ETM
ENGINEERING & TECHNOLOGY MANAGEMENT

Identifying Information Security Vulnerabilities Using HDM

Course Title: **Engineering Management Synthesis**
Course Number: **ETM590**
Instructor: **Dr.Anderson**
Term: **Summer**
Year: **2013**
Author(s): **Chris Perrenoud**
Greg Wease
ThanapornNgarmnil
RachanidaKoosawangsri

ETM OFFICE USE ONLY

Report No.:
Type: Student Project
Note:

Table of Contents

1. Abstract

The innovation of IT technology has grown and become utilizes by many organization and business. Utilization of IT solution across industries increase an emergence of information security has international concerns as cyber-attack, system exploitation, and malicious hacking has grown in severity as a trend. This research discusses on identifying information security vulnerabilities through implementation of IT security practices extracted from multiple resource of literature review that is integrated into methodological approach of the Hierarchal Decision Model, a flexible decision-making tool. The focus of the discussion is center through the HDM that incorporates the participation of selected experts coming from technology and education sector. The expert weighting through pairwise comparison of weightings output a combine result of identifying potential vulnerabilities of information security in organization to indicate appropriate focus for strengthening information security.

2. Introduction

The emergence of information system revolutionizes business operation where intelligence, information, and data is become “oil of the millennium.” Information and data has become valuable assets as on the fundamental key for sustaining organizations, innovation, intellectual properties, and competitive advantage on the market. The trends of information and data have grown in values that introduces to the issues of cyber-attacks, corporate espionage, and compromised data from cyber intrusions.

To protect the valuable data of the company, information security framework has come into play in the sense of protecting organizations from hacking. In the present day, there are many hacking issues in most competitive businesses, for example, PlayStation Network Hack (Sony) that their clients’ information was stolen [1]. Another evident says thatintellectual property (IP) in the U.S. has been stolen from their best friend, namely China. The theft of American IP is increasingly high and the passive defenses are no longer effective. The article also reported that 80% of the valuable data, including merchandizing sector and government, is being attacked by Chinese Hacker [2]. WikiLeaks was also one of the cyber-attack victims. It became one of the worldwide concerns due to the national security that is mainly about the secretive data for example, nuclear-armed regime in North Korean, leader Muammar Gaddafi in Libya, and the British royal family [3]. The U.S. organizations are still valuable targets for hackers. Iranian hackers attacked into the computer system of U.S. international organizations to steal their database of energy companies [4].Cyber attackers also influence even the strongest data center, America's research universities. However, to effectively protect the university systems would be difficult to do so due to thousands of students and staff members logging in with their own computers [5].

Due to there are highly possibility for the company to get an attack from the hackers, many organization invest lots of money to protect their information. Research firm, Gartner, said that the security technology and services market across the globe is expected to reach USD 67.2 billion in the year 2013, up by around 8.7 percent as against the year 2012. "Increasing number of security threats such as mobile security, big data and advanced targeted attacks will propel the sector to witness strong constant growth." Gartner continues, "To support the growing need for security analytics, changes in information security people, technologies, integration methods and processes will be required, including security data warehousing and analytics capabilities, and an emerging role for security data analysts within leading-edge enterprise information security organizations," said Eric Ahlm, Research Director at Gartner. The highlight: The market is expected to reach $86bn in 2016 [6].

To that end, public, private and government based organizations must decide when and where to invest in security measures in order to protect their digital assets. The purpose of this paper is to help identify the areas of security vulnerability, and to open the discussion as to the next appropriate steps a given organization may take to ensure they maximize their risk-based return on investment [7].

3. Literature review

3.1 Information System Security

"Embedding Information Security into Organizations" suggests the five important findings in order to build the information security in organizations. The first is to protect intellectual property in the companies' environment by requiring a change in security thoughts from a technology to a behavior focus. The second is for security groups to be prepared for monitoring the information flow in business units because the needed levels of security is significantly high, demanded by customers and business alliances. The third is to integrate the security metric to the business and to communicate in uncomplicated terms that would lead to better decision-making process. The fourth is to invest in information security that is coordinated to the company's strategic goals. This would help business partners understand the important of the risk and the development of coordinated approaches. The last factor is the top-down communication on security matters that would help building a secure culture in the company and educating employees to clearly understand about the information security [8].Thus, investing money in Information Security is an essential activity that organizations should perform in order to protect their valuable information from intruders.

However, because there is a limited budget in IS issue, it is not easy for the people who are responsible to allocated the budget more efficiently. According to Arora [9], "Information security problems cost millions of dollars for US companies and billions for the overall US economy… the question is not whether organizations need more security, but how much to spend for added security."

With that said, IT management needs structured cost-benefit methods to evaluate IT security solutions, especially when precise security breaches are not clearly obvious.

There are many journal articles purpose methods for calculating, allocating, or selecting the effective way to spend the budget to improve and maintenance the IS system. For Example, Arora's paper [9] gives a first-hand look at estimating risk-based return on investment, and shows how a given company can calculate various security risks and how much it may cost in order to prevent such security intrusions. The author also suggests that in order to calculate what security systems to pursue and how much money to spend, the organization will need to look at two concepts: incident type – "refers to the various types of cyber security-related incidents…" and bypass rate – "the rate at which an attack results in observable damage."Once this has been documented, the next step is to calculate the net benefits and risk-based ROI.

Key formulas:

Incident Risk = Observed damage ÷ Net bypass rate. "This represents the damage that a company would have incurred from each incident type if no security solutions were in place.

Risk-based ROI = Baseline scenario – Residual risk – Cost ÷ Cost "the ratio between net benefit in implementing an IT solution and the implementation cost."

Baseline scenario is "the grand total of all incident risks to the organization if it had no security solutions in place."

Residual risk is "the expected value of damage with only one installed security system. Once the above has been estimated and calculated, the organization can evaluate which security solutions to pursue, and determine if a multi-tiered approach, with multiple security characteristics would achieve the greatest ROI. Armed with this information, the CIO or other IT management will have sufficient information to secure financing to effectively support and justify security expenditures.

Even though the organization can calculate how much they should spend in order to get highest return, they remain struggling in choosing an appropriate approach to control the problem of cyber-attacks. One approach was purpose by Bodin[10]. His research team used AHP or Analytical Hierarchy Process to help the organization making the decision in choosing the proposal that has the highest benefit to the company when investing money to improve their IT security. In their research, the chief information security officer (CISO) will evaluate the criteria which are Confidentiality, Data Integrity, and Availability which has Authentication, Non-Repudiation, and Accessibility as the sub-criteria. The score will be collected, and AHP software package will be used to calculate the weight for each criteria and sub-criteria. It is very effective tool to help the organization making the decision. However, it cannot guarantee that the answer from the model is the right decision for the real world problem that hackers and attackers continually improve their intrusion to be more sophisticated.

Due to the cyber intruders frequently change their method to attack the company's information, seeing the weakest point of the system under the adversary's eyes might help organizations create a more efficient system. Evans and their college [11] suggest the Morda or Mission-Oriented Risk and Design Analysis methodology to help organization to investigate the risk that which attack objectives; Confidentiality, Integrity, and Availability, has the highest possibility that might get attack from the intruders, so the security system engineer can develop the stronger system to straighten the weak point.

As mention earlier that company's information is very valuable, so the organization should find the weak point in their Information Security system. One of the studiestries to fulfill this awareness by measuring the Information Security level to prevent their information from hackers. Alshboul [12] states that “Determining the exact requirements for security for a given organization is essential for implementing the proper security measures.” According to the annual CSI conducted by the FBI, the average financial loss due to security breaches is estimated at $288K per responder (144 responders out of 522 invited to share financial data). The estimated financial impact within the US economy is estimated at $117.5 billion. In order for an organization to ensure security requirements are well defined, they must be able to evaluate current security demands as well as the measures taken to achieve such requirements.

Vulnerability is defined as the weakness of information systems, which can lead to an attack. Attacks defined as [13]: Destruction (hardware or software is destroyed), Disclosure (unauthorized users obtain access to information and disclose the confidential info), Modification (unauthorized users change information), Interruption (the computer network becomes unavailable for access), and Interception (unauthorized users copy information that resides in a computer system or while data is in transmission mode)

Because there are many ways for intruding security system of the company, identifying the gap between the current level of IS and the capability of the hackers in order to optimizing costs and reducing the possibility from getting attack from outsiders. The surveys were conducted to gathering information of IS level and getting confidentiality, integrity, and availability to find the relation between these two measures [13].The result is illustrated in Table 1.

Table 1 Responses of current information security level within given industry. [13]

Industry	Low	Moderate	High	Total
Banking	0%	62.5%	37.5%	100.0%
Education	16.7%	66.7%	16.7%	100.0%
Information Technology	0%	50.0%	50.0%	100.0%
Medical	0%	25.0%	75.0%	100.0%
Retail	14.3%	42.9%	42.9%	100.0%
Transportation	0%	100.0%	0%	100.0%
Telecommunication	0%	58.3%	41.7%	100.0%

The result, defining information security levels, enables organizations to implement proper security measures. Implementing security measures helps organizations to decrease possible damage and loss due to security attacks.

According to Goodhue's[14], a given computer user's concern about information security is a function of three different constructs: industry risk (the potential for abuse in a given industry), company actions (specific actions that a company has taken to maintain security), and individual awareness (computer literacy, managerial role, etc.).

Overall awareness of information security (sufficient or insufficient) is based on the following: "without a major loss due to lax security, it may be that security concern will generally be quite low… it takes a major loss from computer abuse to initiate or reinforce the security administration function [14]." As such, "Top executives, therefore, may continue to be reluctant to grant status and commit resources to thecomputer security function [14]."

Information Security has been a subject of concern dating back to pre-internet days. The paper demonstrates that "insufficient computer and data security is a major problem in many organizations and that low levels of concern contribute to the danger." The paper also shows a link between security concern of a given organization, a security lapse, and the protective measures taken to protect against potential risk. Managers should be more concerned when the risk of a security incident is greater, and they should be less concerned when they know their company is taking stronger action to protect them.

3.2 Hierarchical Decision Model

There are many methods for selecting or evaluating alternatives. One of them is AHP or Analytic Hierarchy Process. It was developed by Thomas Saatyusing the eigenvector method to help decision makers to make a decision in a complex problem [15]. However, HDM or Hierarchical Decision Model is another tool that also helps in the decision-making process by using the constant sum method, such that the lowest level will be alternatives of the model. This methodology was created by Cleland and Kocaoglu in 1981 [16].

The basic idea behind the HDM is MOGSA Decision Hierarchy; Mission, Objectives, Goals, Strategies, and Actions that the bottom level will support the higher level such as goals and objectives and then transform to the mission of the organization. In hierarchical methodology, the number of levels and elements can be very simple such as two or three to very complex layers, because there is no limit in the number of levels. However, the typical ideas are separated into three major levels; Impact Level, Target Level, and Operational Level as illustrate inFigure 1 [17].

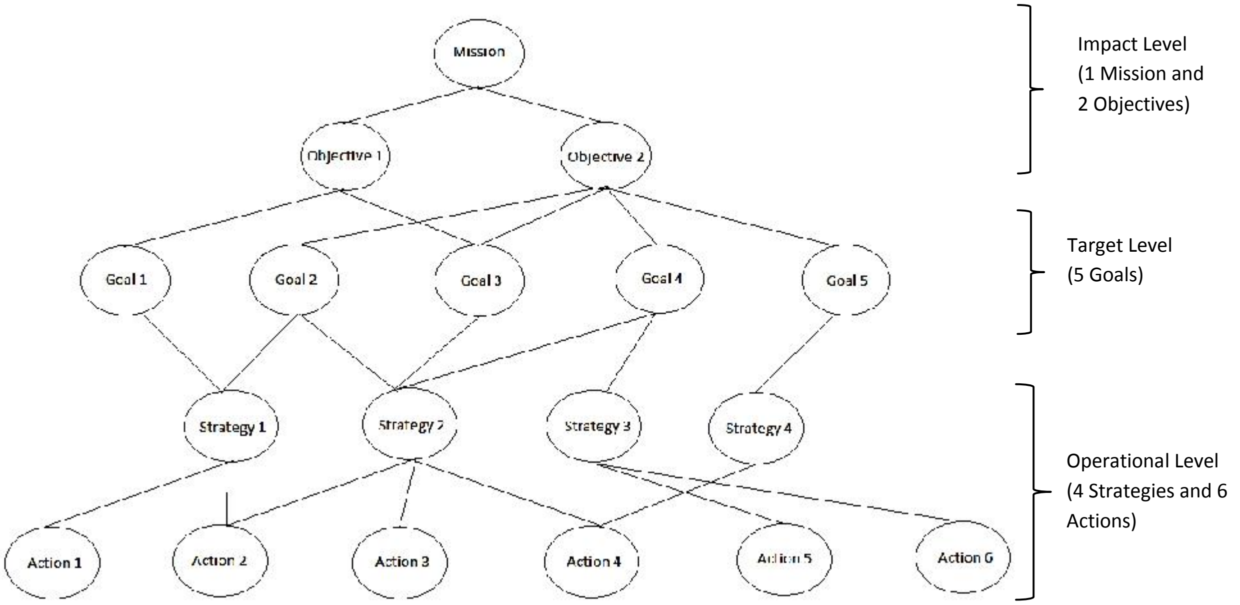


Figure 1 MOGSA Decision Hierarchy with three major levels

Each level of the model can consist of multiple criteria that the bottom level will affect the top level. To obtain one objective might require multiple goals. Likewise, one action can contribute to multi-strategies. Nevertheless, the elements must be preferentially independent, mutually exclusive and collectively exhaustive to avoid the conflict between elements. [18]

Pairwise Comparison is an idea that has been used behind the Hierarchical Decision Model. It is the idea of using the expert judgment estimation technique. The expert will be asked to compare two elements and then distributes the score of 100 between each of the two elements, based up the experts' opinion. The score will be present in relative value of two elements with respect to each other. For example, if one element is seemed to be more important than the other, the score allocation can be 75 and 25, 90 and 10, or 55 and 45. [19] Previously, after the results from the expert are made, the researchers will use the PCM software, the PC based, to normalize the value and obtain the relative degree of importance in each element. However, after the development of the web based tool, the expert can distribute their value directly to the model and see the relationship between the elements easier.

4. Research Methodology

4.1 Research Design

Defining the Problem

In order to identify which penetration points may be the most vulnerable, as well as which path may be the best to secure a company's proprietary data, we decided on a two-pronged research approach to help answer that question. First, utilizing an HDM to help identify the potential areas of weakness. And second, using an in-depth and diverse Literature Review (journals, papers, articles and books) to help cross-validateresults gleaned from the HDM.

Selecting Research Tools

Hierarchical Decision Making (HDM) was selected as a means to simplify and quantify potential information security breach points, and at the same time, enable the expert panel to fully grasp the intent behind the research. Secondly, and equally important, Literature Review was utilized to help architect the HDM node inputs, as well as cross-reference expert opinion on any given node comparison.

Please note, the HDM in its final form contained four unique levels, not five as exhibited in the MOGSA example. It is our intention with our HDM model to consolidate levels four and five into one comprehensive "Operational" layer, thereby giving clear insight as to where a given organization or institution may direct future security research as it pertains to security technology and services.

Selecting the Experts

Of the various industries whereby security breaches can have a financially devastating impact (Banking, Education, IT, Medical, Retail, Transportation and Telecommunications), we decided to focus our research resources in two Industries – Education and Information Technology. Of these two industries, we identified the following organizations to be representative of their respective industry:

Education: Portland State University

- CIO of Office of Information Technology (OIT)
- OIT Helpdesk
- Assistant Dean of Business Administration

Technology: IBM and Tektronix

- Business Manager – Power System
- Software Engineering
- Helpdesk Service

Building and Verifying the HDM: Utilizing the MOGSA Framework as a starting point helped define the HDM structure. The MOGSA model is illustrated previous in Figure 1.

Again, our model is a slight variation of the MOGSA, whereby we have merged the Strategy and Actions level into one inclusive classification. The idea was to simplify the final end point because of the broad job functions associated with our expert panel. Further, we checked the validity of the HDM with thought-leaders in this field. Our final HDM, enclosed, again coupled with in-depth literature review, was the combined recommendation of HDM experts.

Literature Review: Multiple journals, case studies and journals were studied to help architect the HDM and to help cross-reference expert input.

Data Gathering / Analysis: The HDM was originally constructed within an excel file format, enabling ongoing data input where needed, without requiring much additional time from the expert panel. Upon the reaching final version of the HDM, we decided to use the web-based tool developed via the ETM department at Portland State University, as the best means for data capture.

A total of three experts were contacted at Portland State, and three each from IBM and Tektronix. All three at PSU completed the HDM and the four out six from the technology side completed the HDM.

4.2 Model Implementation

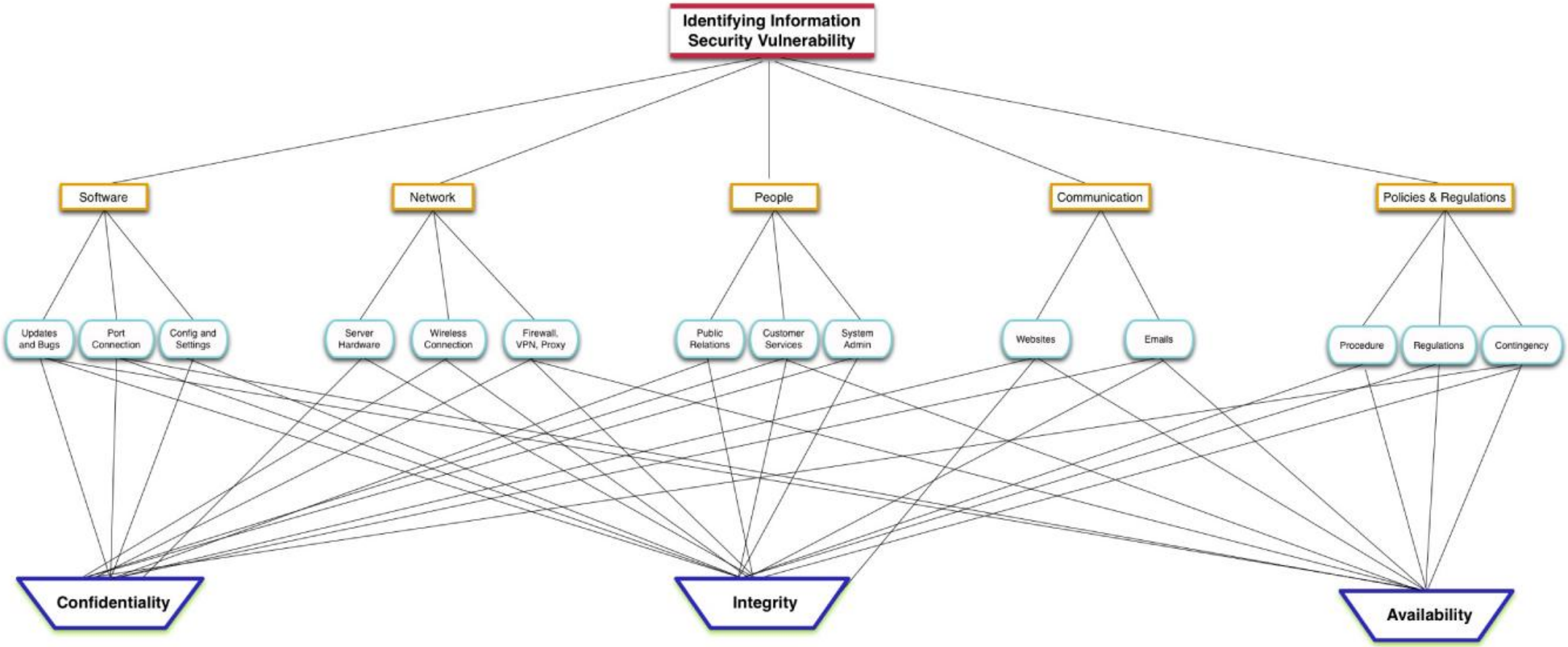


Figure 2 Hierarchical Decision Making Diagram for Identifying Information Vulnerability

Level 1

Identifying Information Security Vulnerabilities and Weaknesses

The mission of the research is to identify information vulnerabilities and weakness by utilizing pairwise comparison under expert judgment under methodological approach of the Hierarchy Decision Model introduce by Kocaoglu. The structure is known as MOGSA define Mission, Objective, Goals, Strategies, and Attributes.

The first level is the mission of the research, in this information security vulnerabilities and weaknesses. The sub-levels of the model pertains toe the supporting the first level mission. The approach to how the model was built is based off of the fundamental of penetration testing and information securities concepts at the top surface level. The principles are combined through studies literature review and information securities model is transcribe to the HDM.

Level 2

Software

Information systems are very center around software. Software has become an important factor for business operations in all types of industries. As software are becoming utilize through business operations, an increase of vulnerabilities of attacks also emerges through software. Especially, where business trends are revolving around the World Wide Web and connected to wide area networks increases the vulnerabilities and loopholes for exploitation to system infrastructures. Software such databases if breach can cause serious calamity where confidentiality of data from customers or client are available to malicious hackers or distributed to the public of mass audiences.

When assessing information security in organization, managers needs to considered vulnerabilities that comes from software as well IT factors the stability, reliability, and solution to meet business strategies and operations. The HDM 2nd level includes important security factors that needs to be considered for security evaluation, identification of security flaws, and penetration assessment,

Software in the HDM pairwise comparison is defined as ‘Computer program and virtual applications.

Network

Network nodes for the second level also includes IT hardware aspect and functionality aspect. Network and hardware are the primary of the IT system in organization as connection are made, processing, data input and out, and running software for operations. With multiples hardware for network hubs, host machines, routers, switchers, and mass-storage devices connected and accessible via network, can cause great threat into information security if breached.

The vulnerabilities in network system can greatly come through the connected hardware such as host machines, where host machines are pathway to central system exploitation [20]. For example vulnerabilities can come from unsecure host machines that can be compromise that allows attackers to continue through chains of networked host machines bypassing security layers and accessing mainframe system. As networking hardware are evolving with complexity to meet business needs, vulnerabilities grows along with issues of information security.

Network in the HDM pairwise comparison is defined as ‘Bundles of host machines that enable for data exchange between computers.’

People

People are one of the most important resources in organization as people are the main drivers for business. Organizations are depended on employees, managers, staff members, and executive officers to sustain the organization in the competitive market. As organization grows and expand, a increasing demand of people are taken in, with increase risk of information security.

People are important assets in an organization as vulnerable threat in terms of information security. As a higher density of people who are unfamiliar with IT security can pose greater threat to security.

People in the HDM pairwise comparison is defined as 'Individuals that are employed by given institution or organization.'

Communication

Communication is essential for running an organization and business operation. Communication can takes many forms and styles to exchange information across. When looking into IT, many forms of communication platform are used digitally into everyday life through evolution of the Internet. Emails has become standard platform for communication and website are use as a mean of mass communication on the World Wide Web.

Communication is the activity to exchange or conveyed information between two or more individuals. Such information can share internally in organization that is valuable, can be share with customers, and can be unintentionally be shared with hackers and attackers.

Before the process of breaching and compromising system, attackers to usually to reach that level dueto having access and recollecting large amount of information about the target. Such information can come from multiple communicative platforms that organizations are using to share information. When organization or people take pride in what they do and share excessive amount of information can lead to being prey by attackers [20].

When using platform for communication where data and information are being exchange between to a more entities vulnerabilities such as sniffing, inception, interruption, and eavesdropping are various means that can violate information security and increase vulnerabilities.

Communication in the HDM pairwise comparison is defined as 'The platform of how information is exchanged.

Policies and Practices

Organizations are often requiring following various rules and regulation either by government or third partying such credit card company where data confidentiality customer financial information must remain private. Policies are set up to prevent access of information getting into the wrong hands and ensure business ethics and compliant business practice.   Such policies and practice can be seen in HIPAA (Health Insurance Portability and Accountability Act) practice under the medical industry and SOX (Sarbanes-Oxley Act) that protects the medical and financial data [22][23].

Practices are often seen in customer support or tech support in banks or tech support help desk where 3 to 4 identity verification is required before providing information or offering any sort of support, commonly prompting on verification of address, phone number, SSN, date of birth, etc... Such practices can also prevent attackers from collecting information during reconnaissance phase especially through social engineering.

Policies and Practices in the HDM pairwise comparison is defined as 'Rules that govern a given institution or organizations, establish compliance rules of conduct within an organization, as it relates to proprietary and shared data security.'

Level 3

Level 3 are the sub-layer that corresponds to the Level 2 nodes.

Software

- Updates and Bugs

Software is not perfect and often there are bugs hidden within the source code. As software packages, OS, and application are a must for a PC or server to run. Without software, OS, and application computer would nearly be non-functional. Since software are such vital piece to information system and everyday use, software bugs can lead to security threats and loopholes to system prone for attacks [24]. Software that involved internetwork communication or connection to the World Wide Web are at even greater risk of vulnerabilities with potential intrusion to information system by exploiting software bugs, attacker access to system connected by internet and continue to intrude into internal network leading to security breach[25].

Software such as ERP, CRM, and databases center software contains valuable information and with security breach where attackers are accessing confidential data can be a serious issues for organization.

Software developers and companies releases update that fixes bugs, patches security issues and a provides patches and updates that are important to maintain information security as known bugs, issues, and vulnerability are discovered and reported. Update from original sources and vendors can increase information security, but software, applications, and updates can also come untrusted and misleading sources that can numerous security intrusion and issues that can threaten to an organization [20].

Updates and Bugs in the HDM pairwise comparison is defined as ‘New release of software packages that fix coding errors and introduces new features.

- Port Connections

Host machines, computers, network, and software are communication and exchanging information through ports. Ports allows incoming and outgoing connection from internetwork, outside, and the World Wide Web. Software and application are using ports to communicate with inside and outside network through ports. Where unused closed ports blocks incoming and outgoing connection, ports left open are gateways to system intrusion that can lead to system attacks and exploitation [26].

Port scanning is often used to identify problems with network and provide information network, open and close port. This is common practice where network engineering uses various port scanning tools to assess the current state of the organization network in ethical manner, unlike ethical hackers, system attackers are using port scanning as a mean to obtaining data and information to proceed with a system breach and targeting open ports as a gateway into the system [20]. In network protocol layer such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) ranges from 1 to 65,535 ports.

Port Connection in the HDM pairwise comparison is defined as ‘Entry gateways for data transmission and communication between computers.’

- Configurations and Settings

Network hardware, software, communication devices, and host machines involve the requirement to be configured with proper setting in order to function as intended. Configuration and setting is crucial aspect with networking and communication system, when configuration and setting are done correctly can result with an optimized, reliable, and high performing system with smooth operation. Poorly configure system can lead to network collapse with stagnating problems and issues [27]. This can be applied to information security, poor configuration can promote intrusion and exploitation attacks.

Poor configuration and settings can be critical to exploitation of information security. Many aspect of network security can apply configuration such as turning on firewalls, closing ports, and proper setting for ACL (Access Control List) are critical factors for a defensive approach to securing system and networks. Another example can be seen in setting permission in OS's (Operating System) for users, where cases of administration rights should not be granted to be standard users or root level access to should configure for system administration only [28].

Configurations and Settings in the HDM pairwise comparison is defined as 'Defining and implementing customize controls commands.'

Network

- Server Hardware

Server hardware is the physical devices that are running the software and applications that is operating the network system. Server hardware includes various devices that are connected together such as hubs, switches, routers, physical firewalls, host machines, NAS (Network Attached Storage), etc… The devices are connected together and communicating both internally and externally.

Physical access to server hardware by unauthorized personnel can be dangerous to information security and commonly be secured behind isolated and locked areas. Poor design of server hardware connection and or maintained hardware can be a threat to information security. Because of all the connected server devices, when attackers compromised one hardware it can continuously lead to linked to another server hardware [27].

Server Hardware in the HDM pairwise comparison is defined as 'Defining and implementing customize controls commands.'

- Wireless Connection

WLAN (Wireless Link Access Network) has increasingly grown in use in popularity as a mean to access networks and the internet., compared to predecessor conventional LAN. Wireless solution has grown across many household, colleges and universities, business, and organization as an accessible mean communicative connection through wireless access points. Wireless brought for network innovation, portability, and convenience but has also known for its weak security and vulnerabilities.

Wireless Access Point depending on various hardware and specification can provide wide range of frequencies and signal strength parameters – the further in proximity to access point the weaker the signal strength. This is allows attackers to connect and intrude wireless from a far distance such as wireless sniffing. The technology that WLAN offers can relatively easy to attack, exploit, and compromise vulnerabilities to information security. Various possible threat of WLAN security can perform through sniffing, packet spoofing, packet injections, and sniffing [29].

Wireless Connection in the HDM pairwise comparison is defined as 'Point to point Data transmission through frequencies without electrical conductors.'

- **Firewall, VPN, and Proxy**

Firewall can be both hardware and software that inspects incoming data and filter or blocks data, leaving only certain types of data to pass through into the network. Firewall monitor and control and act as a gateway of inbound and outbound data in order to protect from intrusion and attackers. Firewalls with the right configuration and settings can significantly reduce threats of information security and vulnerabilities.

VPN (Virtual Private Networks) uses data tunnel as mean of connection of two points on a network where the channel being use is encrypted for security and privacy. VPN moves data from a remote client to host machines or network that can be connected anywhere with Internet access. Data moving through the network in VPN is isolated from other network traffic and requires proper authentication with username and password.

Proxy Server is network computers or applications that are intermediary gateway between a local network and a large internetwork or the Internet that provides increased performance or various form of security. Proxy provides various purposes include anonymity, increase performance through caching webpages from a web server, logs and auditing, and can be uses a form of firewall and block internet services. Proxy can also provides means to access-restricted site that is filter out or blocked by an institution, in which can be a mean to bypass security.

Firewall, VPN, ad Proxy in the HDM pairwise comparison is defined as:

Firewall – 'Protected gateway that blocks and filters ingoing and outgoing connection.'

Proxy Server is defined as 'Virtual network intermediary client server.'

People

- Public Relation

Public Relation informs and communicates between organization and outsider. The roles behind are to share information with customers, investors, and shareholders. Informing about companies updates, news releases, and events.   Various companies take pride of who they are and at times can share information that can cause potential security risk and provide information that can increase potential vulnerabilities.

Reconnaissance is one basic and foremost phase that both ethical and malicious hacker performs before continue with a vulnerability assessment or an attack. Collecting valuable information from multiple resources. Many of these information gatherings resources can comes from companies news releases and PR updates about the companies. News release that involves information like system updates, migration, services shutdown can provide sufficient amount of information to lead to system exploitation and attacks [20].

PR at worse case may also require to the report to public about security breaches that occurs and informs customers, investors, and shareholders about system breaches. Such events may cause a threat to organization reputation as well publicizing the current vulnerabilities of the organization information security system.

PR in the HDM pairwise comparison is defined as ‘ Public Relation that interacts between customer and company.’

- Customer Services

In various types of organization, customer services provide support and accommodation for customers. Customer services contribute to multiple types from general support to a degree level of technical support. Customer services are usually the first point of contact who has access to various kind of information or data. Apart from contributing to support customer, customer services are a source of potential target for malicious hackers to obtain information data as mean of reconnaissance or utilizing the information for to assists in vulnerability attack [20].

Social engineering has been a popular technique to deceived and trick representative to provide private information or data that can useful for system attacks. Customer services would fall as victims to social engineering. The reconnaissance phase of hacking involves process of collecting various kinds of information, some of the information obtain can be use increase the chance for attackers to perform a successful social engineering from customer services or help desk representative and obtaining enough data to proceed in full attack and system breach.

Customer Services in the HDM pairwise comparison is defined as ‘Institute or organization's representative that provides support and accommodations.’

- System Admin

System administrations are responsible for system operations, functionality, control, account ownership, and system management. System admin usually the top level who has administrative access to network and system with the root level or administrative access to IT and IS system. System admin holds great power and control and has great responsibility. Mistake or incompetency at the system level can be serious problems. Attackers who gain access as a sys admin can become a very serious threat to information security, system breach, and compromising organization’s IT system.

System Admin in the HDM pairwise comparison is defined as ‘Top level technical administration that is responsible for system operations, functionality, control, account ownership, and system management.’

Communication

- Websites

The innovation of the Internet established the World Wide Web as mean of communication to mass audiences. The use of the web has expended that connected the world of information sharing and digital communication in real time. Websites has become a popular choice as communicative platform to share information for many organization and business.

Web 2.0, social media, and the transition to the 5th generation of HTML introduce many use of IT solutions for organizations and institutes. Through innovation provides solution to real world also introduce new problems. The World Wide Web and website has turned into a goldmine for obtaining massive amount of information and data.

Web technology uses for website has it's security vulnerabilities for exploitation. Confidential information can obtain without authorization from website connected to database. Website can be an opportunities for malicious hacking form reconnaissance to information security breach.

Website in the HDM pairwise comparison is defined as 'Data and information that is accessible through the World Wide Web by the use of a electronic devices via supported web browsers.'

- Email

Email (Electronic Mail) with innovation of the Internet and networking technology has grown in popularity has communication platform. Email has revolutionize the way communication that is nearly instant and became widely use across organization and users. In organization and even for personal, email can store valuable data and private information. Through the World Wide Web personal and corporate email has transition web based email services such as Hotmail, Gmail, and yahoo mail.

Email even though require login credentials can also be use as form recon to gather information such as email servers, server information, IP address, and whether response is sent back. Phisher are also utilizing email to phish and steal information from users. Spamming and email bombs are also a tactic as attacks. Emails are also resources that pose a great threat to security vulnerabilities and exploitation.

Email in the HDM pairwise comparison is defined as 'Electronic mails that transmitted digital messages through computer network and the Internet.'

Policies and Practices

- Procedure

Procedures are the defined steps that are applied to various requirements, task, or scenario to follow in given situations. Many organization departments such as help desk, customer services, and human resources have various procedures to follow either through regulation, standards or compliancy. Procedure such identify verification that is implemented for help desk or customer service to follow to validate one identity who the individual is really the person they claim to be. Such procedures are mandatory to for the sake of security and prevention of issues, problems, or crisis.

Especially with techniques such social engineering that design to trick an individual to provides confidential information, procedures are establish to reduce such risk as mean of prevention. Procedures are also applied to how task are perform when information is being shared or perform where security or privacy is established as factor of success. In information security, procedure is view as steps and guideline to increase system security.

Policies and Practices In the HDM pairwise comparison is defined as 'Defined sequences of instructions and / or recommended or enforces steps to follow in order perform a specific task.'

- Regulations

Regulations are necessary to be applied or enforced in organization that conforms to state laws, governmental policies, standards, and in consensus of moral ethics. Such regulations are often with consequences varying in severity of consequences and penalties if violated.

This can be illustrated in various organization that stores credit cards and information that follows strict regulations of security and if violate than penalty fines are enforce. Health industries conform to HIPPA and finance need conform to SOX.

Regulation are established, enforced, and regularly monitored that abides to conformity that helps to increase information privacy and security for stakeholders and the organization.

Regulations in the HDM pairwise comparison is defined as ‘A process of the promulgation, monitoring, and enforcement of rules. Regulation creates, limits, or constrains a right, creates or limits a duty, or allocates a responsibility.’

- Contingency Plan

Contingency plan is often becomes valuable asset to have especially when things goes wrong. Identifying potential risk that is likely to happen can anticipate on how to increase security, identify vulnerabilities, and how to take corrective action when the unexpected emerges and uncertainty is at hand.

Contingency plan can reduce damaged being done by taking the proper measure and putting plans to actions. This can defined procedures that needs to be followed after security breach has occurred and type of attack that was inflicted. Identifying what the goals and purpose of attacker and responding to preventive measure with a solid contingency reduces impact on organizations.

Contingency Plan in the HDM pairwise comparison is defined as ‘Is a plan devised for an outcome other than in the usual (expected) plan. It is often used for risk management when an exceptional risk that, though unlikely, would have catastrophic consequences.’

Level 4

The nodes at level are the key principles of information security, often represented as foundation or basis of information security model. The 3 nodes are concept that is use with security professional as terminology when security issues surface.

Confidentiality

Confidentiality in terms of security is defined as the ability to protect information and data from unauthorized access or ownership of unauthorized individuals or party. Confidentiality includes the notion of privacy. Various business and organization are often to maintain confidentiality between it customer and clients. This is can be seen in banking and finance industries, health industries, educational industries, and governmental through retirement or social security. Violation of confidentiality in such industry can pose threat on both sides [28].

Confidentiality can easily violate either intentionally or by mistake, especially where situation such as lost of stolen mobile devices such as smart phone or notebook that stores personal information. Confidentiality can be threat with shoulder surfing where looking over another person when entering password or pin number and eavesdropping. Breaching into information system to previewing confidential information and data are common cases.

Confidentiality in the HDM pairwise comparison is defined, as 'Component of privacy and the ability to protect data from those not authorize to see it.'

Integrity

Compared to the traditional pen and paper, digital format can easily be changed and altered. Integrity is the ability to prevent any form of unauthorized change or deletion of data. Unauthorized change and deletion of data can be problematic or serious issue in information security. The concept and practice behind integrity is in consideration to undo, reverse, or recovery of any data that change or deleted [8].

Data changes can cause serious security threat especially administrative rights or root level permission on IT systems. This can also involve changing authorization and permission level on Access

Control List. Violation of integrity can cause serious security threat especially when authorize users are restricted from performing task or under the unknowingly working with inaccurate and false

Integrity in the HDM pairwise comparison is defined, as 'Component of privacy and the ability to protect data from those not authorize to see it.'

Availability

Accessing and obtaining information that are seeking in timely manner has grown in importance. This can be refers as availability where the ability to have access to wants and needs. Interruptions of accessibility from availability violation can be problematic for organization and for individuals such as loosing availability to access to bank accounts, cloud storage, email, patient medical records, and various critical data and services [28].

Loss availability can be caused various problems including system breach or various system attacks such DoS (Denile of Service). Various kind organizations are operating off services that are depended on IT systems, databases, or the Internet. Depending types of organization and system, downtime can cause problem that can lead to security vulnerabilities.

Availability in the HDM pairwise comparison is definedas 'the ability to access our data when we need it. Involve loss of availability and wide variety of breaks in the chain that allow and access of data. Includes power loss, OS or App problems, network attacks, compromise of system, and DoS.'

5. Result

The impact level is the Mission and Objectives in the HDM Model that represent the overall purpose of the research – Identifying Information Security Vulnerability that combines with five main Criteria – Software, Network,People, Communication, and Policies and Practices. Then, the target level is the Goal level that in the research model consisted of fourteen different nodes as the sub-criteria of the Objective level. Lastly, the operational level within the purpose model, the research team combined the Strategy and Action level from MOGSA Hierarchy to one level – called Alternatives. This final level was separated into three nodes; Confidentiality, Integrity, and Availability.

Hierarchical Decision Model (HDM) web based Beta version 2.0 that created by Portland State University; Engineering and Technology Management [29] had been used as the research tool. The experts could access the HDM model directly from the expert link that the researchers provided. Also, the instruction of how to pairwise comparison the model was also sent to help the participants had clearly understanding in evaluating the model. After experts in each sector; Information Technology and Education, finished weighting their judgment to the model, individual results and also the mean value of the overall judgmental for each individual segment were collected.

With the useful of the HDM web based tool, the calculation of the experts' pairwise comparison would be done by the software. The tool also calculated an inconsistency value and a measure of disagreement among the respondents. In this research, the inconsistency rate should be less than 0.1 to confirm that the result from this expert is acceptable. For the disagreement value, it will show that how each expert agrees to each other within the same mission. Same as inconsistency, the acceptable disagreement is also 0.1.

Information Technology

The experts from this segment consist of four people from different companies; Tektronix and IBM. The documented results are based on the responder's personal view (experience and skill set), and does not necessarily reflect their company's perspective.

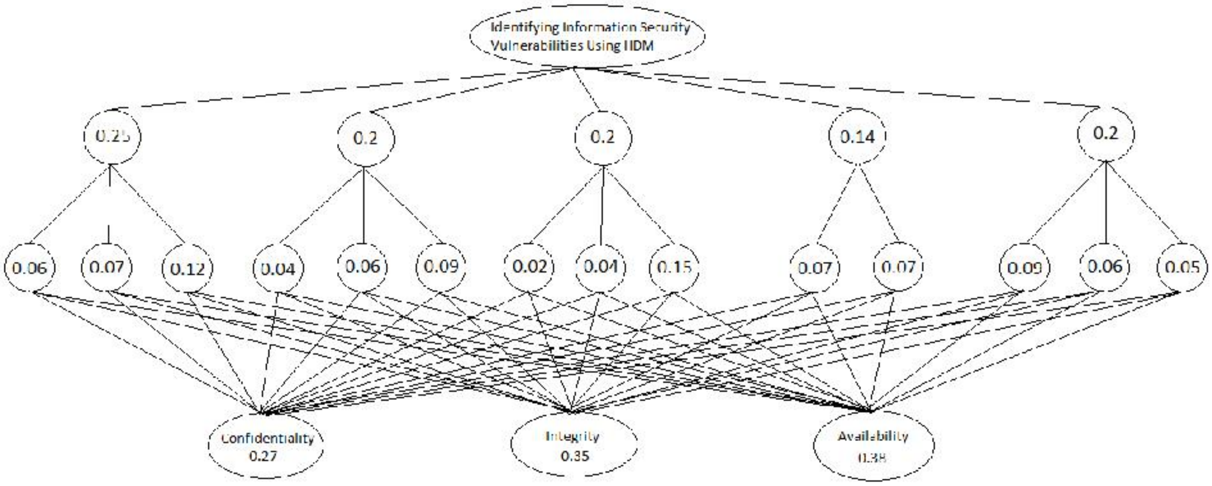


Figure 3 HDM Result for Information Technology Sector

Figure 3 above illustrates the dispersed weight of the model, the overall contribution value to the mission of the research project. It is seen that Availability, with a weight equal to 0.38 should be the highest priority for participating Information Technology companies to focusing to prevent business loss associated with down-time. Availability is closely followed by Integrity, which holds the value at 0.35. Lastly, Confidentiality has the lowest of the three options, with a contribution value of 0.27. From the result, it shows that Availability is more important than Integrity and Confidentiality for 1.1 and 1.4 times, respectively.

The following Table is displayed the individual result of the experts' contribution weight to the mission. Each expert will have different opinion based on their personal experience. However, the HDM software will calculate the mean which is the group decision, inconsistency, and overall disagreement value for the overall model. For example, after expert 1 finished the pairwise comparison the model, the HDM tool would calculate the result for the final level. It showed that expert 1 believed that Integrity is the most important action in order for the company's information is being protected from an adversary who attempts to modify, remove, or recover the data. Integrity for the expert 1 is more important 1.13 times than Confidentiality and Availability, which are equally important, as illustrated in Table 2.

Table 2 HDM Result for Each Individual Experts and the Group Decision in Information Technology Sector

Information Security Vulnerabilities	Confidentiality	Integrity	Availability	Inconsistency
Expert 1	0.32	0.36	0.32	0.01
Expert 2	0.19	0.3	0.51	0.03
Expert 3	0.22	0.4	0.38	0.01
Expert 4	0.35	0.34	0.31	0.01
Mean	0.27	0.35	0.38	
Minimum	0.19	0.3	0.31	
Maximum	0.35	0.4	0.51	
Std. Deviation	0.07	0.04	0.08	
Disagreement				0.06

The findings of the overall result also show an inconsistency value from each of the four experts range from 0.01 to 0.03, which means the four experts are consistent with their opinion when evaluating any given comparison option. Further, the disagreement value amongst the Information Technology panel is very low at 0.06, which means all the experts tend to agree with each other when applying a given weight to a specific topic. However, Expert 2 shows a slightly higher inconsistency rate coming in at 0.03. In this case, Availability has by far the highest rate of significance when compare to the others: Confidentiality and Integrity. If we were to normalize the input from Expert 2 as the input relates to Availability, the mean value for Integrity would increase, thereby equalizing both Availability and Integrity. As such, our recommendation would be to equalize investment across these two areas.

Table 3 Level 3 Weight Contribution to the Mission in Information Technology Sector

Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
	0.06	0.07	0.12	0.04	0.06	0.09	0.02	0.04	0.15	0.07	0.07	0.09	0.06	0.05

When looking to the third level of the model,as illustrated in Table 3 above, the researchers discovered that at the Goal level, the element that has the highest contribution value to the mission is System Administration with the weight 0.15. It can interpret to that all the experts from the IT sector agreed that cyber hackers tend to use this channel as a means to attack the company when compared to the others. Configuration and Setting is also a dangerous passage that the hackers might penetrate to the organizations' security system because it has relatively high weight at 0.12. Experts from Information Technology sector tend to agree that Public Relation (PR) is a source that has the lowest risk (0.02) that would generate attacks from outside company boundaries.

Table 4 Level 2 Weight Contribution to the Mission in Information Technology Sector

Level-2	Software	Network	People	Communication	Policies & Practices
	0.25	0.20	0.20	0.14	0.20

At the second level, or Objective level of the HDM, the result as in Table 4 displayed that within the Information Technology sector, experts' opinions confirm that Software is the criterion that has the highest contribution to the mission, Information Security Vulnerabilities, at 0.25 which mean Software may have the highest possibility in getting intrusion from outside the organization, or from unauthorized use/access within the company. The other variables, Network, People, and Policies & Practice are also important variables because their contribution to the mission at 0.2. Communication coming in at .14, appears to be the activity that IT experts agree that the cyber attackers will have least possibility of generating attacks that will interfere with the company's security system. When comparing the highest value to the lowest, Software is viewed as nearly twice as vulnerable when compared to Communication.

Education

In Education are, the researchers got three responses from one university which is Portland State University. Two experts are from Office of Information Technology (OIT). That one of them is the CIO of OIT, and the other is the helpdesk of OIT who also has a related experience with the Information Security issue. The last expert is come from Business Administration at PSU who also familiar with the Information System and Technology.

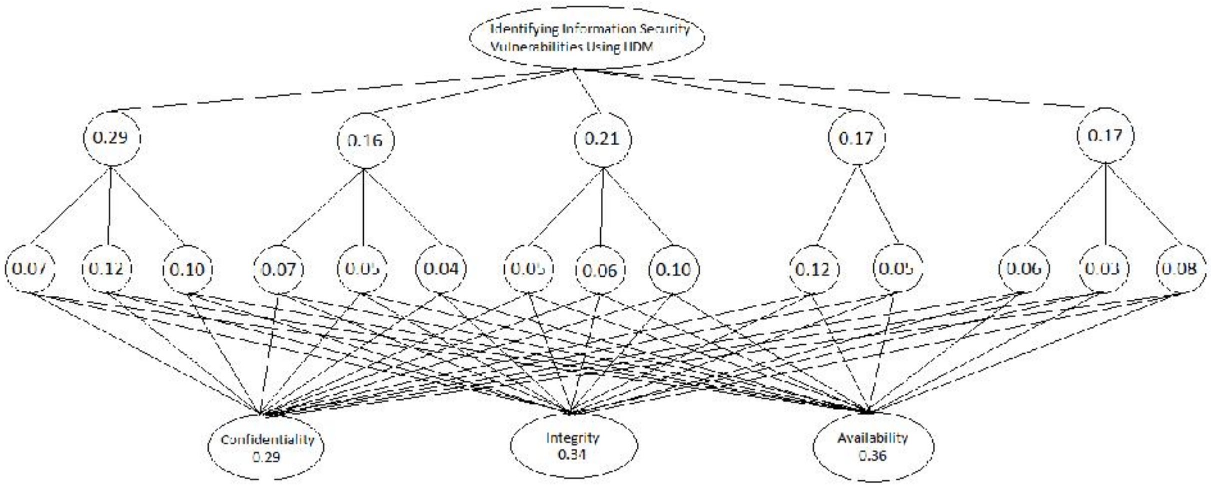


Figure 4 HDM Result for Education Sector

According to the results that the researchers got for the alternative level as depicted in Figure 4 above which based on experts' experience and technical skills. The highest score in the Education sector goes to Availability, with the mean value of 0.36. The mean of Integrity from all experts is 0.34. And the mean value of Confidentiality is 0.29. Initially, these results indicate that within the Education sector, investment should be weighted higher towards Availability in order to avoid the problem of unavailable access their system due to a system attack. Integrity is also an additional strategy that education should pay attantion to increase the improvement on preventing data from modifying. For Education area, the Availability is more important than Integrity 1.1 times and Confidentiality for 1.2 times.

Table 5 HDM Result for Each Individual Experts and the Group Decision in Education Sector

Information Security Vulnerabilities	**Confidentiality**	**Integrity**	**Availability**	**Inconsistency**
Expert 1	0.38	0.35	0.27	0.01
Expert 2	0.36	0.3	0.33	0
Expert 3	0.14	0.38	0.48	0.09
Mean	0.29	0.34	0.36	
Minimum	0.14	0.3	0.27	
Maximum	0.38	0.38	0.48	
Std. Deviation	0.11	0.03	0.09	
Disagreement				0.08

According to the Table 5 result above, the inconsistency value is 0.09, which is on the high side of acceptability (0.10 or higher would require further investigation as to why a given responder was considered inconsistent with their responses). The inconsistency value of 0.09 is due to one of the three experts has strong opinion in academic field more than Information Security issue. This expert may evaluate the HDM from different aspects while people from IT sector would prioritize confidentiality over other alternatives. Thus, the group decision might be changed to the high weight on confidentiality because it would be more reasonable action for the university to focus on due to the level of high daily access to the university's website.

Table 6 Level 3 Weight Contribution to the Mission in Education Sector

Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
	0.07	0.12	0.10	0.07	0.05	0.04	0.05	0.06	0.10	0.12	0.05	0.06	0.03	0.08

As depicted in Table 6, the third or mission level, the highest contribution values are port connection and websites with the same normalized weight of 0.12. The second highest contribution value is configuration and setting and system administration with the weight of 0.10. These two highest values indicate that the institution should pay close attention. The least risk from being attacked, depict that firewall, VPN, and proxy and regulations would have lower risk than other channels in the same level. The normalized weights of firewall, VPN, and proxy and regulations are 0.04 and 0.03, respectively.

Table 7 Level 2 Weight Contribution to the Mission in Education Sector

Level-2	Software	Network	People	Communication	Policies & Practices
	0.29	0.16	0.21	0.17	0.17

The results from Table 7 illustrate the second level of HDM in the education section that the experts' judgments agreed that Software with the weight of 0.29 is the highest contribution to our HDM's mission, "Information Security Vulnerabilities." The second highest contribution is People that have the weight of 0.21. For both Communication and Policies & Practice share the weight of 0.17. Lastly, the experts agreed the least weight of 0.16 on Network with lowest possibility of being penetrated by cyber attackers.

6. Discussion

Examining the key factors based on the expert results key factors indicates that Software has the highest security threats that was identify by the model. Looking into the sub-levels can identify that configuration and setting is critical that components. Assessment of these results can explain that software plays an important role when running in IT system, as system performs business operation and holds valuable data for an organization such as ERP system (Enterprise Resource Planning) and Relational Database. Software are prominent IT solution and critical for business operations and interruption of availability can put an organization to a halt. System administration holds great responsibility in maintaining and sustaining such software in order to keep the system operating smoothly and mistake causes at the System admin level can lead serious threat if the mistake were to be discovered and exploited.

On the academic side where university on depended IT and networking as a solution to serve many operation across department and campuses, having consistent availability of services is a critical aspect to the whole. Many system such Learning Management System (LMS), Lightweight Directory Access Protocol (LDAP), student Information repositories, Customer Relation Management System (CRM), etc. are widely use application in university. Vast network infrastructure seen in university involves a large amount input and output of data transmission passing through ports and are required for network to software connection, leaving vulnerability of information security when attackers perform port scanning and vulnerability scanning. When attacks are made to university that holds massive information of all types, establishing a solid contingency plan is good defensive approach.

7. Conclusion

The passing of the millennium along with the emergences of web 2.0 and the expansion of the Internet brought forth trends of rising values of information and data. Businesses and organizations are turning towards IT solutions to serve business needs and operations. IT solutions become widespread in the market, information security becomes an increasing concern with issues of malicious hacker, cyber-attack, corporate espionage, system exploitation, and cyber intrusion.

Offensive information security trend continues to increase at a rapid pace that's becoming an international concern with various events including wikileaks' releases of highly confidential government information. A single example in the consumer market, malicious hacker's successfully compromised Sony's vast amount of customer's personal information. With respect to cyber-warfare, China and Iran, among others, continually try to infiltrate US national systems leading toward a highly offensive threat to national security.

The recent trends of intrusion targeting innovation and intellectual property have escalated towards continuous attacks against Universities and other educational institutions. Numerous current events of information security breaches across multiple sectors have grown in severity, causing international threats ranging from national, corporation, educational, and individual security threats.

Existing and growing threats indicate information security leads to a higher demand of investment in IT security practices. Neglecting on the investment of information security can lead to serious consequences of system breach and intrusion. Through the research of information security from literature reviews shows the widespread potential of information security vulnerabilities, and depending on the type of business or organization. Focus on where to strengthen information security can vary on the type of organization and businesses, where one section of information security would require greater attention because of nature of that area is center around the business operation and any interruption or security breach can negatively impact business operations.

Combining information security CIA (Confidentiality, Integrity, Availability) model with various technology sources of IT security and networking into the HDM introduces a systematic approach on identifying various aspects that are applicable for organizations to apply as a means to review security vulnerabilities of an organization. This research utilizes the methodological model of the HDM together with IT aspect and resulted in a four-level model weighted by various selected IT experts in the technological industry and educational industry.

The weighting allocated by experts indicating 'Availability' is the main focus for information security, and should be prioritized to strengthen security vulnerabilities. The results from HDM expert weighting indicates which nodes can pose a greater vulnerabilities and through the mean of exploiting such vulnerabilities like software vulnerabilities, the threshold of disagreement between is within an acceptable range of 0.06.

Within the education sector, expert weighting resulted in similarities to that of the technology sectors. Education IT expert results are also show 'Availability' as the leading choice. The result indicates that vulnerabilities would be through software and system configuration and settings. The result of expert disagreement is slightly higher, however still an acceptable level of 0.08.

The implementation of Information Security and HDM through expert weighting presents a tested model that can provide contribution to fields of information security and introduce methodological approach for managers to consider on contributing resources to where it would be most appropriate an investment of information security based on the results of the HDM. Additional research can significantly contribute towards prioritizing information security. The contribution of this research and the future of information security and HDM studies can provide path for business and IT strategy:

increase information security, reduce or prevent cyber-attacks, and increase the protection of valuable digital assets of a business, institution or organization, all leading towards a secure future.

8. Lesson Learned

As a team, we worked diligently on building the HDM and went through a series of draft versions before finalizing the Objective, Goal and Strategy level. The process we went through was to prioritize each node within the model and remove the topics/items that we felt did not meet certain threshold. To identify where the threshold should reside, we relied on past experience in conjunction with literature reviews. However, to further validate a given threshold, it is considered advisable to get input from outside our team, possibly from the list of potential survey participants.

In that same vein, we increase the overall pool of potential experts, thereby giving us a change to vet them and only invite those that have experience, exposure and skills as it relates to Information Security, to participate in the HDM.

Another key take-away would be to go outside the academic norms of journals, papers and reach deeper into trade publications, associations and business groups to identify other written case studies, thereby further beefing up all written research on security topics.

9. Future Work

The proposed HDM model for the research is design centered to the time limitation of class. Implementation of information security for this research was design to meet the time limitation requirement was filter off the basics of penetration testing, hacking, and networking practices. Advance subjects of those practices can be very further examined and applied to the HDM for an in future in depth research that contributes towards the future of identifying information security by utilizing the HDM. These methodologies introduce in this research with further research and testing may provide greater knowledge of scalability and potentials of identifying advance information security and cyber threats.

Moving forward, we suggest the following action items in order to effectively continue this study:

1) Target more companies/organizations within the same sector (industry). Education Example: All participating Oregon Universities – public and private. Then do the same with other regions of the country. Technology Example: Tektronix, Agilent, and LeCroy, etc.
2) Target other industries to see if there is a divergence in responses or do they reflect similar Information Security priorities. Key industries: Banking, Health Sciences/Medical, Transportation, and Telecom.
3) Another area to explore would be to take this study to a global level, using the two prior strategies. This may give insight regarding cultural differences as it relates to Information Security.

10.Reference

[1] K. Stuart and C. Arthur, "PlayStation Network hack: why it took Sony seven days to tell the world," The Guardian, 27 Apr 2011. [Online]. Available: http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony. [Accessed 2013].

[2] The Economist, "Fighting China's hackers: Is it time to retaliate against cyber-thieves?," The Economist, 25 May 2013. [Online]. Available: http://www.economist.com/news/united-states/21578405-it-time-retaliate-against-cyber-thieves-fighting-chinas-hackers. [Accessed 2013].

[3] M. Calabresi, "WikiLeaks' War on Secrecy: Truth's Consequences," Time Magazine, 2 Dec 2010. [Online]. Available: http://www.time.com/time/magazine/article/0,9171,2034488,00.html. [Accessed 2013].

[4] S. Gorman and D. Yadron, "Iran Hacks Energy Firms, U.S. Says," The Wall Street Journal, 23 May 2013. [Online]. Available: http://online.wsj.com/article/SB10001424127887323336104578501601108021968.html. [Accessed 2013].

[5] R. Perez-Pena, "Universities Face a Rising Barrage of Cyberattacks," The New York Times, 16 July 2013. [Online]. Available: http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0. [Accessed 2013].

[6] STAMFORD, Conn., "Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013," Gartner, 11 June 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2512215. [Accessed 2013].

[7] A. Arora, D. Hall, C. A. Pinto, D. Ramsey and R. Telang, "Measuring the Risk-Based Value of IT Security Solutions," *the IEEE Computer Society,* pp. 35-42, 2004.

[8] M. E. Johnson and E. Goetz, “Embedding Information Security into the Organization,” *IEEE Security Privacy*, vol. 5, no. 3, pp. 16–24, 2007.

[9] A. Arora, D. Hall, C. A. Pinto, D. Ramsey and R. Telang, "Measuring the Risk-Based Value of IT Security Solutions," *the IEEE Computer Society,* pp. 35-42, 2004.

[10] L. D. Bodin, L. A. Gordon and M. P. Loeb, "Evaluating Information Security Investment Using the Analytic Hierarchy Process," *Communication of the ACM,* vol. 48, no. 2, pp. 79-83, 2005.

[11] S. Evans, D. Heinbuch, E. Kyle, J. Piorkowski and J. Wallner, "Risk-Based Systems Security Engineering: Stopping Attacks with Intention," *IEEE Security & Privacy,* pp. 59-62, 2004.

[12] A. Alshboul, "Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks," *Communication of the IBIMA,* vol. 2010, pp. 1-9, 2010.

[13] A. Alshboul, "Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks," *Communication of the IBIMA,* vol. 2010, pp. 1-9, 2010.

[14] D. L. Goodhue and D. W. Straub, "Security concerns of system users: A study of perceptions of the adequacy of security," *Information Management,* vol. 20, pp. 13-27, 1991.

[15] E. H. Forman and M. A. Selly, "Decision by Objectives," *The Journal of the Operational Research Society,* vol. 54, no. 10, pp. 1108-1109, 2003.

[16] J. Belding, E. Loanzon, H. Millward, L. Seboni, D. Sibanda and T. Torgeson, "A Decision Model for Purchasing the Highest Value Printer for Home use for the Least Cost," in *PICMET '09 - 2009 Portland International Conference on Management of Engineering*, Portland, 2009.

[17] D. F. Kocaoglu, Engineering Management, New York: McGraw-Hill, 1981.

[18] D. F. Kocaoglu, "Hierarchical Decision Modeling (HDM)," Portland, 1987.

[19] D. F. Kocaoglu, "MOGSA Decision Hierarchy," Portland, 2013.

[20] P.Engenbretson. "The Basics of Hacking and Penetration Testing." Syngress, Massachusetts, 2011.

[21] US Department of Health & Human Services "Summary of the HIPPA Privacy Rule", Available: [http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html] Last Access: 08/12/2013.

[22] U.S Security and Exchange Commission. “Sarbanes-Oxley Corporate Responsibility 15 USC 7201”. Online: [http://www.sec.gov/about/laws/soa2002.pdf]. Last Accessed: 08/12/2013.

[23] K.Hapner. “PC’s Vulnerable to Security Breaches, Expert Say.” The New York Times, Feb 24, 2000. Online: [http://www.nytimes.com/2000/02/04/us/pc-s-vulnerable-to-security-breaches-experts-say.html]. Last Accessed: 08/09/2013.

[24] S.Harris, A.Harper, C.Eagle, J.Ness. “Grey Hat Hacking.” 2nd Edition. McGraw Hill. New York. 2008.

[25] G. Lyon. “NMAP Network Scanning.” Insecure.com LLC. California. 2008.

[26] C, M. Kozierok. “TCP/IP Guide” No Starch Press. California. 2005.

[27] J. Andress. “The Basics of Information Security.” Syngress. Massachusett. 2011.

[28] V. Ramachandran. “Backtrack 5 Wireless Penetration Testing.” Packt Publishing. Birmingham, UK. 2011.

[29] PSU ETM, "HDM (Hierarchical Decision Model) Verssion: Beta 2.0," Portland State University, 2013. [Online]. Available: http://research1.etm.pdx.edu/hdm2/. [Accessed 8 2013].

11.Appendix

HDM and Results

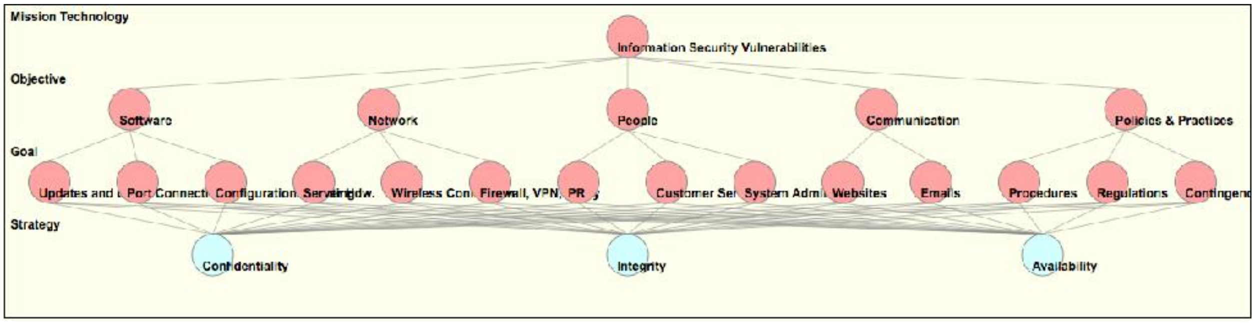
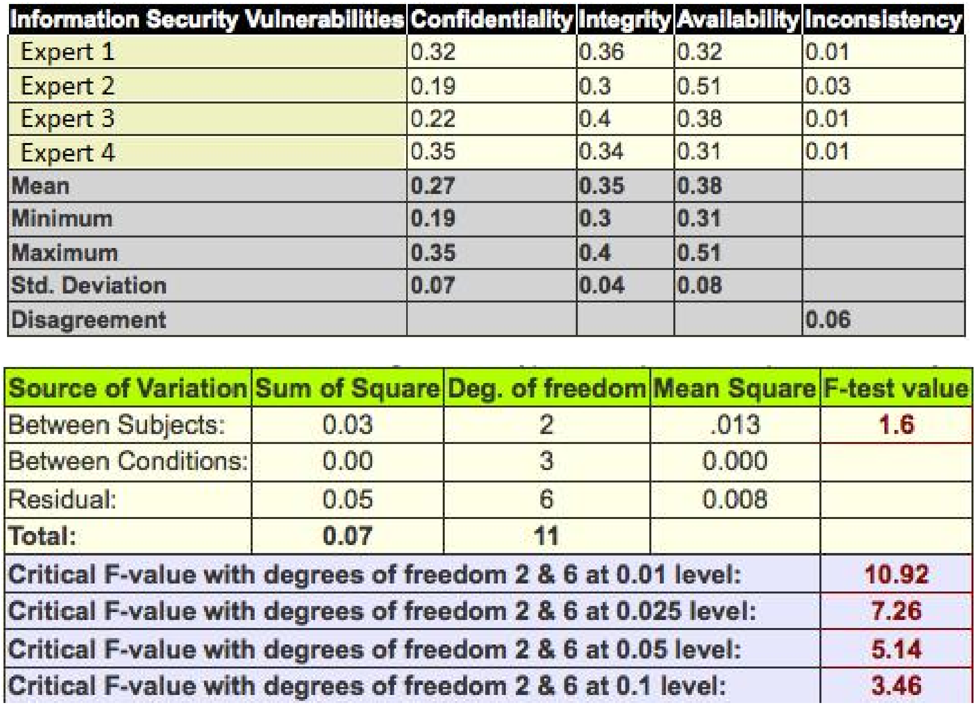


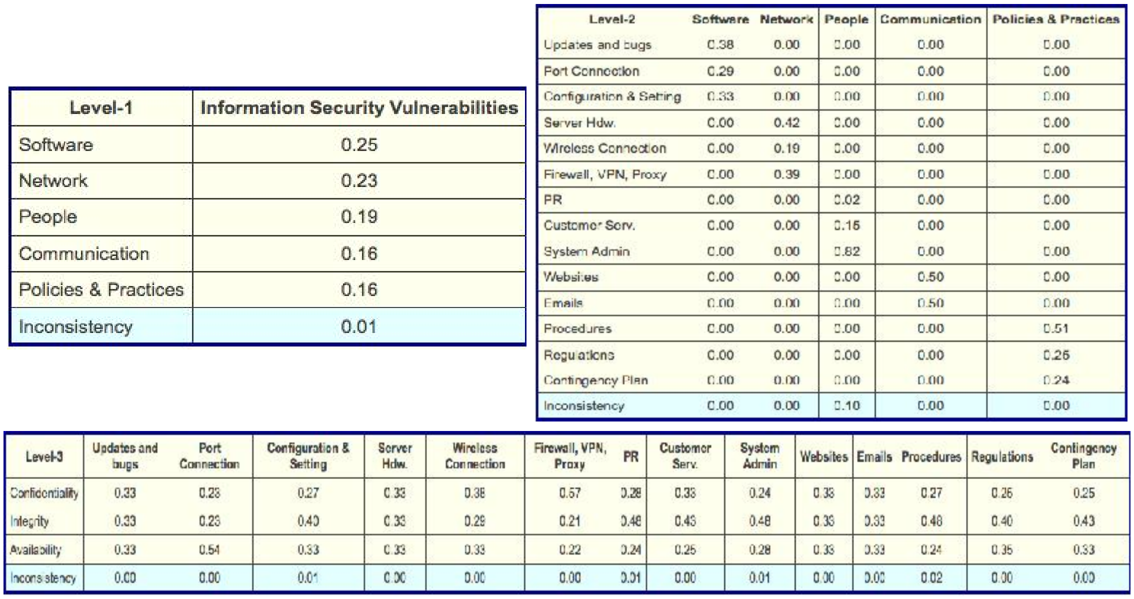
Figure 1: Technology Sector HDM



Information Security Vulnerabilities	Confidentiality	Integrity	Availability	Inconsistency
Expert 1	0.32	0.36	0.32	0.01
Expert 2	0.19	0.3	0.51	0.03
Expert 3	0.22	0.4	0.38	0.01
Expert 4	0.35	0.34	0.31	0.01
Mean	**0.27**	**0.35**	**0.38**	
Minimum	**0.19**	**0.3**	**0.31**	
Maximum	**0.35**	**0.4**	**0.51**	
Std. Deviation	**0.07**	**0.04**	**0.08**	
Disagreement				**0.06**

Source of Variation	Sum of Square	Deg. of freedom	Mean Square	F-test value
Between Subjects:	0.03	2	.013	**1.6**
Between Conditions:	0.00	3	0.000	
Residual:	0.05	6	0.008	
Total:	**0.07**	**11**		
Critical F-value with degrees of freedom 2 & 6 at 0.01 level:				**10.92**
Critical F-value with degrees of freedom 2 & 6 at 0.025 level:				**7.26**
Critical F-value with degrees of freedom 2 & 6 at 0.05 level:				**5.14**
Critical F-value with degrees of freedom 2 & 6 at 0.1 level:				**3.46**

Figure 2: The Overall HDM Results – Technology Sector

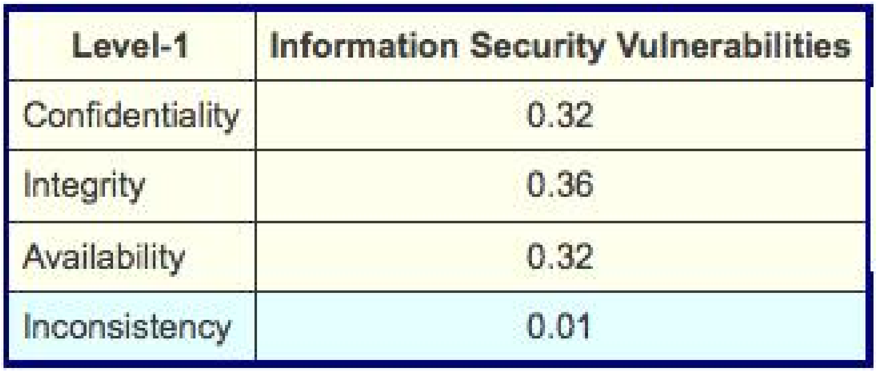


Level-1	Information Security Vulnerabilities
Software	0.25
Network	0.23
People	0.19
Communication	0.16
Policies & Practices	0.16
Inconsistency	0.01

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.38	0.00	0.00	0.00	0.00
Port Connection	0.29	0.00	0.00	0.00	0.00
Configuration & Setting	0.33	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.42	0.00	0.00	0.00
Wireless Connection	0.00	0.19	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.39	0.00	0.00	0.00
PR	0.00	0.00	0.02	0.00	0.00
Customer Serv.	0.00	0.00	0.16	0.00	0.00
System Admin	0.00	0.00	0.82	0.00	0.00
Websites	0.00	0.00	0.00	0.50	0.00
Emails	0.00	0.00	0.00	0.50	0.00
Procedures	0.00	0.00	0.00	0.00	0.51
Regulations	0.00	0.00	0.00	0.00	0.25
Contingency Plan	0.00	0.00	0.00	0.00	0.24
Inconsistency	0.00	0.00	0.10	0.00	0.00

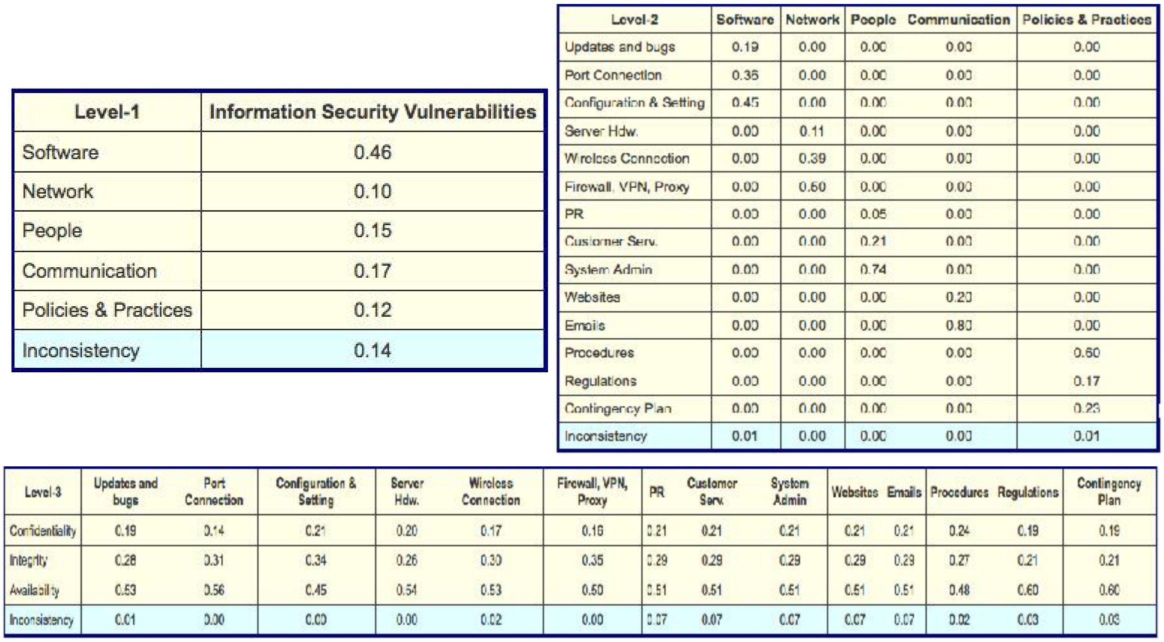
Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.33	0.23	0.27	0.33	0.38	0.57	0.28	0.33	0.24	0.33	0.33	0.27	0.26	0.25
Integrity	0.33	0.23	0.40	0.33	0.29	0.21	0.48	0.43	0.48	0.33	0.33	0.48	0.40	0.43
Availability	0.33	0.54	0.33	0.33	0.33	0.22	0.24	0.25	0.28	0.33	0.33	0.24	0.35	0.33
Inconsistency	0.00	0.00	0.01	0.00	0.00	0.00	0.01	0.00	0.01	0.00	0.00	0.02	0.00	0.00

Figure 3: Expert 1 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.32
Integrity	0.36
Availability	0.32
Inconsistency	0.01

Figure 4: Expert 1 Final Results

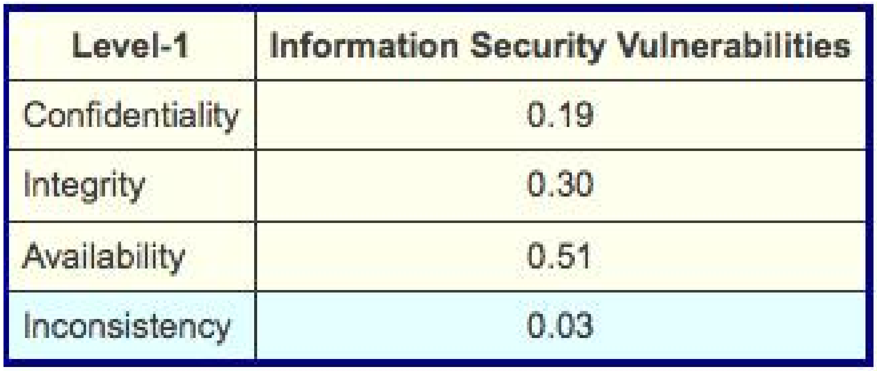


Level-1	Information Security Vulnerabilities
Software	0.46
Network	0.10
People	0.15
Communication	0.17
Policies & Practices	0.12
Inconsistency	0.14

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.19	0.00	0.00	0.00	0.00
Port Connection	0.36	0.00	0.00	0.00	0.00
Configuration & Setting	0.45	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.11	0.00	0.00	0.00
Wireless Connection	0.00	0.39	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.50	0.00	0.00	0.00
PR	0.00	0.00	0.05	0.00	0.00
Customer Serv.	0.00	0.00	0.21	0.00	0.00
System Admin	0.00	0.00	0.74	0.00	0.00
Websites	0.00	0.00	0.00	0.20	0.00
Emails	0.00	0.00	0.00	0.80	0.00
Procedures	0.00	0.00	0.00	0.00	0.60
Regulations	0.00	0.00	0.00	0.00	0.17
Contingency Plan	0.00	0.00	0.00	0.00	0.23
Inconsistency	0.01	0.00	0.00	0.00	0.01

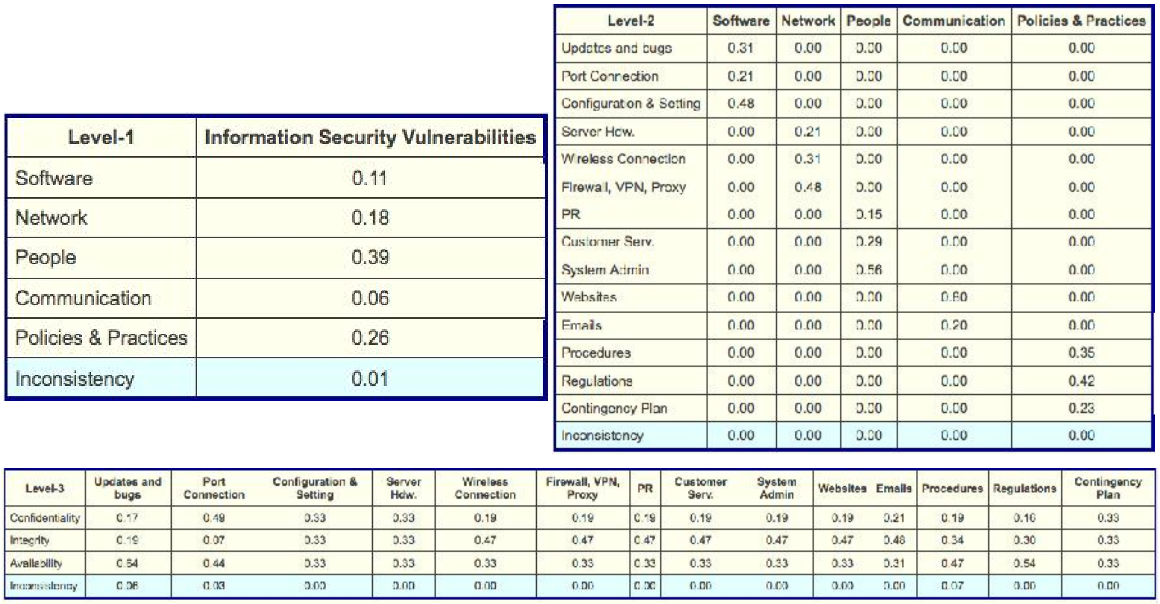
Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.19	0.14	0.21	0.20	0.17	0.16	0.21	0.21	0.21	0.21	0.21	0.24	0.19	0.19
Integrity	0.28	0.31	0.34	0.26	0.30	0.35	0.29	0.29	0.29	0.29	0.29	0.27	0.21	0.21
Availability	0.53	0.56	0.45	0.54	0.53	0.50	0.51	0.51	0.51	0.51	0.51	0.48	0.60	0.60
Inconsistency	0.01	0.00	0.00	0.00	0.02	0.00	0.07	0.07	0.07	0.07	0.07	0.02	0.03	0.03

Figure 5: Expert 2 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.19
Integrity	0.30
Availability	0.51
Inconsistency	0.03

Figure 6: Expert 2 Final Results

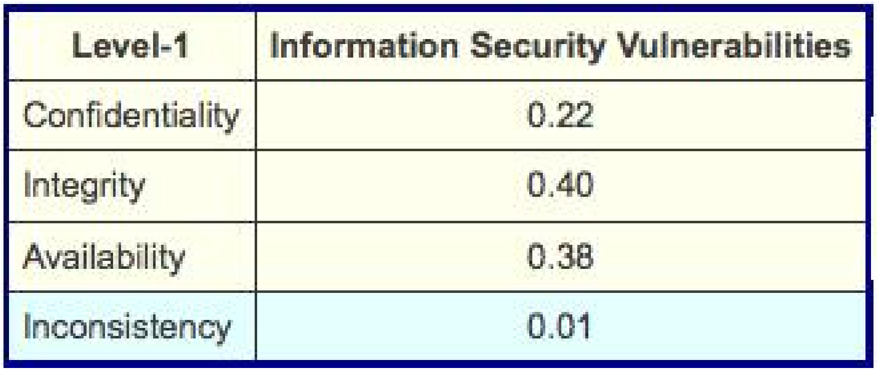


Level-1	Information Security Vulnerabilities
Software	0.11
Network	0.18
People	0.39
Communication	0.06
Policies & Practices	0.26
Inconsistency	0.01

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.31	0.00	0.00	0.00	0.00
Port Connection	0.21	0.00	0.00	0.00	0.00
Configuration & Setting	0.48	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.21	0.00	0.00	0.00
Wireless Connection	0.00	0.31	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.48	0.00	0.00	0.00
PR	0.00	0.00	0.15	0.00	0.00
Customer Serv.	0.00	0.00	0.29	0.00	0.00
System Admin	0.00	0.00	0.56	0.00	0.00
Websites	0.00	0.00	0.00	0.80	0.00
Emails	0.00	0.00	0.00	0.20	0.00
Procedures	0.00	0.00	0.00	0.00	0.35
Regulations	0.00	0.00	0.00	0.00	0.42
Contingency Plan	0.00	0.00	0.00	0.00	0.23
Inconsistency	0.00	0.00	0.00	0.00	0.00

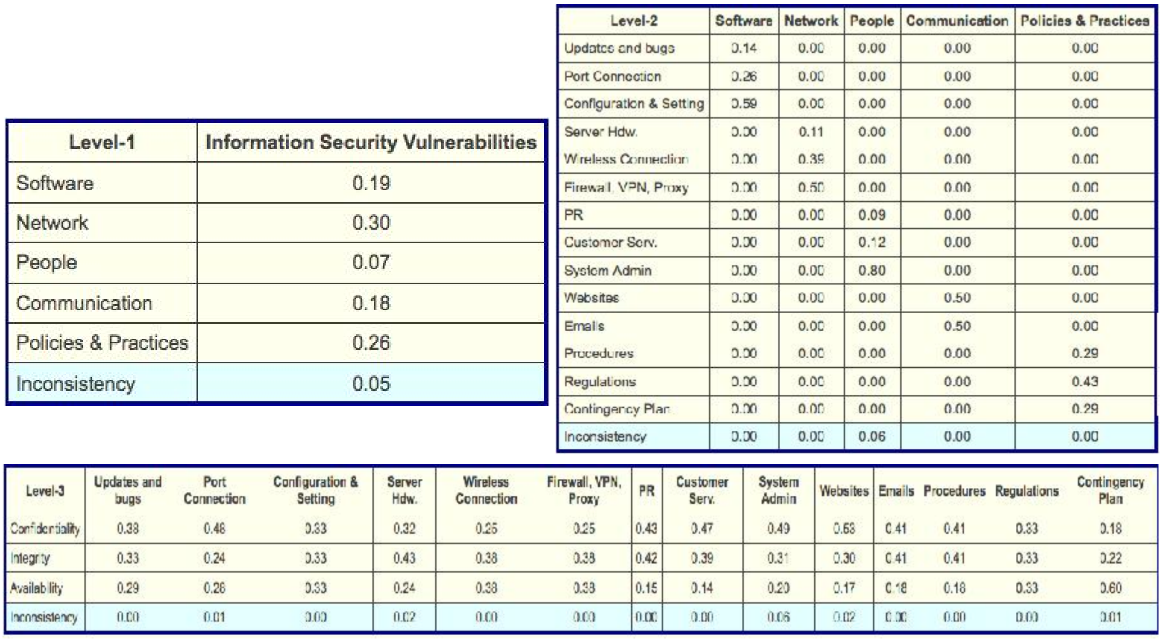
Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.17	0.49	0.33	0.33	0.19	0.19	0.19	0.19	0.19	0.19	0.21	0.19	0.16	0.33
Integrity	0.19	0.07	0.33	0.33	0.47	0.47	0.47	0.47	0.47	0.47	0.48	0.34	0.30	0.33
Availability	0.54	0.44	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.33	0.31	0.47	0.54	0.33
Inconsistency	0.06	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.07	0.00	0.00

Figure 7: Expert 3 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.22
Integrity	0.40
Availability	0.38
Inconsistency	0.01

Figure 8: Expert 3 Final Results

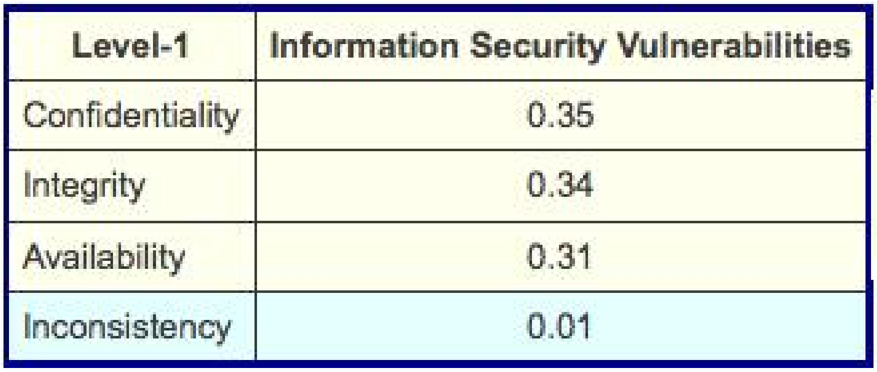


Level-1	Information Security Vulnerabilities
Software	0.19
Network	0.30
People	0.07
Communication	0.18
Policies & Practices	0.26
Inconsistency	0.05

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.14	0.00	0.00	0.00	0.00
Port Connection	0.26	0.00	0.00	0.00	0.00
Configuration & Setting	0.59	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.11	0.00	0.00	0.00
Wireless Connection	0.00	0.39	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.50	0.00	0.00	0.00
PR	0.00	0.00	0.09	0.00	0.00
Customer Serv.	0.00	0.00	0.12	0.00	0.00
System Admin	0.00	0.00	0.80	0.00	0.00
Websites	0.00	0.00	0.00	0.50	0.00
Emails	0.00	0.00	0.00	0.50	0.00
Procedures	0.00	0.00	0.00	0.00	0.29
Regulations	0.00	0.00	0.00	0.00	0.43
Contingency Plan	0.00	0.00	0.00	0.00	0.29
Inconsistency	0.00	0.00	0.06	0.00	0.00

Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.38	0.48	0.33	0.32	0.25	0.25	0.43	0.47	0.49	0.53	0.41	0.41	0.33	0.18
Integrity	0.33	0.24	0.33	0.43	0.38	0.38	0.42	0.39	0.31	0.30	0.41	0.41	0.33	0.22
Availability	0.29	0.28	0.33	0.24	0.38	0.38	0.15	0.14	0.20	0.17	0.18	0.18	0.33	0.60
Inconsistency	0.00	0.01	0.00	0.02	0.00	0.00	0.00	0.00	0.06	0.02	0.00	0.00	0.00	0.01

Figure 9: Expert 4 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.35
Integrity	0.34
Availability	0.31
Inconsistency	0.01

Figure 10: Expert 4 Final Results

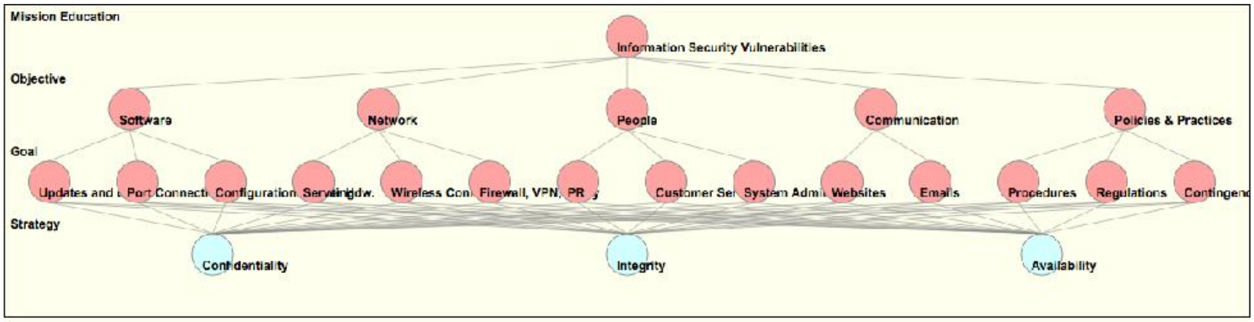
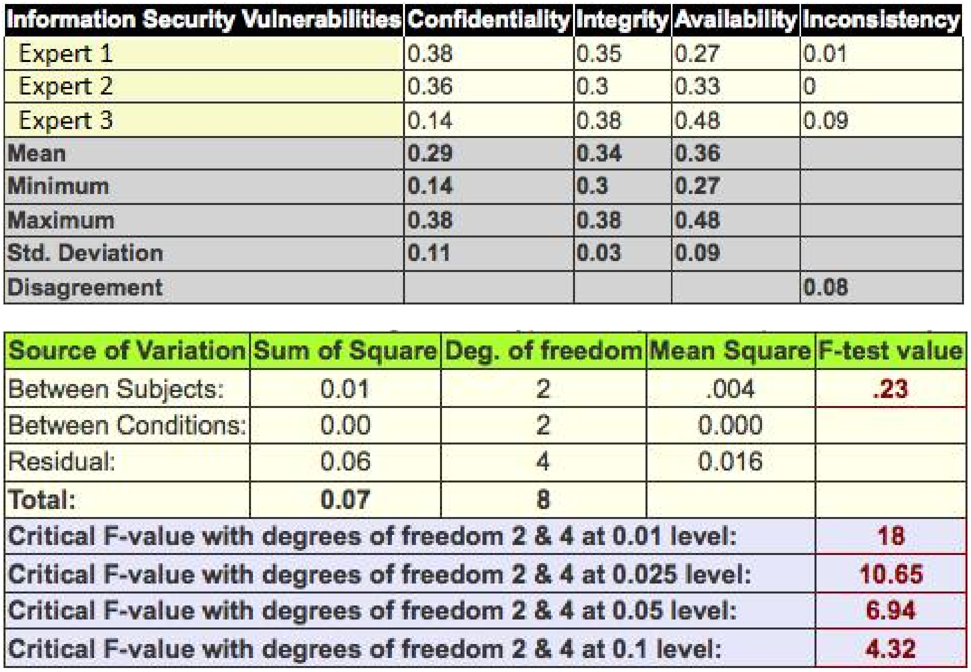


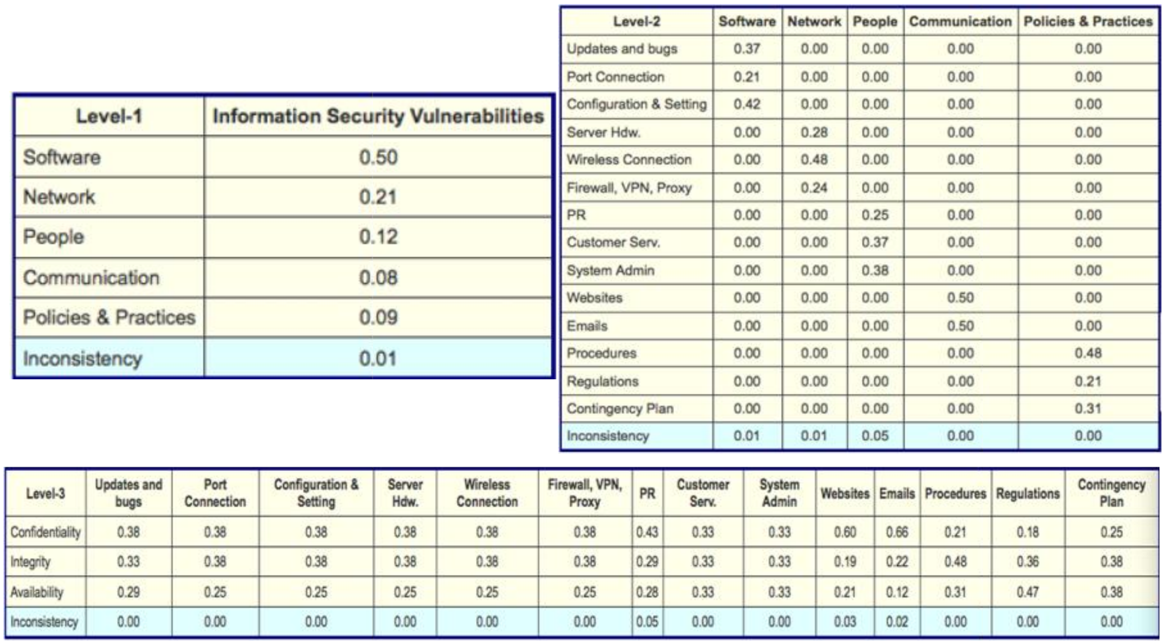
Figure 11: Education Sector HDM



Information Security Vulnerabilities	Confidentiality	Integrity	Availability	Inconsistency
Expert 1	0.38	0.35	0.27	0.01
Expert 2	0.36	0.3	0.33	0
Expert 3	0.14	0.38	0.48	0.09
Mean	**0.29**	**0.34**	**0.36**	
Minimum	**0.14**	**0.3**	**0.27**	
Maximum	**0.38**	**0.38**	**0.48**	
Std. Deviation	**0.11**	**0.03**	**0.09**	
Disagreement				**0.08**

Source of Variation	Sum of Square	Deg. of freedom	Mean Square	F-test value
Between Subjects:	0.01	2	.004	**.23**
Between Conditions:	0.00	2	0.000	
Residual:	0.06	4	0.016	
Total:	**0.07**	**8**		
Critical F-value with degrees of freedom 2 & 4 at 0.01 level:				**18**
Critical F-value with degrees of freedom 2 & 4 at 0.025 level:				**10.65**
Critical F-value with degrees of freedom 2 & 4 at 0.05 level:				**6.94**
Critical F-value with degrees of freedom 2 & 4 at 0.1 level:				**4.32**

Figure 12: Figure 2: The Overall HDM Results – Education Sector

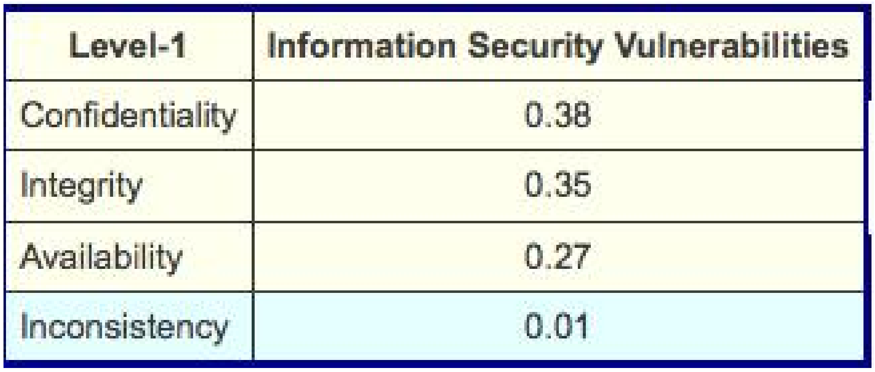


Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.37	0.00	0.00	0.00	0.00
Port Connection	0.21	0.00	0.00	0.00	0.00
Configuration & Setting	0.42	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.28	0.00	0.00	0.00
Wireless Connection	0.00	0.48	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.24	0.00	0.00	0.00
PR	0.00	0.00	0.25	0.00	0.00
Customer Serv.	0.00	0.00	0.37	0.00	0.00
System Admin	0.00	0.00	0.38	0.00	0.00
Websites	0.00	0.00	0.00	0.50	0.00
Emails	0.00	0.00	0.00	0.50	0.00
Procedures	0.00	0.00	0.00	0.00	0.48
Regulations	0.00	0.00	0.00	0.00	0.21
Contingency Plan	0.00	0.00	0.00	0.00	0.31
Inconsistency	0.01	0.01	0.05	0.00	0.00

Level-1	Information Security Vulnerabilities
Software	0.50
Network	0.21
People	0.12
Communication	0.08
Policies & Practices	0.09
Inconsistency	0.01

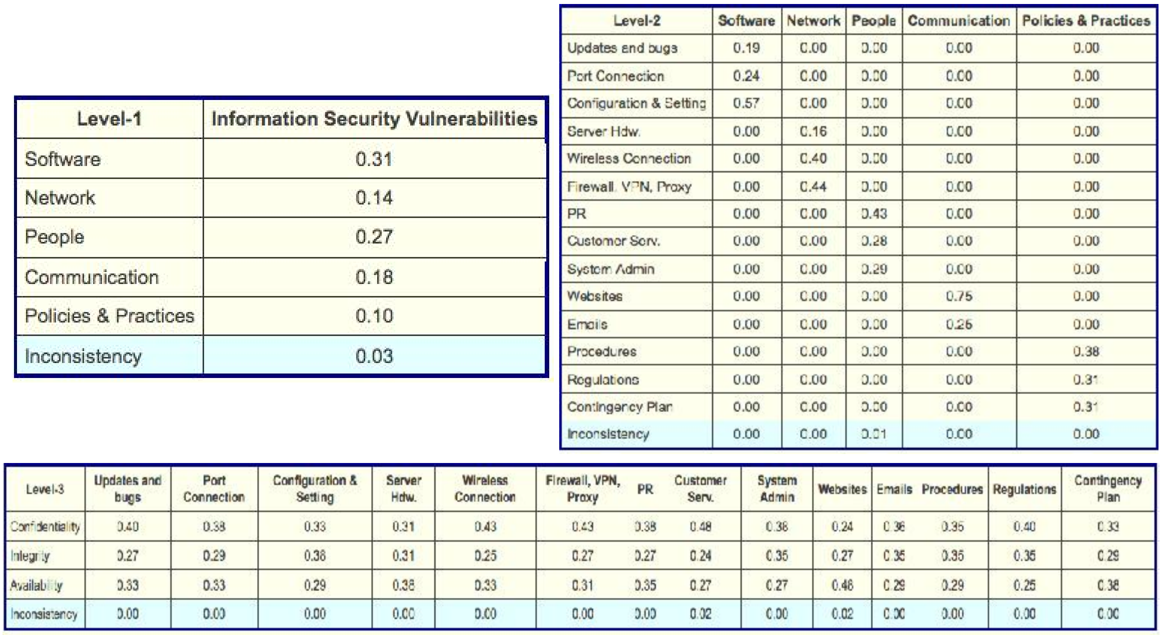
Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.38	0.38	0.38	0.38	0.38	0.38	0.43	0.33	0.33	0.60	0.66	0.21	0.18	0.25
Integrity	0.33	0.38	0.38	0.38	0.38	0.38	0.29	0.33	0.33	0.19	0.22	0.48	0.36	0.38
Availability	0.29	0.25	0.25	0.25	0.25	0.25	0.28	0.33	0.33	0.21	0.12	0.31	0.47	0.38
Inconsistency	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.00	0.00	0.03	0.02	0.00	0.00	0.00

Figure 13: Expert 1 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.38
Integrity	0.35
Availability	0.27
Inconsistency	0.01

Figure 14: Expert 1 Final Results

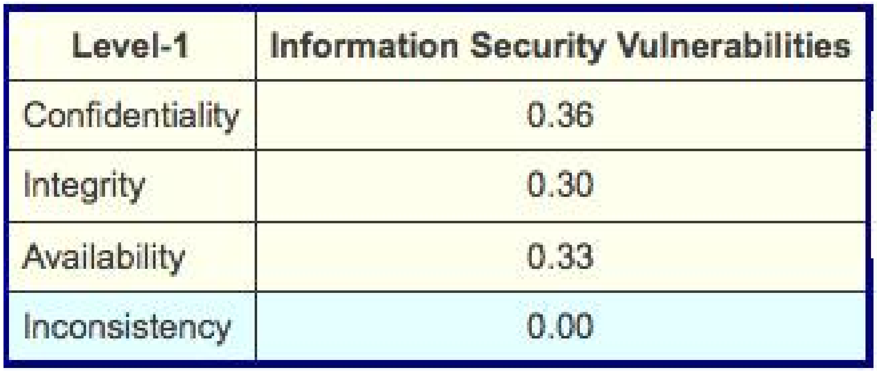


Level-1	Information Security Vulnerabilities
Software	0.31
Network	0.14
People	0.27
Communication	0.18
Policies & Practices	0.10
Inconsistency	0.03

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.19	0.00	0.00	0.00	0.00
Port Connection	0.24	0.00	0.00	0.00	0.00
Configuration & Setting	0.57	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.16	0.00	0.00	0.00
Wireless Connection	0.00	0.40	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.44	0.00	0.00	0.00
PR	0.00	0.00	0.43	0.00	0.00
Customer Serv.	0.00	0.00	0.28	0.00	0.00
System Admin	0.00	0.00	0.29	0.00	0.00
Websites	0.00	0.00	0.00	0.75	0.00
Emails	0.00	0.00	0.00	0.26	0.00
Procedures	0.00	0.00	0.00	0.00	0.38
Regulations	0.00	0.00	0.00	0.00	0.31
Contingency Plan	0.00	0.00	0.00	0.00	0.31
Inconsistency	0.00	0.00	0.01	0.00	0.00

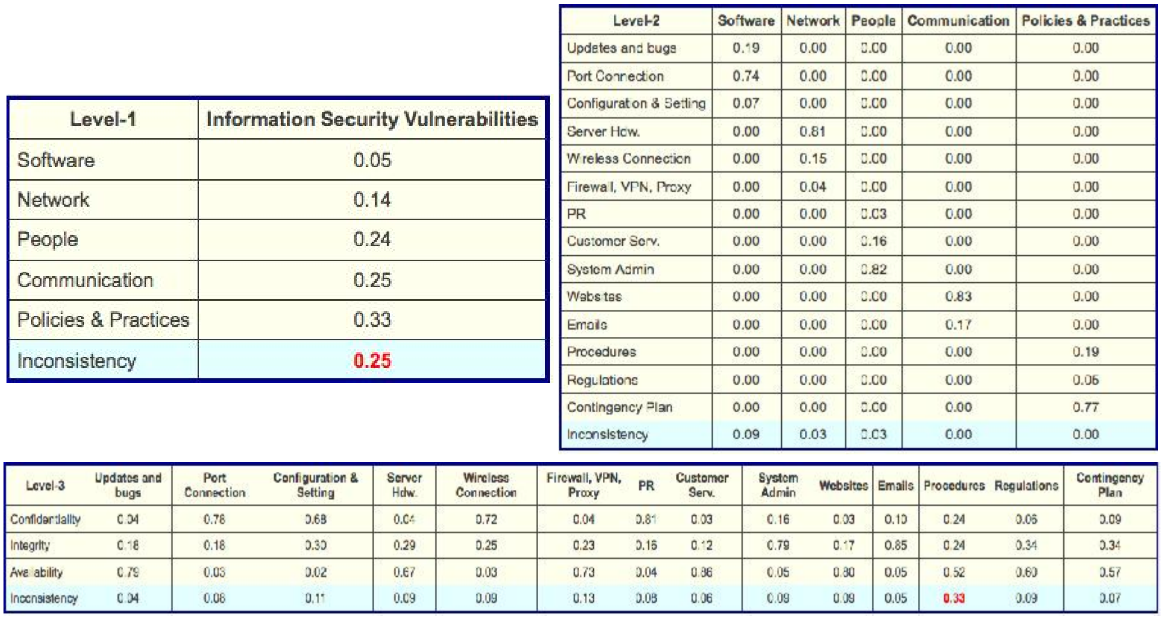
Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.40	0.38	0.33	0.31	0.43	0.43	0.38	0.48	0.38	0.24	0.36	0.35	0.40	0.33
Integrity	0.27	0.29	0.38	0.31	0.25	0.27	0.27	0.24	0.35	0.27	0.35	0.35	0.35	0.29
Availability	0.33	0.33	0.29	0.38	0.33	0.31	0.35	0.27	0.27	0.46	0.29	0.29	0.25	0.38
Inconsistency	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	0.02	0.00	0.00	0.00	0.00

Figure 15: Expert 2 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.36
Integrity	0.30
Availability	0.33
Inconsistency	0.00

Figure 16: Expert 2 Final Results

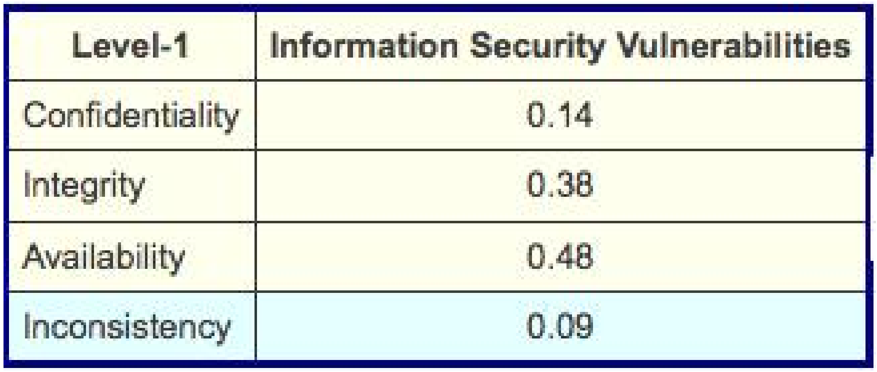


Level-1	Information Security Vulnerabilities
Software	0.05
Network	0.14
People	0.24
Communication	0.25
Policies & Practices	0.33
Inconsistency	0.25

Level-2	Software	Network	People	Communication	Policies & Practices
Updates and bugs	0.19	0.00	0.00	0.00	0.00
Port Connection	0.74	0.00	0.00	0.00	0.00
Configuration & Setting	0.07	0.00	0.00	0.00	0.00
Server Hdw.	0.00	0.81	0.00	0.00	0.00
Wireless Connection	0.00	0.15	0.00	0.00	0.00
Firewall, VPN, Proxy	0.00	0.04	0.00	0.00	0.00
PR	0.00	0.00	0.03	0.00	0.00
Customer Serv.	0.00	0.00	0.16	0.00	0.00
System Admin	0.00	0.00	0.82	0.00	0.00
Websites	0.00	0.00	0.00	0.83	0.00
Emails	0.00	0.00	0.00	0.17	0.00
Procedures	0.00	0.00	0.00	0.00	0.19
Regulations	0.00	0.00	0.00	0.00	0.05
Contingency Plan	0.00	0.00	0.00	0.00	0.77
Inconsistency	0.09	0.03	0.03	0.00	0.00

Level-3	Updates and bugs	Port Connection	Configuration & Setting	Server Hdw.	Wireless Connection	Firewall, VPN, Proxy	PR	Customer Serv.	System Admin	Websites	Emails	Procedures	Regulations	Contingency Plan
Confidentiality	0.04	0.76	0.68	0.04	0.72	0.04	0.81	0.03	0.16	0.03	0.10	0.24	0.06	0.09
Integrity	0.18	0.18	0.30	0.29	0.25	0.23	0.16	0.12	0.79	0.17	0.85	0.24	0.34	0.34
Availability	0.79	0.03	0.02	0.67	0.03	0.73	0.04	0.86	0.05	0.80	0.05	0.52	0.60	0.57
Inconsistency	0.04	0.06	0.11	0.09	0.09	0.13	0.08	0.06	0.09	0.09	0.05	0.33	0.09	0.07

Figure 17: Expert 3 Results



Level-1	Information Security Vulnerabilities
Confidentiality	0.14
Integrity	0.38
Availability	0.48
Inconsistency	0.09

Figure 18: Expert 3 Final Results

HDM Instructions

The HDM compares two given nodes, one pitted against the other, and assigns a total weight that cannot exceed 100. This is based on 0 to 100 weighting / point system.

Each node has a unique name for comparison, such as “Software” and “Network”. If you have any questions as to what a given node means, mouse over the node (circle) for a more detailed explanation.

Level 1 and 2

The first and second level is a straight comparison against each categorical node and can be done fairly quickly. To start the HDM, please begin with the very top node, “Information Security Vulnerabilities”, then continue by clicking on “Save & Go to the Next Node”.

Ranking Example: *If you feel Node A is 50% “greater” than Node B, you would score that as: Node A=60 and Node B=40. Conversely, if you feel Node A is 3 times greater than node B, you would score that as Node A=75 and Node B=25.*

Level 3 and 4

The third and fourth level will be slightly more complex and requires a little more time to complete. The comparison again is in sets of two, but the weighted comparison will be in regards to the variation of subjects under investigation.
Example:
In regards to ***'x'*** *Node A = 30 to Node B = 70*
In regards to ***'y'*** *Node A = 20 to Node B = 80*
In regards to ***'z'*** *Node A = 10 to Node B = 90*
The comparison may seem repetitive because of the comparison of same node sets under different subject of investigation.

Please note that each comparison is unique and your weightings are critical to final result of the model and the research.

For all sets of comparison, please indicate your assigned weighting based on your knowledge and personal experience with respect to information and IT security.

The set of pairwise weighting will specifically identify which of the two nodes you think is of greater priority, conversely, the other representing the lessor priority; that is less prone to system vulnerabilities. The one node with **more vulnerabilities** is prioritized with a **greater weight**.
Example:
In regards to “Confidentiality”, Email = 80 and Websites = 20.

This will be interpreted that you feel Email requires a substantially higher level of security because it is more vulnerable compared to Websites, as it relates to Confidentiality, therefore the weight is greater.

Introductory Email

Dear Mr. Expert,

By way of introduction, my name is Greg Wease, and I am a graduate student in the Engineering & Technology Mgmt. department at Portland State University. The course my teammates and I are taking is Technology Synthesis and the class project is to rank “Information Security Vulnerabilities”. This does not necessarily have to reflect your company’s perspective, simply your personal view.

Based on your role at IBM, we thought you would be a great candidate to get your feedback. If you have 10-15 minutes, responses to the following questionnaire will help us better understand the value behind Information Security technologies. If you like, we would be happy to share the overall results once compiled.

Attached are the HDM instructions, and the following link will start the online questionnaire.http://research1.etm.pdx.edu/hdm2/expert.aspx?id=d671c788dcbb7792/98b2fb8d2cd003fc

Thank you in advance for your time and consideration.

Greg Wease

cc: Chris Perrenoc, RachanidaKoosawangsri, ThanapornNgarmnil,