Discussion Board 1

After reading today's discussion article, I am more interested in Cloud Security Architect and Cybersecurity Law (Freeze, 2021). More often than not, we think of these jobs as falling into the discipline of Computer Science. Still, after careful examination, we can conclude they intertwine with several fields. For example, Cybersecurity law involves Criminal Justice and Criminology while dabbling in Sociology and Victimology (Kirkpatrick 2022). One could argue that philosophy is also a discipline involving cybersecurity law. Also, as we look into Security Architect, fields like engineering, computer science, and IT heavily involve themselves.

While keeping the previously mentioned idea of interdisciplinary and their parent disciplines in mind, it is easy to delve deeper into what exactly these two occupations (security architect, cybersecurity lawyer) accomplish daily and their various occupational standards. It is no surprise a cyber lawyer involves both "large and small companies as well as individuals" (*What Is Cyber Law? | Becoming a Cyber Lawyer*, 2018). An industry standard for a cybersecurity lawyer is, as any lawyer, successfully passing the bar. However, cybersecurity law is so challenging because of how quickly tech advances versus the legal world. Interestingly enough, in our lecture for this module Professor Kirkpatrick also makes the previously mentioned correlation. But how does this relate to our topic of discussion involving various disciplines?

Simply put, cyber lawyers delve into sociology, philosophy, psychology, and victimology while being knowledgeable in political sciences and information technology. It sounds like quite a bit of mingling for one occupation. This intermingling is also true for an amazon cloud security architect.

While last to mention, a cloud security architect is no lesser than a cyber lawyer by any means! From IT, engineering, and computer science to sociology and leadership, a cloud security architect provides solutions, expertise, delivery, and insights with AWS engineering in creating roadmaps to AWS tech (*Cloud Security Architect*, 2022). They are your A to Z types, and what an absorbing field of disciplinary knowledge! After researching the above two occupations, which one could you see yourself doing? None of the above? Or maybe, let's get crazy here, both?

Discussion Board 2

Understanding the NIST Framework as an entry-level cyber security analyst helps to describe, identify, assess and communicate cybersecurity topics within an organization. Understanding the NIST Framework reduces cybersecurity risks ("Framework for Improving Critical Infrastructure Cybersecurity," 2018, p. 2*).*

Describing and Identifying

The NIST Framework is not an A-to-Z checklist but a structure beginning with the framework core. The "core presents industry standards, guidelines, and practices "(p. 3). In most workplace settings, it helps to describe an issue. Arguably an even more important skill is to be able to

identify a problem. In other words, you can't win UNO if you don't know what each card means. Think of a cybersecurity threat as the elusive draw four cards.

Assessing and Communication

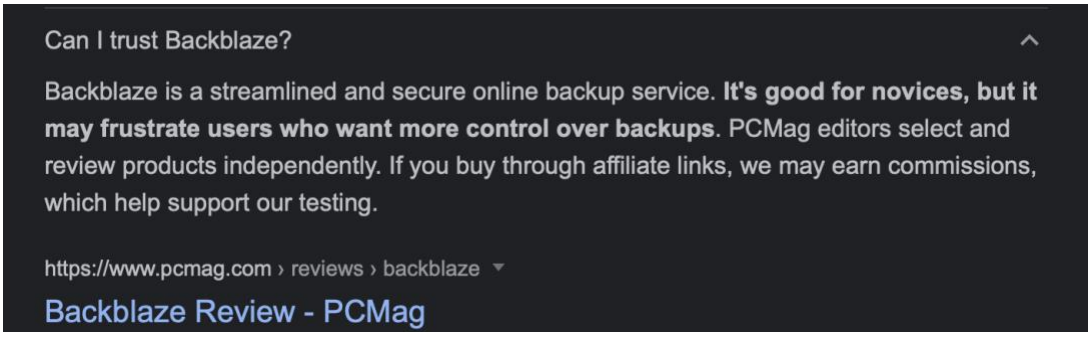
Once an organization knows they have or have the potential of a draw four card being in play, it's time to assess and communicate. The NIST Framework considers an organization's current cyber security risk and defense/offense for dealing with cyber threats (p. 3). Another way to think about it is; how many cards are in a player's (organization) hand, and how many cards are left (do they have the infrastructure)? What if a player (organization) can't count or is blind (tier-1)? Are there other ways to win at UNO in these scenarios? They can; it boils down to communication. The NIST Framework profile describes an organization's current and future cybersecurity goals. It is crucial to note that "profiles can be used to conduct self-assessments and communicate with an organization "(p. 4). An organization produces a better product or service when it knows who holds the cards, what the cards mean, and how to win.

As an entry-level cyber security analyst, my overall strategy in UNO is identifying possible data breaches within a system and effectively relaying this information to my supervisor. Hopefully, I will be successful in reducing an organization's cybersecurity threats!

Discussion Board 3 Response

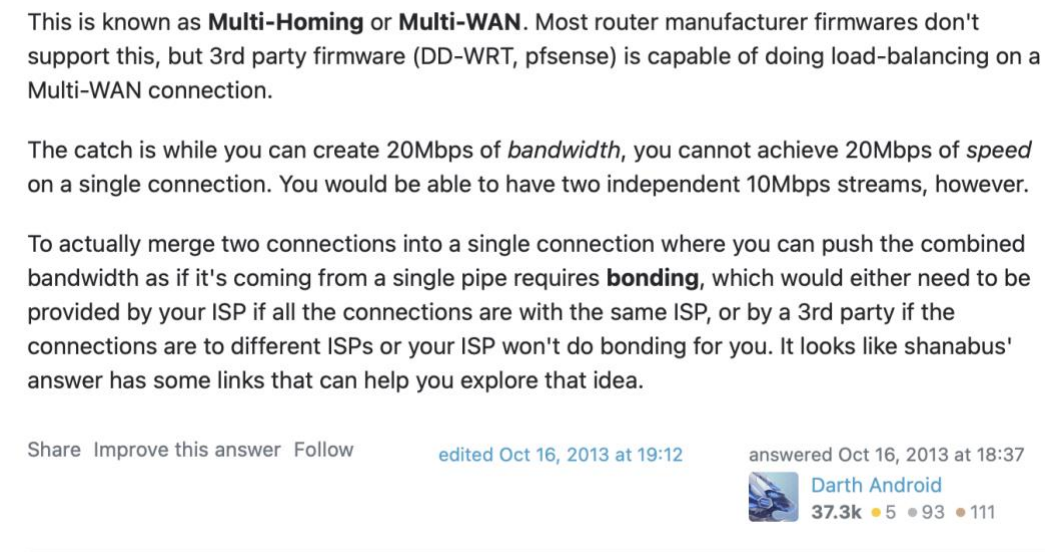
Great post! See linked videos and answer personal questions at your leisure/discretion. I enjoyed reading your post, and I ended up researching all of your recommendations. Thank you for providing me with some insight!

Comment and Recommendation
Fantastic job integrating our required readings into your post; I will look for your name from now on when scanning through our discussion boards (I love the use of "whilst"). Here is my email (jali004@odu.edu) if you are open to collaborating on the coming exercises or connecting with me on LinkedIn ,But back to you! What are your thoughts on the comment below (linked article)?



Because you mentioned protecting your firewall and single-point failure, here is., a video I think you'll enjoy. If you have time, can you explain how you would load the balance of two one-gig

lines? When I researched the matter, it seemed like a person couldn't with a broadband connection. Here is what I found most helpful:



This is known as **Multi-Homing** or **Multi-WAN**. Most router manufacturer firmwares don't support this, but 3rd party firmware (DD-WRT, pfsense) is capable of doing load-balancing on a Multi-WAN connection.

The catch is while you can create 20Mbps of *bandwidth*, you cannot achieve 20Mbps of *speed* on a single connection. You would be able to have two independent 10Mbps streams, however.

To actually merge two connections into a single connection where you can push the combined bandwidth as if it's coming from a single pipe requires **bonding**, which would either need to be provided by your ISP if all the connections are with the same ISP, or by a 3rd party if the connections are to different ISPs or your ISP won't do bonding for you. It looks like shanabus' answer has some links that can help you explore that idea.

Share Improve this answer Follow edited Oct 16, 2013 at 19:12 answered Oct 16, 2013 at 18:37

Darth Android

37.3k ● 5 ● 93 ● 111

Personal Qs as CISO

What is your preference for physical backup storage? Would you consider hiring security as well? I am 100% onboard with security, but after watching the upcoming lectures in module four, I think as CISO, we may advise, but the decision ultimately lies with a different department. What are your thoughts?

Reference to Required Reading (NIST.IR.7621 revision 1, p.6)

Regarding business resources, what is the likelihood of a private company outage because of a hostile actor, or is there more likelihood of environmental causes? My best guess is hostile actors in the form of phishing attacks.

As always, I look forward to reading your post's response and thoughts on the above commentary.

Discussion Board 3 Main Post

As acting CISO my main goal in ensuring the core value of availability is efficiently communicating while balancing IT department morale, workload, and threats with company goals and continually training all departments on safe data/device usage.

What is a Public Trade Company?

Companies whose shares are available for public trade in an open market, for example, amazon, apple, and Microsoft (Bowman, 2022).

What is a CISO?

Chief Information Security Officer or Senior Agency Information Security Officer (SAISO)

Carrying out responsibilities under FISMA and serving as liaison (Nieles et al., 2017, p. 14).

What is Availability?

Access to data, services, and systems that are on time and reachable (pp. 14, 21, 28).

Gameplan (Ensuring Availability of Systems)

Maintain proper and efficient communication with the CEO while maintaining other business connections for outsourcing incident teams if needed (Ommern et al., 2014). Also, map goals of CEO and company while setting boundaries and limits on own staff. Involve the CEO and CFO in creating a data recovery plan (Chai, 2022).

Keep staff up to date with training and handling of devices.

Emphasize CYOD versus BYOD with the CEO and educate the CFO on both advantages and disadvantages.

Employ a 24/7 *dream team* (monitor/incident team), a 48-person group consisting of two persons per shift who work four-hour shifts with mandatory breaks every hour, one person at a time. Also, no person shall be working within the same 16-hour period. Cycling of employee readiness is essential and valuable in maintaining a fully functional available system. Lastly, use automated tools "to help uncover a variety of threats and vulnerabilities" (p. 14). A system cannot be open to employees if compromised; therefore, purchasing systems will heavily depend on if the system was created with security in mind, as Ommen et al. mention various times in our module's required reading. Develop a working inventory with *the dream team*. Within *the dream team,* assign roles for each risk area: environmental, business resources, and hostile actors (Paulsen, 2016, p. 6).

Also, employ a 24/7 *hardware team* of 44 persons divided into four-person shifts, who work six-hour shifts with mandatory breaks every hour, one person at a time. Also, no person shall be working within the same 16-hour period. Overall responsibilities include data protection from natural disasters and maintaining hardware, such as repairs, cleaning, temperature, and bandwidth speeds (Chai, 2022). Lastly, employ a hybrid network topology and block all social media and music streaming platforms.

Conclusion

In all, keeping an open line of communication with the CEO and CFO is mandatory to create a positive environment for workers and ensure systems' availability.

Discussion Board 4

Our discussion post will look into the normative ethics category in CRISPR software usage. Simply put, CRISPR-Cas9 technology companies should have better oversight of CRISPR software.

4 Ethics

Before debating an ethical question, below is a quick summary of the four common categories of ethical discussions (Four Branches of Ethics, 2022):

Descriptive

Punishments under law/custom

Compares laws/customs past and present

People's views of moral beliefs

Normative

"ought to act."

Rightness and wrongness of an action based on what should be happening.

Meta

Origin of concept

Debating Terms

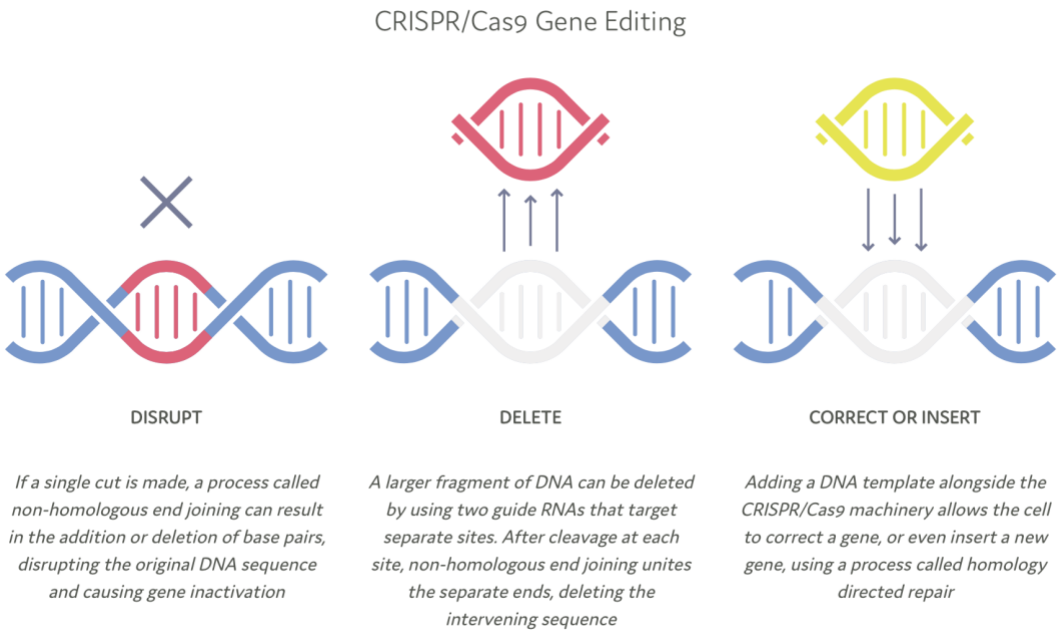
Not judging the rightness and wrongness of an action

Applied

Matters of moral judgment in private and public life

For further exploration, please see the full description of each here.

CRISPR-Cas9 Summary for Context



(CRISPR/Cas9 Gene Editing, n.d.)

"Ought to" have better oversight.

With the hacking of DNA serving as a "symbolic milestone in the increasing overlap between the digital and the biological" (Coldewey, 2017), our discussion turns to what humanity is faced with. While the list of crimes against humanity spans every corner of the globe, for at least this class, we can agree on one critical question needing an answer.

> How can we protect the manipulation of DNA from malicious intent?

One possible answer requires increasing the dollar amount, expenditure, or budget for monitoring. In other words, protection over profit. A separate independent ran team must oversee CRISPR-Cas9 users with the highest ethical standards. While this answer may be a faraway dream, it is what *ought* to be happening. We can never stop malicious intent entirely (Rizkallah, 2018, p. 3). But what would humanity be if we didn't at least try?

Conclusion

Organizations should hire a team to oversee CRISPR-Cas9 gene editing to ensure the ethical use of software and prevent malicious usage. Adding a group may require increasing the budget and an honest normative discussion within organizations/companies.

Discussion Board 5

The office-provided computers using company Wi-Fi and limited oversight involving browsing controls create opportunities for workplace deviance.

Web Shopping & Workplace Deviance

From our required reading, one example of workplace deviance is using a device during working hours for Internet shopping (Payne & Hadzhidimova). If a company provides its employees with MacBooks at their desks, it creates a massive opportunity for someone to take a few minutes out and shop online. While admittingly shopping online during working hours may not be a threat for every company, it is becoming an increasing trend to mix personal and workplace time. It is common knowledge that when we increase activity in the cyber world, there is always an equal reaction and sometimes even greater answer from malicious entities.

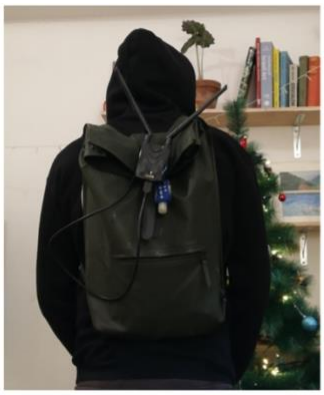
Is shopping on company time an issue?

According to Leng, in their article analyzing poll results asking gen z if they shop during work, 66% admitted to doing so (2021). Also, another poll saw a spike in 81% of employees who admit to shopping on company time (Babati, 2019). One can argue, what's the problem? Most people can multitask, and it's not like anyone can see what I'm doing. Unfortunately, this is not the case; most cybercriminals can easily see what an employee is shopping for, and more often than not, employees use work-provided Wi-Fi. BYOD or CYOD doesn't matter to CTA or cyber threat actors.

Conclusion

Computers in the office with little to no browsing controls using company Wi-Fi create a perfect storm for workplace deviance, especially when 81% of employees admit to shopping from their computers on company time.

Bonus Reading Material for Ethical Knowledge:



The PMK is computed as follows:

PMK = PBKDF2(Passphrase , SSID , 4096)

Figure 3- PMK calculation

- Passphrase – The WiFi password — hence, the part that we are really looking for.
- SSID – The name of the network. It is freely available at the router beacons (Figure 3).
- 4096 – Number of PBKDF2 iterations

[CyberArk: Experiment to Hack Wi-Fi]

Note from Jessica: I enjoyed this article; let me know what you guys think!

Discussion Board 6

Main Takeaways from Required Reading

Gathering from the audio notes from this week's reading, we should develop cyber-policy and infrastructure based on specific concepts, as follows:

1. We need to understand our limitations in predictive knowledge (Jonas, 1973).
2. We should not rely on common sense because it is not entirely applicable in our world in terms of a technological one (audio notes).
3. Understanding time is artificial; we make time exist, not the other way around, and we tend to see only our present ethical dilemmas (Jonas, 1973).

Main Takeaways From Wittkower Videos

1. We should understand cyber-policy and infrastructure effects before making decisions, so we don't create new problems as a society.

2. Good Enough for the time = Short arm of predictive knowledge. We need to switch this type of thinking and analyze it.

Conclusion

To sum up, my answer, we should approach cyber-policy and infrastructure by continuously asking questions about the present and past. Although we may be limited in our scope of data privacy affecting humanity, we must still try. If we do not try to fully understand how cyber-policy and infrastructure change humanity by asking the big questions, we may change ourselves to fit the environment for cyber-policy and infrastructure when arguably, our audio notes point out, the policies and infrastructures ought to accommodate us.

Discussion Board 7

Markets, businesses, groups, and individuals ought to be regulated via distributed responsibility in the face of diminished state power & intelligification (Verbeek, p. 217) & networking of the material world. It is also important to consider the context of tech during 2015.

Wittkower Video Conclusions (My Opinion)

If I were to pick one thing to hone in on from the reading, lectures, and videos provided is this: it can't be one entity regulating, and it for sure is going to differ per scenario. Some examples mentioned were self-driving cars and apple watches. Two very different designs in the realm of cybersecurity. While it can be argued both have to do with security, the discussion of responsibility is vastly different and ought to be treated as such. Therefore, asserting a single entity to regulate each would be a misinformed decision in most cybersecurity professions. A possible assertion is requiring multi-expert in various disciplines taking part in regulation of said scenarios during the design and judicial process.

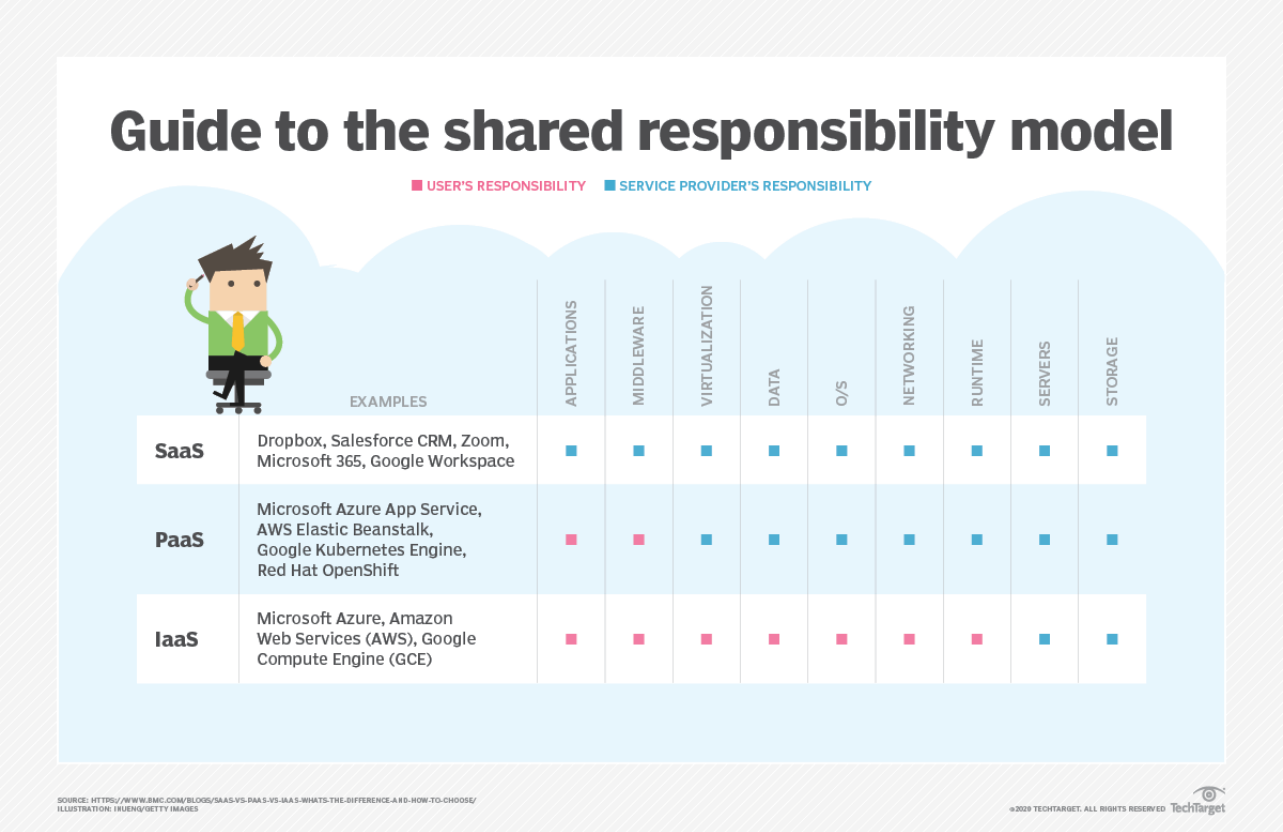
Distributed Responsibility

Example of Empowering "The User" in cybersecurity context

https://hyperproof.io/resource/strengthen-security-posture/

Example of Shared Responsibly in Cloud Computing Context

If my memory serves me correct, a lot of us wrote about being interesting in working in cloud computing. I have included this portion of my discussion board for “funsies”.



Context of 2015 when Verbeek Published
https://www.businessinsider.com/the-15-biggest-tech-events-of-2015-2015-12

https://www.computerworld.com/article/3007854/5-most-important-tech-advancements-of-2015.html

Abstract of Verbeek Require Reading

Designing the Public Sphere: Information Technologies and the Politics of Mediation

Peter-Paul Verbeek

Chapter | Open Access | First Online: 16 November 2014

39k Accesses | 6 Citations | 1 Altmetric

Abstract

After a few decades of living with Information and Communication Technologies, we have got so much used to their presence in our daily lives, that we hardly realize that the societal and cultural revolution they are causing has only just begun. While most discussions still focus on privacy issues and on the impact of social media on interpersonal relations, a whole new generation of ICTs is currently entering the world, with potentially revolutionary impacts that require careful analysis and evaluation. Many everyday objects are currently being equipped with forms of 'ubiquitous computing' or 'ambient intelligence'. At the same time, 'augmented reality' technologies are rapidly gaining influence. ICTs will result in smart environments, and new social relations. Rather than merely assessing and criticizing these developments 'from the outside', we must to learn to accompany them critically 'from within'. The public sphere requires 'technologies of the self': the capability to understand technological mediations, to take them into account in technological design, and to shape our existence in interaction with them. The real choice is not between accepting of rejecting new ICTs, but between critical engagement and powerless opposition.

References

Babati, B. (2019, December 10). *Employee Shopping Online & Exposing Company To Cyber Threats - Hoxhunt*. Retrieved October 11, 2022, from https://www.hoxhunt.com/blog/employees-shopping-online-could-expose-your-company-to-cyber-threats.

Bowman, J. (2022, July 6). *Publicly Traded Companies: Definition and Examples*. The Motley Fool. Retrieved September 13, 2022, from https://www.fool.com/investing/stock-market/basics/publicly-traded-companies/.

Brokowski, C., & Adli, M. (2018, January). CRISPR Ethics: Moral Considerations for Applications of a Powerful Tool. *Journal of Molecular Biology*, *431*(1), 88–101. https://doi.org/10.1016/j.jmb.2018.05.044.

Cloud Security Architect. (2022). Amazon.Jobs. https://www.amazon.jobs/en/jobs/1538340/cloud-security-architect.

Coldewey, D. C. (2017, August). *Malicious code written into DNA infects the computer that reads it _ TechCrunch.pdf*. Google Docs. Retrieved September 22, 2022, from https://drive.google.com/file/d/1tJfWKjsY04Tha9QLZK0TJHd4U_m6JDxV/view.

Chai, W. (2022, June 28). *confidentiality, integrity, and availability (CIA triad)*. WhatIs.com. Retrieved September 13, 2022, from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

CRISPR/Cas9 Gene Editing. (n.d.). CRISPR Therapeutics. http://www.crisprtx.com/gene-editing/crisprcas9#:~:text=CRISPR%2FCas9%20edits%20genes%20by,revolutionary%20technology%20into%20transformative%20therapies.

Four Branches of Ethics. (2022, March 25). GKToday. Retrieved September 23, 2022, from https://www.gktoday.in/topic/four-branches-of-ethics/ .

Framework for Improving Critical Infrastructure Cybersecurity. (2018). *National Institute of Standards and Technology*, *1.1*, 1–21. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Freeze, D. (2021, April 28). *50 Cybersecurity Titles That Every Job Seeker Should Know About*. Cybercrime Magazine. https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/.

JONAS, H. (1973). TECHNOLOGY AND RESPONSIBILITY: REFLECTIONS ON THE NEW TASKS OF ETHICS. *Social Research*, *40*(1), 31–54. http://www.jstor.org/stable/40970125.

Kirkpatrick, C. (2022). *Mod 1b: InterdisciplinaryCyberSecurity* [Slides]. Canvas. https://canvas.odu.edu/courses/116081/assignments/532994?module_item_id=3325574

Leng, A. (2021, September 7). *6 in 10 workers are shopping online during virtual meetings*. Digital.com. Retrieved October 11, 2022, from https://digital.com/6-in-10-workers-are-shopping-online-during-virtual-meetings/ .

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017, June). An introduction to information security. *National Institute of Standards and Technology*. https://doi.org/10.6028/nist.sp.800-12r1.

Ommern, E., Borrett, M., & Kuivenhoven, M. (2014, April). *Staying Ahead in the Cyber Security Game: What Matters Now* (1st ed.) [PDF]. Sogeti and IBM.

Paulsen, C. (2016, November 3). *NISTIR 7621 Rev. 1, Small Business Information Security: The Fundamentals | CSRC*. Retrieved September 13, 2022, from https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final.

Payne, B.K., & Hadzhidimova, L. (2018). Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections. *International Journal of Criminal Justice Sciences, 13*, 385.

Rizkallah, J. R. (2018, November). *Hacking Humans_ Protecting Our DNA From Cybercriminals.pdf*. Google Docs. Retrieved September 22, 2022, from https://drive.google.com/file/d/17vZTrd3tyRkIuXtLfYKSeZypU7WpCkmM/view.

What is Cyber law? | Becoming a Cyber Lawyer. (2018, August 21). Legal Career Path. https://legalcareerpath.com/what-is-cyber-law/.