S2: Discuss the positives and negatives of automated security alert systems with regard to usable security.

The International Standard (ISO 9251-11:2018) defines usability as "the effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments". This statement suggests that assessment for usability should be based on three factors: effectiveness, efficiency, and user satisfaction. Automated security alert systems are systems trained to analyse alert data autonomously, in order to reduce the strain put on the security analysts. It is a type of autonomic computing control loop, such as MAPE-K, which monitors the system and responds to changes in the environment.

Firstly, one could argue that the biggest benefit is the reduction of alert fatigue for the security analysts operating these automated alert systems. With Misuse and Anomaly Detection, a threshold must be set by which the automated system classifies logs as 'alerts' – if the threshold is too high, attacks may slip through unnoticed, but if it is too low, many false alarms show up for 'normal' logs, and the security analyst would have to sift through these manually. As humans have limited capacity, an increase in alert signals can cause significant alert fatigue, which can lead to analysts becoming blind to common false alarms, some of which may represent real threats. Pietraszek's 2004 paper on 'Adaptive Learner for Alert Classification' argues that by classifying alerts into true and false positives using machine learning, we support human analysts by facilitating their work, thus reducing the problem of alert fatigue. Therefore, automated security systems improve usability as they increase user satisfaction and make the security systems more efficient, placing less strain on the human.

Secondly, automated systems are arguably less likely to err than a human when presented with large quantities of data. Humans are often presented as "security's weakest link" (Robert Kress, Accenture) due to being prone to error; as Alexander Pope wrote in 1711, "to err is human". Humans have limited capacity and attention, which is why autonomous security systems exist in the first place – we have been able to use artificial intelligence and machine learning to make up for this disadvantage. Therefore, using automation such as Intrusion Prevention Systems is beneficial as it increases the effectiveness and efficiency of the security system; the system itself is more likely to pick up on security breaches, and the human involved, with a reduced burden, is less prone to error.

However, one downside of automated alert systems is that they can make humans less attentive due to automation bias. Automation bias is a form of cognitive bias in which we overly trust automated systems. Parasuraman and Manzey (2010) argue that this is due to human tendency to take the least cognitive approach when decision-making, as well as the belief in the superior analytical ability of machines. A study in the field of aviation (Parasuraman et al, 1994) exposed the risks of this bias by comparing the impact of low and high levels of automation on pilot performance; the study concluded that pilots working with a high level of automation spent less time reflecting independently on flight decisions. Therefore, autonomous alert systems can affect security negatively as they cause automation complacency, making humans less attentive, more prone to error and therefore less efficient at combating security threats.

Finally, automated security alert systems are most prone to failure when any latent failures in the systems align with human errors from the analysts, as described by Reason's Swiss Cheese model (2020). Due to the threshold set in Misuse and Anomaly Detection systems, there is always a possibility of a breach slipping through unnoticed, especially if it is due to an attack pattern not previously seen by the machine learning algorithm. This latent failure would have most significant impact if it aligned with a security analyst's alert fatigue; human error in this case would cause catastrophic consequences, such as with the Chernobyl tragedy in 1986; operators violating procedure by overriding safety systems (human error) whilst there was a critical reactor design flaw known to party officials (latent failure) let to a fatal catastrophe. Therefore, usability may be impacted as the effectiveness of the system can be damaged by this alignment of error.

S4: Describe three different ways lay users conceptualise security threats, and discuss how these mental models affect user behaviour.

Lay users are defined by Cifter and Dong (2009) to be the users who have limited or no training in a particular area, such as security, despite being likely to have personal interests or special needs facilitated by technology which requires security. Their characteristics differ from professional users, who may be more aware of security and therefore more likely to act on it. Lay users are generally poor at recognising security risks and errors, and are unfamiliar with security concepts, thus causing them to follow their own beliefs about the importance of security and its necessity.

Firstly, many lay users view security as a secondary, 'enabling' task to their productivity, such that they are more interested in completing their primary task than protecting against an 'invisible' threat. Humans naturally prioritise primary, 'production' tasks as these are what they initially set out to do; security, on the other hand, is often viewed of as an obstacle to productivity, leading users to find work-around solutions to avoid spending too much time on it. For example, if a user is seeking to visit a website, then reading the 'Privacy Terms and Conditions' or cookie instructions would be an obstacle to their desired goal, making them more likely to click anywhere that will allow them to remove the pop-up from their screen. This desire of lay users for functionality is one factor behind the Mirai botnet attack of 2016 – users were handed working routers, and did not feel the need to read the manual to increase security, believing the engineers had already done the work to protect their devices. Therefore, the conceptualisation of security as counteracting non-important or irrelevant threats, such as 'cookie theft', causes users to avoid taking security measures when completing production tasks.

Secondly, many lay users view hackers as either 'basement enthusiasts' or 'corporate professionals', whose main interests involve chasing after 'Big Fish' or being 'contracted' by companies to steal data from corporations. This is a finding from Wash's 'Folk Models of Home Computer Security'; Wash categorised lay user beliefs about hackers, finding that many thought hackers were only interested in exposing financial or personal information. The main finding was that the users interviewed had decided that they were unlikely to be targets as they weren't 'rich' or 'powerful' enough to be targeted by one of these hacker professionals. This belief about hacker culture stems from the portrayal of hackers in films, often as a powerful computer geek working for a big company, whose only targets are dangerous criminals or big corporations. Leonie Tanser, in "50 Shades of Hacking", accounts for this historical shift in portrayal, arguing that there is a skilful movement between representing hackers as 'ethical or criminal', as well as 'autonomous or collective'. Therefore, lay users are unlikely to take secure measures to prevent their computers or accounts from being hacked, as they do not view themselves as likely targets.

Finally, Wash also found that many users don't view viruses as a security threat; they instead see them as 'Bad' or 'Buggy Software', with many calling "any malicious computer program a 'virus'". People with these particular folk models argued that viruses typically have no purpose, and it is 'bad' to "catch" one, but are not concerned about the safety of their data. Therefore, "respondents with this model did not feel that they needed to exert a lot of effort to protect themselves from viruses". This means they are unlikely to install anti-virus software, especially if it is expensive, as it would be seen as unnecessary protection against a non-dangerous threat. These users are also unaware of the possibility of becoming part of a botnet, although if they are not concerned about something which has no visible effect on their productivity or data protected, then it is unlikely that they would be concerned about any harmless botnet malware on their devices. Therefore, as they are not incentivised to purchase anti-virus software, and don't fully recognise the threats, lay users are unlikely to take measures to protect their devices against viruses.

L1 "Professionalisation of cybercrime has made everything better for cybercriminals" – Discuss

Professionalisation is defined as "a process whereby occupations have become, or seek to become, publicly recognised as professions according to the degree to which they meet the alleged criteria". The professionalisation of cybercrime in particular refers to the maturity of cybercriminal economies, services, and markets, as well as an increase in resources available to learn trade secrets, giving anyone with an internet connection the ability to take part in the profession of cybercrime. Cybercriminals can be considered to be anyone who takes part in cyber-enabled or cyber-dependent crimes. Arguing that professionalisation has made 'everything better' suggests that all aspects of the cybercriminal sphere have been improved for those taking part in it; in actuality, some cybercriminals have profited significantly more from professionalisation than others.

Firstly, one could agree with the statement by arguing that the development of services in the cybercriminal economy has led to easier access to resources, as well as the ability for anyone to learn a new trade. In 'The Professionalisation of Cyber Criminals', Gilles Hilary describes the development of the "Cybercrime-as-a-Service" framework which has stemmed from the professionalisation of the industry. Instead of one cybercriminal needing to possess all skills and software necessary to carry out an activity, they are now able to hire other cybercriminals who have greater expertise, allowing them to focus more specifically on their goals. An example of this can be seen in the spam email economy, where someone may choose to hire a 'harvester' to collect email addresses for them, or hire the use of a botnet from which to send the emails, rather than creating one themselves. Additionally, professionalisation has led to an increase in resources available for learning new trades; this can be seen in forums where 'eWhoring' has become increasingly popular. Hutchings and Pastrana (2019), in their paper titled 'Understanding eWhoring', describe forums in which "offenders readily share information about how it [eWhoring] is committed in a way that is almost prescriptive". This quotation indicates that fraudsters are willing to help one another engage in cybercrime in a way that would not be possible before such activities were professionalised. Therefore, the development of "Cybercrime-as-a-Service" has led to greater resources and support available to cybercriminals, making cybercrime more accessible and profitable.

Secondly, one may argue that professionalisation's biggest benefit to cybercriminals is the expansion of cybercriminal trading markets, as it gives them the ability to purchase a large range of illegal goods with little risk of being caught. For example, cybercriminals keen to get involved in fraud or identity theft can join an IRC network or Carding Fora, where a user can request to purchase one of a selection of types of credit card accounts, ranging from 'CVVs' containing generic card information, to 'fullz', which provide all security information necessary to commit identity theft. These markets also allow sellers to set prices for their goods, and provide a reputation scheme in which users of the forums can back trustworthy vendors. Additionally, cryptomarkets such as 'Silk Road' provide secure trading platforms that allow people to interact anonymously online. Nicolas Christin described 'Silk Road' as selling "insurance and financial products", with the business model being to "commoditise security". Cybercriminals were able to buy and sell goods, set their own prices, rate sellers, and pay securely through an escrow system, which helped to prevent scams. Cryptomarkets are still very prevalent in the dark web today, despite a large-scale takedown of marketplaces in 2015, due to many more being created when others are removed. This shows that professionalisation of cybercrime has led to a highly valuable global network of trade, which is benefiting cybercriminals by giving them the resources and opportunity needed to profit off of their profession.

However, one may argue that professionalisation of cybercrime has not made 'everything better' for all cybercriminals as it has led to an increase in competition between actors in the cybercriminal economy. Firstly, it is hard to profit as a newcomer to a trading platform due to the reputation system; buyers are much more likely to purchase goods from reputable sellers. This was particularly evident in the findings of a paper on eCrime, which saw that up to 70% of sellers in Carding Fora attract no obvious business, whereas a

few top users dominate 40-50% of business (Haslebacher, Onaolapo, Stringhini, 2017). This is evidence that not all cybercriminals are experiencing an improvement in sales due to professionalisation. Additionally, competition can lead to cybercriminals intentionally jeopardising one another, as is often seen in the spam industry: many malware programs installed on victim systems are programmed to identify and delete malware from other users, thus ensuring that the victim's machine is exclusively part of the cybercriminal's botnet. Furthermore, many malware programs are also known to patch vulnerabilities in host machines in an attempt to protect the existing malware and to retain the botnet host. Infighting between botnet operators is a significant productivity limiter, caused by the fierce competition for spam money. This is due to blacklisted email addresses and IP addresses resulting from spam filters, which make it harder for cybercriminals to find fresh emails and hosts to use for their crimes. Therefore, despite some cybercriminals managing to profit extensively from professionalisation, others are finding it harder to build a sustainable business due to competition, and are struggling to build the reputation needed to improve their sales.

Finally, one could argue that not all cybercriminals benefit from the professionalisation of cybercrime due to a lack of trust within the cybercriminal economy, brought about by scammers and 'lemons' in the market. Despite many cybercriminals running a legitimate business, complete with customer service (as is common in spam email economies) or payment via escrow (used by 'Silk Road' and many other cryptomarkets), not all transactions are honest or well-intended. 'Silk Road', in particular, was prone to many 'early finalisations' from sellers, who would ask buyers to confirm receipt of the product prematurely, and then leave with the funds, effectively cashing in on their reputation in the market. In addition, markets themselves would sometimes participate in 'exit scams', where they would trade as normal, allowing escrow wallets to fill up, and then cash in on reputation in a similar way to 'early-finalisers' by taking the money and abandoning the market. These scams remove trust in the cybercriminal economy, and negatively impact their victims, who are less likely to want to trade in a cryptomarket as a result. As well as scams, cybercriminal markets are also considered to "belong to markets for lemons" due to "information asymmetry of quality of goods and services between sellers and buyers" (Hoe, Kantarcioglu, Bensoussan, 2012). 'Lemons' in the market – poor-quality products – cause the price of goods to shrink alongside market demand. A lemon market does not benefit anyone who takes part in it, as products are less likely to sell, and buyers are hesitant to trust sellers. Therefore, professionalisation has led to an increase in scams and 'lemon' sellers, which discourages cybercriminals from participating in markets and reduces the quality of goods.

In conclusion, I would argue that professionalisation of cybercrime has had an overall positive impact on cybercriminals due to the availability of goods and services, especially the accessibility of malware, botnets, vendors, and information used to carry out cybercrime. However, I disagree with the notion that professionalisation has made 'everything better' for all cybercriminals, as it is clear that not everyone profits equally from these fiercely competitive markets. Those who are atop the hierarchy have large businesses with regular sales in forums and markets, but it is important to note that as cybercriminals, most are likely not to be trustworthy, thus it is likely that they may eventually cash in on their reputation and run an exit scam. Additionally, for those starting out in cybercrime, some markets are very difficult to penetrate, and taking part can also mean putting yourself at risk of being targeted by rivals (as is seen with botnets in the spam economy). Therefore, whilst cybercrime is more accessible and profitable than ever, not all cybercriminal professions are equal, and fierce competition paired with a lack of trust creates a system in which some are far more successful than others.