ISAA Theory DA-II

by Sharadindu Adhikari | 19BCE2105

INDEX

A. Question 1

B. Solution 2

1. Introduction to Information Security (IS) revolving around Universities 2
2. Basic Review 2
3. Organizational IS Case Studies summarised ... 4
4. Mainframe : Security Threats & characteristics ... 5
5. Information Security Policies for University ... 9
6. Best practices to drafting ISPs 12
7. ISP Awareness & Compliances 15
8. Conclusion 16

Question :

Take a case study of developing security policies to ensure the protection of your University information from unauthorized access, loss or damage while supporting the information security needs of the University. Develop ISPs including all the components to make the policy to work effectively. Discuss the best practices for drafting the policies.

ISAA Theory DA - II

F2 | Fall 2021

by Sharadindu Adhikari | 19BCE2105

Information security (IS) remains one of the critical concerns for modern organisations. Organisational information and data must be protected from both active and passive attacks. Every organisation should secure data from illegal access, unwanted interruption, unauthorized alteration or data annihilation. IS empaharises confidentiality, integrity and availability of data, which play vital roles in securing organisational data and should be properly implemented. However, in many organisations, people unconsciously disrupt these IS policies (ISPs) due to lack of awareness about related terms and conditions, which higtens the risk of IS attacks.

This work assignment focuses on exploring the Information Security Policies at an educational institution (here, my University), as well as user awareness and compliance with such policies.

◉ Basic Review :

1. Information Security (IS) : Properly implemented IS not only plays a vital role in security University data, but also provides methods for data storage. With growing demand for IS, many experts have stressed the importance of eliminating weaknesses, which

are apparent in many University settings. Such weaknesses appear when people unconsciously disrupt ISPs, due to lack of awareness about related terms and conditions, resulting in socially, economically and physiologically questionable actions.

2. Threats to Information Security :

An University must address all possible human errors while writing ISPs, because such errors can be critical if not handled competently. Major issues/causes of the occurence of human errors include lack of knowledge or skills related to IS. As such, it is essential to introduce ISPs to all stakeholders, including end-users of an University to ensure compliant behaviour.

3. Information Security Policy :

ISPs ensures appropriate behaviour among employees by providing clear instruction of responsibilities to follow terms and conditions of such policies. Clear and practical ISPs help Universities improve IS programmes. After designing and developing an ISP, any variances must be frequently under observation and addressed that may arise in IS assets.

Organisational IS Case studies I've studied :

Manuscripts	Context	Methodology	Key Findings
1. Doughty (2003)	Information security in a medium size organisation	Gap analysis	Implementation of an enterprise security framework is must
2. Khalfan (2004)	IT outsourcing projects of public & private sector organizations in Kuwait	Questionnaire Survey & Interviews	IS risk outdo other project outsourcing concern like loss of control
3. Zakaria (2004)	IS culture challenges in a public sector organization in Malaysia	Reviews of IS documents	Research design on security culture — Identifying employees' IS behaviour
4. Harnes and Lindstrom (2011)	Analysing security behaviours in a public nursing centre	Interviews	Discipline and agility play vital role in shaping security behaviour
5. Parsons, McCormac, Pattinson (2014)	IS vulnerabilities in 3 Australian Govt. organizations	Web-based Questionnaire Survey	Key information security awareness concerns include wireless security, social media and reporting of security incidents.

Main frame:

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations — large and small must create a comprehensive security program to cover both challenges.

Without an ISP, it is impossible to coordinate and enforce a security program across an organization, nor is it possible to communicate security measures to the 3rd parties and external auditors.

Few characteristics make a security policy effivient:

1. It should cover security from end to end across the organisation.
2. Be enforceable and practical.
3. Have space for revision and updates.
4. Be focused on buriness goals of the organization
5. It should establish a general approach to IS.
6. Detect and minimize the impact of compromised information assets, such as misuse of data, networks, mobile devices, computers and application.
7. Document security measures and users accen control policies.

Our University (VIT Vellore) will create an IS policy to ensure the employees and other users follow security protocols and procedures. An updated and current security policy for the University will ensure that sensitive information can only be accessed by authorised users.

Importance of an ISP are creating an effective security policy & taking steps to ensure compliance is a critical step to prevent and mitigate security breaches.

To make University's security policy truly effective, update it in response to change in the University, new threats, conclusions drawn from previous breaches and other changes to the security postures.

The main aim of the University is that its ISP should be practical and enforceable. It should have an exception system in place to accomodate requirements and urgencies that arise from different parts of the organization.

□ A security policy for the University can be as broad as we want it to be, from everything related to IT security and the security of related physical assets, but enforceable in its full scope.

Before implementing security policy for the University, following points must be taken into consideration:

1. Purpose:

The University must state the purpose of its policy which may be to create an overall approach to IS. It should detect and preempt IS breaches. IT should maintain the reputation of the University and uphold the ethical and legal responsibility.

2. Audience:

It is a critical factor that the University, before developing security policies, must take into consideration the audience to whom this security policy needs to be applied. One can also specify which audiences are out of the ~~of~~ scope of the policy.

3. Taking objectives into consideration :

It focuses on 3 main objectives :

a) Confidentiality :

Only individuals with authorization can and should be able to access data and information assets.

b) Integrity :

Data should be intact, accurate and complete, and IT systems must be kept operational.

c) Availability :

Users should be able to access information or systems when needed.

IT policies ensure that everyone's use of the University's Computing and Telecommunication resources support its educational, research and administrative mission in the best possible way.

⑩ Information security policies (in development) for University :—

1. Inorder to manage IS risks, University must ensure that their actions wrt to Data and IT Resources and their electronic devices and other resources that store, transmit or procers Data meet all the Information Security standards policy.

2. Failure to comply with the policies & its IS standards may result in denied accers to IT resources & disciplinary action.

3. Data must be properly classified, labelled and handled.

4. Authorized accers to and possession, use and modification of Data must be provided.

5. It is important to maintain a risk management strategy, which includes, but is not limited to periodic assessment and reporting, must be developed and maintained.

6. For our University [VIT Vellore] an information security plan, which includes, but not limited to, aniging appropriate security roles and resources; must be developed and maintained.

7. Account Management. The purpose of this policy is to establish a standard for the creation, administration, use and removal of accounts that facilitate access to information and technology resources at the company.

8. Clean Desk Policy. The purpose of this policy is to ensure that confidential data is not exposed to individuals who may pass through the area such as staff, faculties, students, other service personnel, etc.

9. Firewall Policy. This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to the University's Network and Information systems.

10. Log Management Policy. It can be of great benefit to many scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance.

11. Cloud Computing Adoption. The purpose of this policy is to ensure that the University can potentially make appropriate cloud adoption decisions & at the same time does not use, or allow the use of, inappropriate cloud service practices.

12. Server Security policy. The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on the University's internal network(s) or related technology resources via any means.

13. Vulnerability Assesment. The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects the University's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable & appropriate levels.

14. IOT policy. The purpose of this policy is to define IoT structure & operations to ensure that data is properly secured.

15. Periodic assesments of all security policies or otherwise must be performed to comply with the policy and all pertinent laws.

With all that being said, below are some of the best practices for drafting the Information Security Policies:

1. Information and data classification:

Data classification is generally outlined because the method of organizing information by relevant classes in order that it's going to be used and guarded a lot of with efficiency. On a basic level, the classification method makes information easier to find and retrieve. Data classification is of explicit importance once it involves risk management, compliance, and data security.

Data classification involves tagging information to form it simply searchable and traceable. It additionally eliminates multiple duplications of information, which might cut back storage and backup prices whereas rushing up the search method.

2. IT operations and administration:

IT operations is that overarching term for the processes and services administered by University's data tech department. As such, IT operations embrace body processes with support for hardware and software system. Vital roles of the IT operations team embrace technical school school management, quality assurance, infrastructure management,

and confirmation that finished product meet all the customer's desires and expectations. IT operations support each internal and external purchasers.

3. Security response plan : A cybersecurity incidence response arrange (or IR plan) could be a set of directions designed to assist firms insure, detect, respond to, and endure network security incidents. Most IR plans are technology-centric and address problems like malware detection, information thievery and repair outages.

4. SaaS and Cloud policy : Software-as-a-service (SaaS) is an on-demand, cloud based software package delivery model that allows Universities to purchase the applications they have while not hosting them in house.

5. Acceptable use policies (AUPs) : An AUP could be a document stipulating constraints. It lets IT administrators authorize systems and applications to the right individuals and let employees, University staffs know how to use and authorize/create passwords in a secure way.

6. Identity and access management (IAM) regulations : It helps prevent data breaches that occur through misuse of University resources. Transparent IAMs help keep all personnel in line with the proper use of university technology resources. A simple password policy can reduce identity and access risks.

7. Data security policy : It outlines the technical operations of the organization and acceptable use standards in accordance with the Payment Card Industry Data Security Standard (PCI DSS) compliance. The policy conjointly has to explain the roles and functions within the information protection method, like the responsibilities of the info protection officer (DPO) for GDPR compliance.

8. Privacy regulations : The privacy regulations protect all individually acknowledgeable health information control or transmitted by a lined entity or its business associate, in any kind or media, whether or not electronic, paper, or oral. The privacy rule calls this info "protected health info (PHI)". Goverment enforced regulations such as the GDPR protect the privacy of end users. Universities that don't protect the privacy of their users, risk losing their authority & may be fined, heavily.

9. Personal and mobile devices : Nowadays most organizations, including Universities have moved their data to the cloud. Companies that encourage employees to access company software assets from any location, risk introducing vulnerabilities through personal devices, such as laptops and smartphones. Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.

10. Remote Access Policy: It may be a document that outlines and defines acceptable ways of remotely connecting to the inner network. It is essential in big Universities like VIT, wherever networks square measure geographically distributed and extend into insecure network locations like public networks or unmanaged home networks.

Information Security Policies' Awareness and Compliances:

The role of IT managers in Universities is to maintain the IT infrastructure and ensure the quality of IT services. Most managers however have a common notion regarding compliances, which reads as, "I don't know much about the ISP, but I'm sure we've an IS policy developed by our IT main office, but I couldn't comment on it or its usability as I've not accessed it yet.". Occasionally the main IT office send warnings via email that includes sections of its ISP to inform users might of the policy or to resolve an ISP issue. Most managers agree that to avoid violating any ISP, they must be thoroughly verbatim. In order to do so, they agree that there's a need to include important information for users about appropriate use of email and internet as well as other related IT systems in the institution's ISP. They also want ISP to include a practical guide on how to use IT infrastructure in a secure manner.

⑩ Conclusion :

In this assignment work I've examined factors that impact violations of information security measures by utilizing deterrence theory and organizational justice theory in India's higher educational University. The results indicate that procedural justice, distributive justice, severity and celerity of sanction, organizational security culture, privacy, and responsibility toward information security were significant factors in predicting the violations of IS measures in University education.

Security breaches that are both accidental and deliberate continue to occur in industry. These findings validate past research, at least as they relate to Indian Universities, and should encourage managers to ensure employees are involved with developing and implementing IS measures if it fits within the organizational culture. Additionally, the IS measures should be applied consistently and in a timely manner. The importance of IS should be grounded in University culture. Employees should have a strong sense of treating University data as they would want their own data to be treated.