

Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	Student fill in own ID and attach document for submission
----------------------------------	---

Module Title & Code	<i>WM142 – Information Risk Management</i>
Module Owner	<i>Peter Norris</i>
Module Tutor	<i>Alexandra Samantha Driscoll</i>
Module Marker	<i>Alexandra Samantha Driscoll</i>
Assesment type	<i>Essay</i>
Date Set	<i>3rd November 2021</i>
Submission Date (excluding extensions)	<i>3rd December 2021</i>
Marks return date (excluding extensions)	<i>14th January 2022</i>
Weighting of mark	<i>30%.</i>

Assessment Detail	<i>Please see below</i>	
Additional details	<i>The wordcount is 2,000 words.</i>	
Module learning outcomes (numbered)	<i>1 – Apply a relevant risk management approach to a given organisation or scenario</i> <i>2 – Analyse the organisational consequences that result from inadequate information risk management</i>	
Learning outcomes assessed in this assessment (numbered)	<i>2 – Analyse the organisational consequences that result from inadequate information risk management</i>	
Marking guidelines	Task	Mark
	1: Identify a data breach that occurred within an organisation, and that it is OK to disclose, and provide a brief timeline of events.	25
	2: List any relevant information risks you believe are responsible for the data breach. Pick one information risk and identify and discuss its components (asset affected, vulnerability, threat, threat actor, impact, and likelihood).	25
	3: Discuss any potential consequences the organisation or asset stakeholders could have faced. Your answer should discuss if any of the principles of information security were affected.	40
	4: Provide a variety of references from a variety of sources, including academic sources	5
	5: The assignment should be presented in an essay style with suitable headings. Marks will be awarded for presentation, including spelling & grammar	5
	TOTAL:	100

	<i>Please see below for a more detailed marking scheme</i>
Submission guidance	<i>The assignment should be submitted as a single pdf file via tabula (https://tabula.warwick.ac.uk).</i>
Academic Guidance	<i>Academic guidance to be provide throughout the module.</i>
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that “earliest opportunity” means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of 5 marks per University working day after the due date, up to a maximum of 10 working days late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means after the submission deadline time as well as the date – work submitted after the given time even on the same day is counted as 1 day late.

Assessment

Introduction

Data breaches are a common occurrence. A data breach can have a variety of consequences for an organisation, ranging from minor to severe. Many data breaches have been reported in the media.

As an Information Risk Management practitioner, it is important to understand the potential consequences of a risk event occurring, including a data breach. One approach is to look at the consequences of previous events. In this assignment you will focus on a data breach, examining why it occurred and any consequences. To achieve this, you will identify a data breach which has been covered by the media, create a timeline showing what occurred, identify any relevant information risks, and explore the potential consequences of the data breach. It is common for only certain details of a data breach to be publicly available. Because of this assumptions may need to be made to gain a full understanding of what occurred and the consequences. For example, assumptions may be made about who the threat actor is, what happened or the consequences. Examining similar events or looking at how certain types of attacks are conducted can assist with this.

Assumptions are often used in academia, when there is no clear answer to a problem or question. Any assumption needs to be justified and backed up with evidence. Essentially you are making an

argument backing up what you believe. Your answers will not be marked based on the markers own opinion of what occurred. The marks will be determined by your arguments and how you defend any assumptions you make.

While academic articles related to data breaches exist, in cyber security we often must rely on grey media. This is especially true for events which occurred recently. When analysing an event which has occurred, there are a variety of potential sources. These include media reports, announcements made by any organisation involved, documentation related to any investigations, blog articles and other social media posts made by experts.

Tasks

1. Identify a data breach that occurred within an organisation, and that it is OK to disclose, and provide a brief timeline of events.
2. List any relevant information risks you believe are responsible for the data breach. Pick one information risk and identify and describe its components (asset affected, vulnerability, threat, threat actor, impact, and likelihood).
3. Discuss any potential consequences the organisation or asset stakeholder could have faced. Your answer should discuss if any of the principles of information security were impacted.

Important notes

1. You should use the Harvard referencing system
2. The wordcount is 2,000 words.
3. Your assignment must include references, including references to academic sources
 - a. Academic sources include journal articles and conference papers
4. The assignment should be presented in an essay style with suitable headings. Marks will be awarded for presentation, including spelling & grammar
5. This is an individual assignment
6. The assignment is due on Friday 3rd December 2021 at 12pm
7. Submissions should be made in PDF format and uploaded via Tabula
8. Late submission penalties will apply
9. Contact Alexandra Driscoll if you have any questions: alexandra.s.driscoll@warwick.ac.uk

Marking Scheme

The following marking scheme will be used. The assignment has a total of 100 marks.

Task	Criteria	Mark
1: Identify a data breach that occurred within an organisation, and that it is OK to disclose, and provide a brief timeline of events.	1a: Identify a relevant data breach	10
	1b: Provide a brief description of the data breach, including a timeline of events	15
2: List any relevant information risks you believe are responsible for the data breach. Pick one information risk and identify and describe its components (asset affected, vulnerability, threat, threat actor, impact, and likelihood).	2a: Identify appropriate information risks	10
	2b: Identify the main components of one of the identified risks (asset affected, vulnerability, threat, threat actor, impact and likelihood)	5
	2c: Provide a description of each component of the risk discussed in 2b	10
3: Discuss the potential consequences the organisation could have faced. Your answer should discuss if any of the principles of information security were affected.	3a: Identify any potential consequences	10
	3b: Discuss the identified potential consequences, including any potential impacts	15
	3c: Answer discusses the principles of information security	15
4: Provide a variety of references from a variety of sources, including academic sources	4a: Sources included	1
	4b Academic sources included	1
	4c: Sources referenced correctly using the Harvard referencing system	3
5: The assignment should be presented in an essay style with suitable headings. Marks will be awarded for presentation, including spelling & grammar.	5a: Assignment written in an appropriate format (essay)	1
	5b: Spelling and grammar	2
	5c: Tables and figures appropriately labelled and cited within the document text	2