CYBERCRIME FIGHTING READINESS EVALUATION USING ANALYTIC HIERARCHY PROCESS

[1]MOHAMMED OTAIR, [2]AIMAN AL-REFAEI

[1] Amman Arab University, Department of Computer Information Systems, Jordan
[2]Royal Jordanian, IT Department, Jordan
E-mail: [1]otair@aau.edu.jo, [2]Aiman.AlRefaei@rj.com

Abstract- Since the first cybercrime was recorded in 1820 and with the fast growth of the Internet usage and computerized systems, it has become critical to know what the affect that cybercrimes may cause. Organizations have to estimate their readiness to fight such kind of crimes by determining the main significant factors that may affect their readiness level. Upon that they work on enhancing the low-weighted factors. This paper provides a new approach of evaluation method to Cybercrimes fighting readiness using Analytical Hierarchy Process (AHP). The major idea of this paper lies in showing how to identify the readiness of an organization to fight Cybercrimes and how to determine the critical factors that affect this readiness, and the weights (relative importance) of the factors for the goal (Cybercrime fighting) and for each other hence reaching the percentage of readiness level of Cybercrime fighting for an organization. It is important to note that the factors are provided by the organization and depend on the setup that the organization uses to reduce the potential risk that may come from cybercrimes. Finally, to clarify the proposed idea and as a proof of concept, a case study is illustrated in the paper. The paper takes the Royal Jordanian Airlines in particular the Information Technology department as a case study showing details and results so as to arrive at conclusions.

Keywords- Cybercrime, AHP, Decision Making, and Fighting Readiness.

I. INTRODUCTION

With the spread of computers and the Internet there emerged several fields to make use of them. However, there also emerged a culture whose traditions and values contradict with the traditions, values and traits of some societies. Due to the sudden exposure to the world's civilizations and due to providing a sudden mass of information to individuals, the Internet has severed the interests and fulfilled the needs of individuals and organizations. It has, on the other hand, become a source from which comes into sight a new kind of crimes called cybercrimes. Although cybercrimes are radically different from other kinds of crimes, the damage caused by cybercrimes cannot be separated from the damage that results from other kinds of crimes, and so it should not be underestimated. The objectives of cybercrimes [1]:

1. To access information illegally.
2. To cause malfunction or to damage the servers that have certain information.
3. To extort.
4. To access credit card details and use them illegally
5. To promote terrorism and ideological extremism throughout spreading them over the Internet.

To reduce the number of cybercrimes, there is a need for an intense investigation and effort in setting rules and ways to reduce the damage that results from these crimes. Counteracting cybercrimes must develop in the same pace of development of cybercrimes themselves. It is the way to reduce the potentially damaging and dangerous effects of cybercrimes which are usually material and moral losses for users. Therefore, this proposed approach of this paper aims at measuring how ready the institution is to counteract cybercrimes using AHP for alternatives selection. It measures the organization's readiness based on the factors used by the organization to protect and secure its information, the objectives behind this protection of the information and the relative importance of these factors and objectives to the organization. The proposed approach of this paper aims at:

1. Measuring how ready the organization is to counteract cybercrimes.
2. Deciding the factors on which the organization depends in its fight against cybercrimes.
3. Assessing these factors and showing the points of weakness in them so as to fix them.
4. Showing the level of consistency on how important the factors are to the organization in fighting cybercrimes.

The paper consists of five sections, involving this introductory section. Section two makes up background information necessary and literature review to the paper related topics. Section three is entitled "Decision Making and Analytic Hierarchy Process". It provides prolific description of decision making and decision making process along with an abundant explanation of Analytic Hierarchy Process (AHP) as one of decision making methods. Section four consists of two parts; the first one explains the proposed approach with its details, steps, notations and calculations. The second is a case study that was conducted on Royal Jordanian Airlines showing a proof of concept of proposed approach. Section five presents the conclusions; this section presents the conclusions drawn from this research.

II. BACKGROUND

In the beginnings of the Internet, there was no concern about "crimes" that may defile the network due to the restricted number of the users who were limited to a specific category of users who were university students or researchers. However, with the growth of the network access and use of all portions of society to a lot of users, new crimes have begun to present on such network that raise during time with many forms and manifestations. Therefore the network is not safe in its design and construction.

There are several definitions of cybercrime - There is no standard or unified definition – and the following is some definitions of the term:Cybercrimes known technically as a criminal activity using the computer technique, directly or indirectly, or as a target for the implementation of the criminal act in question [3].

The phenomenon of cybercrime came immediately after the start of the use of network directly connected to computers, so some people tried to use this technology for illegal and illegitimate targets [2].

This decade has also witnessed the start of the laws and legislations for the protection of computer programs throughout intellectual property protection laws and legislations which are more mature and clear computer laws [5] and many of the world countries followed the laws that criminalize the misuse of some of the computer activities, such as Israel and Iceland 1981, Canada and Australia in 1982, the UK in 1984, Finland in 1987, and both in Japan and the Republic of Ireland and Switzerland in 1988 [4]. The beginning of Arab interest in this phenomenon was with holding a symposium on information security in computers which was organized by the National Information Center Saudi Interior Ministry in 1986 [6]. In addition to the issuance of a number of scientific studies, Arabic literature, some aspects of the relationship phenomenon were discussed i.e. the PhD researcher MubdarAlwees [7], entitled the impact of technological development on the personal freedoms, and a book of legal protection for software by Hossam Mohamed Lutfi [8].

The nineties and the early years of the twenty-first century have highlighted new orientations of computer-related crimes which are associated with the transformation of the Internet from being academic in nature to a network that serves commercial and personal purposes. This commenced to a raise in the number of users is large [9].

With the large increase in the number of users, a new and dangerous dimension was added to cybercrimes, as it made it all the user has to potential criminals by the criminal justice in any country in the world.

In 21st century, the problem of cybercrime grew and emerged as computing became available, cheap and easier. These days, every person in world countries can use their own computer technology or they can access Internet cafes or business centers. So, the issue of cyber warfare, cyber competitiveness, and cyber security has significant impact on the opinions of policymakers over the last decade. The attacks oriented against both the private and public sectors, are the caused by heterogeneous networks whose impacts are encouraged by a several number of factors. For the next generation, the governments should achieve a high level of worthiness for the most issues of cyber security [10]. To better prevent, detect and deal with cybercrimes, one might strive to understand the profiles and the motivations of cybercriminals.

III. DECISION MAKING AND ANALYTIC HIERARCHY PROCESS

Decision-making is an operation of selecting amongst alternative sets of actions in order to accomplish objectives and goals. Simon in [15] wrote that the entire operation of managerial decision-making is equivalent with the management practice [16]. Consequently, the heart of all managerial tasks is a decision-making processes. For instance, planning includes determining what, when, how, where should be done and by whom. In addition, other managerial tasks like controlling, implementing, and organizing depends extremely on the decision making processes.

The Analytic Hierarchy Process (AHP) is defined as a method of general problem-solving technique. It is valuable in making sophisticated a decision (i.e. multi-criteria) depends on parameters that do not have perfect numerical outcomes. Further, it is a planned method for handling complex decisions. Instead of recommending correct decisions, the AHP assists the decision maker to search the decision that adequate their understanding and needs of the problem.
The AHP users should break-down their problem components into a hierarchy of sub-problems. Each one is to be separately looked into. Upon founding the hierarchy, decision makers methodically assess its diverse components by contrasting each two at a time. The essence of the AHP lies in the fact that human judgments along with the underlying information can be used in achieving the assessments [11].

When a decision maker has multiple criteria, AHP is the best method [12]. That is it helps to choose the alternative that best matches the decision criteria, and then leads to develop numerical scores to categorize every decision alternative depends on how every alternative matches them.
Saaty [13] has presented AHP as a decision technique to assist in solving unstructured problems in

management, social, economic and sciences since 1977. The AHP makes it possible for the decision-makers to formulate a sophisticated problem in the shape of a hierarchy and to assess a huge number of qualitative and quantitative factors. The implementation of the AHP for sophisticated problem mainly takes four key steps [14]:

1. Divide the sophisticated problem into a number of small components and then arrange them in a hierarchical shape.
2. Conduct a set of pair-wise comparisons along the components regarding to a ratio scale.
3. Use the eigenvalue method to estimate the weights of each components or elements.
4. Assemble these weights and synthesize them for the final measurement of specific decision alternatives.

After that, decision makers compared each group in the same level in a pair-wise fashion relying on their own knowledge and experience. For example, every two criteria in the second level are compared at each time with respect to the goal, while every two attributes of the same criteria in the next level are compared at a time with respect to its corresponding criterion. Since the comparisons are achieved through subjective judgments and some degree of inconsistency may occur. To guarantee that judgments are harmonious, the final operation, consistency verification, which is regarded as one of the most advantageous parts of the AHP, is incorporated in order to measure the degree of consistency among the pair-wise comparisons by computing the consistency ratio. The consistency ratio should exceed the limit, decision makers are to revise and review the pair-wise comparisons.

Once all pair-wise comparisons are conducted at each level and proved to be consistent, the judgments can then be synthesized to detect the priority ranking of each criterion and its attributes.

IV. CYBERCRIME FIGHTING READINESS EVALUATION

This proposed approach uses to evaluation the readiness level that the organization already has to fight and counteract the potential Cybercrimes, and it's fully dependent on the organization's factors that used to counteract and prevent Cybercrimes.

The decision maker in organization who's responsible to determine those factors and to give importance weight for each one (regarding to the goal and for each others). The steps of this approach will be presented in this chapter by details. Second part of this chapter is a case study. This case study was conducted in Royal Jordanian Airlines to show and clarify the proposed approach we by number.

The proposed approach is Cybercrime Fighting Readiness Evaluation (CFRE) using Analytic Hierarchy Process (AHP), but before using AHP, the preparation phase should be done by executing the following steps [18]:

1. State the objective or goal; Cybercrime Fighting Readiness Evaluation (CFRE).
2. Define the goal criteria (criterions), which can be qualitative or quantitative, (e.g., Physical security, Information security, Security procedures performance, etc).
3. Define goal sub-criteria (sub-criterions) for each criterion, which can be qualitative or quantitative also, (e.g., Physical security standards, Physical security procedures, Information security policies, etc).

The following are the steps to build the proposed approach [19]:
1. Problem hierarchy with its graphical representation is developed; state thorough goal, criteria (criterions) and sub-criteria or alternatives.

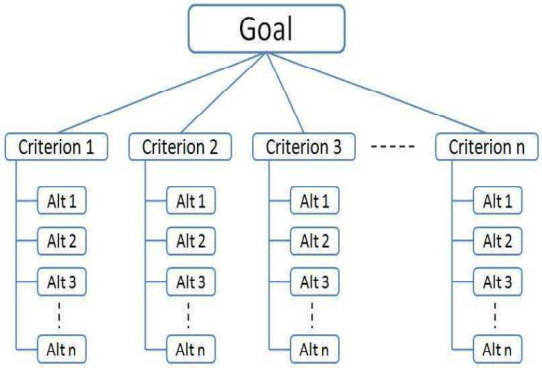


Fig. 1. The hierarchy model [17].

2. Construct pairwise comparison matrices; two criteria (criterions) or alternatives are compared at each time to find out which one is more important.

Here is the explanation of what paired comparison is. It is always easier to explain by an example. Assume there are two criterions (alternatives) X and Y. If you like the X better than Y, you thick a mark between number 1and 9 on left side, while if you advocacy Y more than X, then you mark on the right side.

The number of comparisons depends on the number of criterions (alternatives) according to the following equation:

$$No.of\ Comparisons = \frac{n(n-1)}{2}$$

3. Synthetization of judgments [20]; calculate the priority of each criterion (alternative) and sub-criterion (sub-alternatives) in terms of their contributions to the overall goal.

A Case study

The proposed approach will be used to evaluate Cybercrime Fighting Readiness Evaluation (CFRE); also a numerical illustration will be used to show the proposed approach.

First of all, the model should be prepared though applying the preparation phase, which consists of following steps:

1. State the goal or objective.
The goal is to conduct Cybercrime Fighting Readiness Evaluation (CFRE).
2. Define goal's criteria.
The goal's criteria decided by concerned people in

Royal Jordanian Airlines are:
I. People's Education – Qualitative criterion.
II. Security Enhancement – Qualitative criterion.
III. Law Enforcement – Qualitative criterion.
3. Identify goal's sub-criterions, criterions were as following.

I. People Education sub-criterions:
i. Security Training.
ii. Security Awareness.
iii. Risk Assessment Training.

II. Security Enhancement sub-criterions:
i. Confidentiality, this sub-criterion has another level of criterions:
1. Encryption.
2. Intrusion Detection System/ Intrusion Prevention System (IDS/IPS).
3. Penetration Testing.
4. Software Security.
5. Identification and Authorization.
6. Firewall.
ii. Integrity, this sub-criterion has another level of criterions:
1. Logging.
2. Documentation.
3. Firewall.
iii. Availability, this sub-criterion has another level of criterions:
1. Backups.
2. Incident Handling Procedures.
3. Physical Security.
4. Disaster Recovery.
5. Contingency Plan.

III. Law Enforcement sub-criterions:
i. Policy and Procedures.
ii. Enforcement Procedures.
iii. Roles and Responsibilities.
iv. Management Support.
The following steps are to build the proposed approach:
1. Developing the hierarchy of Cybercrime Fighting Readiness Evaluation in graphical representation.

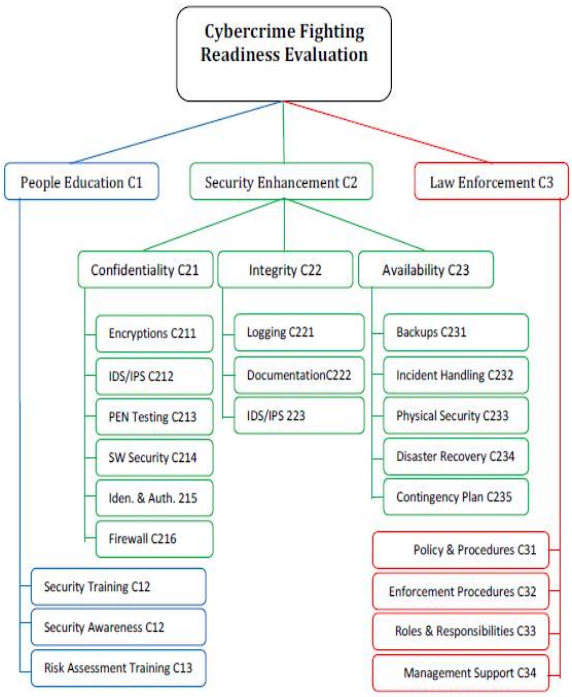


Fig. 2.The hierarchy of Cybercrime Fighting Readiness Evaluation in graphical representation

2. Constructing pairwise comparison matrices, two criterions (sub-criterions) are compared at each time to find out which is more important.
a. Constructing Analytical Hierarch Process (AHP) comparison matrices using Saaty's scale:

- **Comparison for criterions that achieve the comprehensive goal (Cybercrime Fighting Readiness Evaluation).**

Table 1: AHP pairwise comparison for goal.

	C1	C2	C3
C1	1	1/8	1/3
C2	8	1	6
C3	3	1/6	1

Where
C1: People's Education
C2: Security Enhancement
C3: Law Enforcement

□□Comparison for criterions that achieve People's Education (C1).

Table 2: AHP pairwise comparison for people's education criterion.

	C11	C12	C13
C11	1	4	7
C12	1/4	1	6
C13	1/7	1/6	1

Where
C11: Security Training
C12: Security Awareness
C13: Risk Assessment Training

- **Comparison for criterions that achieve Security Enhancement (C2).**

Table 3: AHP pairwise comparison for security enhancement criterion.

	C21	C22	C23
C21	1	7	3
C22	1/7	1	1/3
C23	1/3	3	1

Where
C21: Confidentiality
C22: Integrity
C23: Availability

- **Comparison for criterions that achieve Law Enforcement (C3).**

Table 4: AHP pairwise comparison for law enforcement criterion.

	C31	C32	C33	C34
C31	1	1/2	3	1/4
C32	2	1	1/4	1/3
C33	1/3	4	1	5
C34	4	3	1/5	1

Where
C31: Policy and Procedures
C32: Enforcement Procedures
C33: Roles and Responsibilities
C34: Management Support

- **Comparison for sub-criterions that achieve Confidentiality (C21).**

Table 5: AHP pairwise comparison for confidentiality sub-criterion.

	C211	C212	C213	C214	C215	C216
C211	1	1/5	1/4	1/5	1/8	1/9
C212	5	1	1/3	1/4	1/2	1/2
C213	4	3	1	1/5	1/3	1/5
C214	5	4	5	1	1/3	1/4
C215	8	2	3	3	1	2
C216	9	2	5	4	1/2	1

Where
C211: Encryption
C212: IDS/IPS
C213: PEN Testing
C214: Software Security
C215: Identification & Authentication
C216: Firewalls

- **Comparison for sub-criterions that achieve Integrity (C22).**

Table 6: AHP pairwise comparison for integrity sub-criterion.

	C221	C222	C223
C221	1	3	1/5
C222	1/3	1	1/7
C223	5	7	1

Where
C221: Logging
C222: Documentation
C223: IDS/IPS

- **Comparison for sub-criterions that achieve Availability (C23).**

Table 7: AHP pairwise comparison for availability sub-criterion.

	C231	C232	C233	C234	C235
C231	1	1/5	4	1/2	1/3
C232	5	1	5	3	2
C233	1/4	1/5	1	1/4	1/6
C234	2	1/3	4	1	1/2
C235	3	1/2	6	2	1

Where
C231: Backup
C234: Disaster Recovery
C232: Incident Handling Procedures
C235: Contingency Planning
C233: Physical Security

The main objective of the case study is to provide a high level description and understanding of the proposed approach. The Cybercrime Fighting Readiness Evaluation Using Analytical Hierarchy Process approach that was conducted in the Royal Jordanian Airlines produced the following results:

- Royal Jordanian Airlines is 80.130% ready to fight and prevent Cybercrimes.
- The factors (and their weights) that Royal Jordanian Airlines depends on to counteract and fight Cybercrimes are as follows:

Factor	Weight
Firewall	0.0875
Iden. & Auth.	0.0869
Security Training	0.0686
Roles & Responsibilities	0.0678
Incident Handling	0.0630
SW Security	0.0626
IDS/IPS (Integrity)	0.0609
Contingency Plan	0.0521
Management Support	0.0518
IDS/IPS (Confidentiality)	0.0511
Policy & Procedures	0.0495
Enforcement Procedures	0.0454
PEN Testing	0.0430
Disaster Recovery	0.0415
Security Awareness	0.0385
Backups	0.0319
Logging	0.0255
Physical Security	0.0210
Documentation	0.0157
Risk Management Training	0.0153
Encryptions	0.0151

- The three most high-weighted (important) factors are: “Firewall”, “Identification & Authorization” and “Security Training”.
- The three most low-weighted (weak) factors are: “Documentation”, “Risk Management Training” and “Encryptions”.

CONCLUSIONS

In this study, we use integrated approach to determine attributes weights and priorities in Cybercrimes Fighting Readiness Evaluation as a multi-criteria problem solving method using Analytic Hierarchy Process. This approach can take into consideration both subjective and objective, qualitative and quantitative factors, and at the same time the decision maker's preferences. We presented in details the proposed approach; the first conclusion is that the proposed approach developed and discussed in this thesis offers a useful and comprehensive method to evaluate organization’s readiness to fight Cybercrimes. More specifically, we conclude that this approach can give decision makers the factors that may affect organization’s readiness to counteract or fight cybercrimes with its relative importance to the goal and to each other. Furthermore, we conclude that the proposed approach offers dynamic model that may be useful in different types of organizations.

REFERENCES

[1]. Abdallah A., Internet and Information Crimes book, Alhalabi, 2007.
[2]. Syngress, Scene of the Cybercrime: Computer Forensics Handbook, 1st edition, ISBN: 978-1931836654, 2002.
[3]. J. Evers, Computer crime costs $67 billion, http://news.cnet.com/2100-7349_3-6028946.html, CNET News.
[4]. Sieber U., Legal Aspects of Computer-Related Crime in the Information Society, University of Wurzburg - Study Prepared for the European Commission, http://europa.eu.int/ISPO/legal/en/com-crime/sieber.html, 1998.
[5]. Younis Arab, Computer law handbook, 2001, Beirut.
[6]. Security challenges associated with the new means of communication, the first scientific conference of the legal and security aspects of electronic operations, Dubai police academy, UAE.
[7]. Alwees M., The impact of technological development on the personal freedoms, 1982.
[8]. Lutfi H., Legal protection of software, 1987.
[9]. Al Obaid M., Internet, the future investment handbook, 1996, Riyadh.
[10]. Carafano J., Building cyber security leadership for the 21st century, Ph.D. and Eric Sayers, December 16, 2008, http://www.heritage.org/Research/NationalSecurity/bg2218.cfm.
[11]. Saaty T., Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors - The Analytic Hierarchy/Network Process, RACSAM "Review of the Royal Spanish Academy of Sciences, Series A, Mathematics", 06-2008.
[12]. Taylor B., Introduction to Management Science, Pearson Education Inc., New Jersey, 2004.
[13]. Saaty T., The Analytical Hierarchy Process, Mc Graw Hill, New York, 1980.
[14]. Cheng C. and Yang K., Evaluating Attack Helicopters by AHP Based on
[15]. Linguistic Variable Weight, and Hwang, C. L., European Journal of Operational Research, 116, 423-435, 1999.
[16]. Simon H. and March J., Organizations, New York, Wiley, 1958.
[17]. Simon H., The New Science of Management Decision, (New York: Harper & Row), pp. 40 - 43, 1960.
[18]. Craig Borysowich, Chief Technology Tactician, Toolbox for IT, The Analytic Hierarchy Process, http://it.toolbox.com/blogs/enterprisesolutions/the-analytic-hierarchy-process-12849, posted 11/9/2006.
[19]. Taylor G., Logistics Engineering Handbook, CRC Press, ISBN: 978-0-8493-305307, 2008.
[20]. Teknomo K., Analytic Hierarchy Process (AHP) Tutorial, KardiTeknomo's Homepage, http://people.revoledu.com/kardi/tutorial/ahp, 2006.
[21]. Kris Kniaz website, Analytic Hierarchical Process.NET, http://www.kniaz.net/software/ahp.aspx

★★★