**CSCI 415 Ethics, Law and Cybersecurity**

**Final Quiz**

**NAME: \_\_Ashish Acharya\_\_\_\_\_                            DATE:\_\_11/28/2023\_\_**

**1.(a) Describe and give examples of the 2 most significant computer security threats that are impacting the world at the present time.  (b) What steps are being taken to minimize or thwart these threats?  (c) Will the efforts proposed to protect individuals, companies and the governments from these threats still protect the rights of citizens?  (d) Do you think that the steps taken or to be taken are ethical and will not cause a backlash in society?  *Please elaborate (beyond a yes or no answer)***

In today's digital era, the proliferation of cloud computing and the sophistication of AI-driven malware pose significant challenges to computer security. This essay explores the threats associated with cloud computing and AI-enhanced malware attacks and discusses measures to address them.

Cloud computing, marked by data sharing and vast information storage, faces risks of unauthorized access and data breaches (Mello, 2022). Robust encryption and stringent access controls are vital defenses, while regular audits and continuous monitoring help identify and resolve vulnerabilities promptly.

AI-powered malware, with its adaptive nature, challenges traditional security measures (Cassetto, 2023). User and entity behavior analytics (UEBA) and security orchestration automation and response (SOAR) emerge as critical tools to detect anomalies and automate responses to AI-driven threats.

Efficient prevention of threats necessitates the incorporation of threat intelligence into security procedures. Organizations can rapidly ascertain the characteristics, seriousness, and established methods for mitigating or containing identified threats by comparing threat intelligence data with a security system's detection capabilities. Moreover, utilizing artificial intelligence in security measures, such as employing machine learning algorithms for spotting anomalies, strengthens the capacity to recognize and address emerging threats (Cassetto, 2023).

In the face of these challenges, it is crucial to uphold individual rights. The implementation of encryption and access controls should prioritize the protection of data without jeopardizing personal privacy. Emphasizing security, regular audits, and monitoring should concentrate on safeguarding measures rather than unwarranted surveillance of individuals.

Striking a balance between security and privacy, guided by ethical guidelines and regulations, ensures public trust. Transparent communication about AI and security practices is crucial to mitigate potential societal backlash.

Confronting these challenges underscores the importance of safeguarding individual rights. Prioritizing the safeguarding of data without compromising personal privacy, the deployment of encryption and access controls becomes imperative. Focusing on security, routine audits, and monitoring should emphasize protective measures over unnecessary surveillance of individuals.

**References:**

Cassetto, O. (2023, February 7). *Cybersecurity threats: Types and challenges*. Exabeam. Retrieved November 28, 2023, from

<https://www.exabeam.com/information-security/cyber-security-threat/>

Mello, J. (2022, July 4). *11 top cloud security threats*. CSO Online. Retrieved November 28, 2023, from

<https://www.csoonline.com/article/555213/top-cloud-security-threats.html>

**2. (a) Describe at least 3 of the most significant ethical/social issues for individuals and at least 3 of the most significant ethical/social issues for businesses/organizations in the field of Computer Science.  (b) Which, if any, of these issues overlap both individuals and businesses/organizations?  (c) For each issue that you identified that is causing a major ethical/social problem for society, suggest a solution for this problem.  Be as concise as possible in your answer and do not address the issue of security threats in this question.  *Please elaborate (beyond a yes or no answer)***

The swift progression of computer science has ushered in a plethora of ethical considerations, posing significant challenges for both individuals and organizations. In the domain of personal ethics, issues such as hacking, privacy concerns, and algorithmic bias come to the forefront. Unauthorized access to personal devices, or hacking, not only compromises security but also risks privacy theft. Addressing this requires individuals to prioritize data security, engage in responsible online behavior, and stay abreast of evolving security measures (Sweeney, 2022).

Privacy risks have intensified with the growing digitization of personal information, necessitating robust privacy policies, user education, and advocacy for stringent data protection regulations. Algorithmic bias, an emerging concern, involves unintentional biases in technology that affect specific groups and contribute to misleading statistics. This challenge can be tackled through regular algorithm audits, promoting diversity in development teams, and ensuring transparency in decision-making processes.

In the organizational realm, intellectual property concerns, data collection practices, and security threats take precedence. Ambiguities in defining intellectual property in the digital era have led to issues of copyright infringement. Organizations can address this by clarifying and strengthening intellectual property laws, raising awareness about copyright infringement, and fostering responsible content creation practices.

Ethical dilemmas in data collection practices present challenges related to balancing the benefits of data-driven insights with user privacy and consent. Crucial solutions include transparent data collection policies, obtaining informed consent, and adhering to strict data protection regulations. Additionally, cybersecurity threats, particularly hacking, pose serious risks to businesses, financial institutions, and governmental organizations, potentially compromising national security.

A common ethical challenge shared by both individuals and organizations is hacking. Reinforcing data security measures, promoting responsible online behavior, and advocating for stringent cybersecurity protocols are collective efforts that can mitigate potential threats. In conclusion, the ethical challenges in computer science underscore the need for proactive and collaborative solutions. Individuals and organizations must navigate these challenges responsibly, ensuring the ethical use of technology for the benefit of society.

**Reference:**

Sweeney, M. (2022, February 11). Ethical dilemmas in computer science. ZDNET Retrieved

November 28, 2023, from

https://www.zdnet.com/education/computers-tech/ethical-dilemmas-computer-science

**3.The field of computer science has changed during your lifetime and will continue to change in the future.  When the Computer Science department at this University was created in 1974 students were using keypunch cards to run programs on the main frame.  There was no PC, no cell phone, no phone aps, no internet, no Facebook, no Twitter, no Google, no Microsoft, etc.  The field of computer science has changed dramatically from then till now.  Over your entire life the changes could be as dramatic as it has been since the CS Department was created.  (a) How important is it to you to keep up to date with the coming changes in hardware, software and ethical issues?  (b) What specific steps will you in engage in to make sure that you are up to date as a computer professional?  *Please elaborate (beyond a yes or no answer***

The landscape of computer science has undergone a profound metamorphosis, transitioning from the era of keypunch cards to the contemporary age of smartphones and advanced technologies. This radical evolution underscores the imperative for professionals to maintain a vigilant awareness of changes in hardware, software, and the ethical considerations intrinsic to technological progress.

In essence, the importance of staying up to date with the dynamic field of computer science cannot be overstated. Continuous adaptation is requisite to ensure ongoing competence in an environment that continually shapes the digital world. As technology becomes increasingly user-friendly, the responsibility to contribute to its development becomes a shared commitment among professionals (Watters, 2023).

To remain relevant and contribute meaningfully, computer professionals must engage in continuous learning. Platforms like Coursera and edX provide accessible resources, facilitating ongoing education in emerging technologies and ethical considerations. Regularly updating computer systems, staying informed through industry publications, and actively participating in research are integral steps in understanding the evolving hardware and software landscape.

Preserving and responsibly utilizing technology emerge as fundamental practices. Beyond individual professional growth, there is a shared responsibility to adopt sustainable practices for the benefit of future generations. Proactive learning of new technologies ensures that professionals remain abreast of the rapidly changing field, embracing advancements and staying

relevant.

Ethical considerations are inseparable from the dynamic evolution of computer science. Recognizing the significance of ethical practices, including responsible data use, privacy protection, and the ethical adoption of disruptive technologies, is paramount (Watters, 2023). In understanding and addressing ethical challenges faced by businesses, such as the misuse of personal information and responsible use of AI, computer professionals can make a positive impact on societal well-being.

In the context of our country, computer professionals play a pivotal role in driving innovation, economic growth, and societal progress. Staying updated not only ensures competitiveness on the global stage but also enables professionals to address country-specific ethical considerations. This includes issues like data protection and privacy, which are essential for responsible contributions to the national and global digital ecosystem.

In conclusion, navigating the dynamic evolution of computer science demands a lifelong commitment to learning and ethical practices. Embracing change, staying informed, and actively participating in ethical discourse are fundamental steps for professionals to remain competent and responsible contributors to the ever-changing world of computer science.

**Reference:**

Watters, A. (2023, February 3). 5 ethical issues in technology to watch for in 2023. CompTIA

Blog. Retrieved November 28, 2023, from

<https://connect.comptia.org/blog/ethical-issues-> technology](https://connect.comptia.org/blog/ethical-issues-in-technology)