Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(6):56-60

Research Article ISSN: 2394 - 658X

Ethical Implications of Cyber Security

Mohammed Mustafa Khan

ABSTRACT

Considering the development of technologies in recent years, cybersecurity plays an essential role in protecting data and ensuring the stability and availability of data storage systems. However, this increasing dependence on cyber systems creates new, unanticipated ethical problems. The moral issues in cybersecurity are privacies, autonomy, responsibility, social justice, and risks of damage. As such, cybersecurity professionals, governments, and corporations have the challenge of addressing security concerns without violating people's rights and compromising societal values. This essay, therefore, looks at the ethical issues surrounding cyber security, which include data privacy, surveillance, ethical hacking, and role. It also assesses the principles and standards employed when dealing with cybersecurity issues to promote fairness in cyberspace.

Keywords: Cybersecurity, ethics, data privacy, surveillance, autonomy, accountability, fairness, ethical hacking, digital rights.

INTRODUCTION

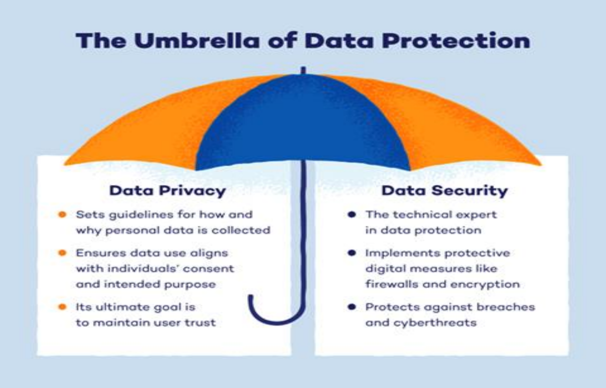
Technological advancement and internet technology have increased the implementation of computers and computer systems. People use the Internet to transfer data, exposing the data to many cyber threats. Organizations and individuals are often attacked for financial or other malicious intentions involving their data. Hence, we must apply security measures to our data to prevent cyber-attacks [1]. Cyber security safeguards essential and crucial information and prevents it from being attacked. It involves safeguarding the organization's systems, networks, documents, and programs against risks such as attack, harm, or intrusion. Information technology security protects the organization's networks and systems from outside or local personnel [4]. External threats refer to threats from outside an organization: hackers, spammers, and cybercriminals. However, the measures explicitly taken to protect information against cyber threats often pose specific ethical issues beyond the technical layer.

The ethical issues that arise include the extent to which the need for security may infringe on one's liberty, the amount of monitoring citizens by the government, and the accountability that companies have for the consumers' data [3]. Cyber security ethics identify permissible or non-permissible acts depending on society's standards. They are best practices that cybersecurity professionals should follow. These ethical considerations deny hackers the right to be referred to as cybersecurity professionals. These ethical considerations are what separate cybersecurity professionals from hackers. This essay will cover the theoretical attribution in determining ethical principles in computing, especially concerning security. It will show how critical players can manage these challenges responsibly and moderately.

ETHICAL DIMENSIONS OF CYBERSECURITY

Data Privacy

Privacy is one of the significant ethical issues that should be addressed in cybersecurity. In the recent digital world, it has become relatively easy to gather, store, and process personal information, which is highly individual and sensitive in this digital world. From social media profiles and bank details to health records, this information, if improperly secured, can be misused, leading to severe consequences for individuals [2]. The ethical concern concerns the data's accumulation, processing, and application. For example, a company harvests user data without the user's consent, or privacy policies that can be exploited or used to sell the data to third parties are ambiguous. Ethically, individuals are entitled to authority over their information or data collected by companies, and they are to be informed of how the organization will use the data and information. This principle is the informed consent principle that is key to autonomy [8]. However, many users do not know how much data is being collected or gladly sacrifice their privacy to use the product or service without care. However, an important ethical principle that needs to be enhanced is data minimization, using only the amount of data strictly required for processing [3]. Business entities and corporations should develop effective measures for protecting user data and ensure that data collection is done for genuine reasons.


The Umbrella of Data Protection
Data Privacy
Sets guidelines for how and why personal data is collected
Ensures data use aligns with individuals' consent and intended purpose
Its ultimate goal is to maintain user trust
Data Security
The technical expert in data protection
Implements protective digital measures like firewalls and encryption
Protects against breaches and cyberthreats

Source: *https://www.pandasecurity.com/en/mediacenter/src/uploads/2023/08/data-privacy-and-data-security.png*

GOVERNMENT SURVEILLANCE AND NATIONAL SECURITY

This is usually done under security pretext, where intelligence agencies claim that spying assists in preventing criminal and terrorist activities. Yet, surveillance technologies and data collection methods are incredibly influential. Despite being very helpful in security measures, they violate people's rights to privacy [6]. Technologies through which personal data can be collected and analyzed at large scales raise considerable ethical issues. The moral rightfulness of such monitoring and concerns about how the obtained data might be used or misused are pivotal to this discussion.

Surveillance devices such as CCTV cameras, facial recognition systems, and internet monitoring technologies limit people's privacy by keeping them under observation in the social and domestic context [4]. The collection of personal data where users' consent is not sought correctly, or the process is not sufficiently monitored poses a risk to individual freedom and privacy. It makes people feel like they are constantly being watched by government or other organizations.

Politically, every government's task is to ensure security without infringing on people's rights and freedoms. The ethical challenge is compounded by the fact that much of government surveillance happens covertly, meaning that individuals are often unaware that their data is being monitored [9]. Furthermore, there must be some checks and balances as well as clear supervision measures when it comes to the surveillance carried out by governments [7]. This is even true since most of the government surveillance is done secretly, and the people concerned do not know that their data is being monitored. This development erodes the general public's trust in public organizations and thus presents an ethical problem supporting such complex measures.

Source: *https://assets.aclu.org/live/uploads/2021/09/Social-Surveillance.jpg*

ETHICAL HACKING

Ethical hacking, also called 'white hat hacking,' is gaining access to computer systems to assess their security weaknesses and correct them before other unauthorized persons can access them. Though this is useful in boosting the security of personal computers, it has several ethical questions regarding the techniques used and where exactly the line should be drawn. Among the most salient ethical concerns is consent [8]. However, even if hacking is done for a noble cause, accessing a computer system without the owner's consent may be considered an unlawful infringement of the owner's property rights. Organizations typically contract or authorize ethical hackers to carry out these activities to ensure legality and maintain ethical integrity, which provides explicit consent [3].

Another issue is what will become of the discovered loopholes and vulnerabilities. While they are supposed to communicate the vulnerabilities to the particular authority or owners of the respective system, there is always the opportunity to act unethically, for instance, sell the information to other parties with devious intentions [1]. This possibility emphasizes appropriate compliance with codes of ethical hacking conduct, transparency, and accountability. To prevent misconduct, ethical hacking must be guided by well-defined standards and oversight, ensuring that hackers remain focused on their goal: to maintain and defend the structures and principles of cyber security without adversely affecting the liberty of others and destabilizing the trust [1]. This commitment to ethical behavior is essential in preserving the integrity of ethical hacking practices.

Source: *https://danielsfund-wpmedia.s3.us-west-2.amazonaws.com/wp-content/uploads/2021/02/ethical-hacking-web.jpeg*

CYBERSECURITY RESOURCE ALLOCATION

The allocation of resources is one of the most significant ethical dilemmas in cybersecurity since organizations are forced to ration a few resources, such as time, finances, and human resources, to meet many cybersecurity requirements. This is about coordinating the steps in the execution of security agendas, countermeasures to threats, and the way they treat themselves while bearing in mind the stakeholders' concerns and their agendas [4]. The ethical challenge is based on the decisions regarding the distribution of limited resources within the organization to maintain an optimum impact on the cybersecurity programs regarding the overall organizational objectives.

Further, there are ethical issues regarding usability and the overall economic sustainability of the resources in question. There's no doubt that measures for enhancing security must be implemented, especially since threats are on the rise [6]. Still, the stronger the protection against cyber threats, the more the usability and productivity of the organization and its users will be impacted negatively. Furthermore, security costs could be high, and such costs could significantly affect organizational budgets, thus posing a long-term viability issue for heavy investments in security [9]. IT security management has, therefore, remained with an ethical dilemma concerning the functionality and the financial mode since the provision of security measures to support the functionality of an organization does not always guarantee the achievement of the set goals without compromising the overall performance of the organization and the satisfaction of its users [10].

CORPORATE RESPONSIBILITY IN CYBERSECURITY

It is ethical for companies, especially those dealing with significant traffic of users' data, including social media sites, banks, and hospitals, to ensure the data is safeguarded from hackers. Losing data means that identity theft, financial loss, or severe emotional problems are inevitable for users of such services [4]. One ethical dilemma companies face is the conflict between profit and security. Enhancing and updating a good cybersecurity program can be expensive, and some Organizations are willing to compromise to save some cash for their client's safety [10]. Ethical companies should prioritize the security of their users' data above financial considerations. Also, they should disclose information on cybersecurity measures in place and inform users of the occurrence of data breaches as soon as possible. Another concern is how such information is employed by the organizations or companies involved in the sales process and development of the product [2]. While the collected data can be gathered legally, it is still wrong to use it in ways that will harm or take advantage of the users of those social networks. It is also essential for companies that handle consumers' data to respect the consumers' privacy and autonomy.

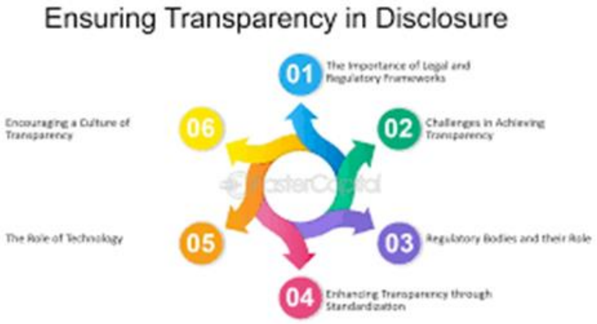
CYBERCRIME AND THE ETHICAL USE OF COUNTERMEASURES

The rise of cybercrime presents significant ethical challenges, particularly regarding how organizations respond to such attacks. Measures such as firewalls, encryption, and intrusion detection systems are standard, although some responses are unethical [3]. For instance, some organizations may actively participate in hackbacks, where they start attacking the attackers in their systems. Although fighting for one's life might appear reasonable, it is unethical for several reasons. First, sometimes it is challenging to assign a cyberattack to the right perpetrator; second, hacking back can result in collateral damage and affect innocent parties [11]. Also, hacking back infringes the principle of proportionality, whereby it amplifies the situation rather than setting a solution. Organizations must pay particular attention to the fact that their cybersecurity responses must be ethical and reasonable [10]. Hacking retaliation can be replaced by ethical countermeasures, including aiding the police in arresting the hackers, enhancing their defenses, and carrying out employee awareness programs.

TRANSPARENCY AND DISCLOSURE

Security threats and disclosure of such threats are significant in enabling the user to take appropriate measures to safeguard data and systems. Nevertheless, the issue of the right level and type of disclosure raises specific ethical dilemmas [4]. Thus, it should be carefully considered in the context of the common good and the benefit of all the interested parties. It is mandatory to evaluate the pro-actively disclosed amount of information along with regulatory and legal requirements by considering the consequences on the parties involved, the nature of the vulnerability, and the probability of the event being exploited. In the same regard, premature or partial revelations might escalate risks to users because they are presented with threats before they can effectively prevent them [8]. Conversely, delayed disclosure could hinder efforts to patch vulnerabilities, leaving systems unprotected for extended periods.

The mode of disclosure also raises ethical concerns. Organizations must navigate the tension between transparency and the risk of causing undue alarm or aiding adversaries by providing detailed information about vulnerabilities. Much effort should be put into clear communication since stakeholders do not want to be intimidated or have some new information conveyed in a way that creates new security threats [8]. In so doing, this approach helps improve the security status of entities within an organization or a community and strengthens security overall.


Ensuring Transparency in Disclosure
01 The Importance of Legal and Regulatory Frameworks
02 Challenges in Achieving Transparency
03 Regulatory Bodies and their Role
04 Enhancing Transparency through Standardization
05 The Role of Technology
06 Encouraging a Culture of Transparency
FasterCapital

Source: *https://fastercapital.com/i/Unveiling-Truth--The-Power-of-Transparency-in-Disclosure--Ensuring-Transparency-in-Disclosure.webp*

ETHICAL FRAMEWORKS IN CYBERSECURITY

Different ethical theories are available to assist the individuals involved in decision-making in cybersecurity since morality is not plain in cybersecurity.

Utilitarianism

The most common ethical theory in cybersecurity decision-making is utilitarianism, or the ability to get the best for the most people. For example, surveillance in government security sectors is perceived as the requirement for the safety of the majority of the populace from threats like terrorism and cyber aggression [12]. Such measures are considered constructive in the large population by emphasizing safety and security concerns in the general population. However, what has been noted is that specific ethical issues are brought out by utilitarian approaches, significantly where the rights of the individuals or the minority are infringed to benefit the majority [5]. At times, the privacy and liberty of some citizens may be considered and compromised, thus raising issues of equity. This conflict between public protection and individual liberties points to the weakness of using utilitarian theory in analyzing cybersecurity, as it eventually leads to discrimination against certain groups if the majority is in favor. This tension between these competing concerns is a classic problem of ethical precariousness in cybersecurity policy.

Deontological Ethics

Another theoretical approach to analyzing cybersecurity ethics is deontological ethics, which includes principles and duties. This approach emphasizes the non-violation of individuals' rights irrespective of the consequences, such as the right to privacy. From the deontological perspective, which holds water with the concept of principles, the actions performed are considered ethical or unethical depending on their approximation to or deviation from these principles [4]. For instance, in the case of surveillance programs, even if these measures effectively deter terrorism or other threats, from a deontological point of view, these measures are unethical since they violate individuals' right to privacy. The invasion of people's privacy would be regarded as immoral even if their action contributes to the 'general welfare' of the population [7]. Therefore, deontological ethics upholds the importance of duties of dignified respect to rights and fundamental principles while thinking about information security ethical dilemmas based on the clash of interests of individual rightful claims and security needs of the common good.

Virtue Ethics

Virtue ethics emphasizes the moral character and integrity of individuals and organizations. In cybersecurity, this approach advocates for stakeholders—such as ethical hackers, corporate executives, and government officials—to embody virtues like integrity, transparency, and responsibility [4]. While the rules and consequence-based theories aim at providing rules for the right actions and are prescriptive, virtue ethical theory urges individuals to cultivate moral virtue in themselves, and then virtue will not fail to lead one to the right actions [13]. Therefore, virtuous behavior in a cybersecurity context involves promoting the rights of the users and the creation of trust in cyberspace. Sustainability refers to ethical activities that participants undertake to ensure that the public can trust organizations, such as data privacy and transparency [9]. The idea is to educate people to make the right choices by adhering to globally accepted values, hence developing virtuous cybersecurity environments that uphold integrity in organizations and the general information technology environment.

CONCLUSION

The ethical implications of cybersecurity are intricate and wide-ranging, encompassing concerns like privacy, surveillance, hacking, corporate responsibility, and moral responses to cybercrime. With the progression of digital technologies, there is a need for various stakeholders, including governments, corporations, and individuals, to counter these issues with a high level of ethical consciousness. Analyzing moral theories, including utilitarianism, deontology, and virtue ethics, helps the decision-makers rationalize integrating security measures about recognizing and respecting people's rights, fairness, and accountability. From the perspective of utilitarianism, security measures can be warranted to enhance the general welfare, although this has some implications for the minorities' rights. The other approach is deontological, which requires the protection of moral rules such as privacy even when it hinders general security. Virtue ethics encourages people and companies to be trustworthy and take appropriate action in digital technology. At some point, the notion of cybersecurity should protect not only technology but also the values that define a decent society.

REFERENCES

[1]. P. Formosa, M. Wilson, and D. Richards, “A principlist framework for cybersecurity ethics,” Computers & Security, vol. 109, no. 109, Oct. 2021, doi: https://doi.org/10.1016/j.cose.2021.102382.

[2]. T. Johanson, “Understanding National Security as Contextual: The Implications for Small State Defence Policy,” National Security Journal, vol. 4, Jul. 2022, doi: https://doi.org/10.36878/nsj20220712.04.

[3]. M. Manjikian, Cybersecurity ethics: an introduction. Abingdon, Oxon; New York, Ny: Routledge, 2018.

[4]. J. T. F. Burgess, E. Knox, and R. Hauptman, Foundations of information ethics. Chicago: Ala Neal-Schuman, 2019.

[5]. M. Christen, B. Gordjin, and M. Loi, The Ethics of Cybersecurity. Cham, Switzerland Springer, 2020.

[6]. P. W. Singer and A. Friedman, Cybersecurity and cyberwar: what everyone needs to know. Oxford: Oxford University Press, 2018.

[7]. K. M. Rajasekharaiah, C. S. Dule, and E. Sudarshan, “Cyber Security Challenges and its Emerging Trends on Latest Technologies,” IOP Conference Series: Materials Science and Engineering, vol. 981, p. 022062, Dec. 2020, doi: https://doi.org/10.1088/1757-899x/981/2/022062.

[8]. “A CRITICAL ANALYSIS ON CYBER SECURITY IN LATEST TECHNOLOGIES,” REST Journal on Emerging trends in Modelling and Manufacturing, vol. 7, no. 2, Mar. 2021, doi: https://doi.org/10.46632/7/2/2.

[9]. Y. Antil, “Ethical Hacking and Hacking Attacks,” INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, vol. 06, no. 01, Jan. 2022, doi: https://doi.org/10.55041/ijsrem11411.

[10]. J. Rajamäki and H. Hämäläinen, “Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES,” Information & Security: An International Journal, vol. 50, pp. 103–116, 2021, doi: https://doi.org/10.11610/isij.5002.

[11]. J. Pattison, “From defence to offence: The ethics of private cybersecurity,” European Journal of International Security, vol. 5, no. 2, pp. 233–254, May 2020, doi: https://doi.org/10.1017/eis.2020.6.

[12]. P. Timmers, “Ethics of AI and cybersecurity when sovereignty is at stake,” Minds and Machines, vol. 29, no. 4, Oct. 2019, doi: https://doi.org/10.1007/s11023-019-09508-4.

[13]. J. D. Michels and I. Walden, “Cybersecurity, Cloud and Critical Infrastructure,” SSRN Electronic Journal, 2021, doi: https://doi.org/10.2139/ssrn.4204847.