COMS30036 - Security Behaviours

1 Question 1 - S1

An example of a market failure in security is the repeated data breaches many companies suf er from, millions of users data is regularly leaked by giant companies such as Uber, Facebook, Twitter, Slack, also including the U.S. Army and Department of Defense.[1] A lot of these are preventable as the method listed is "poor security" or "social engineering", and in the case of U.S. Army, "accidentally published".

The real issue however is that not a great deal happens to the companies after a breach happens, they give a public apology and commit to improving and doing better, and pay a small f ne relative to their prof t. Using Facebook as an example they had three data breaches in 2019 alone, either they did not learn from their mistakes and improve security, or they decided the f ne was cheaper than implementing better security. Either way the users of Facebook were arguable worse of as it was their data leaked.

The most obvious solution to tackling this is to actually hold the companies accountable, just increasing the f ne to be a larger percentage of annual revenue for example so that it is not the equivalent of a speeding ticket may be enough encouragement for them to put more ef ort into security.

Another solution could be having a clearly def ned set of rules and requirements that need to be met in order for your company to be eligible to store user data. The idea being if these rules and requirements are created and updated properly it should increase general security of data. As nice an idea this is it is unlikely to actually work due to the huge scale it would operate on and the inability to update fast enough to keep up with new attacks.

The f nal idea is to reduce the amount of personal information companies are able to store. Obviously some information like email addresses for logins will need to be stored, however users have the option to create an email address such as "anon-facebook-user@gmail.com" or equivalent to increase their privacy. There is no need for companies to keep the amount of mass information they currently do other than to sell for prof t or for targeted advertising. Clearly this af ects usability and features such as Amazons "1-Click purchase" may not work without the ability to store real name, address and card details, however it would be ef ective at reducing data leaked in the event of a breach.

Out of these approaches the most realistic is larger f nes, with the bigger idea being actually holding companies liable for their mistakes. While not even close to a perfect solution I believe it is a step in the right direction as companies will have an incentive to focus more on security as now the punishment isnt the equivalent to a speeding ticket.

2 Question 2 - S2

Before discussing the positives and negatives of automated security alert systems with regard to usable security it is important to define what this means. An automated security alert system is a system that will alert a user that something to do with security has gone wrong. A vulnerability has been discovered and they are at risk, they appear to be under attack, or some anomaly has occurred etc. To cover all bases this system should span system, network and application level. An example could be an intrusion detection system (IDS) which will monitor the network for anything suspicious. While an IDS can be setup to automatically deal with the issue for this case we imagine it just alerts.

Usable security is the idea of fitting the task to the human, rather than fitting the human to the task. To most people security is a secondary task and only blocks their progress towards their main task, by making security as easy and usable as possible it increases the chance people will use it as intended and not try to get through it as quickly as possible.

To begin on a positive note, an automated security system has a lot of benefits, the most obvious being it will reduce the workload on the user. As an example, not even security conscious individuals will want to read though pages and pages of logs looking for an anomaly they may or may not spot, which may or may not be anything important. Doing this on a home computer will be bad enough but imagine a system administrator doing this in a large organisation with 1000s of people. Does not sound like a good use of time. Something like an IDS as previous mentioned will be able to automatically monitor all these logs in the background and if an anomaly or malicious behaviour is spotted it will be able to alert the user. Once they have this alert they may want to manually check the logs but they will know exactly where to look and hopefully already have an idea of what is going on.

Security tools should be assessed for usability base on the following:

- Effectiveness - "Can users achieve their goals?"
- Efficiency - "What resources are expended to do so?"
- Satisfaction - "What is the user level of comfort and acceptability?"

In the context of what we are discussing, an automated alert system is effective assuming the users goal is to be alerted about possible security breaches. It is a lot more efficient than the user doing the monitoring themselves and so less resources are expended by the user. Satisfaction is obviously harder to arbitrarily guess however it is probably fair to say the user will be satisfied with their workload being decreased and knowing their systems are being monitored. So based on these criteria an automated security alert system seems to be very usable.

A drawback to automated alert systems is alert fatigue. This ties in to the idea of humans having limited capacity, if the alert system is on the safe side and alerts for any anomaly there will be a lot of false positive alerts. Filtering out all the false positives is a high cognitive load and so eventually the user may ignore an alert thinking they see it all the time and it is a false positive, when in reality that alert was correct. The system also may give a false sense of security, even the best systems have the potential to miss things, and if you believe the system is perfect and will save you if necessary may lead you to being less cautions. Venaf, an Australian cybersecurity company agreed with this in the context of ransomware saying "our

research shows that while most organisations are extremely concerned about ransomware, they also have a false sense of security about their ability to prevent these devastating attacks".[2] While in a different context it still is a real life example of having a false sense of security towards cybersecurity.

3 Question 3 - L1

Has professionalisation of cybercrime made everything better for cybercriminals? First it is important to discuss how cybercrime has become more professional. In the grand scheme of crime, cybercrime is relatively new, and as such is continuously evolving, however more recently there has been a clear shift towards commercialisation and organisation, and with this sophistication. For example instead of scam and phishing emails being sent to every inbox possible, now there is spear and whale phishing, targeting individuals and executives respectively, generally with the plan to get a specific bit of information or access to a specific network.

A reason for the increase in professionalisation may be that traditional organised crime groups are being introduced to the world of cybercrime, and not wanting to miss out on their share of the profit join in themselves. Generally they will begin with cyber-enabled crime, this is the traditional crime they were already involved in just moved online e.g. drug dealing, instead of selling drugs on the streets they will sell them on a darkweb marketplace.

If you discount these traditional criminals as cybercriminals for now as they are just starting, you may think their involvement would not be a good thing for the preexisting cybercriminals as they are effectively stealing their jobs. While this may be true to an extent as there is now more competition in certain categories such as drug dealing, someone had to make the website, someone has to host it (while hosting a website is obviously not a cybercrime the hosting companies who turn a blind eye to what they are hosting are at least partially aware what is going on), there has to be site moderators and admins etc, you get the idea. The organised crime group is just one moving cog in the wheel, and in fact a lot of people will benefit from the extra work, e.g. the person who created the website likely will take a few percent of each sale, the more sales, the more money they make.

Looking towards cyber-dependant crime now, this is crime that is not possible without computer systems and commuication networks. Think DDoS attacks, ransomware, malware, darkweb market exit scams, cryptocurrency thefts, the list goes on and on. Originally hackers were just interested in reputation, with certain fourms (fourms and IRC seemingly being the de facto method of communication) wanting you to show a certain level of skill such as HackFourms wanting you to show possession of a botnet.[3] Wanting the feeling of belonging or thinking hacking is cool, whatever it may be, encouraged individuals to do things such as create a botnet to join these communities.

However now these skills are in high demand, and understanding basic supply and demand says these skills come at a high price. Suddenly what was a hobby now has the potential to turn into a well paying job, assuming you factor in the danger pay due to the whole thing being illegal. With this increased professionalisation of cybercrime it now has similarities to any other industry, with specialisation and specific roles, and people being hired to do tasks like contractors. Sophisited cybercrime may involve multiple coders, social engineers, darkweb

market vendors, cashiers and money mules. This is a clear benef t for preexisting cybercriminals as they have already passed the moral barrier of committing cybercrime, now they get paid as a bonus.

There is also the benef t of interest in your skills from legitimate companies and governments. Unsurprisingly the best way to defend against hackers, is to hire a hacker. A hacker will have inside knowledge of how a range of hacking techniques work, and likely be as up to date as possible as they are part of the group creating new techniques, compared to a computer science graduate or cybersecurity professional who will lack the insider knoledge and unfortuantely always be behind because as soon as something is written down it is practically out of date as someone is already working on a new technique.

Using Marcus Hutchins[3] as an example, he temporarily stopped the WannaCry ransomware attack by f nding the killswitch via reverse engineering the ransomware, a skill he learned by being apart of hacker fourms and creating malware himself. While Marcus Hutchins already had a job at the time he did this, he was hired when the CEO noticed his blog about reverse engineering, and so was hired based of of his skills learnt from hacking.

Certain governments, namely China and Russia being the biggest, also either hire hackers for state-sponsored cybercrime, or just encourage non-state cybercrime against states other than their own. This is a similar situation to Marcus Hutchins when having preexisting knowledge will give you an advantage in getting these jobs. In the case of encouragement of non-state cybercrime it is not out of the realm of possibility the individuals behind these attacks would be rewarded in some way even if it is not directly with a job.

In answer to the question I think professionalisation of cybercrime has made most things better for cybercriminals. For preexisting cybercriminals, if they continue to do what they were doing, creating malicious software and conducting attacks, assuming they f nd a buyer which is seemingly getting easier and easier as more people want to get involved in cybercrime, they will get a paycheck as a bonus.

An obvious drawback is the attention brought upon cybercrime and harsh punishments being given out to those caught as an example, however tracking down cybercriminals is dif cult to begin with, then there are troubles with jurisdiction and lawmakers as they do not always understand the technology. So as long as you are careful and not unlucky you have a good chance of getting away with it. Also if you live in some countries (Russia, China, etc) this may not even be a worry as long as you do not target your home country.

References

[1] "List of data breaches," Jan. 2022, page Version ID: 1066068334. [Online]. Available: https://en.wikipedia.org/w/index.php?title=List_of_data_breachesoldid=1066068334

[2] "False sense of security plagues organisations threatened by ransomware." [Online]. Available: https://securitybrief.com.au/story/falsesenseofsecurityplaguesorganisationsthreatened-byransomware

[3] "Marcus Hutchins," Jan. 2022, page Version ID: 1066019193. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Marcus_Hutchinsoldid=1066019193