Assignment

Faculty Name:	Information Technology
Module Code:	ITSC311
Module Name:	Social Practices and Security
Module Leader:	Dr Timothy Adeliyi
Copy Editor:	Mr Kevin Levy
Total Marks:	100
Submission Date:	16/03/2020 – 20/03/2020

This module is presented on NQF level 7.

Mark deduction of 5% per day will be applied to late submission, up to a maximum of three days. Assignments submitted later than three days after the deadline or not submitted will get 0%. [1]

This is an individual assignment.

This assignment contributes 20% towards the final mark.

Instructions to Student

1. Remember to keep a copy of all submitted assignments.
2. All work must be typed.
3. Please note that you will be evaluated on your writing skills in all your assignments.
4. All work must be submitted through Turnitin[2] and the full Originality Report should be attached to the final assignment. Negative marking will be applied if you are found guilty of plagiarism, poor writing skills or if you have applied incorrect or insufficient referencing. (See the table at the end of this document where the application of negative marking is explained.)

[1] Under no circumstances will assignments be accepted for marking after the assignments of other students have been marked and returned to the students.

[2] Refer to the PIHE Policy for Intellectual Property, Copyright and Plagiarism Infringement, which is available on *my*LMS.

5. Each assignment must include a cover page, table of contents and full bibliography, based on the referencing method applicable to your faculty as applied at Pearson Institute of Higher Education.
6. Use the cover sheet template[3] for the assignment; this is available from your lecturer.
7. Students are not allowed to offer their work for sale or to purchase the work of other students. This includes the use of professional assignment writers and websites, such as Essay Box. If this should happen, Pearson Institute of Higher Education reserves the right not to accept future submissions from a student.

Assignment Format

Students must follow the requirements when writing and submitting assignments as follows:

- Use Arial, font size 10.
- Include page numbers.
- Include a title page.
- Print submissions on both sides of the page.
- Write no more than the maximum word limit.
- Ensure any diagrams, screenshots and PowerPoint presentations fit correctly on the page and are referenced.
- Include a table of contents.
- Use the accurate referencing method throughout the assignment.
- Include a bibliography based on the applicable referencing method at the end of the assignment.
- Include the completed the Assessment/Project Coversheet (available on *my*LMS).
- Check spelling, grammar and punctuation.
- Run the assignment through Turnitin software.

Essential Embedded Knowledge and Skills Required of Students

- Report-writing skills
- Ability to analyse scenarios/case studies
- Understanding of subject field concepts and definitions
- Ability to apply theoretical knowledge to propose solutions to real-world problems
- Referencing skills

[3] Available on *my*LMS.

Resource Requirements

- A device with Internet access for research
- A desktop or personal computer for typing assignments
- Access to a library or resource centre
- Prescribed reading resources

Delivery Requirements (evidence to be presented by students)

- A typed assignment[4]
- A Turnitin Originality Report

Minimum Reference Requirements

At least five references for first year, ten references for second year and fifteen references for third year.

Additional reading is required to complete this assignment successfully. You need to include the following additional information sources:

- Printed textbooks/e-books
- Printed/online journal articles
- Academic journals in electronic format accessed via PROQUEST or other databases
- Periodical articles e.g. business magazine articles
- Information or articles from relevant websites
- Other information sources e.g. geographic information (maps), census reports, interviews

Note
• It is crucial that students reference all consulted information sources, by means of in-text referencing and a bibliography, according to the applicable referencing method. • Negative marking will be applied if a student commits plagiarism i.e. using information from information sources without acknowledgement and reference to the original source. • In such cases, negative marking, also known as 'penalty scoring', refers to the practice of subtracting marks for insufficient/incorrect referencing. • Consult the table at the end of this document, which outlines how negative marking will be applied as well as the way in which it will affect the assignment mark.

[4] Refer to the Conditions of Enrolment for more guidance (available on *my*LMS).

Section A

Learning Objective

Evaluate the enterprise systems used within functional areas of the organisation and evaluate specialised Information Systems that can be applied in organisations.

Assignment Topic

Enterprise Systems

Scope

The scope of this assignment is centred on week 1 – 7. Resources needed to accomplish this are the prescribed textbook and relevant materials that are available on the web.

Question 1 30 Marks

Study the scenario and complete the question(s) that follow:

City of Johannesburg Security Breach

The City of Johannesburg says security experts are investigating the security breach which is expected to last over 24 hours. They have warned the general public that due to a network breach several of its online systems, including its website, e-services and billing system have been shut down for 24-hours.

In a Tweet, the City of Johannesburg says security experts are investigating the incident, which is expected to last 24 hours. It has requested that any queries be directed to the city's call centre or that residents keep an eye on their Twitter updates. Meanwhile, it has been reported that the hack occurred at the same time on Thursday that several banks also reported internet problems, believed to be related to cyber-attacks. According to Business Live, the group is called the Shadow Kill Hackers. They have reportedly demanded the payment of four bitcoins by October 28 and have threatened to upload all the data onto the internet if the banks fail to comply.

Source: http://www.sabcnews.com/sabcnews/city-of-joburgs-online-systems-shut-down-due-to-security-breech/. (Accessed- 13 January 2020)

1.1 Identify and justify what approach to information security you would implement to protect further attack to the City of Johannesburg's online systems. (7 Marks)

1.2 It is the responsibility of the City of Johannesburg to ensure that they implement relevant laws to ensure that the hackers that caused security breaches are prosecuted. Identify and explain two laws that the City of Johannesburg can use to prosecute attackers on their online systems (6 Marks)

1.3 Identify and justify if the above scenario can be regarded as an incident or disaster. (3 Marks)

1.4 Mitigation control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. Explain the mitigation procedure plan that you will advise the City of Johannesburg to implement for your response in Question 1.3.

(8 Marks)

1.5 Identify and briefly describe three business continuity strategy sites that the City of Johannesburg's chief information officer can implement. (6 Marks)

[Sub Total 30 Marks]

End of Question 1

Question 2 55 Marks

Data Security Deficiencies in South Africa

The speed of technological change is leaving gaping holes in highly sensitive company IT infrastructure. These vulnerabilities are being targeted by cybercriminals at an increasing rate as South Africa is starting to feel the heat from attackers across the globe.

It was revealed at the 2015 Security Summit, in Johannesburg, that South Africa is the most attacked country on the African continent over the past six weeks.

Vernon Fryer, Chief Technology Security Officer at Vodacom, presented alarming statistics from the Vodacom Cyber Intelligence Centre revealing a 150% increase in the number of DDoS attacks in the last 18 months in Africa. These attacks occur where multiple compromised systems, usually infected with a Trojan, are used to target a single system causing valuable downtime to assets like websites.

Symantec’s Antonio Forzieri says that one in 214 emails sent in South Africa last year was a spear fishing attack. Don’t let the exotic naming fool you. These attacks can cause serious personal distress, financial loss and are achieved by the simple click of a malicious link in an email. Interestingly, the effectiveness of a spear fishing attack rises from three to 70% when private personal info is included. “Most times this information is accessed easily online or hacked through open source websites,” says Ignus Swart from the Council for Scientific and Industrial Research.

It is very unfortunate that businesses in South Africa won't take a new local data privacy law seriously until there’s a high-profile hacking breach in the country. This is according to Nader Henein, who is the Regional Director for Product Security at BlackBerry in the Middle East and Africa.

This law restricts how companies handle personal data to safeguard individuals from security breaches. The law is intended to close the gap between South Africa and the likes of Europe with regard to data privacy laws. However, Fin24 has previously reported on how adoption of the law is sluggish among local companies.

According to research from Trustwave, 51% of South African companies have not made a significant effort to comply with the legislation. And BlackBerry's Henein, who is in Johannesburg for this week's IDC CIO Summit, told Fin24 that full adoption of the new law could only be spurred on by public hack attacks. He said that the likes of big banks in the country are currently adopting the law but other businesses still have a way to go.

"Breaches are not yet very public," Henein told Fin24. "It's not going to really grab hold with a lot of companies until you start seeing companies getting fined." And then it starts ringing true with members of the board and the C-level," he said. South Africa is still in the process of appointing a regulator to look over the implementation of this new law. But once a regulator is established, companies that experience cyber breaches could face heavy fines.

Source: https://www.payu.co.za/press-room/sa-companies-under-cyberattack (Accessed- 13 January 2020)

According to the article, Africa has seen a 150% increase in the number of distributed denial of service (DDoS) attacks since 2015, and South Africa is one of the most attacked countries on the African continent.

2.1 Explain Distributed Denial of Service (DDoS) attacks in detail. Explain further how DDoS differs from Denial of Service (DOS) attacks. (9 Marks)

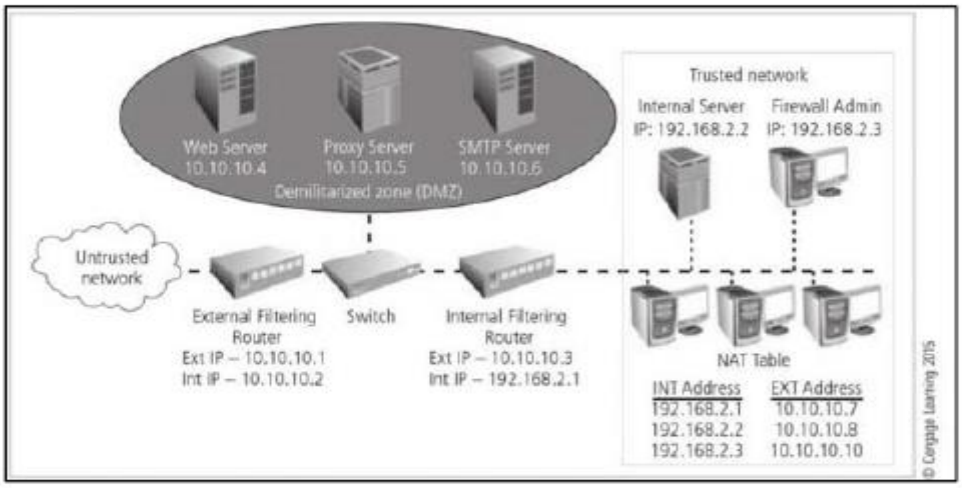
2.2 How can you prevent or stop a DDoS attack? Highlight the steps that should be followed in such an event. (15 Marks)

2.3 You have been hired as a security specialist by an organisation that has fallen prey to a recent cyber-attack. When analysing the organisation's systems, you realise that the company does not have a defence strategy in place to prevent unauthorised access to its systems. Describe and analyse two commonly used security strategies. In your answer, also explain the practical implementation of each strategy. (25 Marks)

2.4 In what ways are these strategies similar and different from each other? What is their relationship? (6 Marks)

End of Question 2

Question 3 15 Marks



To implement the architecture specified above, Alice the IT Director decided to secretly talk to Bob the Chief Financial Officer (CFO) in the organisation so that he can make the necessary funds available. She wants to keep the message secret and Bob should be the only one who should be able to read the message. During lunch she texted Bob the key that he should use to decrypt the message and this key is the same as the one that she used to encrypt.

Source: Whitman, M.E. and Mattord, H.J., 2015. Principles of information security. London: Cengage Learning.

Suppose Alice sent the following message to Bob: ‘I enjoy studying information technology at PIHE’. What is the cipher text received by Bob, if the message was encrypted using:

3.1 Caesar cipher key = -3 (4 Marks)

3.2 Transposition cipher with keyword = APPLE and a key = 14532 (11 Marks)

End of Question 3

Section B

Plagiarism and Referencing

Pearson Institute of Higher Education places high importance on honesty in academic work submitted by students, and adopts a policy of zero tolerance on cheating and plagiarism. In academic writing, any source material e.g. journal articles, books, magazines, newspapers, reference material (dictionaries), online resources (websites, electronic journals or online newspaper articles), must be properly acknowledged. Failure to acknowledge such material is considered plagiarism; this is deemed an attempt to mislead and deceive the reader, and is unacceptable.

Pearson Institute of Higher Education adopts a zero tolerance policy on plagiarism, therefore, any submitted assessment that has been plagiarised will be subject to severe penalties. Students who are found guilty of plagiarism may be subject to disciplinary procedures and outcomes may include suspension from the institution or even expulsion. Therefore, students are strongly encouraged to familiarise themselves with referencing techniques for academic work. Students can access the PIHE Guide to Referencing on *my*LMS.

Negative Marking

Third-year Students

- A minimum of 15 additional information sources must be consulted and correctly cited.
- If no additional information sources have been used, a full 15% must be deducted.
- Deduct 1% per missing resource of the required 15. For example:
- If only five resources cited, deduct 10%.
- If only three resources cited, deduct 12%.
- Markers to apply the penalties for Category A for insufficient sources and incorrect referencing style.
- To determine the actual overall similarity percentage and plagiarism, markers must interpret the Turnitin Originality Report with reference to credible sources used and then apply the penalties as per the scale in the PIHE Policy for Intellectual Property, Copyright and Plagiarism Infringement.
- The similarity report alone is not an assessment of whether work has or has not been plagiarised. Careful examination of both the submitted paper/assignment/project and the suspect sources must be done.

Category A

Minimum reference requirements	Deduction of final mark
No additional information sources have been used or referenced.	15%