CRIMSON PUBLISHERS
Wings to the Research

COJ Technical & Scientific Research

Research Article

Emerging E-Threats and Data Security Model for Organizations in Nepal

Gajendra Sharma[1]* and Ashok GM[2]

[1] *Department of Computer Science and Engineering,Kathmandu University, Nepal*

[2] *HimalayaCollege of EngineeringChysal, Nepal*

***Corresponding author:** Gajendra Sharma,Kathmandu University, School of Engineering, Department of Computer Science and Engineering, Dhulikhel, Kavre, Nepal

Submission: June 26, 2018; **Published:** July 09, 2018

Abstract

This research mainly focuses on identifying most emerging e-threats that have been evolved by the date and distinguishes the effects they produce within the infected organizations. The research is conducted to distinguish various factors that play roles in data security requirements and data security approaches. The research also focuses on the study of various security models adopted by various private commercial organizations and governmental organizations that operate on sensitive/critical information in Nepal. The study was conducted using survey questionnaire and direct interview as a method of data collection and mixed research method as a research paradigm. This analysis is based on defined conceptual framework and policies which describes and classifies the techniques and processes that has to undergo within an organization in order to secure data and application from threats in organizations. The study highlighted some of the areas which could be vulnerable to the organization's operations such as not having a proper information technology policy. The data security model suggested in this report recommends different phases and tasks that need to be performed in order to get increase the performance of the data security model as well as optimize the data security cost.

Keywords: Malicious software; Encryption;Authentication;Data protection technologies;Data classification;Malware;Data security models

Introduction

Organization is defined as a social unit of people that is structured and managed to meet a need or to pursue collective goals. All organizations have a management structure that determines relationships between the different activities and the members, and subdivides and assigns roles, responsibilities, and authority to carry out different tasks. Organizations are open systems-they affect and are affected by their environment [1]. There are a variety of legal types of organizations, including corporations, governments, non-governmental organizations, political organizations, international organizations, armed forces, charities, not-for-profit corporations, partnerships, cooperatives, and educational institutions. Organizations may operate on data that may be transactional (example: time, place, price, discount, payment methods, etc.), analytical (example: numerical values or measurements related to customer, product, account, location, and date/time) and master data [2]. Security relates to the protection of valuable assets against unavailability, loss, misuse, disclosure or damage. In this context, valuable assets are the information recorded on, processed by, stored in, shared by, transmitted from or retrieved from any medium. The information must be protected against harm from threats leading to different types of impacts, such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents, and intentional damage [3].

A threat, in the context of computer security, refers to anything that has the potential to cause serious harm to a computer system. A threat is something that may or may not happen, but has the potential to cause serious damage [4]. Threats can lead to attacks on computer systems, networks and more. NIST of United States of America defines threat as 'Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a information system vulnerability [5,6].

The main objective of this research was to analyze the emerging e-threats encountered within an organization and propose a data security model.

The specific objectives of the study are:

A. To study the major emerging e-threats encountering on organizations

B. To study the various technologies used as a preventive measures for data security by organizations of Nepal

C. To benchmark various data security models acquired by organizations and challenges faced by them in Nepal.

D. To propose the data security model for the organizations in Nepal to normalize data loss risk due to e-threats and provide the data secured organization environment.

The following research question was formed I this study:

A. What are the major e-threats faced and what are the data security technologies used by organizations of Nepal?

B. What is the current data security models implemented in Nepal and which data security model can be implemented to make a data loss riskless environment in organizations?

Literature Review

In Elevating the Discussion on Security Management Grandison et al. [7] introduced the Data Centric Security Model (DCSM), which leverages the business value of data to determine and implement the appropriate level of overall IT security. Grandison et al. [7] examined the perspective of a C-level executive (i.e. CEO, CIO, CTO etc.) and highlighted the tasks important to them in security management process. The team also presented the conceptual details of DCSM and the process how the DCSM can be deployed. They have also presented the workflow of DCSM. The main two components of DCSM are the policy and the data pillars. The policy pillar starts by summarizing the business requirements and regulations that will be addressed by the security architecture. The goal is to identify the overall data governance that needs to be implemented. The data classification and the policy rules are encoded into data control rules (DCR).

On top of the data pillar is a role-based authentication component that identifies users and assigns roles to the users based on authentication policies provided by the policy pillar. To enable protection with only minimal changes to the applications, they have leveraged an application abstraction model that maps terminology between application-specific contexts to the corporate data governance rules. This enables the DCL to understand application context without requiring that this context is adapted to the security policies.

In cloud computing's effect on organization Rehan [8] has discussed about how the information of organizations can be secured using the cloud computing. And he has also concluded the drawbacks and benefits of adopting cloud computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing" [9]. According to Gartner [10], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. Yanpei et al. [11] believed that two aspects are to some degree new and essential to cloud: the complexities of multi-party trust considerations, and the ensuing need for mutual auditability. They also point out some new opportunities in cloud computing security.

Jensen presented the technical security issues in Cloud computing; however, these issues are more related with the problems of web services and web browser and not of Cloud Computing [11]. Governance domains are broad and tackle strategic and policy issues within Cloud Computing environment, whereas the operational domains address more tactical security concerns and implementation within the architecture vary [12]. The European Network and Information Security Agency (ENISA) also worked with the security issues in Cloud Computing and provided the most critical security risks while adopting Cloud Computing and which should be kept in mind before switching to Cloud Computing. They presented 35 risks which are involved with the security while adopting Cloud Computing [13].

Ted Holland, in the paper understanding IPS and IDS has defined the intrusion detection system, host-based intrusion detection system, and intrusion prevention system [14-16]. IPS and IDS are two of many resources that can be deployed to increase visibility and control within corporate computing environment. In the paper, it details the assets of the internet infrastructure (structured into eight types: hardware, software, information, human resources, protocols, services, interconnections, and infrastructure) and list the threats applicable to these Internet infrastructure assets. These results are structured into mind maps. The study then classifies Important Specific Threats of the Internet infrastructure-namely Routing threats, DNS threats, Denial of Service, and Generic threats-and links each threat with a list of assets exposed. Eugene [17] in his paper Securing Enterprise web applications at the source: an application security perspective has discussed variety of application level threats facing enterprise web applications and how those can be mitigated to promote security. The main objective here in this paper is to itemize the most emerging e-threats by the date as well as to figure out the data security models adopted by the organizations in Nepal. Along with this interviews and questionnaire were conducted to know the challenges faced by organization in using the data security models. Finally a data security model is proposed which can provide a data security environment in an organization so that they can be assured with the security of data.

Emerging e-Threats causing data breaches

According to the Internet Security Threat Report (ISTR) 2015 published by Symantec corporation, Spam, phishing, and malware data is captured through a variety of sources including the Symantec Probe Network, a system of more than 5 million decoy accounts, Symantec cloud, and several other Symantec security technologies. Over 8.4 billion email messages are processed each month and more than 1.8 billion web requests filtered each dayacross14 data centers. Symantec also gather phishing information through an extensive anti-fraud community of organizations, security vendors, and more than 50 million consumers.

According to McAfee Labs threat reports 2016, McAfee GTI received on average 47.5 billion queries per day. Every day more than 157 million attempts were made (via emails, browser searches, etc.) to entice their customers into connecting to risky URLs. Every day more than 353 million infected files were exposed to their customers' networks. Every day an additional 71 million potentially unwanted programs attempted installation or launch. Every day 55 million attempts were made by their customers to connect to risky IP addresses, or those addresses attempted to connect to customers' networks. Advanced computing and pattern-matching capabilities mean data is collected on even the most private citizens [18]. 2016 Dell Security Annual Threat Report details top four developing trends in cybercrime [19]. The threat report marks up the evolution of exploit kits to stay one step ahead of security systems, a continued surge in SSL/TLS encryption that is giving cybercriminals more opportunities to conceal malware from firewalls, the continued rise of Android malware and a marked increase in the number of malware attacks.

Risk ware programs are applications that may pose a security risk when used inappropriately, or by an attacker [20]. For example, key loggers are utilities that may be used by system administrators in the course of their authorized work, but may also be maliciously used to secretly monitor users. If end-users are aware of the threats, understand how their actions could be a contributing factor and have clear steps to follow if they see something suspicious, then the chances are that security will improve [21,22].

Normalization of targeted attacks

Advanced threats are more than a buzzword. Already, we have seen the likes of Stuxnet and Flame as widely recognized examples of carefully crafted attacks focused on specific goals in targeted organizations. While cyber-attacks previously employed a mass scale opportunistic strategy, advanced-threat hackers are well organized, working together as part of a professional team, taking a slow-and-low approach to work their way into specific target companies [23].

Malware effects and anti-malware technology

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency [20]. Malware leverages a range of techniques used to get around sandbox technology. Using these evasive techniques, they have bypassed both effective firewalls and gateways, and they can also evade discovery by Sandboxes. According to Lakhani, there are four fundamental evasion techniques used by malware. Another technique used is the diagnosing of the sandbox. "This is an ingenious technique whereby the malware scans a system and virtual machines characteristics to identify the sandbox environment" [24]. Additionally, malware programs look for human interaction within the system before executing. "Checking for human pulse is a technique that identifies the users of the system as one of the frailest links in the chain of security using sandboxes in malware detection" [24].

Stalling code

Stalling code-this is the same method seen from previous authors whereby malware delays their execution so that the sandbox times out. A sandbox injects hooks into a program to get notifications for routine calls. The hooks introduce vulnerability in that the program needs alteration, a weakness that can be detected by the malware or that tampers with unpacking or dynamic code generation. The sandbox will then fail to identify any instruction that the malware executes due to the hooks [25].

Data security models and getting rid of e-threats

What happens at application layer?: Occupying the top-end of the stack, the Application Layer is the most open ended of all of the layers, and can be considered the catchall for any issues not addressed within the other six layers. Taking a more narrow view from a protocol perspective, user-oriented protocols such as naming(DNS, WINS), file-transfer (HTTP, FTP), messaging(SMTP,TOC/OSCAR[used by AIM]), and access (Telnet, RDP) all fall within the Application Layer in a more strict interpretation that views even higher level functions as outside the model completely. For the purposes of information security, the Application Layer can be considered the realm where user interaction is obtained and high-level functions operate above the network layer. These high level functions access the network from either a client or server perspective, with peer-based systems filling both functions simultaneously. The open-ended nature of the Application Layer may present threats. Some of the threats can be summarized as follows [26].

Application security maturity model (ASM): The Application Security Maturity (ASM) model helps organizations understand where they are in terms of their overall approach to software security. The model was developed by Security Innovation in 2007 from analyzing and plotting over ten years' worth of data about organizations and their security efforts, in particular their investment in tools, technology, people, and processes. By understanding and using the ASM model, organizations can uncover their current maturity level and then understand the most effective course of action to increase this level quickly and pragmatically while introducing as little disruption as possible to their current development process and in-production application management [13].

Threat model for web application: Threat modeling is an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.

Data security process model (DSPM): Zhao & Barroso [27] developed a security model that advocate for two levels in approaching security of data. This levels are; discovery and mitigation. The first phase results in the discovery of risks, allowing this output to be utilized for a mitigation strategy in the second phase. Each phase contains a list of tasks and deliverables.

Business model for information security: The Business Model [28] for Information Security began life as a model for systemic security management, created by Dr. Laree Kiely and Terry Benzel at the USC Marshall School of Business Institute for Critical Information Infrastructure Protection. In 2008 ISACA acquired from the university the rights to develop the model to help embed its concepts in information security practices globally.

Performing risk assessment

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The risk management guide for information system, provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help organizations to better manage IT-related mission risks.

Research Methodology

The aim of this chapter is to discuss about the general research methodologies used in this study and discuss the tools used in data collection and analysis.

Selection of the case

Considering the Authenticity, reliability, integrity, availability of the regular information and data, Financial Organizations of Nepal and telecommunication service providing company of Nepal are selected for the study, among them 23.8% were taken from banking institutions, 28.6% from Private commercial organizations, 19% from telecommunication service providing company of Nepal like NTC, NCELL and UTL, 14.3% from Academic Institutions and remaining from others. The malicious activities due to threats may cause loosing of organization's mission critical information/data in financial sector leading much loss in, monetary as well as reputation for their valuable customers and ultimately leads them to loss in company's revenue. Due to threats the software resources as well as personal data may get infected which may lead to high maintenance cost as well as high recovery cost [29].

Data collection method

For the data collection purpose several techniques like documentation of real facts about emerging e-threats and data loss due to them in the real worlds, archival records, interview, direct observations on many corporate organizations, participant-observation and physical artifacts based on the scenario were used during the research process. In this research work primary as well as secondary data collection techniques were used. The primary data are collected by the visiting the financial companies, inquiry with the employee of the company by preparing and distributing questionnaire whereas the secondary data used in this report are collected from the magazine, annual reports of the company, website, newspapers etc.

For this research, questionnaire, interviews, observations, documents, and reports have been extensively used as a form of data collection. Both closed and open ended questions were used in the questionnaire, and the interviews were performed in direct meeting of respective banks and telecommunication sector IT employees or communicating in email system. Along with this, security journals, and Information Security books are used in collecting the data. The entire questionnaires set that have been prepared during research are presented in Appendix I of this report.

Population

Nepalese financial sector consist of 265 institutes registered as financial institutes in the Rastra Bank of Nepal as of Mid-July 2012. Those 265 institutes contain 32 commercial banks, 88 development banks, 69 finance companies, 24 micro finances, 16 Saving & Credit Co-operatives and 36 NGOs. As per the feasibility study shows that most of the small scale 16 Saving & Credit Co-operatives and 36 NGOs are not heavily dependent on information technology. Therefore, it is decided to use only the registered commercial banks, development banks and some finances as the population of this research. According to Nepal Telecommunications Authority 2065 there are total 29 companies providing telecommunication services. Among them 22 are internet service providers, 2 are Cellular Mobile Service Providers, 2 are Fixed Telephone Service Providers, 3 are VSAT Network Service Providers. All these organizations dealing with telecommunication services use the customer's data extensively thus these are taken as population of this research. According to the Nepal academic institutions Directory, there are 63 academic institutions in Nepal. Each Institute works on the official as well as personnel data every day. So all these academic institutions are also taken as population of this research.

Data analysis

The research followed following steps: data coding, data reduction, data presentation, and conclusion drawing and verification for data analysis. The important and relevant data are discussed in empirical way. Microsoft Excel is used for data analysis purpose. Data coding and data reduction are done to draw Bar charts and Pie charts whenever required for analysis purpose. The inter-case comparisons are carried out as part of data analysis. Finally we draw conclusions and verified the findings. As a means of sampling different aspects of respondents views for different options in the questionnaire, we used weighted mean. A weighted mean is used when we want some data values in a set to factor more often into the calculation of the mean than others. In this case, we attach a numerical weight (w) to each value and calculate the mean as follows:

$$\bar{x} = \frac{\sum(x \cdot w)}{\sum w}$$

Survey as scientific method for research

A survey is a systematic method for studying behavior that cannot be observed or experimented on directly. This method is key in determining attitudes, opinions, needs, and preferences. A

How to cite this article: Gajendra S, Ashok G. Emerging E-Threats and Data Security Model for Organizations in Nepal . COJ Tech Sci Res. 1(1). COJTS.000502.2018.

survey is any activity that collects information in an organized and methodical manner about characteristics of interest from some or all units of a population using well-defined concepts, methods and procedures, and compiles such information into a useful summary form [30].

Interviews: An interviewer assists the respondent to complete the questionnaire. The interview is conducted in person, usually at the respondent's residence or place of work, although it can be conducted in a public place (e.g., airport, shopping centre). When paper-based, this method is called Paper and Pencil Interviewing, when computer-based it is called Computer-Assisted Personal Interviewing.

Self-enumeration: With self-enumeration, the respondent completes the questionnaire without the assistance of an interviewer. Compared with the task of managing interviews, self-enumeration is relatively easy to administer. It is also usually cheaper than interviewer-assisted methods, so larger samples can be selected. There are a variety of ways that the questionnaire can be delivered to and returned by the respondent: by post or facsimile, electronically (including the Internet) or by an enumerator. Questionnaires (structured and semi structured) are a written form of questions that can be mailed, e-mailed, or distributed to a group of people, employees or users. This method allows a researcher and respondents to come into contact with each other. Questionnaires that were used in this research contained short questions with predetermined choices of answer. In some causes an option of answer not included in the choices was given. Multiple choices and or continuum questions were used to increase the number of responses, as they were easiest and fastest for participants to respond to and to facilitate analysis.

Data Analysis and Presentation

Background information

The survey was taken within various organizations where huge amount of data were processed per day. The data include personnel data, customer sensitive data as well as crucial official data. The survey was conducted among 16 different organizations of various sectors which include 4 banks, 4 private commercial organizations, 2 telecommunication service provider company, 2 Academic Institutions and 4 multinational outsourcing companies working with various projects related to IT. The survey form was sent to 100 different respondents of various sectors and out of them 42 were the valid respondents. For the survey, peoples related with the knowledge of IT were prioritized first. Along with them some of the staffs who are working as a technical person in IT field were also taken into account. The respondents participated in the survey are seen experienced with the management and organization of IT related problems and operating application software like antivirus, firewall, VPNs and IDS/IPS technologies. The survey shows that 57.1 % had more than 5 years experiences and 42.9% had 1-5 years experiences in the related field.

Data classification

Data classification is the process of organizing data into categories for its most effective and efficient use. A well-planned data classification system makes essential data easy to find and retrieve. This can be of particular importance for risk management, legal discovery, and compliance. Written procedures and guidelines for data classification should define what categories and criteria the organization will use to classify data and specify the roles and responsibilities of employees within the organization regarding data stewardship. The survey shows that most of the organizations are aware of having criteria or policies to classify data. According to the respondents 81% of the organizations had policies for data classifications where as 9.5% were unware about data classification policies and rest 9.5 % had no any criteria or policies for data classification.

It was seen that most of the organization considered that data classification was highly relevant for the data security policy and data security aspect. Some of them agreed data classification should be carried for ease of use and access of data. As shown in Table 1 below was considered for highly relevant, 2 for relevant, 3 for relevant to some extent and 4 for not relevant.

Table 1: Factors relevant towards data classification in the organizations.

	Factors Relevant Towards Data Classification					
Factors	**Highly relevant**	**Relevant**	**Relevant to some extent**	**Not relevant**	**Total**	**Weighted mean**
Data Characteristics (age, owner, source, sensitivity)	12	24	6	0	42	1.86
Data Security policy requirement	36	6	0	0	42	1.14
Data Security requirement	36	6	0	0	42	1.14
Ease of use and access of data (performance)	16	20	6	0	42	1.76
Storage optimization	14	14	14	0	42	2

Data classification can have significant meaning with the day to day operations and achieving the goal of an organization. In the research conducted, with the weighted mean 1.14, data classifications were highly relevant for data security policy requirement as well as data security requirement. 85.7% of the respondents categorized that data classification was relevant to

How to cite this article: Gajendra S, Ashok G. Emerging E-Threats and Data Security Model for Organizations in Nepal . COJ Tech Sci Res. 1(1). COJTS.000502.2018.

data security policy and data security requirement. Similarly with weighted mean of 1.86 and 1.76, data characteristics and ease of use and access of data were the factors respectively were relevant.

In the research with the weighted mean of 1.3, the respondents answered that the data classification helps to improve data security implementation process. With the same mean the respondents also strongly agreed that the data classification helps optimize data security and performance. It means that 66.67% respondents support the statement that data classification would help in the field of data security. Data storage cost in an organization is an extra financial burden for it. Data classification can optimize the cost of data storage. In the research, 76.1% respondents agreed that data classification can help to optimize the data storage cost.

Sources of data in the organization: There are two main sources of data

A. Internal Sources: Internal sources of data are those which are obtained from the internal reports of an organization. For example annual report on total production, total profit and loss, total sales, loans, wages to employees, bonus and other facilities to employees etc.

B. External Sources: External sources refer to the information collected outside agencies.

Most of the organizations source of data is both external and internal. Only few of the organizations sources of data are internal. The survey shows that 76.2 % of the organizations sources of data are both external and internal and remaining 23.8% organization source of data are internal. From the above data in percentages, it can concluded that data classification process is an essential task or process to be conducted within an organization to the data security aspect as well as keeping data safe from e-threats.

Data security challenges and problems faced by the organization in current context

The objective of research is also to figure out the security challenges and problems faced by various organizations in Nepal. The research is conducted to find out the cause of the data breach or malicious functionality on data of organizations. The survey also tried to bench mark the various techniques used to mitigate or normalize the effects of e-threats on data which are the most valuable assets of any organization. The research sort to identify key e-threats that contribute immensely towards data security incidents in an organization, these factors are also considered as the main source of data security breaches or incidents of an organization. As discussed in section 2.3, there are various types of e-threats hovering over the data system of an organization and trying to get access through loop holes in the system so that they can intrude inside it with the theme of stealing or tempering the original data as a criminal intentions.

Frequently appearing e-threats: The survey was conducted to know type of network used by the organization as a means of communication. The questionnaire was composed of the options LAN, WAN, Wireless LAN and all of above. From the research it was found that 81% of the organization used all types of networks. It shows that organizations are always vulnerable to the threats attacking at application layer. The survey was conducted to figure out major causes of data breaches with the options as Malicious attacks via e-threats, negligence or mistakes by employee, system glitch and don't know. The data shows that 61.9% of the organization faces the data breach incidents often and 76.2% of the respondents feel that these data breach was caused due to malware attacks via e-threats. 71.4% of the respondents feel that the data breach also occurred due to the negligence or mistakes by employees working within the organization. Very few in number nearly 33.3% or the respondents did not experience any data breach incidents during their services days. Some of the commercial banks seem very conscious with the data security mechanism. Among these respondents 23.07% were working as IT experts in the banking institutions. The research shows that most of the organizations were victim of Malwares, Web threats and Targeted attacks. As shown in Figure 1 among various types of e-threats 81% were malware 38.1% were targeted attacks 33.3% were Web threats 14.3% were DDoS attack. Still there are other types of threats like adware, spywares, trackware which are less destructive but they may also cause a links to the phishing activities. The research showed that 33.3% were other threats.

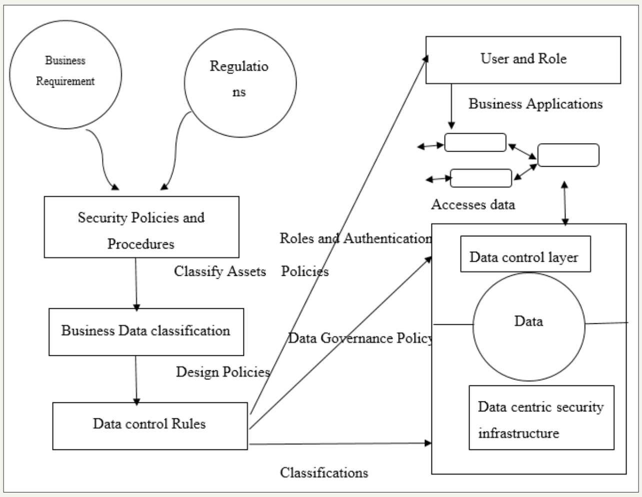


Figure 1: The components of DCSM [7].

Techniques used by organization in Nepal to normalize the effects of e-threats: As discussed in section 2.4, there are various technologies and techniques developed as a medicine to the e-threats. There are different techniques for different threat type. As shown in the Figure 2, Malware detecting sandbox invasion techniques were used at most with 52.4%. There are other techniques used in which 47.6% used content filtering, 42.9% used new adjacent technologies, 33.3% used data exfiltration techniques, 33.3% used Integrated prevention and response strategies, 28.6% used SIEM analysis (Security Investment and Event Management) techniques. Along with these techniques some of the organizations automate security through IT compliance controls.

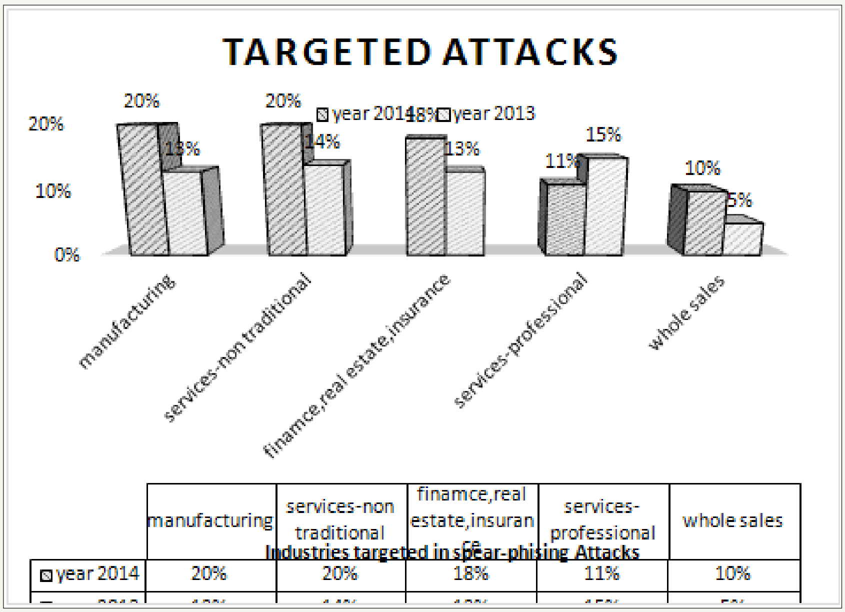


Figure 2: Phishing attacks [17].

Factors contributing the data breach incidents inside organization on Nepal: As survey data already discussed, in many organizations data breach incidents occurs often. From the Table 2 for weighted means 1 was assigned for strongly agreed, 2 for agreed,3 for agreed to some extent and 4 for disagreed, from the observation, the respondents strongly agreed that lack of clearly defined data security policy and its implementation mechanism is one of the major factor for data breach incidents. Another subject to concern is that employee related factors (e.g. Poor training) for which 38% respondents strongly agreed for reason on data breach within organization. Another factor to concern is that 61.9% respondents agreed that data breach occurred due to lack of management commitment and support towards data security. 47.6% respondents agreed that flaws within data security mechanism are also another cause of data breach incidents.

Table 2: Importance of data classification.

Fields	Importance of Data Classification					
	Strongly agreed	Agreed	Disagreed	Strongly disagreed	Total	Weighted mean
Data classification improves data security implementation process	28	14	0	0	42	1.33
Data classification helps optimize data storage costs	8	32	2	0	42	1.86
Data classification helps optimize data security and performance	28	14	0	0	42	1.33
Data classification helps improve data security management	24	18	6	0	48	1.63

Types of information under risk due to e-threats: The survey was conducted within organizations with a big variation on the type of data they operate on. The research had described some of the type of information in which the organization operates on and surveyed on which data might be prioritized first for vulnerability to the e-threats. As seen in the Table 2, each type of information was computed 1 as rank 1, 2 for rank 2, 3 for rank 3 and so on. After calculating the weighted mean it is shown with

How to cite this article: Gajendra S, Ashok G. Emerging E-Threats and Data Security Model for Organizations in Nepal . COJ Tech Sci Res. 1(1). COJTS.000502.2018.

weighted mean 1.8,thecustomer/consumer data are ranked first by many respondents. Employee data and data related to research/development were ranked second by most of the respondents with mean 2.7. If the frequencies of respondents for data about finance and accounting, sales/marketing, logistics/supply chain and legal and compliances were counted, they are also accounted in the list of risky data which resides within the organizations and ranked to the third rank with means 3.1, 3.4, 4, 3.6 respectively. This research can conclude that organizations who operate on customer data are at high risk to e-threats. As the country Nepal has organizations like banking, telecommunication service provider, Private commercial organizations like IME and software facilitating companies etc. are high risk to e-threats in comparison to academic institutions and governmental institutions like Nepal Electricity Authority (NEA).

Types of data handled by organizations: As discussed in section 4.4.4, the customer data were most vulnerable to the threats. The research was conducted to know which types of information were used by the organization at most during their day to day office hour. As shown in the Figure 3 employee data 66.7% and customer data 61.9% were handle at most. Customer data excluding credit card information were also handled at most rating second position with 42.9% as a survey result.

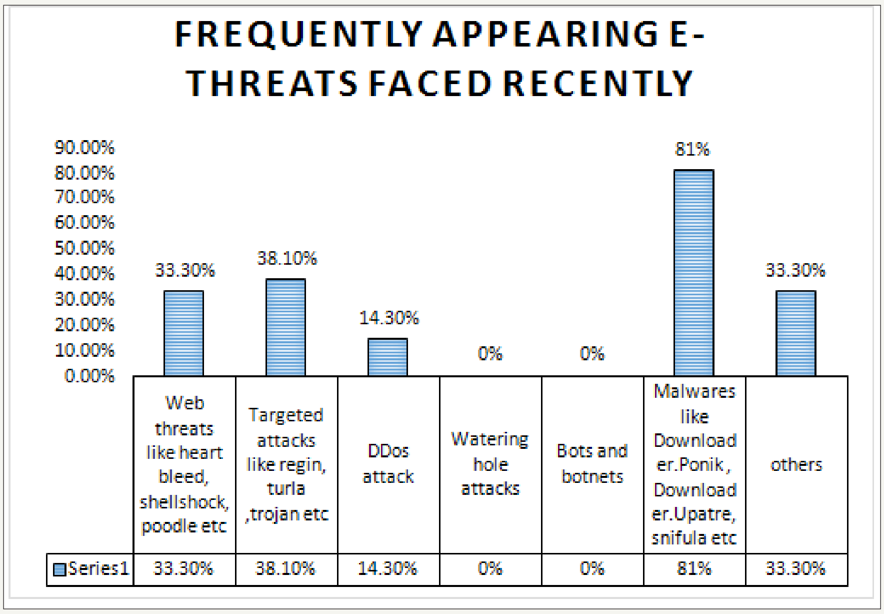


Figure 3: Frequently appearing e-threats in organizations of Nepal.

Data security requirements

In the research, most of the organizations were well equipped will the plan, policies and procedures for enhancing data security mechanism were found in the organization. According to respondents 76.2% were well known about the information risk management framework, policies and procedures. Only 23.8% of the organizations had not made or gone through the framework or procedures. Most of the organizations in Nepal use centralized data security management policies, procedures and guidelines. In the survey it was found that 75% organizations used centralized data security management guidelines, 18.8% used hybrid data security management guidelines and 6.3% used decentralized data security management procedures and guidelines.

The policies and procedures should be guided throughout the specified time frame otherwise it may mislead and hence the target cannot be met. For this purpose a dedicated staff or IT professional should be assigned the task. According to the respondents 90.5% of the organizations have hired a dedicated staff for this responsible task. The survey also found that in most of the organizations these policies were distributed among the employees so that they are aware about the security guidelines the organization is following through the time stamp. As shown in the Figure 3 85% organizations flows the security procedures and plans across the employees. Among them 55% respondents feel that the policies and guidelines provided are not fully adequate and they need to be revised with the time and trends. Because of the unrevised policies, the current data security guide lines might not fulfill the security requirements of the organization. 30% of the organizations have a fully adequate and up to date policies and guide lines which helped their organizations to have an extreme security towards data security.

Handling of sensitive information and audit of data/system/security aspects: It is risky to the data breach if sensitive information is moved to and fro, from one machine to other and while handling with portable devices like flash drives and hard drives. The survey shows that still 55% of the respondents are not sure whether their information within the organizations are fully secured of not. Among the respondents 40% respondents were very much sure about their data and information being handled are safe. As the result of survey it was found that 45% of the employees use removable devices for carrying data to work at home and office. 38.1% employees store their sensitive information in their laptops or removal devices. From this result the research can conclude that still the organizations are not risk free for their data tempered or stolen. Since data are stored in the laptops of removal devices they are always vulnerable to the e-threats like malwares and phishing. Millions of threats exist today. Hundreds of e-threats are developed per day. The existing data security mechanism may not meet the level to protect information from these newly emerged e-threats. Thus all aspects like data, software, systems must be audit in some time span. The survey was conducted on this aspect and found that 76.2% of the organization had gone with audit of data system or software. They had audit on different time span. The following Figure 4 shows the time period of audit performed. It shows that highest 52.9% organizations perform their system and data condition audit quarterly.

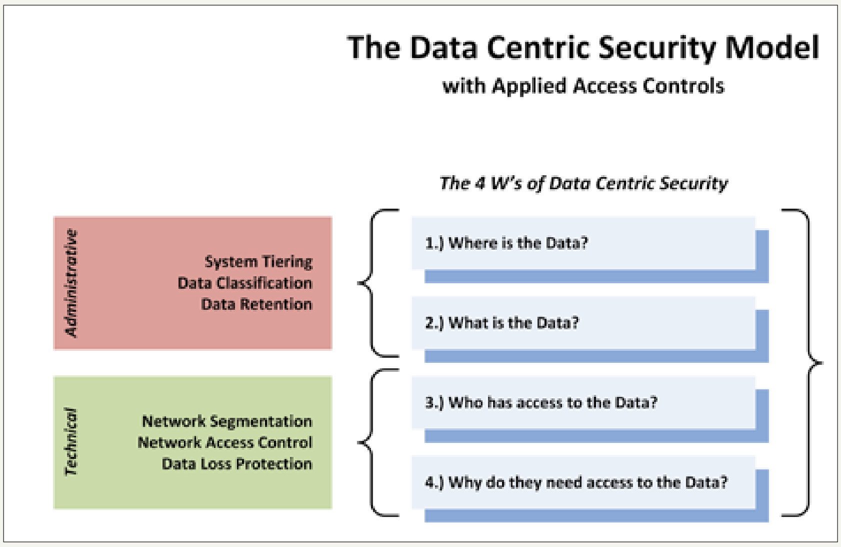


Figure 4: Data centric security model.

Information security activity within organizations: For the sake of data security requirement within organizations, different activities should be performed like providing security trainings and awareness, Defining mechanism for managing system logs, integrity, audit management OS, application and network device management, applying procedures and mechanism for contingency planning and recovery and disaster preparedness, applying system access controls authorization and authentication mechanisms etc. As shown in the Table 3, the survey was conducted with options those activities existed, not exist of not aware of. For the weighted mean, there exist was assigned 3, not exist was assigned 2 and not aware of was assigned 1.From the weighted mean calculated, the research found that all security activities exist in the data security system of the organization except that respondents were unware about third parties management policies. The research shows that 80.9% organizations had defined mechanism for managing system logs, integrity, audit management OS, application and network device management mechanisms.76% organizations were equipped with recovery and disaster preparedness mechanisms. 66.6% respondents say that the organization they are working with had proper data security trainings and awareness policies and there exist the system access controls authorization and authentication mechanisms. This shows that all the organizations carry out some of the data security activities.

Table 3: Factors contributing data breach incidents inside organization.

Factors	Factors Contributing Data Breach Incidents					
	Strongly agreed	Agreed	Agreed to some extent	Disagreed	Total	Weighted mean
Poor data classification	12	14	12	4	42	2.19
Employee related factors(eg. poor training)	16	14	12	0	42	1.9
Complexity of data security management tools and infrastructures	10	20	10	2	42	2.1
Lack of clearly defined data security policy and its implementation mechanism	24	16	0	2	42	1.52
Lack of management commitment and support towards data security	8	26	6	2	42	2.05
Flaws within data security mechanism	10	20	12	0	42	2.05

Data security approaches

The survey was conducted to know what the organizations used as a means of data security approach. All the respondents participated in the survey were very clear about the security approaches. The Figure 3 shows that 61.9% respondents have stated that data approach in their organization is guided technical

How to cite this article: Gajendra S, Ashok G. Emerging E-Threats and Data Security Model for Organizations in Nepal . COJ Tech Sci Res. 1(1). COJTS.000502.2018.

skills available in the organization. 57.1% stated that data security approach was guided by risk analysis and same number of respondents responded as data security approach was based on value of data to be protected. Data classification factor also plays a vital role on guiding the data security approach since 52.4% respondents were in a side with this statement. Specific data security requirements like availability, integrity and confidentiality are also the factors to guide the data security approach within an organization. The research shows that few organizations only exist where their data security approach is guided by the budget allotted for it. There were 33.3% to be on side with this statement.

Information protection technologies used within organizations of Nepal: There are various technologies developed and used till the current date in order to protect the data and information from malicious attacks or hackers. In this context, the survey was conducted to know the present scenario of technologies used by the organizations of Nepal in order to protect the information from the intruder. As shown in the Figure 3 85.7% organizations used antivirus and 81% used firewalls to protect the information from malicious attacks intended for stealing of corrupting the critical information. Apart of antivirus and firewall, secure VPNs were used by 51.7% and Intrusion detection system/Intrusion prevention system (IDS/IPS) were used by 33.3 % of the organizations. Only few in count nearly 10% organizations were equipped with network data loss prevention software. The research shows that at least all type of organizations used some type of technologies in order to keep their mission critical information. Besides the technologies accounted in above research, there are also some other methods through which organizations can protect the sensitive information. These include using access controls, encryption of data or file, backup or recovery, trainings to users etc. Among the respondents, we had conducted the research about the criticality of different technologies used to protect data. As shown in the Table 4 weighted mean were considered 4 for very critical, 3 for critical, 2 for not very critical and 1 for not critical. As shown in Table 5 all the factors had a weighted mean above 3, which means that all the factors play a critical role on data security. IDS and firewall is the highest weighted mean with 3.7, which means that they are rated as the most important activity area for the data security purpose.71.4% respondents rated this as most important. User training factor has been calculated as second most very critical to the data security approach which is 52.38%. Antivirus software and access control mechanism are weighted 3.4 each which states that they are critical to the data security. Beside that Encryption and recovery/backups mechanism are also critical too.

Table 4: Priority of information types in risk due to e-threats.

	Which Type of Information is Risky								
Type of data	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5	Rank 6	Rank 7	Total	Weighted mean
customer/consumer	24	8	6	0	4	0	0	42	1.86
employee	8	16	8	2	6	2	0	42	2.71
research and development	6	16	6	4	2	8	0	42	3.1
sales and marketing	10	8	8	0	6	6	4	42	3.43
Finance and accounting	10	12	4	4	4	4	4	42	3.19
Logistics/supply chain	2	10	8	4	4	10	4	42	4.05
Legal and compliance	10	4	6	8	2	10	2	42	3.62

Table 5: Information security activities.

	Information Security Activity Exists in the System?				
Activity areas	There exist	Doesn't exist	Not aware of	Total	Weighted mean
A defined information systems change control and management system	26	14	2	42	2.57
Defined mechanism for managing system logs, integrity, audit management OS, application and network device management	34	8	0	42	2.81
Procedures and mechanism for contingency planning and recovery and disaster preparedness	32	8	0	42	2.71
Training and security awareness policy	28	12	2	42	2.62
System access controls authorization and authentication mechanisms	28	6	4	38	2.63
Third parties management policies	10	12	20	42	1.76

Factors contributing on data security approaches: Various factor play roles for configuring and managing data security of an organization. We had conducted a research to find the criticality of some factors that may contribute as a key to design and implement the data security mechanism within an organization. As shown in the Table 6 with the weighted mean rated 4 for very critical, 3 for critical, 2 for not very critical and 1 for not critical and rounding ups and down the decimal points, the research found that all factors included in the questionnaire were critical with weighted mean score 3. The result shows that 81% suggested that IT security staff preferences are one of the critical factor contributing the data security. 57% respondents suggested that number of reported data breaches contribute to the data security. This is true since by studying the type and characteristics of data breaches, we can renew the technological aspects of data security. Others factors like data security attributes, fund for security, recovery mechanism and overall organization business strategy contribute equally as a critical factor for data security with score 52% each.

Table 6: Factors criticality to data security.

	Is Security Activity Critical to Key as Data Security?					
Security activity area	**Very critical**	**Critical**	**Not very critical**	**not critical**	**Total**	**Weighted mean**
IDS and firewall	30	12	0	0	42	3.7
Access controls	16	22	2	0	40	3.4
Encryption	12	16	10	0	38	3.1
Antivirus	26	8	8	0	42	3.4
Recovery, redundancy and Backups	14	26	2	0	42	3.3
User trainings	22	18	2	0	42	3.5

Data security models and problems encountered within organization of Nepal

From the research it was found that 61.9% organizations had used some standard data security models where as 38.1% organization still had not followed them. Among them 66.6% of banking institutions and private commercial organizations have followed the guidelines provided by the data security models. Only 25% of the telecommunication service providing companies has used the data security models. We had conducted research with some of the popular standard data security models and the responses from the respondents. The Figure 3 describes that 23.1% of the organizations used Data centric security Model as well as same percentage of organizations used Business Model. Other models like Application Security maturity Model (ASM) and Data security Process models are also used accountably with score 15.4%. Apart of these models 15.4% of the organizations used other models which can meet their organizations data security need. In the case of banking institutions and private commercial organizations most popular data security models are Application Security maturity Model, Data centric security Model and Data security Process model.

Table 7: Factors and their criticality on data security approach.

	Criticality of Factors as a Key to Contribute Data Security Approach					
Factors	**Very critical**	**Critical**	**Not very critical**	**not critical**	**Total**	**Weighted mean**
Data security attributes	20	22	0	0	42	3
Available fund for security	14	22	6	0	42	3
IT security staff preferences	6	34	2	0	42	3
Number of Reported data breaches	10	24	8	0	42	3
Number of recovery mechanisms invoked	8	22	12	0	42	3
Data security goals	16	20	6	0	42	3
Overall organization business strategy	20	22	0	0	42	3

Using these data security models, in 52.6% organizations had a fully data secured environment. They hadn't observed any data tempering or data breaches but rest 47.4% organizations often observe some incidents of data tempering and data breaches. The survey was conducted to know the views of the IT security personnel's to know which of the data security models can meet the data security requirements of their organizations allowing some standard data security models and the responses from the respondents are shown in the Table 7 & 8. For calculation of weighted mean, 4 for strongly agreed, 3 for agreed, 2 for agreed to some extent and 1 for disagreed was assigned. Respondents with weighted mean score 4, strongly agreed that data centric security Model as well as Business Model can meet their organizations data security requirement. With weighted mean score 3, the respondents agreed that application security maturity model, threat model and Data security process model also can meet their data security requirement. 79% of the respondents argued that organization's data security need, can be fulfilled by business model and 68.5% of the respondents argued that data centric security model is the best.

Table 8: Data security models to prevent data form emerging e-threats.

	Which Data Security Models can Prevent from E-Threats					
Types	**Strongly agreed**	**Agreed**	**Agreed to some extent**	**Disagreed**	**Total**	**Weighted mean**
Application Security Maturity Model (ASM)	16	18	4	0	38	3
Threat Model	6	28	4	0	38	3
Data Centric Security Model (DCSM)	26	12	2	0	40	4
Data Security Process Model(D-SPM)	18	18	2	0	38	3
Business Model	30	8	0	0	38	4

Problems faced within organizations due to e-threat (Respondent's view): The survey was conducted to diagnose the problems faced due to e-threats on the organizations data or information apart of using the data security technologies and here we have listed some:

A. unwanted email spreading

B. Content misleading towards the attackers.

C. Lack of awareness about data security in clients and lack of policies for data

D. We are receiving continuous threat emails to violate the organizational secure information/ datum.

E. adware and continuous emails occurring

All the above problems are faced within the organizations that are using some of the standard data security models. It means that still the data security models consist some flaws within them of some of the factors are still missing which play a vital role in data security approach. The survey was conducted to collect the respondents view on some task that must be followed as an implementation of data security model to meet the organizations data security requirement. The tasks were categorized on three types:

1) Type I

Tasks:

A. Make strategy, policies and perform risk analysis.

B. Renew technologies

2) Type II

Tasks:

A. identify threats

B. choose appropriate application programs

3) Type III

Tasks:

A. Discovery of risk

B. Apply mitigation techniques (e.g. Refine Access control, Audit systems and applications, developing training plan etc.)

C. Choose appropriate application programs

The research data shows that 60% respondents choose type I and 40% respondents choose type III. None of them were on a side to the Type II category. In my opinion, all the respondents felt that making strategy, policies and performing risk analysis can identify the threats or close the door to enter inside the system for the threats. So none of the respondents were on a side to the type II category.

Data security and cost aspects

In the context of this research it was important for the researcher to consider various approaches to security with focus on cost implementation efficiency and effectiveness. In the data security models discussed in chapter 2.5, cost aspect of security was not thoroughly addressed. This research therefore deliberately sort to understand whether organizations have budget for security and how much is allotted in various data security activity areas. The research shows that 81% of the organization allocates the budget for the data security aspect. The allotment of the budget varies from organization to organization. The Figure 4 shows the current situations on allotment of budget for data security out of IT budget.

The Figure 3 shows that most of the organizations 41.2%% allocate 10% to 20% of total IT budget. 29.4% of the organizations allocate less than 10% of IT budget. Few in numbers, 11.8% of the organizations allocate 20% to 30 % of IT budget for data security approach. The survey was conducted on respondents view to know the range of budget in data security to meet the current data security requirement. The following Figure 4 shows the respondents view on expected budget on IT data security. The research shows that 47.7% of the respondents felt that 30% to 50% of the IT budget should be allotted for IT data security to meet the current need.14.3% respondents state that data security budget should be greater than 50% of IT budget.

Consideration of factors on total budget allocated for information security: As the research shows that almost all of the organizations are allocated with the IT budget. There may be the case in which IT security staff couldn't consider the factors that are very important for the expenditure of the data security budget. This may also can decrease in the efficiency of data security approach. The research was conducted on the importance of factors for consideration on total budget allocated to information security. For the weighted mean, 4 for highly important, 3 for Important, 2 for Not very important and 1 for Not important at all were assigned. The respondents result shows that with weighted mean score 4, risk analysis is highly important that should be considered for total budget allocation. The Table 9 shows the responses. Similarly security solution cost is also highly important for the allocation of budget for information security. Other factors like security incident report, benchmarking a comparing with best practice are important factors that should be considered on budget allocation for data security.

Table 9: Consideration of factors on total budget allocated for information security.

	Factors on Total Budget Allocation for Information Security					
Factors	Highly important	Important	Not very important	Not important at all	Total	Weighted mean
Security solution cost	24	16	2	0	42	4
Number of security incident reported in the past	16	22	2	0	40	3
Data security needs identified from risk analysis	28	14	0	0	42	4
Need to benchmark and compare with best practices	22	16	4	0	42	3
Available funds for investment	10	30	2	0	42	3
Others	0	14	2	0	16	3

Data security model for organization of Nepal

Some of the popular and standard data security models were discussed earlier which are being implemented in the enterprises or organizations throughout different countries over the world. Among the discussed standard data security models, only some of them are into practice within some of the organizations of Nepal. In the survey conducted, 38.1% of the organizations have not used any data security models and 100% respondents felt that data security model must be deployed for the sake of data security within the organization. To meet the current data security issues within organizations, some of the task or step by step procedures must be followed. As research was conducted on different task that should be followed by the organizations to meet their data security requirements, 60% respondents were with the option i) Make strategy, policies and perform risk analysis. ii) Renew technologies and 40% were with the option i) Discovery of risk. ii) Apply mitigation techniques (e.g. Refine Access control, Audit systems and applications, developing training plan etc.). iii) Choose appropriate application program. It shows that making strategy, policies about data security aspect is very essential. Another key task is to perform risk assessment which gives the information about various threats, vulnerabilities, control analysis, impact analysis etc., their activities to be performed, and their methods along with their outputs. Another essential part is to choose appropriate application programs or renewing them in order to meet the current security requirement.

As discussed in section 2.5.7 with various data security models in practice, all the above discussed task or objective related to the data security aspect can be highly met if the rules and activities stated in Data Centric Security Model and Business Models were followed. The survey was conducted to know the present scenario on data security models and effectiveness of those models, with weighted mean score 4 each, respondents have opinion that the data centric security model as well as business model can meet the data challenges faced within their organization and make the mission critical information safe against recent emerging e-threats. A deep study with these two models was performed and found Business Model to be more effective in the aspect of cost and performance compared to data centric model in contrast to organizations of Nepal.

Optimizing cost of data security model

As discussed in section 4.8, 81% of the organizations allocate budget for data security aspect in which most of the organizations 29.4% allocate 10% to 20% of total IT budget. 23.5% of the organizations allocate less than 10% of IT budget. Few in numbers, 11.8% of the organizations allocate 20% to 30 % of IT budget for data security approach. It shows that the organizations are not serious or keen to increase or allocate big percentage in data security aspect. This is why optimization on cost of data security Model was needed. As discussed in section 2.6, while implementing data security model for a given control or security activity and security requirement we minimize security cost and maximize security level of a given data by selecting the security activity that is necessary for a given data security requirements.

Improving performance of data security model

The performance is the key factor to judge the success and effective implementation of the data security model. To improve the performance of Business model, the data classification and risk assessment task need to be included as a critical process that need to be performed in model implementation. Data classification as discussed in section 2.7 helps to categorize the data according to confidentiality, integrity and availability and find the levels for potential threats as low, moderate and high. Figure 4 summarizes on data security model of this study. A risk assessment as discussed in section 2.8 report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. A risk assessment report should be presented as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses.

Limitation of the study

A. Survey on all type of organizations could not be taken into account as research area. The research area is mainly confined to certain commercial banks, development banks, multinational software developing companies, Telecommunication service providing companies, some academic institutions and some regulatory bodies of Nepal.

B. The findings are based entirely upon the research conducted on some of the financial organizations, some telecommunication service providing companies and private commercial organizations of Nepal and hence may not be applicable to other countries of the world on counts of technological diversity and contextual forces.

C. The research may not be able to provide the exact financial figures or the financial impact due to the occurrence of the Information Security Threats and the Risk that is followed because of the reputation risk involved in it. The respondents might not provide complete and authentic information regarding the questions posed for the survey.

Summary of research data analysis

The research data analysis and presentation can be summarized as below:

A. 57.1 % respondents had more than 5 years experiences and 42.9% had 1-5 years experiences in the related field within the organization.

B. 76.2 % of the organizations sources of data are both external and internal and remaining 23.8% organization source of data are internal.

C. 76.2% of the respondents feel that data breach was caused due to malware attacks via e-threats. 71.4% of the respondents feel that the data breach also occurred due to the negligence or mistakes by employees working within the organization.

D. 81% of the e-threats were malware 38.1% were targeted attacks 33.3% were Web threats 14.3% were DDoS attack.

E. 80.9% organizations had defined mechanism for managing system logs, integrity, audit management OS, application and network device management mechanisms.76% organizations were equipped with recovery and disaster preparedness mechanisms. 66.6% respondents say that the organization they are working with had proper data security trainings and awareness policies and there exist the system access controls authorization and authentication mechanisms.

F. 85.7% organizations used antivirus and 81% used firewalls to protect the information. VPNs were used by 51.7% and Intrusion detection system/Intrusion prevention system (IDS/IPS) were used by 33.3 % of the organizations. Only few in count nearly 10% organizations were equipped with network data loss prevention software.

G. 61.9% organizations had used some standard data security models whereas 38.1% organization still had not.

H. 23.1% of the organizations used Data centric security Model as well as Business Model. Application Security maturity Model(ASM) and Data security Process models are also used accountabliy with score 15.4%. Other models used by 15.4% of the organizations.

I. 47.4% organizations often observe some incidents of data tempering and data breaches even after implementing data security models.

J. 60% respondents were with the option i) Make strategy, policies and perform risk analysis ii) Renew technologies as the tasks that the security models should include.

K. 79% of the respondents argued that organization's data security need can be fulfilled by business model.

Contribution of the research

The sectors to which this research can contribute can be broadly categorized as below

A. Practical contributions: This research study can be practically applied to the commercial organizations where huge amount of data are processed day to day which include the critical information about the customers of employees working within the organization. A part from the commercial organizations, the government sectors which handles the mission critical information can also be benefited from this study work to implement the data security model to make their organization with a threat free environment.

B. Theoretical contributions: The research has identified the various causes of data breaches, factors contributing on data security approaches, problems faced within organizations, task to be performed to fulfill the organization data security aspects etc. This may be a good theoretical basis for those who want to have a theoretical knowledge about data security aspects within organization of Nepal. The study also has discussed various types of e-threats, their activities, the data security models widely used by the organizations over the world and the status about the data security models deployed within organizations, thus it can provide the theoretical information to those who are keen about these subjects.

C. Research contributions: This study can be the beneficial to those researchers who are conducting their study on the field of data security of mission critical information. It can also help to those researchers who are studying about data security aspects within different layers of OSI reference models as well as data security aspects within cloud.

D. Managerial Contribution: The management committee of any organization is keen to get high profit with less amount of investment. Unknowingly the management are investing a huge amount in data security without knowing the priority of data they are using. They may be unnecessarily using the technology beyond the need. Thus this study might be beneficial to them to select proper technology reducing the amount of investment and increasing the reliability of the data security system.

Conclusion and Recommendation

Conclusion

The goal of this study was to figure out the emerging e-threats that are repeatedly attacking the critical data and information rested within organizations and found that Malwares, Web threats and Targeted attacks are the most frequently appearing e-threats. Some of the organizations of Nepal are in practice with the technologies like antivirus, firewalls, malware detection techniques, authentication, access controls, and encryptions technologies as e-threat mitigating techniques. The organizations of Nepal were found that different organizations are in practice with different security models in each. Data security models like Application maturity model, threat model, data centric model, data security process model and business models are used in common. Finally the objective of the study was to propose a data security model in the context of Nepal and the research concluded that Business Model is an appropriate data security model for organizations of Nepal.

Recommendation

The study shows that some of the organizations of Nepal still have not implemented any data security models. The organizations that have used data security models have also not performed the complete processes that conforms the data security aspect of organizations. As this research proposes a *Business Model* as a data security model that best fits the organization of Nepal, still the following task are mandatory to achieve the best performance and optimize security cost budget.

Tasks:

A. Sense the organization goal and design strategy, plan and policies to meet the goal and data security requirement.

B. Perform data classification for internal and external form of data

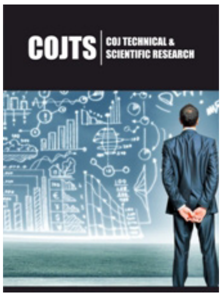
C. Perform risk assessment

D. Audit the information system, state of technologies, plan and policies, operating system, security controls, recovery plans, equipment

Conduct awareness program and trainings to the human resources entangled with data security system. Renew and adopt technologies that can fulfill the data security requirements of the organization.

References

1. Business Dictionary (2016) What is an organization?
2. Bi-insider (2011) Types of enterprise data.
3. Notis I (2009) The business perspective of information security. Centre of excellence for research and graduate education, Athens Information Technology, Greece.
4. (2016) What does threat mean.
5. Stoneburner G, Alice G, Alexis F (2002) Risk management guide for information technology systems. NIST Special Publication 800-30, USA.
6. Ateeq A (2016) Type of security threats and its prevention. Int J Computer Technology & Applications, Department of Computer Science, Northern Border University, Saudi Arabia, 3(2): 750-752.
7. Grandison T, Michael B, Luke C, Marcel G, Morton S, et al. (2007) Elevating the discussion on security management-the data centric paradigm. 2007 2nd IEEE/IFIP International Workshop on Business-Driven IT Management, Munich, Germany.
8. Rehan S (2011) Cloud computing's effect on enterprises: In terms of cost and security. School of Economics and Management, Lund University, Sweden, pp. 1-89.
9. Michael A, Armando F, Rean G, Anthony DJ (2009) Above the clouds: A Berkeley view of cloud computing. Technical Report. University of California at Berkeley, USA.
10. (2008) Gartner: Seven cloud-computing security risks. InfoWorld, USA.
11. Yanpei C, Vern P, Randy HK (2010) What's new about cloud computing security? Technical Report No. UCB/EECS-2010-5.
12. Jensen M, Schwenk JO, Gruschka N, Iacono LL (2009) On technical security issues in cloud computing. In IEEE International Conference on Cloud Computing (CLOUD-II 2009), Bangalore, India, pp. 109-116.
13. Cloud Security Alliance (2009) Security guidance for critical areas of focus in cloud computing.
14. Catteddu D, Hogben G (2009) Cloud computing: benefits, risks and recommendations for information security. Technical Report. European Network and Information Security Agency, Austria.
15. Ted Holland, SANS Institute (2004) Understanding IPS and IDS.
16. Cédric LB, Louis M, Rossella M (2015) Threat landscape and good practice guide for internet infrastructure.
17. Eugene L (2016) Securing enterprise web applications at the source: an application security perspective.
18. Internet Security Threat Report (2015) Symantec corporation USA.
19. McAfee Labs Threats Report (2016) Intel security.
20. Wenke L, Rotoloni B (2015) Emerging cyber threat report 2016. Georgia Tech Cyber Security Summit 2015.
21. Dell () Dell Security Annual Threat Report-2015. Dell Corporation.
22. Malware. Techterms
23. Threat categories. f-secure.com
24. Raghavendra K, Sumith N (2012) Application layer security issues and its solutions. Dept of CS & Engg 2(6): 1266-1269.
25. GFI White Paper (2001) Web-based security threats: how attacks have shifted and what to do about it.
26. Calhoun P (2015) A glimpse at the latest sandbox evasion techniques. Security Week.
27. Mimoso M (2015) Malware evasion techniques dissected at black hat. Threat post, USA.
28. Adams Ed (2010) Application security maturity model (ASM): A pragmatic approach to security your software applications. Security Innovation, USA.
29. Zhao X, O'Connor B, Barroso G (2006) Data security process model (DSPM).
30. ISACA (2009) An introduction to the business model for information security. Rolling Meadows, USA.


COJTS
COJ TECHNICAL & SCIENTIFIC RESEARCH