# University of London

# Assessment Submission Document

Complete the sections below and read the instructions below carefully.

**Candidate Number**: **MS0005**

Refer to your Admission Notice

**Degree Title**: MSc Cyber Security

e.g.

**Course/Module Title**: Cybercrime

As it appears on the question paper

**Course/Module Code: CYM030**

This is in the top right corner of the question paper. If there is more than one code, use the first code.

**Enter the numbers, and sub-sections, of the questions in the order in which you have attempted them:**

1, 2, 3

**Date**: 2023-09-26

**Instructions to Candidates**

1. Complete this assessment submission document and begin typing your answers on the page below.
2. Clearly state the question number, and any sub-sections, at the beginning of each answer and also note them in the space provided above.
3. For typed answers, use a plain font such as Arial or Calibri and font size 11 or larger.
4. Handwritten answers (including diagrams or mathematical formulae) must be done on light coloured paper using blue or black ink.
5. Reference your diagrams in your typed answers. Label diagrams clearly.
6. Remember to upload the final version of your completed assessment submission document as a Microsoft Word file before the deadline. You are strongly advised to upload your document as a Microsoft Word file. If you are unable to do this you may submit your work in PDF format.

**The Examiners will attach great importance to legibility, accuracy and clarity of expression.**

## Question 1

### Part a

Law enforcement agencies conduct surveys to show the reach and impact of cybercrime. These surveys support these agencies in bidding for more money, and enabling them to demonstrate the effect they’re having on this criminal activity.

However, surveys of this sort can suffer from certain biases. The most common is selection bias. For example, older men from higher socio-economic backgrounds are more likely to report cybercrime to law enforcement (Van De Weijer et al., 2020).This in turn results in some kinds of crime being under-reported. For example, so-called ‘revenge pornography’ is generally perpetrated against women – who are less likely to interact with law enforcement. Thus, the survey will over-sample certain kinds of crime, and give a misleading image of the true scale of the problem being faced.

There are also problems with delivering the survey and finding respondents at all. Businesses that have been damaged by cybercrime may not want to admit it, and would need to have total confidence in the survey organiser. Although this can be difficult, such surveys have indeed been carried out – for example, the UK government carries out an annual survey of breaches.(*Cyber Security Breaches Survey 2022*, 2022).

In the same domain as struggling to find respondents, we might also consider the question of the distribution of the thing that we’re trying to survey. Assuming a normal distribution allows us to use simple statistical sampling methods. Phishing attacks of the ‘Nigerian Prince’ variety follow this pattern, as they are entirely undirected. However, this is not always the case: in fact, some crimes – as noted above with ‘revenge pornography’ – are not distributed normally through a population. This makes sampling significantly more difficult.

Improving the accuracy of these surveys will require that the surveyors demonstrate that they can be trusted. This may require a certain amount of operational independence from law enforcement, to reassure individuals being surveyed that their answers will be kept in confidence. Additionally, surveyors will need to go to where respondents are likely to gather, rather than relying on individuals to come to them and self-report.

### Part b

Law enforcement across the world currently struggles to combat cybercrime. Overcoming such difficulties will require international cooperation along several axes. In some areas, this has already been achieved – in others, it may never happen.

First, there is the problem of under-reporting. (*Cyber crime*, 2013). Approaches to combat under-reporting are detailed in part 1 of this question, but I have raised it again here to note that as long as victims believe that their report will not be actioned, under-reporting will remain a consistent issue. Erentzen and Schuller (Erentzen and Schuller, 2020) examine this from the specific perspective of hate crime, but I believe it can be generalised to crime as a whole. This problem can only be dealt with by police forces actively combatting the view amongst marginalised groups that the police are not there to support them.

Second, there are operational problems. Europol (*Common Challenges in Combating Cybercrime*, 2019) notes five challenges associated with combatting cybercrime: loss of data, loss of location, challenges associated with national legal frameworks, obstacles to international cooperation, and challenges of public-private partnerships. The report by Europol goes some way to laying out potential solutions to these problems, and such approaches can either be generalised to the UK or apply equally to the UK – particularly as we look towards international cooperation.

Third, there is a question of staffing. Police forces are generally not paid highly, and specialist skills such as those required for digital forensics are in high demand beyond law enforcement (*Cyber security skills in the UK labour market 2022*, 2022). The police face significantly increased demand for such capabilities, as the number of cyber-enabled and cyber-dependent crimes increase, at the same time as their ability to supply such capability decreases as specialists leave the service for equivalent but higher-paid roles in the private sector. To combat this problem, the police (and indeed the wider public sector) may need to consider some alternative approach to the recruitment and retention of staff with specific skills. Policing could look towards a reserves model, such as the one that staffs the UK’s Joint Cyber Reserve Force, or rely on outsourcing the more complex and specialist work. A more radical approach would be to break the link between seniority, management, and salary, enabling specialists to be paid at the same levels as very senior officers without the responsibilities of management.

### Part c

Ethos is a rhetorical device that focuses on the credibility and authority of the speaker. It can be used in social engineering as a way to shortcut what Kahneman calls System 2 thinking (Kahneman, 2012) and trigger the authority bias; alternatively, it can be used to trigger more empathic biases.

As an example, an attacker using social engineering may wear a specific uniform when attempting to gain access to a target building. Claiming to be from a specific organisation, such as the target building’s cleaning staff, will be more believable if the attacker is wearing that uniform. Additionally, they may reference real members of staff when attempting to gain access by socially engineering a member of reception staff. This too will create a sense of credibility in the target’s mind.

Alternatively, Hadnagy (Hadnagy, 2010) discusses the way he used ethos to imitate a charity fundraiser, successfully convincing a CEO to open a PDF file with malware in it. By researching CEO and identifying the kind of charity he would be interested in supporting, Hadnagy was able to appear credible, as the target was already primed to believe that such a person would be getting in contact. Additionally, Hadnagy also gathered information from the financial department of the organisation in order to gather information on previous donations, which further increased his credibility.

## Question 2

### Part a

#### Part i

1. The state of the device should not be changed if at all possible. If the device is on, it should be enclosed in a Faraday bag and remain powered on if at all possible. If it powered off, it should remain that way.
2. The usual rules of evidence are followed, including chain of custody. Where possible, an image or clone of the device should be made. This ensures we don’t accidentally write to the actual device being examined.
3. Photographs and screenshots should be taken as evidence
4. A full log should be kept of any actions taken, and those actions should only be taken by a professional

These steps are adapted from the ACPO Good Practice Guide for Digital Evidence

#### Part ii

If CSAM is found on the devices, MNP may be charged with offences under sections 1(1)(a), 1(1)(b), and 1(1)(c) of the Protection of Children Act. These offences are respectively:

* making of an indecent image of a child, which includes downloading the image as well as actually creating it
* distributing or showing such photographs, if evidence can be found that MNP has done so
* possession of such photographs with a view to them being distributed or shown

MNP may also be charged under Section 160 of the Criminal Justice Act on the charge of possession.

#### Part iii

MNP claims that the images were shared for amusement. If that is the case, then he cannot be charged under Section 33 of the Criminal Justice and Courts Act 2015, which requires that the perpetrator’s aim in sharing the material was to cause distress. At time of writing, there is no offence in relation to taking or sharing an intimate photo. However, the UK’s Law Commission has reported on the need for such a law (*Intimate Image Abuse: a final report*, 2022) and the UK government has accepted the findings and is claims to be seeking ways to implement them.

### Part b

Suler identified the following seven characteristics in the online disinhibition effect (Suler, 2005):

1. individual differences
2. attenuated status and authority
3. dissociative imagination
4. dissociative anonymity
5. solipsistic introjection
6. asynchronicity
7. invisibility

He notes that in general a combination of these characteristics is what generates the online disinhibition effect. We can apply this to the behaviour of an online stalker.

Dissociative anonymity: without any kind of attachment to a real-world social presence, there is little to no social pressure for the online identity to act in a way congruent with the behaviour of the offline identity. This may reduce the inhibitions of someone who would otherwise be forced to reckon with their behaviour.

Invisibility: unless the stalker moves into the offline space to continue their behaviour, they will not have to reckon with the physical signs of “disapproval, hostility, and indifference” (Suler, 2005). This allows them to continue their behaviour for longer than they reasonably could in the offline space, where their behaviours would be noticed by others and acted upon.

Dissociative imagination: Suler argues that people may feel that the online world is inhabited by characters whose actions have no real impact – that they are in essence playing a game, where the normal rules do not apply. For a stalker, the process of gathering details such as often-frequented locales, personal details, and so on may seem like a harmless process of collection. Additionally, because of the ease of such actions, it can seem to the individual that it is not criminal behaviour.

### Part c

|  |  |  |
| --- | --- | --- |
| **Hacker** | **Skill** | **Motivation** |
| Black hat | Generally high | Criminal or financial-by-any-means |
| White hat | Generally high | The protection of data and the improvement of systems by finding and closing vulnerabilities |
| Grey hat | Generally high | Somewhere between white and black hats. They may break ethical standards or laws, but not with malicious or criminal intent |
| Hacktivists | Wide variance in skill | Nebulous, but could be broadly described as anarchic – a motivation for freedom, or perhaps against capitalism and state surveillance |
| Script kiddies | Low | An interest in computers, breaking things, and getting shells. Although they may graduate to more advanced hacking, they may also drop out when the scripts don’t work first time or when things get dangerous |

## Question 3

### Part a

#### Part i

The IT Administrator has committed offences:

* under section 170 of the Data Protection Act 2018, for disclosing personal data without permission
* under section 3A of the Computer Misuse Act 1990, because they created an article that would be used for offences under section 1 of the same Act
* additionally under section 7 of the Fraud Act 2006, for the creation of articles used in the commission of a fraud offence
* if they receive payment for this service, and that payment is made with stolen money, they may also be charged with money laundering under Part 7 of the Proceeds of Crime Act 2002

#### Part ii

The hacker has committed offences:

* under section 1 of the Computer Misuse Act, for accessing an account without authorisation
* section 2 of the Fraud Act 2006, by representing themselves as the account holder
* section 6 of the Fraud Act 2006, as they have possession of the fraudulent material

#### Part iii

The crimes under the CMA are cyber-dependent, while the offences under the Fraud Act are cyber-enabled – they could be carried out without a computer, though their scope would be more limited.

### Part b

Why is the gig economy attractive to cybercriminals, and how do crypto-currencies assist in moving money made in the commission of these crimes? First, let’s consider the alternative: long-lived criminal enterprises. A group of criminals associate together and become more effective operators together. They also build up relationships and ties to each other. This is a valid model for criminal activity, and indeed Europol notes the impact of organised crime groups and networks (*A Corrupting Influence: The Infiltration And Undermining Of Europe’s Economy And Society By Organised Crime*, 2021).

The same report notes that cybercrime does not generally see this level of organisation. Instead, cybercriminals tend to more atomised interactions – closer to Uber drivers than mafiosi.

One reason for a more freelance approach to cybercrime is that cybercriminals can be expensive, and long-running criminal enterprises are similar to their legitimate counterparts in that they are profit-driven. Hiring malware developers full-time may not be cost-effective, as the enterprise may only want these capabilities for a short-term piece of work. This approach also works for the developer, who may not want to be limited to an organisation in a specific niche – but who also may not want to be too closely linked to a specific criminal organisation.

Equally, we could see this as an evolution in the market for the production of assets for the purposes of cybercrime. David Ricardo’s theory of comparative advantage, although originally applied to nations trading with one another, gives us a lens to consider this market. Suppose a criminal organisation *can* conduct hacking operations and committing fraud, but finds it splits its time 70-30 on those two actions. It may find that it is better off focussing on one of those actions and simply buying the inputs. As these organisations find themselves specialising, production and efficiency in the market increases.

Thus, having applied a purely economics lens, we can see how self-interested actors create a marketplace where the actors tend to specialise on one element of the criminal endeavour. We turn now to moving the proceeds of this criminal work.

In traditional crime, banks are eschewed in favour of less-traceable assets such as used cash and unmarked gold, or assets whose value is not centrally controlled, such as artwork. So too in the case of cybercrime, except in this case the preferred medium has been crypto-currencies.

Crypto-currencies are poorly named. A currency must generally hold a stable value. When we see countries whose currency is not stable, we see those countries as a poor investment. Criminals being paid in an asset whose value fluctuates considerably seems counter-intuitive. However, the advantages of crypto-currencies far outweigh this disadvantage, and as long as crypto-currencies can keep most of their (monetary) value, we will continue to see their use.

Taking Monero as the gold standard of criminally-used crypto-currencies, we see it has significant advantages. The software enforces strict privacy, enabling criminals to move the assets around without leaving significant traces. The assets are stored[[1]](#footnote-2) on a decentralised ledger, and are accessible from anywhere with an Internet connection, thus releasing criminals from the onerous business of flying to whichever authority-unfriendly bank they’re using to store their income. Furthermore, as a decentralised ledger, there is no authority that can reclaim the money, and no way of undoing the transaction short of taking over the entire network. Finally, other criminal organisations accept such crypto-currencies as payment – which means it works as a medium of exchange, representing labour performed.

Thus we can see that crypto-currencies, and specifically Monero, offer advantages over traditional means of paying for criminal activities, while retaining the benefits of traditional currencies.

## Bibliography

A Corrupting Influence: The Infiltration And Undermining Of Europe’s Economy And Society By Organised Crime, 2021. , SOCTA.

Common Challenges in Combating Cybercrime, 2019. . Europol.

Cyber crime: a review of the evidence, 2013. . UK Home Office.

Cyber Security Breaches Survey 2022, 2022.

Cyber security skills in the UK labour market 2022, 2022. . Department for Digital, Culture, Media & Sport.

Erentzen, C., Schuller, R., 2020. Exploring the Dark Figure of Hate: Experiences with Police Bias and the Under-reporting of Hate Crime. Can. J. Criminol. Crim. Justice 62, 64–97. https://doi.org/10.3138/cjccj.2019-0035

Hadnagy, C., 2010. Hadnagy Case Study 1: The Overconfident CEO, in: Social Engineering: The Art of Human Hacking. pp. 310–317.

Intimate Image Abuse: a final report (No. Law Com No 407), 2022. . UK Law Commission.

Kahneman, D., 2012. Thinking, fast and slow. Penguin.

Suler, J., 2005. The online disinhibition effect. Int. J. Appl. Psychoanal. Stud. 2, 184–188. https://doi.org/10.1002/aps.42

Van De Weijer, S., Leukfeldt, R., Van Der Zee, S., 2020. Reporting cybercrime victimization: determinants, motives, and previous experiences. Polic. Int. J. 43, 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

1. ‘Stored’ is an abstraction here. There is no such thing as ‘a Bitcoin’, only a record of where all the Bitcoin are. If you have a public/private key pair that the Blockchain records as being the most recent location of some Bitcoin, then you have the capability to spend that Bitcoin. [↑](#footnote-ref-2)