Coursework Guide

IY3501 SECURITY MANAGEMENT

Rachel Player

INFORMATION SECURITY GROUP | ROYAL HOLLOWAY, UNIVERSITY OF LONDON

1. Introduction

This guide describes all the necessary details required to complete the individual report coursework for IY3501 Security Management. This individual report makes up 40% of the final module grade. Completing an individual report can be seen initially as a daunting task. Therefore, it is essential you play close attention to this guide. The rest of this document provides useful information that will help you during the completion of the report. If, after reading this guide, you still have questions or queries, do not hesitate to contact the course coordinator. If the answer will be useful for the whole group, the question and answer will be posted on the course Moodle page and Teams channel.

2. Assignment task

The goal of this assignment is to write an individual report, relating to an information security incident. The report should identify the business context and security management requirements, describe the cause of and the impact of the incident, identify failures or weaknesses in security management that the incident highlights, and suggest possible improvements to security management processes. A detailed description of the contents of the report is given in later sections of this document.

A successful report should:

- Demonstrate an understanding of the need for effective security management and its main elements.
- Suggest appropriate security management requirements for a specific business context.
- Describe a range of security measures that could be used to meet the identified requirements.
- Compare and critically evaluate different approaches to security management.

The marking criteria can be found in the corresponding section of this guide.

3. Key Information

- The individual report makes up 40% of the final module grade.
- The word limit is 2500 words.
- The submission deadline is 23rd March – 10:00 am

4. Selecting an Information Security Incident

Choosing an information security incident can often be the most challenging part of the assignment. In this section, we discuss how to avoid the main pitfalls, where and what to look for and how to develop a plan for your report.

Main Pitfalls

Avoiding these pitfalls will ensure you are on the correct path to produce a high-quality report:

- Avoid non-relevant security incidents: In the recent years, we have seen many relevant information security incidents happening. Highly relevant information security incidents will be analysed and reported from more sources than non-relevant ones. Try to avoid incidents where the information and references are not in English.

- Not enough information: Avoid information security incidents where all the information is taken from a single source. In some cases, you may find that an incident is reported by different sources, but they all provide the same key information. If this happens, you should consider that there is only a single source of information.
- Security incident too broad: In some cases, a security incident may affect more than one company/entity (e.g., WannaCry). If you select such an incident, remember that the task asks you to focus on a specific company/entity. You should make sure that there is enough information available about how the incident affected that specific company/entity.
- Choosing an incident too soon: Before deciding on an information security incident, make sure that you will be able to find enough information to produce your report.

If you have doubts about the suitability of an information security incident, feel free to ask the course coordinator. In your query, please list all the sources of information you have found about that event.

Sources of Information

There are many different sources that you can turn to for information. These sources will present information in different, sometimes even contradictory, ways. When this happens, look for additional sources of information and extract the relevant “facts” as best you can. Please note that any reference or link to an external source of information included in this guide should not be seen as an endorsement from Royal Holloway or any department within the College.

Sources of information that you might find helpful may include some of the following.

Books

There is a plethora of books available on all aspects of information security. Unfortunately, book publication is a very long process, making books a less attractive venue for information about security incidents.

Internet Search Engines

The Internet is a magnificent tool for assisting in a literature search, but searching the Internet is not a literature search. Here is what the Internet is superb for:

- A preliminary investigation of the available resources on your incident.
- Portal sites that provide inter-related links to different resources.
- Dedicated websites that contain quality information on specific information security topics.
- Access to individual sites (and papers) of researchers and organisations.
- Downloadable articles and white papers.
- Easy access to opinions.

Here is why relying only on the Internet is dangerous and inadvisable:

- Much (most) of the information on the Internet has not been formally evaluated (refereed).
- Much of the information on the Internet is subjective and often wrong.
- Much of the information on the Internet is patchy and lacks perspective.
- Not all relevant information is publicly available on the Internet.

The Internet is an essential tool for any modern literature search but you should use it prudently, and not exclusively. It does not have all the information that you need and is not even always the source of the latest information. Be particularly careful to assess the probable quality of information from any web site that you visit and try to look for reputable sources. If you have questions about a specific source, feel free to contact the course coordinator.

Magazines and Newspapers

There are numerous periodicals that are either dedicated to aspects of information security or regularly feature related articles. These are all valid resources that you might choose to consult and are often one of the most reliable resources for timely developments. Obviously, you need to be aware that these may not always be written by subject experts and so you should be careful in your evaluation of their relevance. The following links point to two of these magazines.

- https://www.scmagazine.com
- https://www.infosecurity-magazine.com/

Vendors

Literature produced by vendors is often appropriate and relevant. It goes without saying that while a vendor may be the best source of information on issues relating to their products (and often on related issues), you cannot realistically assume that they are presenting information from a fully balanced perspective. Treat vendor information with caution. The following links point to two blogs written by information security vendors:

- https://www.gdatasoftware.com/blog
- https://blogs.forcepoint.com/security-labs

Government Bodies and Agencies

In recent years, the UK Government has focused on growing the capabilities of the UK in the cyber security area. This has resulted in the creation of new agencies like the National Cyber Security Centre (https://www.ncsc.gov.uk) and strengthening of the roles of other organisations like the ICO (https://ico.org.uk). Both bodies may release public reports analysing and providing advice for organisations to avoid data breaches which may be extremely useful.

What to Look for

When looking for security incidents make sure you avoid the previously mentioned pitfalls. In addition to that, here are some recommendations to take into account when looking for specific security incidents:

- Not all the incidents will be solely caused by some hacking or technical issue. In fact, in most cases, security incidents happen because of a combination of technical, managerial or social issues. Don't restrict your search to technical issues, look for incidents that had an origin in any information security aspect related to the course.
- Look for companies that are publicly listed or that have publicly available information through systems like Companies House (https://www.gov.uk/government/organisations/companies-house). In some cases, the brand publicly used by the company may not directly correspond to the company name.

- A single security incident can generate very different kinds of reports. Always compare different reports and, specifically, look for those that include some detail, but can be explained in your own words.

Examples of Information Security Incidents

The following examples are information security incidents that could be considered as suitable for the assignment:

- British Airways Data Breach: In 2018, BA's systems were compromised, enabling attackers to harvest personal information relating to more than 400,000 customers.
- TalkTalk Hack: In 2015 TalkTalk announced some of they were hacked, resulting in more than 150,000 customers data being accessed by the attackers.

We will look at these incidents in lectures in Unit 7 of the course material. Please select an incident other than the incidents covered in the Unit 7 material. If you have concerns about the suitability of a security incident, get in touch with the course coordinator.

5. Report Structure

You are free to organise and structure your report as you prefer. However, it is very important that you structure your report effectively. There are two important reasons for this:

- A well-structured report aids navigation. It allows a reader to locate information in your report quickly.
- A well-structured report aids comprehension. It will enable a reader to be aware of what stage they are at within the report, how they got there, and where they are going.

The key design aspect of your report is the organisation of the report into sections. Although we do not enforce a particular report structure, we strongly recommend the following sections to be included in the report. In this way, you will ensure your report includes all the relevant and necessary information.

Executive Summary

This section should include a summary of the report with special emphasis on the information security incident.

Business Context

This section should include details about the company affected by the information security breach. Relevant information could include company structure, number of employees, countries of operation, share price (if available) before the breach, 6 months after the breach, today; etc. Depending on the nature of the information security incident, some details may be more relevant than others. You should make clear the legal and regulatory context under which the business was operating at the time of the incident.

Detailed Description of the Security Incident

This section should include a detailed description of the chain of events that lead to the security incident. You should include a timeline of the events, and how the company reacted in the initial stages as the event unfolded. You should describe the causes of the incident, including the associated risks and any mitigation strategies that were in place. The short-term and long-term implications of these events for the company should also be described. These could include fees, changes of share price, cease of activity, changes in the organisation structure, etc.

Security Management Failures

This section should describe the main failures, from a security management perspective, that led to the incident. When describing these, consider if they arise from technical, managerial and/or societal factors. You should also indicate, in your opinion, what are the key lessons that could be learnt from this incident?

Suggestions for improvement

This section is an opportunity for you to give your personal opinions on which security controls, mitigations, etc. the company should adopt that would be most useful, cost-effective, and appropriate to avoid or mitigate a similar incident happening in the future. These suggestions could be contrasted with the steps implemented by the company in light of the incident.

References

Add here the references used in your report (more on this in the next section).

6. Referencing

Referencing is a very important part of the assignment. Unfortunately, referencing is probably the one aspect of report writing that causes the most problems. There is no need for this to be the case, and so it is important that you take the time to ensure your referencing is full and complete.

There are two related purposes for referencing:

1. To enable a reader to trace the sources that have influenced your ideas and work.
2. To enable a reader to access your sources for further detail.

Notice that the first reason not only explicitly attributes credit to sources that you have used during your project but also implicitly separates your contribution from that of existing sources. The second reason implies that your report is not an isolated document. While its main ideas should stand alone, referencing is the tool that connects your report with everything else that has been written on that specific information security incident. If you are writing your report in Microsoft Word, use its referencing tool. It will save you time and avoid more than one headache. When referencing a website, always include the date you last accessed that information. Finally, there is no preferred style for the references.

7. Marking Criteria

The marking criteria for the assignment are provided in a separate spreadsheet that can be found on the following page and on the Moodle page of the course.

	Weighting	0, 15	25, 35	42, 45, 48	52, 55, 58	62, 65, 68	72, 75, 78	82, 85, 88, 92, 95, 98
Business context	10%	Very weak or missing summary of business context. Security management requirements are incomplete, vague, inappropriate, or missing.	Weak summary of business context. Security management requirements are incomplete or not specific to the business.	Basic summary of business context. Some security management requirements are stated but these may be vague or not specific to the business.	Good summary of business context, including brief discussion of legal context. Good summary of security management requirements that are specific to the business.	Very good summary of business context, including detailed discussion of legal context. Clear summary of security management requirements that derive from the security goals of the business.	Excellent, clear summary of business context, including comprehensive discussion of relevant legal context. Security management requirements very clearly identified from business-appropriate security goals.	Outstanding summary of business context, including succinct discussion of relevant legal context. Outstanding attention to detail in identifying security management requirements of most relevance to the security goals of the business.
Critical analysis	20%	Very weak or missing summary of the information security risk(s) that caused the incident. The need for effective security management is only poorly articulated.	Poor summary of the information security risk(s) that caused the incident. Evidence of basic understanding of the need for effective security management.	Basic summary of the information security risk(s) that caused the incident, with some discussion of aspects of the risk management process. Evidence of some understanding of the need for effective security management.	Good discussion of the information security risk(s) that caused the incident, with some analysis of aspects of the risk management process. Evidence of a good understanding of the need for effective security management.	Very good discussion of the information security risk(s) that caused the incident, with analysis of each aspect of the risk management process. Evidence of a very good understanding of the need for effective security management.	Thorough discussion of the information security risk(s) that caused the incident, with detailed analysis of each aspect of the risk management process. Evidence of a strong understanding of the need for effective security management.	Outstanding, comprehensive discussion of the information security risk(s) that caused the incident, with detailed analysis of each aspect of the risk management process. Evidence of a comprehensive understanding of the need for effective security management.
Evaluation	20%	Very weak or missing discussion of the failures in security management that led to the incident. Improvements are not proposed, or are entirely inappropriate.	Weak discussion of the failures in security management that led to the incident. Improvements that are proposed are not justified.	Basic or brief discussion of the failures in security management that led to the incident. Some improvements are proposed that are not justified or may not be appropriate to the business context.	Good discussion of the failures in security management that led to the incident. Some improvements that are appropriate to the business context are proposed. Changes compared to the prior approach are justified.	Very good discussion that clearly articulates the failures in security management that led to the incident. Several improvements that are appropriate to the business context are proposed. Changes compared to the prior approach are well-justified.	Excellent discussion that clearly articulates the failures in security management that led to the incident. A range of improvements that are appropriate to the business context are proposed. Changes compared to the prior approach are very well-justified.	Outstanding attention to detail and precision in articulating the failures in security management that led to the incident. A range of improvements are suggested that are each fully justified in view of the business context.
Background reading	20%	Very weak or missing description of the timeline of the incident and its impact. Little or no evidence of critical reading of relevant sources.	Weak description of the timeline of the incident and its impact. Little evidence of critical reading of relevant sources.	Basic description of the timeline of the incident and its impact, showing some understanding. Limited evidence of critical reading of relevant sources.	Good description of the timeline of the incident and its impact, showing good understanding. Good evidence of critical reading of a range of relevant sources.	Very good description of the timeline of the incident and its impact, showing strong understanding. Strong evidence of critical reading of a range of relevant sources, including academic journals, books and industry reports.	Excellent, thorough description of the timeline of the incident and its impact, showing comprehensive understanding. Very strong evidence of critical reading of a range of relevant sources, including academic journals, books and industry reports.	Outstanding, precise, and articulate description of the timeline of the incident and its impact, showing full understanding. Excellent evidence of critical reading of a wide range of relevant sources, including academic journals, books and industry reports.
Structure and presentation	20%	Very poor organisation of the report. Poor academic writing style.	Poor organisation of the report. Weak academic writing style.	Acceptable organisation of the report. Generally satisfactory academic writing style.	Good organisation of the report. Good academic writing style.	Very good organisation of the report. Very good academic writing style.	Excellent organisation of the report. Excellent academic writing style.	Outstanding organisation of the report. Lucid academic writing style of close to publishable quality.
Bibliography and citations	10%	Very weak precision in referencing. Incomplete or missing bibliography.	Weak precision in referencing. Bibliography is incomplete or poorly formatted.	Satisfactory precision in referencing. Satisfactory precision in bibliographic format.	Good precision in referencing. Good precision in bibliographic format.	Very good precision in referencing. Very good precision in bibliographic format.	Excellent precision in referencing. Full and complete bibliography in consistent and appropriate style.	Outstanding precision in referencing. Full and complete bibliography of close to publishable quality.