International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-6)

Research Article

June 2017

Provide an Approach to Development and Security Preparation Forensic

Reza Sadeghi Rashed[1], Mohammad Bagher Mohammadi Lame[2]
[1] Master of Information Management Azad University, Tehran, Iran
[2] Master of Engineering, University of Shiraz, Iran

Abstract:

In the world, despite the efforts sparse for the use of information and communication technologies in some industries and businesses carried out, due to the lack of capacities and infrastructure required, preparation Forensic, causing a sharp drop in the performance of investments undertaken and the lack of benefits of ICT and mistrust and insecurity in And the vulnerability of information assets. In this regard Forensicpreparation assessment models provide the most help in understanding the status quo. Elements such as access mechanism, event tags, structure, communication systems and operating systems, intrusion detection systems, standards for data collection run by technical and non-technical factors affect protection of witnesses and the time this location. In this paper, according to the progress of society in the field of computer networking vacuum talk Forensic and preparedness in this area due to the emergence of e-government, there is discussed that requires the review process liable to digital evidence is in case any thing happened to information assets to risk losing assets and lowered consumer expenditure in this area to ensure future Forensic assets.

Keywords: Information and communication technologies, Forensic preparation, Electronic business.

I. INTRODUCTION

First, identify national goals before selecting the assessment tool is necessary. Decision-makers must have a clear purpose and specific in order to prepare a community based on the view that the Forensic have to choose. After a difficult election policy makers aim to stage selection tools come standard. Each of these criteria, definitions and different ways to achieve their goals. Each of these criteria, definitions and different ways to achieve their goals.Forensicpreparation of a country's development strategy in the country or society through setting goals and having a global ICT. It should be ready to choose models and indices that measure levels of society do. Next, choose your strategy and your program to run[1].

The objectives of achieving preparationForensic with regard to economic, social, technical and legal are the economic objectives such as to remain competitive digital infrastructure information and communication technology, expanding applications of information and communication technology in order to develop the economic potential and development of foreign investment and social goals such as bridging the digital divide, benefit people and organizations from data quality and confidence in customers, among others.Forensic to assess different models, including CSPP, CID, APEC, MOSAIC, EIU and Information Technology U There are different ways to measure the preparation indexes and Forensicoffered[1].

There preparation assessment models would calculate Forensic enter into the information age and the context provider is monitoring the performance of executive agencies. Unfortunately, in our country a model or parameters specific to assess the preparationForensic there is only evaluation criteria, reporting organizations and foreign entities. Therefore, it is necessary to prepare a report prepared Forensic countries in various fields such as government Forensic, trade Forensic and training Forensic should be considered to assess the strengths and weaknesses of strategies for improving preparedness Forensic which guarantees the realization of the knowledge-based development plans, to be developed.Forensic prepared to develop different models there. This model has its own criteria and methods that are more accurate planning to enter the information age. Unfortunately, there's a certain model that should be considered[1,2].

II. PROPOSED SOLUTIONS

In recent years in efforts to design and implement Forensicpreparation assessment models were made, but no action has been taken in the preparation Forensic network. Although this pattern is not complete and presented in the context of the intended use of the complete picture of the level of preparedness Forensic (network) does not provide, but these models has its own characteristics. By examining different models such as the CID and the EIU and inspired them, according to the studies conducted to assess the model name NFRI Forensic computer networks is provided. This template is within the scope of the network is dependent on four main indicators, including equipment, personnel, politics and economics, each with several sub as well. If an organization is asked how've protected yourself against attacks? Most of them will answer "We have a firewall known and a program antivirus on the server we use, so we attack the safety we will." Note that security is a process not a product that the buyer Fiction in relation to the security of our own comfort.

Managers need proper recognition and initial potentials public a firewall or programs, antivirus be (able to do what he is and what he could not do, for example, if the new virus written in distribution network, the programs antivirus capable of detecting and it will not be dealing with. these types of programs only after analyzing a virus and how it should be updated quotation does apply to the case dealt with the same situation). Tools such as firewalls or programs, antivirus, part of the process to secure sensitive data in an organization and using them can claim that their organization fully against attacks, will protect; and the way existing instruments should also be validation are to be specified that these tools are not designed for espionage purposes. In conjunction with the review of these matters should be focused on localization tools.

There is a hole or security problems can affect an organization in different ways will.

Prevention of damage and the dangerous consequences of a security hole, one of the main reasons for implementing a security strategy are effective and efficient.

There are securities holes in an organization can have negative consequences for an organization to be followed:

- reduced income and increased costs
- damage to the reputation of an organization
- Loss of important data and information.
- disruption to current processes of an organization
- legal outcomes due to lack of negative side effects on the activity of the immune system and other organizations
- confidence in customers
- confidence in investors

With this interpretation the most effective security solution in order to prepare or Forensic, creating an environment that is multilayered. In a multi-layered environment, attackers in each layer will detect and deal with them. The successes of an attacker were to successfully cross all layers depends. Multilayered security strategy of "defense in depth" is also known. In this model, each layer of a certain defensive strategies will be used according to the dynamic nature of information security, information security professionals should be experts periodically review and update them. Each organization must have a framework or active security framework for the establishment and proper maintenance of it.

Security policy, which as a declaration of responsibility for any of the staff (people in the organization have access to sensitive information and systems) associated with information security and network defines and specifies. Document or declaration required as an integral part of every organization's security model is used. The main purpose of this announcement, offering an easy way to knowing and understanding how to protect the systems at the time of use. The outcome of this type of operation, failure and downtime associated with valuable information in one organization.

• Network policies

View logs system, one of the essential steps in the diagnosis of ongoing or imminent threat. Logs, to detect common vulnerabilities and provide relevant attacks. It can scan all the attacks identified, equipped and be safe. In the event of an attack, using system logs provided necessary facilities to track down the attackers. (Of course provided that they have uncorrected). Logs in the form periodic review and store them in a safe place[3].

• Run the scripts service or add unnecessary

The use of network resources and organization, as a personal playground for test scripts and different services, another common mistake made by most of the physically challenged system administrators.

Having such scripts and additional services are executed on the system, causing a series of potential and new entry points for an attacker will (if added services, or scripts on the server are installed and tested, problems can be double). If you need to test the script or run additional services, your desired operation should be done through a computer isolated (no computer connected to the network is not used in this regard).

• Note sensitive data and store them unsafe

Create and maintain strong passwords continuous process that should always be considered. Users always hate it when you create passwords that are not able to remember it. Edited security policy organization must determine how a password must be created and maintained. Remember that your password will always specific issues. In order to solve such problems, users tend to hide notes written them under the keyboard, wallets and or any other place in your workplace maintenance. These notes contain sensitive information related to the data is password and other related items. Using the above methods for storing information, a violation of security. In this way, users need to be justified and are they aware that non-compliance with security cases, the potential for problems in the system will increase. It is necessary to users, methods and techniques taught to use different passwords to remember for registered users of the notes of such sensitive data is reduced. And describe different scenarios for them to say that an attacker using what methods it is possible to record information in the notes, acquire and provide the underlying problem[4].

• Economy

The result of survey by research institutions regarding the security of information and the establishment of lasting security and preparedness against any vandalism and threats, showing the important fact that the raider attacks on the income and expenses of an organization directly or indirectly affect (reduced income, increased costs).

- ✓ In 2003, the attacks of viruses and DoS (from Denial of Service) had the most negative consequences for organizations to follow.
- ✓ In 2004, the highest ranked data theft and DoS attacks, a slight decrease compared to 2003, placed second.
- ✓ While the cost of implementing a protection system is not limited but can be considered as part of the costs that an organization due to lack of immunization, should pay (to deal with the negative consequences).

- ✓ In 2004, seventy percent of organizations have been attacked at least once.
- ✓ In 2003, over 666 million dollars to deal with security problems in the organization.
- ✓ Half of the organizations have acknowledged they do not know how much of your organization's information lost due to attacks.
- ✓ Forty-one percent of organizations have announced they have no plan or program not to report or respond to security threats.

Organizations and businesses to implement a security strategy and spend a little money to develop and maintain secure platform, will benefit from the following advantages:

- reduce the risk of inactivation system and application (the chance)
- Effective use of human and nonhuman resources in an organization (increasing productivity)
- reduce the cost of data loss by viruses or malware and security holes (protection of valuable data)
- Increased intellectual property protection
- The cost of preventing a security problem, always less than the cost of reconstruction is affected by it.
- a security problem that caused the loss of customer information, can have legal consequences for an organization to be followed.

- **failure to allocate appropriate funding to address the security of information.**

Convinced the director of a sufficient budget to address the issue of preparationForensic in the organization, including cases that will have its own challenges[5,6].

By assigning a proper budget to address the issue of preparation and Pricing Forensic in an organization, the necessary precautions in case of critical issues, enabling rapid detection of and response is appropriate.

In other words, with regard to securing adequate funding for the organization appropriate for protecting systems and sensitive data within an organization will be provided.

• Once in connection with security investment

Broad, extensive safety concept which required coordination and investment in both technology and training. Every day we witness the emergence of new technologies as well. We cannot be passive in the face of a new technology or items that we do not have a specific need to use this technology. Using technology effectively save time and material capital in search of better and cheaper and this would provide services to customers. The above issue from the perspective of an organization is important both in terms of customers, because they provide better services at a final price of fit one of the most important goals of any business is and customers are always looking for using the service and quality service and reasonable prices are. The use of new technologies and services associated with them, always follow your particular threat. Therefore, it is necessary to consider the security of an investment linked by responsible, because by employing new technologies to increase productivity in an organization, of addressing the security should be re-associated with the technology review and, if necessary, invest the necessary done about it. Thinking that security is a type of investment disposable, could be one organization in the use of new technologies casts doubt on the other hand, due to the attitude to security (disposable), Pricing has not been given the necessary and appropriate start to implement a security system and do not have the proper protection.

• Personnel

Now the people of America and the world heavily dependent on the cyber world and the nature of cyber infrastructure are; that in fact the security infrastructure of this dependence guaranteed and no laws to deal with crimes such as stripping attacks conducted or the threats were made, thereby strikes cyber infrastructure problems only shows weakness and in fact came instead of closing holes after only thought to influence our attackers. Military systems and nuclear attacks are persistent, in the last six years the Defense Department's America-site laboratory for nuclear and other sensitive parts of America, as well as sites civilian authorities in America have a strong influence has been so stated China for more than ten to twenty terabytes of information. NIPRNet a network of military and sensitive, but not classified as download is America.Almost more than a thousand as protected persons engaged in America are the specific skills that are effective in securing work in cyberspace. Cyber security task force includes those who identify themselves as cyber security professionals as well as those who build and operate systems and network do.

Having a good number of people on issues related to technical skills and the application of four strategic element for efficient human capital challenges in terms of security in cyberspace, will help to increase the security of these environments. Four strategic approaches include:

A) promote the development of detailed training programs to teach efficient manpower training centers, including our schools.
B) support the development and adoption of technical terms is very precise and professional certifications include practical components of the training and oversight are hard.
C) the process employs a combination of business process and educational resources in order to raise the level of technical competence of those who protect government systems or work with them.
D) ensuring there is a career path in order to maintain the high level of technical skill that went to other fields such as civil engineering or medicine.

Now the task of the Commission is focused on training the workforce in cyberspace, no longer with a low of security, like a white screen will start up with a target of topics and training of the workforce cybersecurity described we.Organizations and projects that can go forward in security and stronger than they are: the Ministry of homeland security, Certification Consortium Security of Information Systems International, information systems Association of

Audit and Control, Institute of Electrical and Electronics Engineers, Department of Justice, the Council of Chief Information Officer federal, office of personnel management, Ministry of Foreign Affairs.

Current efforts to recruit more work are done in the field of information security and Forensic. In the United States, these measures by NICE, the National Initiative for Cyber security Education that cyber security is an important component of labor force, is intercepted. Large non-issuance of Certificate Authorities also is heavily involved, such as: «CompTIA and ISC (2) that recently have introduced cloud security professional."

What is not clear, the adaptation of education to the needs and expectations in terms of content. Global Studies Task Force on Information Security ISC (2) in 2015 refers to good things, but we need to continue the investigation[7].

• Education

A computer system of four elements: hardware, operating system, applications and users, is formed. Hardware includes memory, input devices, output processor that has as main sources of information processing are used. Applications including compiler, database systems, business applications, games and a variety of other methods of enlisting hardware to achieve pre-defined targets to specify. Members', including humans, is a machine and other computers. Each of the users trying to solve their problems through the use of software-defined hardware has important applications in the environment. Operating system, how to use different hardware associated with applications that are written and performed by various users, control and guides.

In order to check security in a computer system should be explained to the position of each of the elements to be addressed in a computer system.In this regard, we plan to investigate the role of human factors in information security and the role of each of the elements we have described. If we have the best system hardware or operating system, but we serve the user or human factors involved in a computer system, to violate the security parameters, what of it wrong.

We must Forensic the issue of education in the information age not as a commodity or product, but as a process of looking at the security level of a product, whether hardware or software, and we do not fall. Each of the foregoing, the position of its own weight specified and should not be under the pretext of addressing information security weigh a parameter of what is considered and other parameters ignored or weight unacceptable to specify. However, a surprising emergence of new technologies in this era, threats will follow of its own. What should we do to make effective use of technologies and their direct or indirect threats yet remain immune? Certainly the role of human factors that direct users of these technologies are very sensible and important.

With the spread of the Internet and use it in different sizes, organizations and institutions with new issues related to information security and attacks on computer networks are facing. Regardless of the success or failure of the invaders and despite the latest reforms undertaken in relation to security technologies, the lack of information and knowledge (literacy of Public Safety) users Computer networks and the users sensitive information in an organization, always as important threats to national security and lack of commitment and edited the principles of security, creating potential could be used by attackers to cause a problem in the organization. Attackers are always looking for such opportunities to be achieved by relying on their own goals. In some cases we are wrong about the success of others provides. If we tried on the basis of a reasonable percentage of their errors as well as reduce the chances of attackers will be reduced[8].

• Level of knowledge

Undoubtedly, trained and certified experts are considered one of the most valuable resources in any organization. Should always trained experts in connection with security in an organization. Trial and error opportunities not possible in this area when an organization loses something much more than that to be achieved.Using a non-skilled expert in matters of network and information security in an organization, the security threat that will be added to other threats. (We cannot leave our people in the organization responsible for implementing security strategies that do not have the information and knowledge in this regard).

• Lack of awareness about the impact of a vulnerability on organizational performance

Many managers are of the opinion that "it will not happen to us" and accordingly look and attitude may lead to security. It is obvious that in case of problems in the organization, able to respond appropriately to the risks and possible threats there. This could be due to lack of familiarity with the impact of a security weakness in the organization. In this connection it is necessary to point out that always has no problems for others and we are also going to have a lot of problems. It is necessary to constantly and continually managers about the potential effects of a security weakness is justified and necessary knowledge to them. In the event of a security problem in the organization, there is no limit to your organization and can have negative effects in connection with the activities of the organization to be followed. Intense competition in the information age and the world, just moments organization should not be what it is, and this is enough to weed an organization working for several years and in some cases there will be no opportunity for that as well[9].

- Negative effects on other online business activities Organization
- Operating unhelpful and useless to distribute information in a business cycle
- Customers supply sensitive information to an attacker to compromise private information of customers
- seriously damage the reputation of the organization, followed by the loss of customers and business partners

III. THE AGGREGATE SAMPLE DESIGN AND DATA ANALYSIS IN ORGANIZATIONS TO SUSTAIN AND MAINTAIN PREPARATIONFORENSIC

3.1 Objectives

The project objectives can be stated as follows:

1.Create a database of criminal records in the country as complex

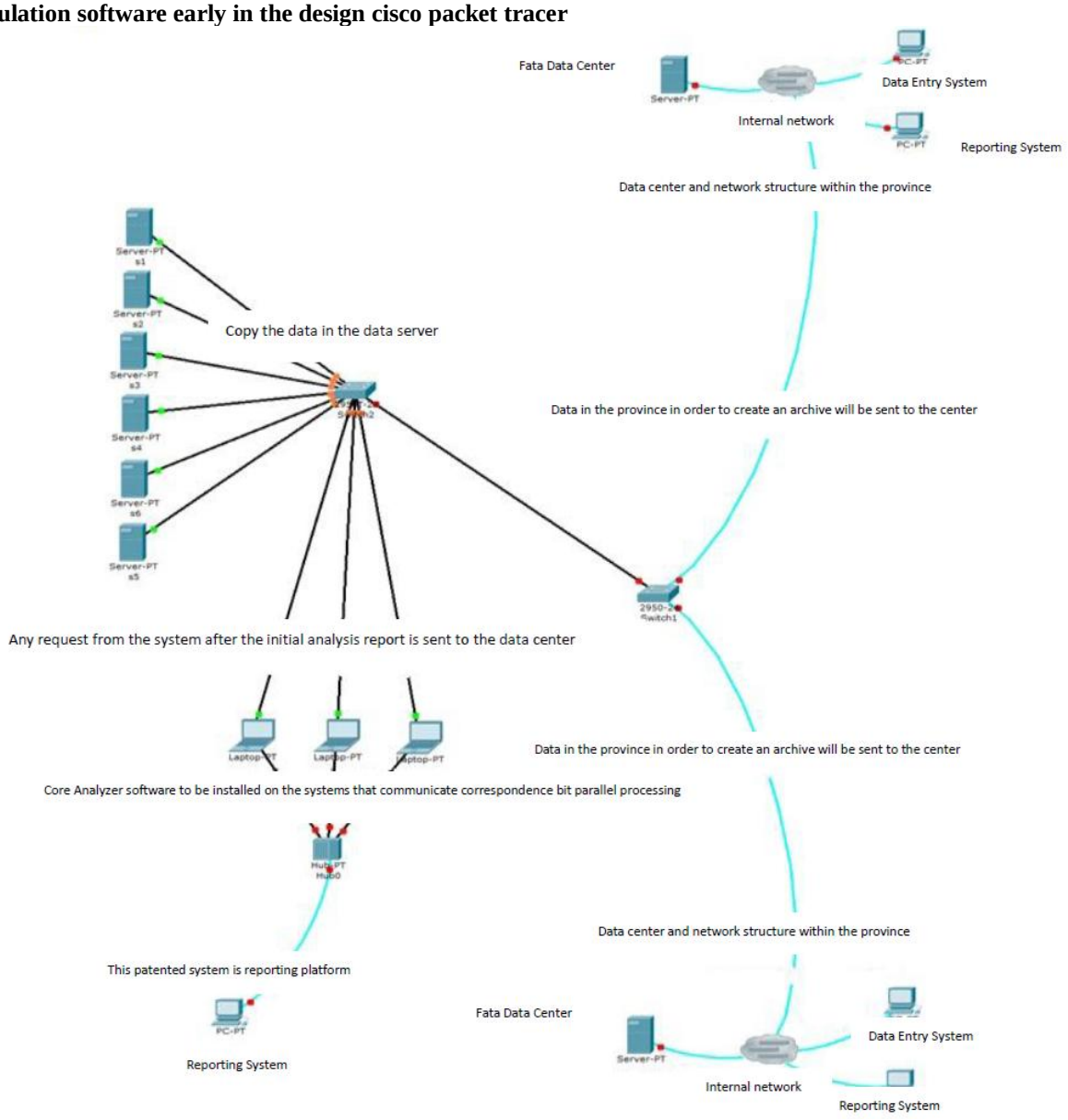
2.Data Analysis

3. qualitative and quantitative analysis
4.solutions for secondary cases
5.predict crime
6.identify offenders
7.grouping crime and criminals
8.identify areas of crime

3.2 Requirements

1- grid system
Network equipment, switches, ...
Security such as Firewall and ...
2-software systems
Software security
Database management system
Integration of information systems
3-systems and power distribution
4-storage systems
Storage
Instant Backup
Retrieval
5-physical systems
Physical access controls
Environmental monitoring systems

3.3 simulation software early in the design cisco packet tracer



The software implementation of the data related to crimes ranging from records and documents in the provincial capitals, provincial servers in the data is recorded. Then in the briefs and reliable documentation of legal data is sent to a central server at the center of the country. Resolve the impasse created when case file documentation associated with the data center to center sent for analysis. It is notable that before sending the data to the primary analysis in the province, according to the files is done in the province.

IV. CONCLUSION

Based on the results of further contacts long-term goals to prepare Forensic critical organizational knowledge and the need to plan for long-term goals organization to achieve preparationForensic in the organization. But unlike professional IT vision and meet the public to discuss preparations Forensic low is.

According to surveys, prioritizing the effective factors in Forensic prepared in advance Forensic goals is very important, and as much priority in the implementation structure and hierarchy should be considered. Substrate Preparation logical Forensic are designed and created. Substrate Preparation Forensic implementation, internal organizational structure also changed, on average, will this factor may also have problems accepting this important organization. The implementation of the organization's links with other organizations to nature will change. In view of the purpose of localization of equipment required in accordance with the principles Forensic will be a great impact on security and ease of Forensic bed.

REFERENCES

[1] AKBARZADEH, S., (KOOS), S., e-preparation.
[2] Bahrampour, Shabanali (1383), and social cohesion in the Information Society: glance at the situation in Iran, Iranian seminar ¬V information society.
[3] Hassanzadeh, Acta (1383), e-preparation criteria, research barriers and the situation in Iran, Computer Engineering Department, Sharif University of Technology.
[4] Rashidi, R. (2006), the status and role of information technology in the information society.
[5] Fathi, M. (1386), concepts, requirements and evaluation methods Forensicpreparation.
[6] Karvlvks, ZafarHeidari, F. (1383), model of e-preparation assessment industry.
[7] Available at: http://ebusiness.mit.edu/. GLOBAL e-PREPARATION – for WHAT? V.Maugis, S.Madnick, M.Siegel, N.Choucri, MIT, 2003.
[8] Available at: http://ecommerce.gov/apec/ (APEC Preparation Initiative: E-Commerce Preparation Assessment Guide). APEC-2000.
[9] Availableat: http://www,ecommerce.gov/apec/docs/preparation_guide _files/preparation_guide_5.pdf,2005

