

CYSE 200T Journals

1. Why are you interested in cybersecurity?

I think the biggest reason I am interested in cybersecurity is because of the challenge that the career holds. I enjoy the problem-solving aspect of cybersecurity. You identify a problem and have to find a way to solve it. Plus, I find it pretty interesting how you are defending and attacking malicious hackers at the same time. Like a big capture the flag game but you're getting paid along the way. Though I have only completed labs regarding preventing and stopping cyberattacks, there's something really rewarding about doing so. Definitely, something I can see myself doing in the future. After experiencing cybersecurity in the few classes I have taken so far, each new thing I learn sparks my interest even more. Everything from pen testing to learning the ins and outs of malicious attacks makes me more excited to use this knowledge and tackle these problems in the real world. Another big reason is the sheer career opportunities cybersecurity offers. . With cybersecurity being interdisciplinary, there is a multitude of different paths to take. You can take a white hat hacker stance and hack for good or even use the knowledge of cybersecurity to enforce the law. Even so, there's not one singular path in cybersecurity and the jobs are plentiful. In a class I took last semester, I learned that the unemployment rate for cybersecurity jobs in Virginia was 0%. Though this doesn't mean a job in the field is a given, it does act as one of the plenty reasons to pursue a job in the career. Along with there being a need for cybersecurity professionals in the workforce, the jobs also come with good pay. I do know that the pay isn't the sole reason to take a job, but it doesn't hurt to be getting paid well for doing something you find really interesting.

2. Select four other majors offered by ODU and explain how those majors relate to cybersecurity

The first major I chose was criminal justice. There are a lot of ways how cybersecurity goes hand in hand with criminal justice. With cybersecurity being multidisciplinary, criminal justice falls in one of the categories of cyber security disciplines. Cybersecurity isn't just the prevention and protection against cyber attacks. Cyber Security also strives to defend against cybercrime in general. One way to look at cybercrime is from a criminal justice point of view. Understanding how to prosecute and charge cyber offenders is just as important as stopping them in the first place. Also using cybersecurity techniques can also assist in the actual prosecution of cyber offenders as well as traditional offenders. The second major I chose was psychology. Psychology is also one of the disciplines that coexist with cybersecurity. Another big part of cybersecurity is understanding the human aspect of why people commit cybercrimes and why people fall victims to such crimes. Using a psychological point of view further helps

the prevention and protection from cybercrime. The third major I decided to talk about was Information systems and technology. With this major focusing on the systems that store and process information regarding its relation to cybersecurity is very prevalent. Cybersecurity can be seen as the steps and safeguards that protect these systems. Understanding how information tech systems work will assist cybersecurity professionals to protect them. The same goes for information systems and technology professionals. Understanding the techniques of cybersecurity can help them create more secure systems to hold our information. The last major I chose was sociology. With sociology being the understanding of how people interact, it can be a big help in understanding cybercrime amongst humans online. With social networks online growing, we are seeing that cybercrime subcultures are forming. Scamming groups, hacker groups, cyberbully culture, etc. Analyzing these groups from a sociology point of view as well as a cybersecurity perspective, we can easier understand and stop these subcultures from committing cybercrime.

3. Describe four ethical issues that arise when storing information about individuals

I think the biggest ethical issue that arises when storing information about individuals is what the companies and the people that hold the information are allowed to do with this information. It has become a big issue regarding companies selling user data and information. Though there are ways to deny companies from doing this, many people are unaware of how to do so and are even ignorant of the fact that their data is being sold in the first place. I think it becomes an ethical issue when the user doesn't know what their data is being used for. Another big issue about storing information about individuals is the protection of the data itself. Every year a handful of companies are attacked with ransomware and other data-threatening cyberattacks. It's the company's priority to protect the data that they are storing. Though most of these companies are relatively transparent and quick to react to these types of data attacks, it still becomes an issue regarding the users' data being stolen. Companies should be liable for any issues the users experience as a result of their data being attacked through the companies. It becomes a problem when the individuals storing the information do not offer any remedies to the user's problems resulting from the attack. The next ethical issue is another way that companies use the user data. Last year I was tasked with reading "Automating Inequality" by Virginia Eubanks. That book outlines how the use of automated systems can create inequality and discriminate against people through their data. One example she wrote about was the welfare problem in Indiana. In Indiana, they tried to automate user data to match them with the correct benefits from the state. Though this would have made it easier and faster to match people with the correct benefits, it actually ended up denying certain people from obtaining the benefits they needed. With this being said, the use of the data to automate systems becomes an issue if

not executed correctly. This was only one of the many scenarios in Eubanks's book where the use of user data harmed the user rather than assisting them. The last ethical issue regarding the storing of user data is the ability of the user to access this data. Users should be able to access all the data the company has on them as well as have the right to request the deletion of such data. It becomes the issue of what certain rights the user have around their own data

4. Compare cybersecurity risks in the U.S and another country

When we look at cyberattacks around the world we see that there is a multitude of motives around when countries are being attacked online. This can be for money, control, or country-sponsored sabotage. When looking at the cyberattacks that take place in the U.S we see that most of them are for monetary gain. Though this may be true, it doesn't mean that the risk of state-sponsored cyber attacks with the goal to hurt the country's infrastructure as a whole isn't there. With tensions being high(as of the time of writing this) between the U.S and Russia, the chance for a state-sponsored cyber attack is pretty high. After completing this module I learned the risk of a cyberattack against the U.S power grid. In my opinion, this becomes a huge risk if the conflict between NATO and Russia escalates to a possible world war. An attack like that would have detrimental effects on U.S operations. We saw the effect the pipeline attack had on the east coast. It caused panic, limited gas, as well as the price of gas to skyrocket. It just goes to show how cyberattacks against the U.S resource and power systems become a huge risk even if the conflict with Russia calms down. I think of it as a ticking time bomb if we don't better secure our critical systems. On the other hand, if we compare these risks to Ukraine in this situation, we see that the risks are somewhat different. With the tensions between Russia and Ukraine growing exponentially, I have read that Russia has been behind multiple cyberattacks against Ukraine as well as promoting disinformation campaigns in Ukraine. Just recently Ukraine experienced a cyberattack shutting down a plethora of Ukrainian governments websites. Though the attackers have not been named, evidence shows it to be a possible attack from Russia. If so, I assume this attack to be a ploy to weaken Ukraine from the inside and create panic within Ukraine's borders. Unlike the U.S risks, this attack isn't as detrimental as some of the possible attacks in the U.S. Like stated earlier, Ukraine also experienced disinformation campaigns from Russia. Though the U.S has the risk of disinformation campaigns the severity compared to Ukraine's isn't as high. In summary, both countries are at risk of cyberattacks. The main difference between these attacks is the motives and severity of these attacks.

5. Use the letters of the world cybersecurity to list legal ways to make money in cybersecurity

- Creating a cybersecurity firm
- Yielding security design principles
- Being a cybersecurity professional
- Ending an attack from a hacker on a business
- Running a proxy server or firewall and charging money for its use
- Selling your cybersecurity skills
- Entering a capture the flag competition
- Cybersecurity professional
- Using your cybersecurity skills in a business
- React to cyber attacks in a company setting
- Implementing a cybersecurity plan for a company
- Talking to other cybersecurity professionals
- You create your own antivirus software

6. How has cyber technology created opportunities for workplace deviance?

With the boom of cyber technology, it makes sense that there have become opportunities for workplace deviance. Companies all around the world have incorporated their finances, operations, and communications all into the realm of the internet. With most of the company's functions and operations residing online, the chance for malicious insiders to exploit this internet-based infrastructure for harm rather than its intended use. Though acts of workplace deviance, in some cases, may not be particularly illegal, it still has the ability to impact the operations of a company. An example that I find to be a reoccurring problem, that I have either read, heard, or seen firsthand, is the use of workplace assets for things other than work. In this, I mean using company property, the internet, resources, for things like browsing the internet, messaging people outside of the work organization, really anything other than work. Though these acts may not be particularly illegal, it is definitely deviant in a company's view. Another topic to look at is how cyber technology has created opportunities for white-collar crime. White-collar crime differs from deviance due to the fact that white-collar crime is illegal while deviance is just seen to be wrong while not actually being illegal. Cyber Technology, in a company setting, has given malicious insiders also more ways to commit crimes. White-collar criminals may have many possible motives with some being financial gain, revenge, or even for the fun of it. The incorporation of cyber tech in companies has only made it easier for this to happen. The fact that companies hold so much of user data and information, is unnerving in a sense because there could be one malicious user in the company that can access this data for harm. Overall though, companies' connection to the internet makes it easier for cybercriminals and deviants to thrive in the workplace setting. Everything being connected through

cybertechnology provides outlets to criminals and deviants in both the workplace setting as well as the internet in general

7. What are the costs and benefits of developing cybersecurity programs in business?

One could argue that cybersecurity programs are a double-edged sword. Cybersecurity programs, though mostly being good, also come with some negative consequences. In my opinion, a cybersecurity program is a necessity in the workplace setting. With almost every company being connected to the internet, the need for cybersecurity is crucial to protect a company from the exploitation of this connection. The good thing about cybersecurity is the fact that it is malleable in a sense. Depending on the size, infrastructure, field of work, or criticality of the business, cybersecurity programs can change to best protect the company's specific scenario. Cyber security programs have the ability to save companies money, keep the company's reputation, and keep the shareholders happy. Regarding saving money, cybersecurity has the ability to do this by stopping money from being taken from the company through a cyber attack. According to cybercrime magazine, cyber attack financial loss was predicted to reach 6 trillion dollars in 2021. This insane number proves that cybercrime is the forerunner of companies' main financial loss. With a Cybersecurity program, the chance of losing money to a cyberattack drastically decreases due to the over-protection it provides. In the sense of reputation, cybersecurity programs also offer protection to the company. Companies that are victims to cyberattacks don't just lose money, but their reputation as a company in general. Falling victim to a cyberattack is never a good look for a company. Luckily such cybersecurity programs can mitigate the risk. Cybersecurity programs, though being helpful, also have their drawbacks. Effective cybersecurity programs have the potential to be rather expensive. An article from securityfoward.com stated that larger companies spend around 20 to 50 million annually on cybersecurity. One must pay cybersecurity professionals, user training, the resources needed to create a secure environment, cybercrime insurance, etc. With this being said it makes sense that companies have to spend so much on cybersecurity. Though being expensive, you really do benefit from being secure. Saves companies money, reputation, legal issues, etc.

<https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

<https://www.securityforward.com/how-much-do-companies-spend-on-cybersecurity/>

8. How can you tell if your computer is safe?

With cybercrime being so prevalent in today's society, it really is somewhat tedious to really ensure the safety of your computer. Cyber attackers have the ability to attack from a broad area of fronts and cause harm to you and your computer. This requires that every possible point of entry is covered. In my personal experience of things, I have found that antivirus software, secure internet connections, strong passwords, and a skeptical mindset while on the internet are best to ensure the safety of your computer. Antivirus software is definitely a smart idea when it comes to protecting your computer. Most antivirus software available today offers the ability to scan your system's files to find any malware. With users not being able to do this manually, it shows that antivirus software is a must to ensure the malware isn't in your system. I, personally, use Norton 360. After using Norton for a year or two now, it has proved to be a worthy asset to my arsenal of safeguards. Norton 360 offers downloaded file scanning, disk cleanups, VPN capabilities, firewall capabilities, website scanning, etc. With this being said, some antivirus software have the capability to be more than just a traditional virus scanning program. I do want to touch on the topic of strong internet connections. This is also one of the most important aspects of keeping your computer secure. An example I can think of is the security of wireless internet connections. There are so many ways hackers can exploit a weak wireless connection. For example, let's say you're at a coffee shop catching up on some CYSE 200T work. Unfortunately, you do not have a hotspot so you must use a wireless network offered at the coffee shop. After scanning you find Free_CoffeeShop_Wifi and think that it is the network offered by the coffee shop but in reality, it is a spoofed network broadcasting from an attacker's computer. After being connected, the attacker can then use your connection to monitor your traffic, and activity online, and possibly redirect you to malicious websites. Making smart decisions is really the key part. Being smart when it comes to cyber tech and the internet is to be vigilant, secure, and not gullible. In conclusion, to first check the safety of your computer, run an antivirus program and scan for any malware. Anything after that, the real way to tell your computer is safe, is to make sure you have the necessary safeguards to keep it safe.

9. Describe three ways that computers have made the world safer and less safe.

I have always liked the bad news first so I will be talking about the less safe ramifications. I think the first and most important way that computers have made the world less safe is due to the fact that it is the medium by which hackers harm others. To attack someone via the internet one must be using either a computer or phone(which could be seen as a handheld computer). I think the second way that computers make the world a less safe place is due to the environmental ramifications the creation of computers has. With millions upon millions of computers being manufactured every year, the old models are bound to become obsolete thus making them waste. Theworldcounts.com stated that we humans throw out up to 50 million tons of unused “e-waste” every year. This growth of computer trash is bound to cause adverse effects on our environment. Another topic I want to talk about is the fact that computers have the chance to take away jobs from humans. Though automating functions saves money and looks like a good idea from a business owner's standpoint, it also has the chance to leave the masses unemployed. Though computers have their lows it also has their highs. One way that computers have made the world safer is by offering quick access to information. By this I mean in areas like first responders, medical, military use, etc. Having data/information easily accessible is crucial in these areas, especially in the medical field. The next way that computers make the world safer is by offering an outlet for those that may struggle in the real world. Computers can act as an escape for some people which is in a sense healthy. This could also be seen as a bad thing but I won't touch on that now. The last way computers make the world safer is by promoting use to create and grow. Computers allow us to create new ideas, new medicines, new structures, etc. With computers almost anything is possible. That in itself causes computers to be a very sharp double-edged sword.

<https://www.theworldcounts.com/challenges/planet-earth/waste/electronic-waste-facts/story>

<https://www.javatpoint.com/what-are-the-disadvantages-of-a-computer>

10. How do engineers make cyber networks safer?

Engineers play many roles when it comes to making cyber networks safer. They are the ones that keep a company's system in its most secure form. One of the ways that engineers make a cyber network safe is by actually setting up the security features of a network. One example of the features these engineers set up is a firewall. A firewall acts as a filter that only allows certain things in and only certain things out. Each company's firewalls have certain rules on such data that is allowed to be sent and received. The engineers in this example are the ones that set such a safeguard up. Alongside setting up the rules of the firewall and its logical location in the network, the engineers are also responsible for the maintenance of these firewalls. Hackers are always evolving which means the way in which they are stopped evolves as well. An engineer must be aware of this change and adapt as it comes. Another way that an engineer can keep a network safe is by creating and or implementing antivirus software on the systems in the network. Software engineers create the antivirus the actual programs to keep them safe while network engineers and security engineers implement it into the network. With there being different types of engineers, the task of keeping a network safe isn't limited to one role of "engineer". In this module, we learned about engineering systems. Everyone in this system could be considered an engineer based on the shared goal of engineering a secure system. Some engineers may be tasked with managing the risk of attacks, some may be the ones creating the software to secure the network, some may be setting up the network, and some may be working the stop the attacks on the network. The list of these tasks goes on. I think overall engineers play a lot of important roles in network security whether it be the policy side of things or the actual technical side of things.

11. What is the overlap between criminal justice and cybercrime? How does this overlap relate to the other disciplines discussed in this class?

With the boom in technology, cybercrime has obviously become a more frequent thing. But with this cybercrime has also come the way to stop it, enforce laws regarding it, and the need to understand it, all through the eyes of criminal justice. Cybercrime has changed the way we look at criminal justice as a whole. Unlike traditional crime, cybercrime has become more frequent and complicated to enforce due to the fact that it is harder to apprehend offenders. The internet and technology, in general, have become the mediums for a surplus of crime due to the ease of committing crime online and getting away with it. This overlap between cybercrime and criminal justice has been prevalent ever since the creation of our internet-based society. Still to this day, the criminal justice system is still adapting to this growth of cybercrime. In this class,

we have talked about attacks against critical infrastructure, white-collar crime, hacking, and the fact that “cyber-criminal justice” and cybersecurity are interdisciplinary. All of these topics have played a role in how the criminal justice system analyzes cybercrimes as a whole. Being able to understand the social, psychological, business, and user-related disciplines regarding cybercrime have only strengthened our knowledge of how to use criminal justice to stop cybercrime. Criminal justice as well cybersecurity have to be adept in every discipline to really understand, prevent, and stop cybercrime. One could argue that cybercrime is even broader than traditional crime, in the sense that cybercrime covers more areas than actual face-to-face/in-person traditional crime. With this being said, in the eyes of criminal justice, the analysis of cybercrime must also be broader to cover all fronts in which cybercrime occurs and takes place. Overall, cybercrime must be a more talked and visited topic in the terms of criminal justice. Personally, I think that it isn't talked about as much as it should be.

12.How does cyber technology impact interactions between offenders and victims?

Cyber-tech in general has offered as a new medium for cyber offenders to thrive. Being that cyber-tech interacts on the internet a the ways for new crime, cybercrime, has broadened significantly. With cyber-tech ranging anywhere from a phone to a company's server, merely anyone using such tech can become a victim someday or another. Cyber-bullying, hacking, extortions, black-mail, cyber-stalking, etc. The list goes on. This new way of crime has caused offender and victim interaction to differ greatly from traditional crime. For example, let's compare stalking and cyber-stalking. Traditionally, the crime of in person stalking can include following someone around physically, stalking them when they're in a private area, overall harassment and fear tactics etc. Fortunately, if the stalker were to be caught and apprehended, the victim could file a restraining order against the offender. This could cause less stress to the victim due to the fact that it would be significantly harder for the offender to offend again without being severely punished. Cyber-stalking on the other hand is a whole new story. Due to the infrastructure of cyber-devices connected to the internet, the offender never makes direct human contact with the victim. The thing about the internet is that even if the victim were to block or report the offender, the offender could just make a new profile or account thus continuing the cycle of offending. Unlike traditional stalking, cyber-stalkers are harder to trace and apprehend. With this being said, the interaction between the offender and the victim can go on for who knows how long. It's harder to pursue legal action against a cyber-stalker compared to a traditional one. With all this being said, one could say that the offender/victim interaction was somewhat worsened due to cyber technology. I only describe one way that cyber-tech has changed the way that offenders and victims interact out of the many. It just goes to show cyber-tech has changed society in general.

