Cyber cecurity risk mangement assessment one

John 12345

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student |  | ID | 1 |

### 

Contents

[Case Study 1: Dealing with cyber attacks 2](#_Toc194392293)

[Scenario 1: 2](#_Toc194392294)

[Scenario 2: 2](#_Toc194392295)

[Task 1: 2](#_Toc194392296)

[Task 2: 2](#_Toc194392297)

[Task 3: 3](#_Toc194392298)

[Task 4: 3](#_Toc194392299)

[Case Study 2: Identify & assess emerging technologies 3](#_Toc194392300)

[Task 5: 3](#_Toc194392301)

[Task 6: 4](#_Toc194392302)

[Task 7: 4](#_Toc194392303)

[Task 8: 4](#_Toc194392304)

[Case Study 3: Evaluate and implement privacy policy 5](#_Toc194392305)

[Task 9 5](#_Toc194392306)

[Task 10 5](#_Toc194392307)

[Task 11 6](#_Toc194392308)

[Task 12: 6](#_Toc194392309)

[Index 6](#_Toc194392310)

**Assessment 1 – Case Study**

***Instructions:***

This task is to be completed individually. You need to analyse number of case scenarios related to cyber security and emerging technologies then complete all the tasks or answer all the questions provided after each scenario.

You may need Internet access to analyse and complete some of the tasks.

***Duration:***

Trainer will set the duration of the assessment

Read the case study carefully then answer the questions following. You may assume any information that has not been mentioned in the case study, however any assumptions you make must be clearly identified as assumptions.

# Case Study 1: Dealing with cyber attacks

Read these 2 scenarios, then answer the questions that follow.

### Contact Us – AS Trading Company**Scenario 1:**

You are the payables clerk of XYZ international trading Company. One morning you receive an email from your boss, the company accountant, urgently requesting that a file of digitally connected suppliers be emailed back to your boss immediately. The email says that this is urgently needed for an electronic document interface review the accountant and CEO are going to undertake during their imminent flight interstate.

You try to call your boss to confirm authorisation for the file transfer, but you learn that the mobile phones of both your boss and the CEO are unable to be reached. The email signature looks familiar, and the email address looks valid. You send the digital supplier file. Later in the day you get through to your boss to make sure she received the file, but your boss tells you no such request was ever sent by her.

### **Scenario 2:**

The Board of Directors at an international financial services organisation, headquartered in Sydney with offices in financial centres throughout the world, including Paris, New York and Hong Kong, were considering a confidential merger offer.

On a Friday afternoon, before a three-day weekend, the CIO received a ransom email from an unknown source stating they knew about the merger plans and had personal details of 150,000 customers. A sample of personal details for 500 customers was included in the ransom email as "proof". Unless a significant ransom was paid in Bitcoin, they would leak the merger plans and sell the customer information.

Scrutiny of the server logs revealed no evidence that 150,000 customers' details had been taken: the log evidence pointed only to the 500 customers' details attached to the original ransom email having been taken.

### **Task 1:**

For each scenario, identify the valuable asset(s) that requires protection, the use an intruder might have for the asset(s), and the risks to the asset(s).

Scenario 1: The valuable asset is information about approved suppliers to XYZ Ltd. Since suppliers are not under direct supervision, they are typically the weakest link of an enterprise’s IT security landscape. This is more so where documents are exchanged digitally. At the same time, outsourcing to vendors is critical for business success, and delaying engagement with vendors while their security is reviewed could adversely affect an enterprise’s operations. The risk is that the supplier list might be used to compromise members of XYZ’s supply chain, because of an error by an XYZ employee.

Scenario 2: The valuable assets appear to be personal information of 150,000 customers and confidential information of upcoming merger plans. However, consideration would need to be given as to whether the hackers were bluffing, both as to the suggestion that. They had 150,000 customers' details but also as to the merger plan. The evidence points only to the 500 customers' details attached to the original ransom email having been taken.

The risk is that the personal customer details could be used for identity fraud and publicity about the breach could inflict reputational damage.

### **Task 2:**

For each scenario, identify the cyber security threat and any current controls that are in place.

Scenario 1: The threat is Social Engineering - the act of manipulating people into giving up confidential data. These attackers aim to take advantage of human nature in order to access private information. Social engineers pose as a person of trust, such as a friend, relative or co-worker. Then they use that position to trick you into opening an email, clicking a link or accepting a download. The only control that seems to be in place is an authorisation requirement, which might be a written internal control (policy) but perhaps the control has not been tested for vulnerabilities sufficiently.

Scenario 2: The threat is Cyber Extortion - the act of cyber-criminals demanding payment through the use of, or threat of, some form of malicious activity against a victim, such as data compromise or denial of service attack. It appears that, if the 500 personal details are genuine, then there has already been a breach of controls which would normally be expected to protect sensitive customer data. The other aspect that needs to be considered is compliance. Is the organisation now in breach of privacy laws for example?

### **Task 3:**

For each scenario, use current legislative and regulatory requirements to identify additional short-term control strategies that should be put in place to protect the valuable assets. i.e. what responses should be made to counter the immediate threat?

For each scenario, current legislative and regulatory requirements may include:

1. data protection legislation
2. notifiable data breach legislation
3. Australian privacy laws
4. established international legislation

Key risk management strategies may include:

1. regular organisational training
2. regular threat assessment
3. cyber security incident response plan
4. clear escalation routes

Organisational policies and procedures, including for:

1. analysing and reviewing risk management methodologies
2. evaluating effectiveness of risk management strategies
3. reviewing currency of risk register

Scenario 1: XYZ should immediately notify the affected suppliers advising them of the nature of the breach and provide advice of the content of the supplier file so the suppliers can understand how the material might be used against them. Access to files, such as the one falsely obtained should be subject to tighter authorisation controls, so that access is only provided to more senior employees. To increase security awareness all employees should be told of a data breach and the consequences.

Scenario 2: The first step was to validate the threat. Investigations of hacker site in the dark-net might reveal that personal information of the account holders was available for sale

The next immediate need is to notify the data subjects whose data had been compromised and to provide them with practical guidance on how to reduce the risk of identity fraud. The data is of extremely high utility to hackers: the opportunity for identity theft or social engineering-based attack. The malware that caused the breach should be located and removed. A search for other malware should also be undertaken. A press briefing should follow, along with notifications to appropriate regulators. Finally, senior management will need to decide if the will pay the ransom or ignore the deadline and accept the consequences.

### **Task 4:**

For each scenario, use current legislative and regulatory requirements to identify additional long-term control strategies that should be put in place to protect against the identified threats.

Scenario 1: The employee authorisation policy should be re-examined to assess whether it needs strengthening after the breach. It should contain a clause that files should never be released without appropriate authorisation.

Access controls for sensitive information files should be reviewed and tightened.

The employee involved with the breach, along with employees who perform similar functions, should be trained to be better aware of the risks of social engineering.

Scenario 2: The most important long-term control relates to finding how the malware was deposited in the network. This may involve bringing in external consultants to perform penetration testing to discover the weaknesses and any others. Then the investigation should centre on what wen t wrong with the current controls, what process failures occurred and who ultimately had the responsibility to ensure the control was working. Subsequent control responsibilities may need to be strengthened, perhaps with more senior oversight.

# Case Study 2: Identify & assess emerging technologies

You work in the IT department of a medium-sized Australian business in the oil and gas sector. The directors of the business are conscious of an impending business dilemma:

1. The community is shifting away from accepting the continued, uncontrolled use of fossil fuels, which is adversely affecting demand for the company’s products.
2. Government is planning to adopt a carbon tax which will increase operating costs and further raise consumer awareness of environmental issues.

You are part of the IT team preparing medium-term forecasts and your job is to identify and assess emerging ICT technologies which may be appropriate for the organisation during the next strategy period. You have been asked to identify the 3 most likely emerging ICT technologies which may be of value to the organisation during this period.

Work with your team to brainstorm for the available options and risk management strategies related to new emerging technologies. Selected technologies will vary for each team member. You may assume any information that has not been mentioned in the scenario, however any assumptions you make must be clearly identified as assumptions.

### **Task 5:**

Complete the following table for the 3 selected technologies. Consider a range of issues as such as technology; data; workforce; risk management, etc

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Technology 1** | **Technology 2** | **Technology 3** |
| **Name** |  |  |  |
| **Purpose** |  |  |  |
| **Features** |  |  |  |
| **Attributes** |  |  |  |
| **Potential**  **Applications** |  |  |  |

### **Task 6:**

Complete the following table for 3 IT practices that may be affected by the introduction of the 3 selected technologies. Consider a range of practices as such as security, user experience, training, etc.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Practice 1** | **Practice 2** | **Practice 3** |
| **Name** |  |  |  |
| **Affected by which technology?** |  |  |  |
| **How affected?** |  |  |  |
| **Likely changes to practice**  **required** |  |  |  |

### **Task 7:**

Identify some potential organisational opportunities and threats resulting from the introduction of the emerging technologies and practices. How could the identified threats be addressed?

Please review my document about Australia Super Account was attacked: Australia's superannuation sector has recently suffered a series of coordinated cyber-attacks that compromised thousands of retirement accounts and resulted in significant financial losses.

### Task 8:

Identify some potential impacts on current organisational technologies and practices following the introduction of the 3 new technologies and new practices. How could the identified impacts be addressed?

Determine scope of risk management appropriate to organisation and industry based on the risk identified including risk registers and incident response plans.

# Case Study 3: Evaluate and implement privacy policy

One evening, a Darwin resident had a disturbing encounter. As she swam naked in her backyard pool, she noticed a drone hovering above. Concerned that it was recording footage of her which could end up on the internet, she went to investigate what her options were. Although flying so close to her was illegal, she discovered that there was no easy way to identify and prosecute offenders or protect her privacy.

Smaller drones are readily available at an accessible cost point that enables use by a large proportion of the population. Many of the drones used commercially are manufactured to detailed specifications for a particular purpose. There are no concrete numbers on how many drones are currently in use in Australia. Es timates have ranged from 50,000 recreational users through to over one million. The rate of drone ownership in America, covering all types of uses, is approximately 8 per cent. A conservative estimate of 5 per cent of Australians owning a drone, would see over 1.2 million drones operating in Australia. Data for the use of commercial drones is based on the numbers of people who hold either a remote pilot licence or a remote operator certificate.

As of mid-June 2020, there are over 16,300 remote pilot licence holders and over 1,900 remote operator certificate holders. There is also data collected by the Civil Aviation Safety Authority (CASA) regarding commercial drone operations carried out in the ‘excluded category’ operations. These data sets are useful, but they still do not provide the complete picture of the actual figure of both commercial and recreational drones operating in Australia. There are many small and large companies working to develop eVTOL vehicle concepts. Some eVTOL vehicles are modelled on familiar helicopter-influenced designs, while others are unique. There are a range of concepts in design that include multiple rotors, fixed and rotating wing, and prop and electric jet engines. At current estimates, the first eVTOL vehicles are expected to enter service in Australia around 2023– 2025, and will initially include a pilot.

Those numbers are expected to grow exponentially over the next decade as the many benefits of RPAs (remotely piloted aircraft) are realised and more applications developed. However, as their popularity take off, potential (and actual) negative consequences also lurk on the horizon. Terrorism and drug smuggling are just a couple of the threats occupying legislators. At the same time privacy is issue is privacy.

### Task 9

If you were the manufacturer or importer of the drone, in what ways could you contribute to this privacy?

The only real solution to the drone privacy issue is to develop national laws regulating their use. To this end the manufacturer/importer could contribute by making submissions to legislators on ways this could be achieved, such as developing engineering solutions, such as SIM cards for drones.

The manufacturer/importer could also assist by including in the drone advertising/sales material recommended best practices for drone use and emphasise the risks to personal privacy by improper use.

The manufacturer/importer could also become active in the development of industry standards covering the ownership and operation of drones, particularly those capable of invading personal privacy using onboard cameras.

### Task 10

What part could a drone-use code of ethics contribute to a resolution of this privacy debate? How effective would such a code of ethics be? What alternative to a code of ethics should be considered?

A drone-use code of ethics must be useful, in that it can clearly define what is acceptable or non-acceptable behaviour on the part of drone users. The code of ethics must consider legitimate uses of drones for deliveries, or authorised aerial photography, but needs to draw the clear distinction between these approved uses and those uses which are invasive of privacy.

A code of ethics would have limited effectiveness, as there is no compulsion on drone users to abide by the code, nor any penalty for non-compliance. For example, the code of ethics may say that persons under the age of 18 should not be allowed to fly a drone without parental guidance. However, this is impossible to enforce without legal penalties.

Probably the only effective way to ensure compliance is for drones of a certain size or capability to require a licence for a drone, which will also have a specific identification, such as a mobile phone sim card. The licence will prescribe who is allowed to fly the drone and what penalties apply if this licence condition is not met. Again, like similar licences for firearms, cars, liquor, the conditions of use need to be clearly defined and penalties for breaches of use set effectively. Even so, as we have seen with gun licencing in some countries, enforcement is key. If penalties are not enforced or are inadequate, then licencing just becomes a revenue raising exercise for government.

### Task 11

If you were a privacy legislator, what sort of drone operator licence conditions would you include in order to safeguard personal privacy, as described in the case study. How could enforcement agencies monitor drone activity to ensure your proposed licence conditions were being met?

The privacy issue in the case study relates to the invasive use of onboard cameras.

So, an obvious licence condition is to ensure that owners of drones capable of mounting cameras need to obtain a licence.

The important condition of the licence is that personal privacy is clearly defined, and drone invasion of that privacy is outlawed, with appropriate penalties for breach of the licence.

The real difficulty is monitoring. As the person in the case study discovered, how could she identify who owned or operated the drone? Where are the camera images being transmitted to? These are the challenge for legislators and for enforcement.

### Task 12:

As IT professional, how would you communicate potential risks and opportunities for improvement of IP, ethics and privacy policy and procedures to relevant personnel?

This short case ‘scenario’ outlines the inconsistent and incomplete patchwork of laws and regulations that govern the use of drones for private recreational purposes. Multiple government departments and agencies at the local, state or federal level have some jurisdiction over aspects of drone use or airspace. Yet when it comes to issues of unauthorised surveillance and enforcement, there are serious gaps. The burgeoning popularity and technical capabilities of drones means that the number of incidents is only set to grow while regulators are still ill-equipped to respond.

In 2014, the Australian Senate released its ‘Eyes in the sky’ report which described the nation’s rather frayed ‘patchwork’ of privacy laws that hadn’t kept pace with technological developments. It recommended updating and harmonising Australia’s privacy laws, with a focus on ‘protecting against intrusions on a person’s seclusion or private affairs. This included creating a tort of privacy, to reflect the new and multiplying ways privacy could be breached.

# Index

A

authorisation 2

E

Extortion 3

P

payables clerk 2

pilot licence 7

popularity 7, 9

protection 2

R

responsibilities 4

S

Senate 9