MANCHESTER 1824
The University of Manchester

COMP61421: Cyber Security – Overview and coursework 1

Job/Activity Number:	COMP61421
Document Number:	1_comp61421_overviewandcoursework_dgd03.docx
Issue:	1.0
Date:	22 October 2020

Please note that these chapters pertain *mostly* to Professor Dresner's part of the module…

Modification History

Revision	Date	Revision Description
0.1	3 August 2020	First collation
0.2	13 August 2020	Edited into sections
0.3	08 October 2020	Collation completed before splitting into separate documents at the 1st level headings
1.0	13 October 2020	Edited for blended learning.

Contents

Figures

Tables

Activities

1. Structure and exercise plan

1.1. Under threat with Professor Danny Dresner

	Topic	Exercised by
	How to take this module *Security is the reward for unceasing vigilance (and only making new mistakes…)*	Case study centric
1	Intelligence led cyber security – Attack structure and deterrence through the kill chain Step through attack… *The Internet has commoditised intelligence for your adversaries. You can use it too!*	Analysis of Security breaches
2	Information asset management – knowing what's important *What's to worry about?*	Building an asset register
3	Information risk management – modelling the threats *Known, unknown, unknowable*	Describe the risk landscape Taxonomy-based risk identification.
4	Risk assessment and profiling	Drawing up a risk profile
5	Risk Treatment – countermeasures against the threats *From trustworthy systems to standards of good practice…*	Creating a risk treatment plan to bring risk down to an acceptable level…
6	Human factors – the systemic view of the wetware components The soft squidgy bit between the chair and the keyboard – stop blaming it! *Diversity in adversity*	Balancing human and technology symbiosis through the risk treatment plan
7	How to pull your SOCs up Crafting the information and cyber security cookbook Digital forensics Plan (Mitre's) Att&ck	Creating a test plan for the risk treatment plan Defining a monitoring and response strategy
8	Penetration Testing	

1.2. Engineering security with Dr Ning Zhang

See Blackboard for materials from Dr Ning Zhang…

1.3. Poking security with sharp stick with Professor Adam Kramer

See Blackboard for materials from Professor Adam Kramer…

2. How to take this module

2.1. Commitment

Before we get started, please note…

1. A university degree is a promise.
2. Punctuality for the times we meet on-line or face to face is a virtue.
3. Live and breathe the topic. Cyber security is for life…not just academic credits.
4. Slides – when used – are signposts…read and research!
5. Use the on-line discussion fora.
6. If you use an electronic device to search for answers to questions do so with critical thinking when you look at the results.
7. Ask questions!
8. Loss of work because of IT failure indicates a complete lack of understanding of the learning.
9. Read relevant news reports daily.
10. Appreciate our guest lecturers…they have a choice of being out there earning or giving up their time for you.
11. Guest lecturers open up your understanding of challenges set in the assessments.
12. All group work shall be in English – including 1:1 and 1:m group discussions.
13. Show mutual respect to your colleagues.
14. Unless you are in the middle of a genuine crisis* or your child's school may need to contact you (etc.)…switch off your 'phone when studying.

Now we're friends, let's get down to the exciting, critical, and complex world of cyber security. Remember that 'security is the reward for unceasing vigilance' (and only making new mistakes… ).

2.2. Introduction

COMP61421 *Cyber Security* is a taught MSc Module designed for students who want to understand and implement the processes and technologies associated with information assurance and cyber security. It's not all about having a go at hacking but rather making a long term investment in the knowledge to use ethical hacking for good and minimise the harm that criminal hackers can do.

On this module you are expected to:

- Understand how to take a systems approach to security.
- Learn how to apply international good practices in cyber security as a business tool.
- Pick up practical advice about information and cyber security.
- Take part in risk assessment and get access to simple but effective templates.
- Know which technologies to deploy and where.
- Understand how mitigate risks associated with computational technologies.
- Appreciate the need to test that an adequate state of security exists – and some techniques for doing so.
- Have a go at deploying the tools to test systems' safety from criminals, nation states, and sometimes your own colleagues.
- Work hard!

So that you can:

- Get a good understanding of how to define system security requirements.
- Be able to prioritise requirements, and match requirements to solutions and countermeasures commensurate with associated risks.
- Develop a good understanding of the correlation of business processes to technology in relation to security requirements .
- Become familiar with the relevant industry security standards, regulations, and their application.
- Reduce cyber risk to an acceptable level in the systems that you design, build, and deploy.
- Understand the technology that detects, effects, and protects.
- Think about build security into a system as part of the core design and test that its effectiveness.
- Test that all those good intentions are implemented effectively.

2.3. Structure

This module has 3 components:

Topic	Led by	Assessment[1]
Threats	Professor Danny Dresner	25%
Tools	Dr Ning Zhang	50%
Tests	Professor Adam Kramer	25%

When you have questions about the course assessment, address them to:

Course work I – The Ruritanian Oxygen Company	Professor Danny Dresner
Course work II – A Drink Vending Machine	Dr Ning Zhang
Course work III – Pentesting exercise with report	Professor Adam Kramer

2.4. Reading

2.4.1. Set books/texts:

- Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*, ISBN 978-0-470-06852-6, John Wiley and Sons, 2008
- BS ISO/IEC 27001:2017 *Information technology. Security techniques. Information security management*
- BS ISO/IEC 27002:2017 *Code of practice for information security management*
- BS 10754-1:2018 *Information technology. Systems trustworthiness. Governance and management specification*, BSI
- Stallings, W., *Cryptography and Network Security*, 7th/e, ISBN: 1292158581, Prentice Hall, 2017, or 6th/e, Pearson Ed.

[1] As a percentage of the mark for the module.

Activity 1: Create your personal security playbook…

When you read the books, pay attention to checklists of actions and recommendations. You will find it useful when taking notes, to develop your own security checklists to help with the work during the lectures and the assignment that you will do afterwards. Always treat this as a practical topic. As you note good practice, apply it to your digital existence too.

2.5. Extra-curricular activity and hands on exercises

This module – and its sister *COMP61411 Cryptography* and the complementary COMP60721 *Governance* module from the *Data Engineering and Systems Governance* theme – are designed to tap your passion for cyber security and give you good insight into the challenges of cyber security.

Students who are really serious about this subject should exercise beyond the formal coursework and for this we recommend turning to Immersive Labs (*www.immersivelabs.com*) Students' Digital Cyber Academy. This is a progressive, on-line cyber security learning experience which complements the class work that Daniel, Ning, Richard, and Adam engage you with.

Your University of Manchester of Manchester e-mail will get you a free registration – *https://dca.immersivelabs.online/signin* – and we expect you to keep in touch to tell us how you're getting on. Enjoy. Learn.

Develop your skills...let's make the connected world a safer place for all.

3. COMP61421 Coursework I – Information risk assessment, treatment, and test plan

3.1. Introduction

The objective of this assignment is to understand working together to create an assured risk treatment plan for the company in the following case study.

Note:

- There's some individual work involved.
- The specification below is quite vague

First draft specifications often are full of whole in the first instance (and often into development)– but this creates the opportunity for you to fill in the blanks with some critical thinking and **design in security to the architecture**.

3.2. Case study exercise – The Ruritanian Oxygen Company

The Ruritanian Oxygen Company (ROC) supplies medical gases (such as oxygen in cylinders) to hospitals and patients at home. ROC operates a network of warehouses and fleet of vans who collect empty cylinders, refill them, and deliver them to the patients. When a patient leaves hospital, the hospital will order a supply from ROC for the patient. That supply is then renewed by the patient (or the patient's representative) through the patient's general practitioner. This is handled by an App – available for desktop machines and smartphones – to support the timely, efficient, and safe delivery of oxygen to those who need it (*see **Figure 1***).

The ROC also has a feature that enable it to track its vans and send them new orders without the drivers having to return to the depot to collect instructions. Patients can also track the delivery of their oxygen.

ROC does not have the capacity to supply the whole country so it will subcontract supply to local medical gas companies when necessary, distributing the App to them as part of the arrangement. ROC – like many of its suppliers – is still phasing out its old system which uses an information system based on printed forms and facsimile machines.

ROCs systems must fulfil functional requirements that include, but are not restricted to:

- Collect real-time data about a patient's orders of medical gases.
- Transmit data about a patient's order to healthcare professionals and update medical records accordingly.
- Contact the patient (or the patient's representative) with for example, progress of an order.
- Validate patient's orders with the need prescribed by the hospitals and general practitioners.

This requires the handling of sensitive information about people who may be made vulnerable through their illness or other issues. However, this is an important, life-critical service that means that those involved must know to whom, when, and where the oxygen must be delivered. The objective of the assignment is to make sure that the risks posed by cyber security threats that may affect the timely, efficient, and safe delivery of oxygen will be mitigated and reduced a level that demonstrates a socially responsible risk appetite.

Figure 1: The Ruritanian Oxygen Company supplies medical gases on demand

3.3. How do we carry out the Coursework I assignment?

3.3.1. Hints, tips, and rules!

(1) Get familiar with the case study.

- Consider how the operational processes will work by looking at the components in the illustration.
- Discuss your ideas with others in your respective group.
- Consider what information assets need protecting. For each asset, consider:
  - Is it transitional? (Such as a temporary file used in processing.)
  - Is it permanent? (Such as dedicated hardware, a central database, application, or operating system code.)
  - Is it critical to any of the stakeholders? (Such as financial data for accountants.)
  - Is it legal? Is it outside the permitted process boundaries? (This won't be in the specification. Think – for example – where a design flaw may encourage someone to keep a spreadsheet with a subset of information 'just in case'.)
  - Boundaries with other systems and the ownership of connected systems.

(2) Catalogue the assets to create an Information Asset Register. Value each asset in terms of confidentiality, integrity, and availability:

- An asset register, risk assessment, and risk treatment plan that sets out how the system will deploy good security practices which will protect:

- Operational aspects of delivering medical gases.
- Information about the stakeholders in the system.

(Use the Asset Register/Risk treatment plan template spreadsheet.)

(3) What are the risks to the information assets in the case study?

- Identify the threats to these assets throughout the system lifecycle (think: what is a threat and what is the lifecycle?)

(4) Build up a risk treatment plan. Collaborate with your group.

- Propose countermeasures for each threat to business continuity (think: what is business continuity? What will make the system resilient?)

(5) Note that the ***penetration testing*** element of the module – that is held for (at least the equivalent of an hour on each taught-content day – will help to inform you about the testing element of this assignment.

Collate what has been done up to here as a piece of group work. Name your group and ***appoint one member of the group*** to submit your completed group risk treatment plan (including the asset register) no later than **25 January 2021**.

(6) Complete the assignment ***individually*** by:

- Designing a **test plan** to assure the effectiveness of the risk treatments in the group-designed plan. (Hint: this module has a significant penetration testing component and you might like consider where this fits with red, blue, and purple teaming, vulnerability scanning, and audits although not necessarily in that order.)
- Include **a table of your '*Technical and technique-al takeaways from the guest lecturers*'** from the guest lectures. Submit – no more than the equivalent of three sides of A4.
- Submit your test plan and table about the guest lecture as a single Adobe PDF. Make sure your name and student ID is clearly visible at the beginning of the test plan. Failing to do so may result in you receiving a mark of 0 for the coursework.

*Note: The test plan and table **must** be your own work – **an individual effort**. You may (and will likely need to) refer to the risk treatment plan that you have worked together on in your group **but do not reproduce all or parts of the groupwork in your individual report**.*

*The risk treatment plan is a group effort so only submit one plan per group **but make it clear** (on your plan) **who is in your group** (names and student ID numbers).*

Please include your name clearly in your filenames. For example:

- ReallySharpGroup.xlsx
- RatherCleverGroup.xlsx
- LiSeng001.pdf
- PaulMetcalfeSecurityReport.pdf
- GroupNumber02_RiskPlan.xlsx
- GroupNumber06_TestPlan.pdf

Up to 10% of the marks can be forfeit if you don't follow these labelling instructions – they're part of the exercise.

3.3.2. Technical and technique-al takeaways from the guest lectures

This is the second part of your individual component of the assignment – a summary of what you learnt from the guest lecturers. Use the tabular format below… ***Note dates and times are subject to change. Listen keenly for alterations to the schedule:***

Topic	Guest	Recorded material available	Question and answer session (live)	Compulsory

Table 1: Material and live schedule for guest lecturers