is "frozen" prior to opening the files.

Must select one (minimum) Threat for each vulnerability selected

Appendix B

Respondent Results Tabulations

SURVEY TAKER	RESIDUAL RISK %	RANKED OVERALL(OUT OF 27)	REMARKS
AFIT1	52.47	6th	2nd out of 4 within AFIT *(Group Median for AFIT)*
AFIT2	49.90	9th	3rd out of 4 within AFIT
AFIT3	52.71	5th	1st out of 4 within AFIT
AFIT4	47.64	10th	4th out of 4 within AFIT
AUPD1	31.15	26th	7th out of 7 within AUPD
AUPD2	39.67	20th	5th out of 7 within AUPD
AUPD3	50.02	8th	1st out of 7 within AUPD
AUPD4	36.98	21st	6th out of 7 within AUPD
AUPD5	44.59	16th *~OVERALL AVERAGE*	4th out of 7 within AUPD *(Group Median for AUPD)*
AUPD6	46.06	13th	3rd out of 7 within AUPD
AUPD7	47.06	11th	2nd out of 7 within AUPD
ECSO1	51.80	7th	5th out of 9 within ECSO *(Group Median for ECSO)*
ECSO2	46.66	12th	6th out of 9 within ECSO
ECSO3	56.94	2nd	2nd out of 9 within ECSO
ECSO4	57.67	1st	1st out of 9 within ECSO
ECSO5	54.87	3rd	3rd out of 9 within ECSO
ECSO6	41.36	19th	9th out of 9 within ECSO
ECSO7	54.84	4th	4th out of 9 within ECSO
ECSO8	45.83	14th *MEDIAN*	7th out of 9 within ECSO
ECSO9	45.01	15th	8th out of 9 within ECSO
OPD1	35.00	23rd	4th out of 7 within OPD *(Group Median for OPD)*
OPD2	42.56	18th	2nd out of 7 within OPD
OPD3	44.35	17th	1st out of 7 within OPD
OPD4	33.39	25th	6th out of 7 within OPD
OPD5	28.23	27th	7th out of 7 within OPD
OPD6	34.39	24th	5th out of 7 within OPD
OPD7	36.41	22nd	3rd out of 7 within OPD

Table 1. Companies' (AFIT, AUPD, ECSO, OPD) no-names disclosed survey results for the Risk-O-Meter study, ranked within and overall, where Median: 45.83 (ECSO8) and Average: 44.73% (AUPD5: 44.59% is the result that comes the closest).