IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

IT Risk Management

Hussin Al Elwani Abdussalam, Ahmed Alarbi Bashir Amer

Lecturer, Department of Computer Science, Higher Institute for Comprehensive Careers, Tarhuna, Libya

Lecturer, Department of Computer Science, Higher Institute for Comprehensive Careers, Tarhuna, Libya

ABSTRACT: More and more companies are concern about their IT risks nowadays, especially the companies relying on IS (Information System) in business. The objective of this thesis focused on what risk in the case company should be paid the most attention to. In short, the aim is to find out what the biggest threat was in the case company and the reason. Moreover, when exploring the answer, it was possible to understand the process of managing IT risks.

The general methodology of this study is deductive research method. It aimed to check if the general IT risks found in literature in the case company. Moreover, the researcher was to develop the theory that organized cyber criminals and hackers are the riskiest security problem in business. Interviews and observation were carried out collect the data.

The study revealed that, inadequate anti-virus software protection is the biggest threat for the case company, and because the manager decided to ignore the existing problems, it will be an even bigger threat in the future.

I. INTRODUCTION

1.1 Background

In the past decades, it was always heard from the press that crises are happening, such as the economic crisis, energy crisis and nuclear crisis. Those crises have an impact on individuals, businesses, organizations, even nations. It may result in incredible impacts if people ignore the upcoming risks. However, not all the people have the crisis awareness. People do not care about it much until they have losses. The definition of risk 'Effect of uncertainty on objectives' (ISO 31000, 2009) was brought up. The bias of risk that represents badness has changed.

Hence, with a serious consideration, risk management is momentous. It is aimed to avoid the potential occurrence of risks, which is proactive. Indeed, not all probable threats are defined when people try to analyze the risks. There are still possibilities that the risk turns to be events that may cause negative impacts. Therefore, finding resolutions to redeem losses and reduce impacts, which refer to crisis management, is vital too (The difference between Crisis Management and Risk Management? 2010). Moreover, no matter which risks represent threats or opportunities, the impacts of event need to be assessed carefully.

As information technology is being used widely in companies to support their business, to secure IT becomes more significant. Every threat can be a disaster, even related to the organization's survival, especially for those companies that depend on the information systems. The better knowing of risks, the more secure the companies are. Therefore, managing IT risks in a company is vital to prevent from threats leading to disasters and to give countermeasures for better problem solving.

1.2 Statement of the problem

DTI (DTI Information Security Breaches Survey, 2006) reported that only less than 20 percent of small companies could survive without IT systems. In other words, large corporations operate their business with IT systems and the numbers has continued growing. Once the system breaks down or has something wrong, it may cause lots of direct losses, such as loss of system facilities, production, sales, communication, and control, also the business possibly fails. For instance, Comair, which is a huge airline company, valued to be $780 million, experienced a fatal hit due to the failure of crew-scheduling system. Thousands of passengers were affected by the crushed system. (Westerman & Hunter, 2007) Moreover, indirect consequences of IS disaster such as undetected fraud, financial loss through lack of billing and payment processing facilities, liability for payment of fines, damages and compensation, loss of customers, diminished public standing. Indeed, any potential risks of information systems could turn out to be a disaster and cause loss.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

1.3 Research objective

With the growing awareness for information technology security, it is worth to study IT risk management in an organization. Managing IT risks was carried out in case of business aiming at finding out which IT risk threatens the business most. Proactive perspectives would be reminded to have about potential risks for companies. In the case any loss is caused, this research would give some suggestions to do the remediation in a short time. It would also support improved decisions making for businesses and could protect them in a suitable way.

The company doing business in patent and intellectual property relies on IT systems.
The researcher did her internship in this business and wanted to study the IT threats there for these purposes. Also, the research could help the company to be aware of its IT security. Therefore, the case is provided as an example of management of IT risks for better understanding.

II. RESEARCH METHODOLOGY

In past decades, research was defined to have different academic meanings. A definition in Oxford Dictionary is "the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions" (Research: Definition of research in Oxford dictionary). The research problem or the hypothesis is a must to begin research. Literature review will assist the research in gaining the specific knowledge for a particular area. Gathering data and analyzing the findings are to refer interactively to the theory. According to the analysis, conclusions could be made for theoretical formulation.

2.1 Research question

Based on the situation that people have been more aware of IT security, the case company allowed the research to be put into practice. The partner in charge of the technical field in the company expected to know the most potential IT related risks, also the countermeasures for them. Therefore, the main idea of IT risk management What IT risk should be paid the most attention for the case company and why?

2.2 Research methods

The methodologies being used to reach new conclusions have many differences. In this study, qualitative research method is adopted. Deductive approach is applied to help the case study.

2.2.1 Qualitative research method

When referring to qualitative research process, it goes through people's behavior, perspective to get a deep understanding about the object, which focuses on the process of exploration and discovery rather than numerical or mathematical process. It also can be represented that subjective consciousness of human beings is using "words" to be expressed for interpretation of an aspect. There are many approaches to adopt in qualitative research. According to the research nature in this study, it was concentrated on the meanings of aspect or findings of people's thoughts and behaviors, in order to acquire detailed information.

Correlative with description and explanation as a case study approach uses in this study. For theory testing and development, the case design is helpful (Ghauri & Gronhaug, 1995).

Therefore, the researcher intends to study the process for making decisions for those IT risks. In other words, characterizing and categorizing on the basis of IT risks management and carrying out proper countermeasures for them are detailed explained in this study. Since the study conducting in the case business, IT risks management concatenating the resolution and recommendations according to the identified risks. Hence, it is helpful to use qualitative research process to provide suitable suggestions for the case company other than quantitative process with numbers and statistics.

Deduction typically utilizes in quantitative research. Nevertheless, it is not absolute.
In fact, in deductive reasoning, theories and hypothesis are tested by samples or data. Certainty becomes the target to reach a conclusion. Hypothesis formulates the beginning, and the findings in the experiment will be adjusted to the hypothesis through data will be focused on the research question:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

III. LITERATURE REVIEW

3.1 IT risk overview

ISO 27001 Standard as Information Security Standard (Threats & vulnerabilities) is to be considered to be the base of the IT risk management in this thesis. Common IT threats listed for different companies at the end of this paper as a reference.

Note worthily, those definitions are not critical, more and more potential IT risks and vulnerabilities would discover in the future. Moreover, it has to be adapted to the different companies.

Venafi, which focuses on certificate management solutions, brought out the top IT security risks expect in 2013. Organized cyber criminals and hackers are the riskiest security problem which infects IT systems with malware. It would cause data disclosure and another associated damage resulting in bad business operation (Venafi, 2013).

3.2 Risk management overview

People have noticed that the harmful influence is not one kind that risks can bring to them anymore. Hence, some professional delimits risk management as an efficiency to manage both potential opportunities and disadvantageous issues through culture, structures and processes (VMIA, 2010).

Since the financial crisis affecting global economy, loads of corporations faced adverse conditions. However, it could be an opportunity to be introspective what issues or risks do exist in theirs. Risk management becomes significant due to the high expectations from stakeholders, as well. The fewer troubles when doing business, the more profits they could get. A better decision may make from risk management as well, so that the work is possibly more productive and efficient in the company. (Hopkin, 2010).

In fact, quite many representations were given to illustrate the process of risk management. Williams (2007) introduced the framework of risk management in M_o_R Guide, involving principles, approach, process that has some similarities to ISO 31000 (2009) standard, and embedding and reviewing .

Twelve principles promote organizations to prepare policies, procedures and plan based on their own requirements (Williams, M_o_R - The Facts, 2007). The approach in the following figure (See figure 3) represents as five arrows to policy, process guide, strategies, risk register and issue log. First, to identify the context to acquire the needed information and the potential risks to avoid or mitigate damage, last but not least, the opportunities to improve the performance. Assessment applies estimation and evaluation to analyze the likelihood and impacts on business. Afterwards, in terms of the detailed countermeasures planned for the threats and opportunities, taking action to fit the expectation is the goal. Communication as an.

IV. CASE STUDY

4.1 Case overview

The researcher chose the company to be the study case because the researcher worked there as an intern for a while. The permission to manage IT risks in the case company admitted, meanwhile the company supported researcher to do the research in the business.

Case company has been trading for years in a 1 storey office, in a building that provides intellectual property monetization and research on global scale services.

IP commercialization services, technology-driven M&A, and strategic advisory service are offered to all potential clients. The company is not an IT company, but relies on IT to survive.

Twenty-one people worked there when researcher arrived in the company. Three people including IT leader worked for the IT department, four partners who launch the company, 1 HR, the remaining people work on the business department, their work includes consulting, scouting, analyzing the patents and connecting clients.

Besides, everybody in the company has a computer with two screens for business.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

Two servers support the system. Two phones prepared in the company for clients calling. Activity goes through the whole process.

V. DATA ANALYSIS

The research is aimed to find out if the hypotheses by the author and answer for the research question matches. The hypothesis, that inadequate anti-virus and anti-malware protection is the biggest threat in the case company, verifies through interviews and observation into groups.

The questions to technical department were different from others, in order to know how manager department dealt with the problems and whether their actions worked. In manager department, only one manager took charge of IT and technical affair.

The interview for this department was mainly specific for him. Answers by technical manager from manager department were given as follows (See box 1):

Q1: What was the IT problem happened before?
– The server for project students 'testing was totally crashed and out of use.
Q2: What caused the problems?
– Unorganized access rights. Everyone had the right to deploy their own work on the server in order to test if their work was working. If the student didn't import the previous student's codes and deployed his new codes, once there were conflicts between their codes, the system must crash over and over again.
Q3: How long did it take to solve it?
– It never solved. The server for students testing was abandoned.
Q4: Why not solved?
– IT people tried, but because there were so many students deployed their codes on the server perhaps in the meantime, and it's very complicated and time-wasting to revert their codes one by one, hence, there was no way except abandoned the server.
Q5: Are you now having a solution for this problem just in case if it happens again?
– Anyone who wants to test his work on the server must ask IT people for access password, also they have limitations on the server, for example they only have the access to import the correct codes which are perfectly working on the production server for business people, but no access to deploy to production server.

Q6: Who is to ask for the access passwords?
– IT team leader and technical manager
Q7: Does the same problem happen again?
– Not yet
Q8: What anti-virus and anti-malware are installed on machine?
– Microsoft Security Essentials
Q9: Why chose this software to be your protection software?
– It's free and build-in software.
Q10: How do you think about the software?
– It's okay; at least there is no virus and malware showing yet.
Q11: Have you thought to change better anti-virus software?
– Nope, we don't want to spend lots of money on it.

Box 1: answers given by manager department from interview

The questions from Q1 to Q7 in up indicated that the technical manager realized the risk after it happened and took actions to prevent. It was a great idea for project students to work individually and combine their codes to the existed system codes, but it had to fail without effective and correct disciplines for deploying codes. They were aware that the proper limitations could prevent the system to crash. From Q8 to Q11, it illustrated that the expenses and convenience for the company on the protection software were the most important factor to be concerned about. Moreover, they thought the protection was so far so good, because nothing happened yet. Answers for each question were prepared in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

interviews. During interviews, researcher asked questions and people to select one of the answers. The outcomes by IT department and business department showed in box 2. There were two IT people and two people from the business department being interviewed. The coding is as follows: I1 = IT leader, I2 = IT intern. B1- B2 = business interns (See box 2- the answer like "A/B" means people have different answers).

Q1: Will you let browsers save passwords on intranet system?(web development carelessness) (Yes, every website/ Not every website, it depends on if I can trust the website)
– I1 - I2: Not every website, it depends on if I can trust the website.
– B1 - B2: Yes, every website.
Q2: How often do you change your password on the intranet system?(web development carelessness) (Very often/Sometimes/Never)
– I1 - I2: Never
– B1 - B2: Never
Q3: How often do you clear your cookies? (attack)(Every week/Every month/Never)
– I1 - I2: Every week
– B1 - B2: Every month
Q4: Will you log out websites before you shut down computer? (attack)(Every time/Sometimes/ Never)
– I1 - I2: Never/Every time
– B1 - B2: Never/Every time
Q5: Do you upgrade software on your machine often? (attack)(Every time when the notification shows/ Sometimes/ Never)
– I1 - I2: Never/Sometimes
– B1 - B2: Every time when the notification shows
Q6: Have you ever clicked pop-ups on websites? (malicious software)(Yes/No)
– I1 - I2: Yes/No
– B1 - B2: Yes/No
Q7: Why did you click the pop-ups on websites or in emails (for people who answered Yes)?(Wrong clicking/ Curiosity)
– I1 - I2: By wrong clicking
– B1 - B2: Curiosity/Wrong clicking
Q8: Will you turn off computer directly when you leave? (misuse IT)(Every time/Sometimes/Never)
– I1 - I2: Never/Sometimes
– B1 - B2: Sometimes

Box 2: answers by IT department and business department from interview

The questions were asked to determine the likelihood for the identified threats. From the given answers, even the interview was in groups, some answers did not have much difference.

However, the box two provided some information, for instance, saving passwords seemed to be convenient for users, but it is risky because it will give a chance to someone who may steal the FTP credential. On this question, business people are more aware of the convenience.

Masquerading the user and make information exposed are easy without changing passwords. Unfortunately, all people involved in the interview provided the answer that they never changed the password on websites. People like to use the same passwords for different websites, once the password lost; intruder may make other thefts on the websites people are usually browse. Hence, password is a significant problem.

Same as cookies, it contains the authentication token, once the cookies exposed, anyone could represent a user's session with an application and so easy to attack the system. People from the IT department were more careful with the cookies and clear it every week; it is a very good way to protect their information. What is more, hackers could hack

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 9, September 2024

|DOI: 10.15680/IJIRSET.2024.1309035|

the system by vulnerabilities such as if people do not log out website or keep signed in or old programs without patches. Interviewees from both departments gave the answer they never log out the website. Thus, the possibility the system being hacked was raised. People clicked the pop-ups on websites by mistakes and curiosities. Malicious software is easy to install automatically on machines. Insiders' misuse IT will damage the machine or lead to data lost. Observation was conducted by concerning the reality of the interview and new discoveries missing from the interview data. Observers were technical manager, random people whoever leaving their machines alone and browsing social media website in the case company and IT interns when applying codes, was selected randomly from each department. Started from manager level, technical manager knew to protect machines by anti-virus software, but without checking the security level of the software.

Researcher pointed out that free anti-virus may not cover much protection for safety.
Nevertheless, for the case company, they are not willing to pay for anti-virus software. From researcher's side, it may be not necessary to pay that much on anti-virus now. Nevertheless, as the company develops and gets stronger, especially for a company who relies on the information system to do business, it will attract lots of troubles to come after without a precise protection. When researcher was in the case business, the potential chances to become a bigger company were foreseen. A good anti-virus protection is impending and needed.
Unfortunately, researcher found that the company did not plan to do so even when researcher left the company.

VI. CONCLUSIONS

When developing the intranet system, whoever the IT people or project students are, carelessness is the most dangerous for system crash. Without clear disciplines for IT usage, making loss is about time. Employees in the company should be educated to strengthen their IT security awareness and teach them how to reduce the risks. How people use information system is based on their benefits, convenience is the first thinking condition. People with IT risks awareness care more about the information disclosure. Lack of IT knowledge can become vulnerable for attackers.

Risk consciousness is low in the company because business goes smoothly with information technology. Only when the risks turn to be an event and cause loss, the company starts to take action to decrease the loss. People think their surroundings are safe without an obvious sign of distress.

On the whole, the top management decision is the key of the IT security factors in the case company. In addition, insiders' behavior and their awareness can enhance or lessen the risks.

Owing to the case company relying on information system to survive, and its data is much more worth, weak anti-virus software protection might lead to the data breach and ruin the business. A lagging action taken by manager side will bring more troubles and loss to the company. People think it is perfectly safe because there is no loss having made since years by using this anti-virus software. Losses mean risks. The anti-software software had not installed until researcher left the company; even there were instructions and warnings. Ignoring the existing problems could threaten the case company.

From the researcher's opinion, inadequate anti-virus software protection is the biggest threat for the case company, and because the manager decided to ignore the existing problems, it will threaten more.

REFERENCES

[1]. Cadle, J., & Yeates, D. (1991). Project Management for Information Systems.
[2]. Cannell, C. F., & Kahn, R. L. (1968). Interviewing.
[3]. Cohen, L., Manion, L., & Morrison, K. (2007). Research Methods in Education.
[4]. CR, K. (1985). Research Methodology-Methods and Techniques.
[5]. Creswell, J. W. (2008). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research.
[6]. Denzin, N. K., & Lincoln, Y. S. (1994). Handbook of Qualitative Research.
[7]. Edmonds, W. A., & Kennedy, T. D. (2013). An Applied Reference Guide to Research Designs.
[8]. Ghauri, P., & Gronhaug, K. (1995). Research Method in Business Studies.
[9]. Hopkin, P. (2010). Fundamentals of Risk Management.
[10]. Oppenheim, A. (1992). Questionnaire Design, Interviewing and Attitude measurement.
[11]. Philpott, D., & Einstein, S. (2011). The Integrated Physical Security Handbook.
[12]. Priest, A., & Wood, K. (2012). IT Risk Analysis.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details