### Introduction

briefing paper and annotated bibliography.

### Requirements

You will need to write a briefing paper to a hypothetical manager on the incident to which you have been allocated.  A range of issues that should be addressed in the briefing paper are noted below.

In marking the report, attention will be given to your understanding of information security concepts and how well you have met the requirements detailed in this document.  Style and technique of your writing will also be considered.

### Issues to be addressed

You should use the linked article as a starting point for your briefing of managers in a relevant organisation.  You can assume that senior management in your organisation saw the article and wants to know more about the issues raised.  This means that you will need to find other literature dealing with the issues connected with the topic and article.  The nature of this literature is described below in the section on the ‘Report’.

The different incidents may have different aspects at play and perhaps not all of the questions raised in this section are relevant to every incident – so use judgement as to what should be reported on given the particular circumstances.  Note that this should not be an excuse for leaving out major elements of your report.

You should assume you are within an organisation where the issues raised by the topic are relevant.

Report on major issues with incident and other incidents like this one.  What were the major control weaknesses?  Are these common?  The extent to which human or technical issues played a role (or both).

What should be done to reduce the risks of such incidents – may need to consider both the likelihood and impact side of things.  Also consider issues around prevention, detection and overall resilience.

Consider the overall cost of controls.  Are these mitigation measures likely to be cost effective?  What sort of residual risks would be reasonable to retain given the cost picture?

### Report

Managers and executives frequently rely on their support staff to research particular subjects and present concise summaries of the relevant issues in the form of briefing papers.  With this assignment, you should prepare a briefing paper as if you were a middle level manager in an organisation advising an executive level manager about the topic of concern.  You should do this by providing a good overview of the key issues associated with the topic along with pointers to additional reading that could be helpful if the reader wanted to explore the issues further.  To help the senior manager, this additional reading should be sign-posted with comments on why an article is relevant to some part of the issues covered by the briefing paper, and why this article is a good choice to consider that aspect of the topic.

The upper limit in this case is 1500 words for the main body of the paper.  The bibliography and its annotations are not considered to be part of the 1500 word limit.

Given that this report is sufficiently brief, it is not necessary to include an executive summary or table of contents, but it is reasonable to include headings throughout the report.  You should provide a brief introduction that outlines the nature of the report.

The pointers to additional reading on the topic should take the form of an annotated bibliography.  This means that you should write a paragraph on selected entries in the bibliography focussing on the relevance of the reference to the topic and the quality of the information in the reference (why it is relevant and why this article is a good choice to read).  It is expected that there will be a minimum of six entries with annotations in the bibliography.  At least two of these annotated entries need to be peer reviewed academic articles.  As the currency of source material is relevant to managers, it is also important that at least two of these annotated references are dated from 2018 or later.  You should avoid the temptation of using material directly from any article abstract as the main basis for your annotations in the bibliography, as typically this won’t address the key issues of relevance and quality and is likely to cause referencing problems.

The bibliography and the annotations will form an important part of the marking of this assignment, with 40% of the marks allocated for this component.  If you don’t include appropriate annotations, your maximum mark will be 14/20.  You will also lose marks if you do not have at least two academic articles and two recent articles (2018 or later) annotated in your bibliography.

### Presentation

Students will also be required to share some of the more interesting aspects of their work on this assignment with the class in a brief presentation (during the week 9 tutorial).  Students allocated to a Friday tutorial time will make an online presentation, as their class falls on a public holiday (Easter).

In-class presentations

Presentations should be no longer than 5 minutes (going over time will cost you marks).  Students working on the same topic are allowed to form into small groups for the presentations, in which case the group as a whole will be allowed a little extra time for the presentation.

It is important that you don’t try to tell the class about everything that you have done in your report during this presentation (you will be marked down if you attempt to do this) – try to focus on one or two information security related issues that are likely to be interesting to the whole group.  While the presentations will be relatively informal, it is desirable that you have some slides to support your talk but keep these to a minimum – as a guide, aim for 3 slides as a maximum.  The slides should be uploaded to the Canvas site prior to the class so that they can be easily accessed from there for the presentation.

The quality of the presentation will be used as the basis for the tutorial work mark for this week.

On-line presentations

Students in each of the Friday tutorials will have a discussion forum provided for their assignment presentations.  You should upload a post to this forum with a summary of one or two of the more interesting aspects of your security project report.  This post should be no more than half a page (and definitely not the whole of your security project report!).

Each student in the class should also post a substantive response to at least two postings in this forum.  These responses need to be much more than a simple comment like 'I agree'.  They should provide some additional commentary on the topic or a question about the issues raised.  If you are posting a question, you should also include some notes on what your initial thinking is around the question you have asked.

Your participation in the forum will provide your tutorial marks for the week 9 tutorial.  Keep in mind that each tutorial is worth just over 2 marks, so you should use this as a guide to the amount of effort you devote to this activity.

### Referencing

All work quoted from other written sources should be appropriately referenced using the UC version of the Harvard style (both with in-text references and a list of all sources used included in the bibliography).  This style is described in detail in referencing guides available at: [http://canberra.libguides.com/referencing (Links to an external site.)](http://canberra.libguides.com/referencing" \t "_blank).  Assignments that have not made a reasonable attempt to follow the standard referencing style will be penalised so please look at the referencing guides if you are unsure how to cite any of your references.

Previous experience with student assignments indicates that some students have significant problems with quoting and paraphrasing work from other sources.  For example, using a quote from a source with minor changes still requires you to use quotation marks.  Paraphrasing (where quotation marks are not used) requires you to write something completely in your own words where you are referring to concepts and ideas from the source.  You should also avoid lengthy quotes (whether exact quotes or paraphrased passages) from any of your sources – as a guide, no more than 20% of your assignment should be quoted or paraphrased from other sources.

### Submission

All assignments should be submitted via the Canvas online assignment submission process.

**Do not use a cover sheet, but you should include your student id number, the title of the topic selected, and the word count for the body of the report.**

In order to maximise the ease of marking, the submission should:

* use a 11pt font as a minimum;
* line spacing should be at least 1.5 lines; and
* have margins of at least 25mm.

find other literature dealing with the issues connected with the topic and article

<https://www.databreachtoday.com/uk-approves-limited-role-for-huawei-in-5g-networks-a-13656>

<https://arstechnica.com/tech-policy/2020/02/us-gave-allies-evidence-that-huawei-can-snoop-on-phone-networks-wsj-says/>

<https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256#comments_sector>

Report on major issues with incident and other incidents like this one.

<https://www.afr.com/opinion/the-technical-reasons-why-huawei-too-great-a-5g-risk-20180614-h11e3o>

  What were the major control weaknesses?

* *Management controls*: The security controls that focus on the management of risk and the management of information system security.
* *Operational controls*: The security controls that are primarily implemented and executed by people (as opposed to systems).
* *Technical controls*: The security controls that are primarily implemented and executed by the system through the system's hardware, software, or firmware.

Are these common?

Consider the overall cost of controls.  Are these mitigation measures likely to be cost effective?

What sort of residual risks would be reasonable to retain given the cost picture?

Link Introduction

**Why Huawei security concerns cannot be removed from US-China relations**

**Introduction**

Huawei is a China based multinational telecommunication company trying to expand their market of 5G network but many countries showed concerns claiming that they have setup backdoors in their system to secretly access the sensitive personal information. Initially this claim was made by US in 2009 when they observed backdoor in 4G network and warned other countries including Australia, New Zealand, Japan, Vietnam and UK of the vulnerabilities in Huawei system. All most all the countries paid attention to this threat, whereas UK still focuses on using Huawei network to build their non-core internet connectivity(<https://arstechnica.com/tech-policy/2020/02/us-gave-allies-evidence-that-huawei-can-snoop-on-phone-networks-wsj-says/> last accessed: 18/03/202).

China is recognized as one of the major cyber-power and its government uses cyber-operations for military and strategic gains. However, many cyberattacks are operated by Chinese hackers and US alone suffers US $300 billion worth of intellectual property theft in a year. China is allied with Russia for it military operations and China’s global trade dominance in area like cyberspace will provide very competitive price for telecommunication equipment and services. This will drive away other competitors resulting in its monopoly in long run. Huawei defends that the accusation is due to diplomatic relation between US and China as well as trade war between these two countries. <https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256#comments_sector> last accessed: 18/03/202).

**Backdoors and vulnerabilities**

This concern has leaded to series of questions and worries what if 5G network of the country is compromised. All the information shared over internet/network will be accessible to intruders. Internet of thing are built on 5G, therefore, any compromise on 5G network means compromise in smart homes, smart cities, driverless cars and many more appliances as they are controlled by intruders resulting in significant damage of property and lives.

Concerns from many countries regarding the use of Huawei technology is that the Chinese government can exploit Huawei technology and steal sensitive information including government, military and corporate secrets. They can also spy on conversations and data transmitted over their network serving them as surveillance web.

So far, no reports of “backdoors” deliberatively introduced by Chinese state in Huawei network are reported by UK’s National Cyber Security Center. But, Huawei’s technology is criticized for being vulnerable to attacks.

**Major Control weaknesses**

1. Management control weakness

Huawei claims to be independent company but they have received funding from Chinese state intelligence and Chinese army. Upon Chinese government’s call to provide information, Huawei cannot deny as per China’s National Intelligence Law, 2017.

1. Technical control weakness

US accuses Huawei for stealing intellectual property and producing faulty hardware and software which could lead to serious security risks. Huawei agreed to spend US$2 billion to fix those shortcomings.

The extent to which human or technical issues played a role (or both).

Backdoor are introduced by hardware and software makers for gaining access to system and application with either good or bad intension. A good intension is for troubleshooting and resolving software issues but in case of Huawei system, US claims that the backdoor are for spying purpose and stealing personal information.

Risk prevention/reduction and possible impact

US president Donald Trump in August 2018 signed a law that prohibits the purchase of any telecommunication products from Huawei and ZTE by US government agencies. New Zealand banned the use of Huawei’s telecommunication equipment marking it as a “significant national security risks”. Australia announced similar ban on purchase of telecommunication products but didn’t explicitly name whether it was from Huawei or ZTE. Under pressure from United Kingdom’s government, Huawei agreed to spend billions of dollar to mitigate shortcomings and rectify their engineering processes that produces security risk.

Banning the purchase of Huawei products can cause trade war as Huawei consider that their success in telecommunication sector is the reason for various allegations. In December 2018, Huawei CEO Meng Wanzhou was arrested by Canadian police alleged of defrauding (<https://www.newyorker.com/news/daily-comment/how-china-views-the-arrest-of-huaweis-meng-wanzhou> Last accessed: 21/03/2020)

Detection and overall resilience.

Huawei Cyber Security Evaluation Center affirms the sufficient mitigation of security risk likely to be appear in UK national security due to Huawei network (<https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017> last accessed: 21/03/2020).

Deutsche telecom is reviewing the security of network equipment from Chinese companies. Germany is willing to deploy equipment from any vendor until it is secure (<https://www.reuters.com/article/us-huawei-europe-germany/deutsche-telekom-reviews-huawei-ties-orange-says-no-on-5g-idUSKBN1OD0G7> Last accessed: 21/03/202).

Huawei should remove all the backdoors from their equipment which are inserted with an intension or accidently and prove that their devices are no more vulnerable or if other countries ban the implementation of Huawei 5G network for complete resilience. These resilience strategy can cause huge impaction on Huawei both positively and negatively. Huawei can extend their international market only if they can spare some budget and resources to eradicate the security vulnerabilities and remove backdoors.

Consider the overall cost of controls.  Are these mitigation measures likely to be cost effective?

What sort of residual risks would be reasonable to retain given the cost picture?

<https://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036>

New Zealand banned the use of Huawei’s telecommunication equipment marking it as a “significant national security risks”. Along with Huawei, ZTE(Chinese hardware maker) are accused of potential security and privacy threat.

<https://www.nytimes.com/2018/11/28/business/huawei-new-zealand-papua-new-guinea.html>