

CYBERSECURITY ETHICS 101

Matthew N. O. Sadiku

*Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX
USA*

Uwakwe C. Chukwu

Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA

Janet O. Sadiku

Juliana King University, Houston, TX, USA

Abstract

Ethics can be defined as a moral code by which a person lives. It prescribes what we ought to do when confronted with specific situations. The goal of ethics is to instill a strong sense of principles that govern behavior or conduct. When applied to cybersecurity, ethics provides an understanding of the rules of ethical behavior that can help practitioners figure out what is expected of them. In the world of cybersecurity, ethical practices are essential for protecting data and maintaining trust. This paper provides an introduction to cybersecurity ethics.

Keywords: cyber attacks, cyber threats, ethics, cyber ethics, cybersecurity ethics, hacking.

INTRODUCTION

Technology is deeply integrated into our lives. Social media and other online interactions can have a real-life impact on our society's governance. Since the inception of the Internet, hackers have labored to exploit it for everything from cyberattacks to theft and espionage. As technology advances, so does the potential for data breaches, security threats, and cyber attacks. Some emerging technologies can be used against us. Thus, we need to uphold a set of standards when handling sensitive information. Many security breaches and criminal behavior among IT experts have been traced to ethical lapses.

Ethics is a branch of philosophy that deals with what is deemed to be right or wrong. It pertains to the moral guidelines that can help us through difficult situations. Ethics and cyber security go hand-in-hand. Ethical issues are a daily occurrence in cybersecurity. There is a need for cybersecurity professionals to understand and to implement ethical principles. Ethical issues, particularly concerning automation, Internet of things, cloud computing, artificial intelligence, and robotics, are now major concerns for businesses, organizations, and governments [1].

OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, cybersecurity involves multiple issues related to people, process, and technology [2]. Figure 2 shows different components of cybersecurity [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and

government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [4].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [5].

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [6]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 3 [7].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [8]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that

passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

WHAT IS ETHICS?

In simple terms, ethics involves doing the right thing. Ethics refers to the standards of what is right and wrong that mention what we have to do when specific circumstances arise. Ethics governs a person's behavior. Data ethics is of increasing relevance as the quantity of data increases. Ethical questions may be considered in terms of accuracy, humane treatment, informed participants, and the necessity and applicability of the work.

Technology has already had an impact on how we live our lives in ourselves. It has become an integral part of all aspects of the society. The use and misuse of technology have increased dramatically. Technology is not neutral. As with all technology, the ethical impact of the digital technology depends on the purposes of its designers and users. This brings us to larger questions of how we should employ technology, what risks new technology may bring, and what the arrival of these new futures means to us as humans. Ethics has been a long time concern in human interaction with technology. Digital ethics is the field of study concerned with the way technology is shaping and will shape our political, social, and moral existence.

Ethics helps us to frame our ideas about what is right or wrong using rational argument. For example, it can be applied in determining whether the use of big data is ethical. Companies must ensure that the data they own is not used against their own subjects without consent. Perhaps the most important rule is similar to the Golden Rule: "Do unto the data of others as you would have them do unto yours." Different components of ethics are shown in Figure 4 [9].

CODES OF ETHICS

It makes sense that cybersecurity professionals have codes of conduct. There are codes of conduct for each profession. For example, doctors, engineers, and lawyers can be penalized for violating the codes of conduct for their respective professions. Professional organization such as the British Computer Society, the Association for Computer Machinery (ACM), National Society of Professional Engineers (NSPE), and the Institute of Electrical and Electronics Engineers (IEEE) have developed widely accepted, comprehensive codes of ethics. They provide us with sample ethics for leading organizations.

They insist that their members should adhere by the codes as a condition for membership. They only become legally enforceable when they are adopted by governmental licensing boards or regulatory bodies. The only problem with these codes is that they are pre-digital ethics. However, some scholars believe that we do not need a new ethics to accommodate digital technology. Traditional ethics deals with privacy, confidentiality, informed consent, professional boundaries, conflicts of interest documentation, client abandonment, and professionalism [10]. As evident in the next section, cybersecurity ethics address the same issues and much more. The rapid emergence of digital technology has added a new layer of complexity to the issues. For example, encryption provides more protection than traditional paper documents.

CYBERSECURITY ETHICS

Cybersecurity ethics play a major role in all fields. Ethics is important because individuals and companies have very sensitive and personal data that increases the chances of threats like identity thefts. In cybersecurity, ethical issues refer to the consequences, whether damages or benefits, that can come from the choices of cyber security professionals [11].

Cybersecurity experts face the following ethical issues [12-15]:

- *Privacy*: The first principle of ethical cybersecurity is to protect the privacy of individuals. This means that any data that is collected should be done so with the explicit consent of the person or

organization. Ethics in cybersecurity determine data privacy to a large extent today. Any data that is collected should be stored securely, and not shared without consent. Cybersecurity is intended to defend us against ransomware and identity theft, two forms of hacking that depend on deeply violating a user's privacy. People with dignity have an entitlement to privacy, both online and offline. Privacy harm is regarded as the negative consequence of a privacy violation.

- *Confidentiality*: This is a critical ethical problem in the field of cybersecurity. Confidentiality is a key ethical issue in cybersecurity. By the nature of their work, cybersecurity professionals will handle personal, private or proprietary information that should be kept strictly secret or confidential. Cybersecurity professionals often have access to confidential data and knowledge about the networks of their clients, which gives them a great deal of power that can be abused.
- *Security*: Security is another ethical issue. Security aims at enforcing divisions, keeping some people safe from other people or things. Cybersecurity professionals are responsible to keep devices, data, and networks secure. Leaving the laptops and other gadgets unattended may constitute an ethical breach and is considered immoral since it violates their company's standards. Leaving computers unattended jeopardizes the company's data and information security.
- *Integrity*: Acting with integrity means taking steps such as encrypting data to protect against potential breaches. Organizations should consider whether they have appropriate controls and processes in place to safeguard the integrity and privacy of their customers and their data.
- *Professionalism*: Another key aspect of ethical practice is professionalism, and transparency about what kind of data an organization collects and why they need it. Cybersecurity leaders must rely on reputation and background checks alone to determine the trustworthiness of potential hires.
- *Credibility*: This includes acting with accountability: making sure everyone involved takes responsibility for their actions. Executives should lead by example and by adhering strictly to company policies related to cybersecurity protocols.
- *Responsibility*: In the event of a cyberattack, it can be challenging to identify the responsible party, and questions may arise about who is liable for any damages or losses.
- *Transparency*: In some cases, organizations may conceal or downplay cyberattacks to avoid negative publicity or other consequences. This lack of clarity can undermine trust in the organization and the broader cybersecurity ecosystem.

APPLICATION OF CYBERSECURITY ETHICS

Cybersecurity refers to the practice of protecting programs, networks, computer systems, and their components from unauthorized digital access and attacks. Cybersecurity ethics can be applied in the following ways:

- *Information Security*: The field of information technology expands and shifts so frequently that a strong ethical core is needed to navigate it. Information in the cyber world can be accessed globally, so the field of cyber security needs to evaluate what is right and wrong. Organizations should have policies regarding how they handle data that customers know their information will remain safe. It is everyone's responsibility to avoid negligence with it comes to handling information. Ethical lapses can also result in fines and other financial penalties.
- *Ethical Hacking*: So-called ethical hacking and protective measures can cause inconveniences for your customers and other employees. Although the term hacking has a negative connotation, ethical hacking has become popular today. Many hackers have deliberately crossed ethical boundaries with ignorance falling short as a defense.
- *Cybersecurity for Attorneys*: Confidential information used by attorneys and law firms faces security threats today more than ever before. Security threats to lawyers and law firms continue to be substantial, real, and growing. The greatest threats today are spearphishing, ransomware, business email compromise, and lost and stolen laptops, smartphones, and portable devices. Attorneys and

law firms that have specified personal information about their employees, clients, clients' employees or customers, opposing parties and even witnesses may be covered by federal and state laws [16]. Figure 5 shows a typical cybersecurity attorney [17].

BENEFITS

Cyberattacks result in the loss and access to confidential data, loss of money, and reputation loss for organizations. A data breach can affect hundreds of millions of people and cause irreparable damage to a company's reputation and bottom line. Hence, it is crucial to prevent cyberattacks. Cybersecurity involves the technical interventions that protect data, identity information, and hardware from unauthorized access or harm. Cybersecurity includes antivirus software, Internet content filters, firewalls, and password protection. Cybersecurity is a form of risk management, and there is a default ethical duty to disclose those risks when identified.

Ethics are codes of conduct that are sometimes enforced by laws. The ethics of cybersecurity falls under the broader topic of the ethics of security. In the cyberspace, ethics is global, interconnected, multicultural, multi-religious, and multi-philosophical. Cyber ethics includes practically all sectors and aspects of society as all parts of the real, physical, emotional, mental, and institutional world are somehow linked to the virtual world of the cyber space. Cyber ethics issues also extend to interactions with consumers.

CHALLENGES

What is right and wrong in the world of cybersecurity is not always clear. There are no mandatory standards for cybersecurity ethics issues that cybersecurity professionals are obligated to follow. There are no mechanism for enforcement. Challenges such as ensuring the privacy of the users, reporting and handling incidental findings, and mitigating biases could have different negative effect on humans if not handled properly. It is impossible to list all of the various unethical behaviors that can be exhibited by someone with cybersecurity skills. There are many areas in cybersecurity that are not covered by laws. Ethics are always complicated, and interrogating them in the digital world is not any simpler.

Cybersecurity professionals face a wide range of other challenges daily. The challenges include the following [18]:

- *Ethical challenges in confidentiality:* Professionals will be exposed to both private and proprietary data and must keep the information confidential. There might be pressure from time to time to divulge juicy information about a user or the company, but professionals must resist such temptation.
- *Ethical challenges in threats:* Response to threats and data breaches is part of the responsibility of cybersecurity professionals. How a Cybersecurity professional responds to threats counts.
- *Ethical challenges in balancing security with other values:* There is a good chance that most cybersecurity professionals will stumble into the shady practices of a business unit. Cybersecurity professionals should explore ways of handling situations of this nature, and the first step is to report such to their supervisors.
- *Ethical challenges in network monitoring and user privacy:* Many professionals often find themselves in the dilemma of carrying out their responsibilities with regards to network monitoring and user privacy without making unjustifiable intrusions on users and their privacy.
- *Ethical challenges in data storage and encryption:* Data storage and encryption are essential because they help to protect an organization's data and keep it safe. Cybersecurity professionals must ensure that encryption practices are well-aligned with the industry's standards.
- *Ethical challenge of cost:* A major ethical issue is the unavoidably huge cost of cyber security. The cost is great because cyber security efforts take up a considerable number of individuals as well as organizational resources like time, money, and expertise.

CONCLUSION

Ethics are moral principles that govern a person's behavior. It is a critical part of any sound cybersecurity defense strategy. Cybersecurity professionals are expected to behave ethically. When you choose to pursue a career in cybersecurity, you should consider ethics. It is important that you have a comprehensive understanding of all IT-related cyber ethics issues. Across many industries, you will be able to prove your value to an organization as a cybersecurity expert with the skills to prevent and protect from the latest security threats [19]. It is wise that you are thoroughly prepared to handle cybersecurity incidents. More information about cybersecurity ethics can be found in the books in [20-23] and the following related periodicals:

- ✓ *Journal of Cybersecurity Education Research and Practice*
- ✓ *Journal of Cybersecurity*
- ✓ *Security Magazine*

REFERENCES

1. S. Sedgwick, "Ethics in technology & cyber security," June 2019, <https://www.linkedin.com/pulse/ethics-technology-cyber-security-shannon-sedgwick-gaicd>
2. "Eliminating the complexity in cybersecurity with artificial intelligence," <https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/>
3. M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society*, June 2019, <https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html>
4. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.
5. M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.
6. "FCC Small Biz Cyber Planning Guide," <https://transition.fcc.gov/cyber/cyberplanner.pdf>
7. "The 8 most common cybersecurity attacks to be aware of," <https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/>
8. Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation*, University of Toledo, 2015.
9. "Ethics in life and business," <https://www.scu.edu/mobi/resources--tools/blog-posts/ethics-in-life-and-business/ethics-in-life-and-business.html>
10. F. G. Reamer, "Evolving ethical standards in the digital age," *Australian Social Work*, 2016, pp. 1-12.
11. "The ethics of cybersecurity: Debating the gray areas," February 2023, <https://sennovate.com/the-ethics-of-cybersecurity-debating-the-gray-areas/>
12. "Ethical issues in cybersecurity,"

<https://www.futureoftech.org/cybersecurity/4-ethical-issues-in-cybersecurity/>

13. "Why do we need ethics in cyber?" March 2023,
<https://www.ukcybersecuritycouncil.org.uk/news/news/why-do-we-need-ethics-in-cyber/#:~:text=In%20the%20world%20of%20cyber,consequences%20both%20legally%20and%20financially.>
14. "Behind the experts' perspective: Ethical issues behind cybersecurity," April 2022,
<https://socradar.io/behind-the-experts-perspective-ethical-issues-behind-cybersecurity/#:~:text=What%20are%20the%20Critical%20Ethical,to%20the%20aforementioned%20regulatory%20vacuum.>
15. "Ethical implications of cybersecurity," Unknown Source.
16. D. G. Ries, "Cybersecurity for attorneys: The ethics of incident response," November 2020,
<https://www.lawpracticetoday.org/article/cybersecurity-attorneys-ethics-incident-response/>
17. "Cybersecurity & data privacy,"
<https://zfzlaw.com/practice/cybersecurity-and-data-privacy/>
18. "Cybersecurity ethics," July 2021,
<https://dcencompass.com.au/blog/cybersecurity-ethics/>
19. "The increasing focus on cyber ethics issues,"
<https://online.maryville.edu/blog/cyber-security-ethics/#:~:text=The%20Increasing%20Focus%20on%20Cyber%20Ethics%20Issues&text=Since%20the%20internet's%20inception%20C%20hackers,and%20wide%20Dranging%20over%20time.>
20. J. Kołodziej, M. Repetto, and A. Duzha (eds.), *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*. Springer, 2022.
21. A. Blackburn, I. L. Chen, and R. Pfeffer, *Emerging Trends in Cyber Ethics and Education*. IGI Global, 2018.
22. M. Christen, B. Gordijn, and M. Loi, *The Ethics of Cybersecurity*. Springer Nature, 2020.
23. M. Manjikian, *Cybersecurity Ethics: An Introduction*. Taylor & Francis, 2022.



Figure 1. Cybersecurity involves multiple issues related to people, process, and technology [2].

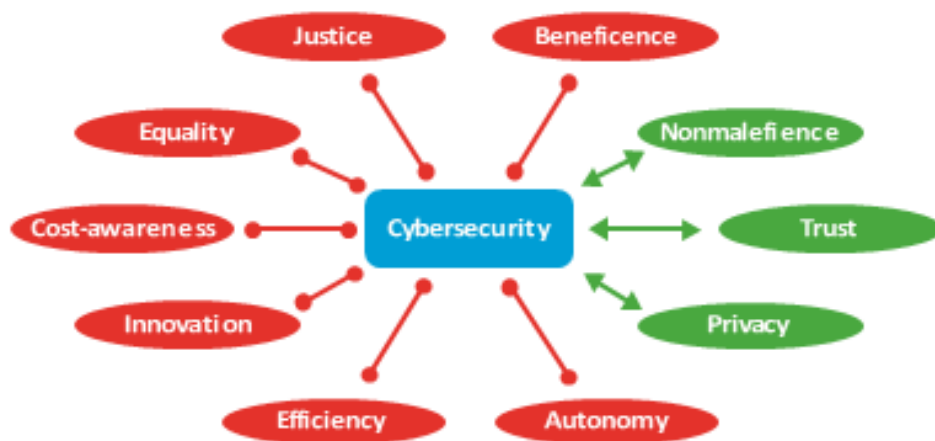


Figure 2. Different components of cybersecurity [3].(Green: supportive; red: in tension)

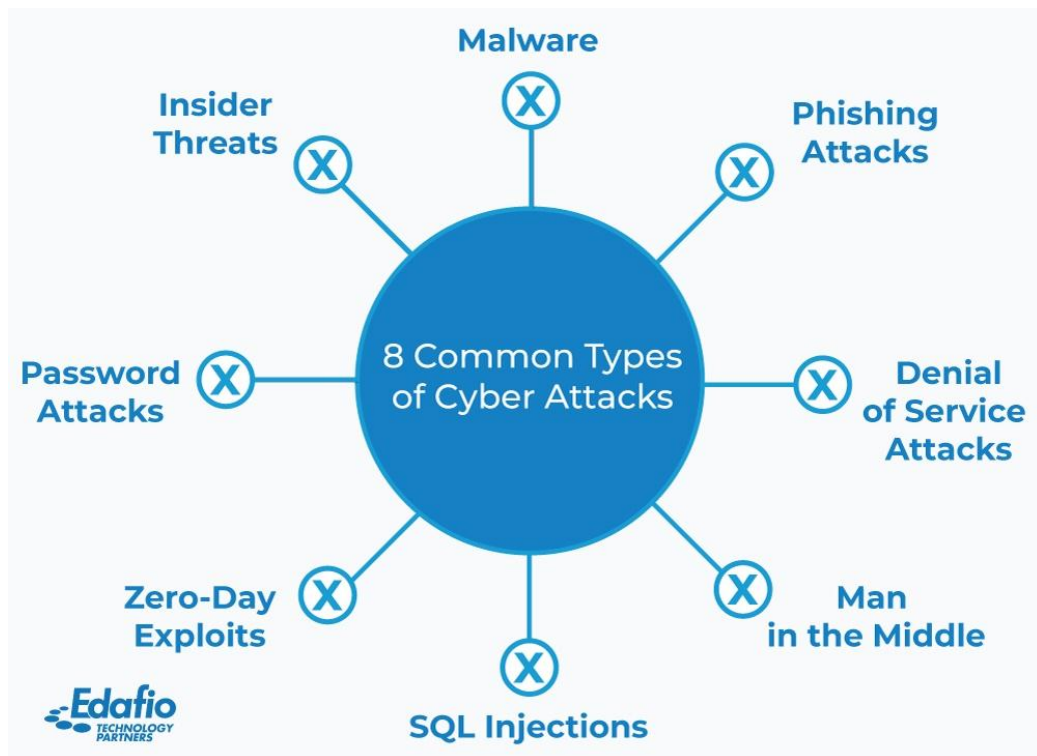


Figure 3. Common types of cyber attacks [7].



Figure 4. Different components of ethics are shown in Figure 4 [9].

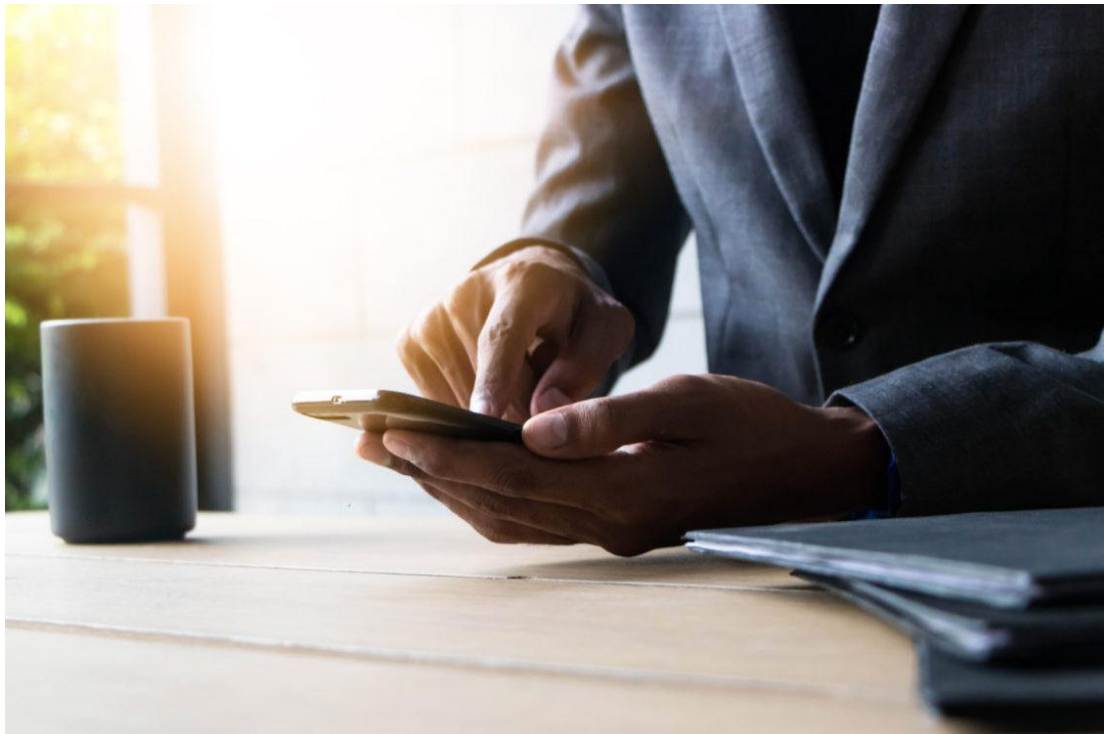


Figure 5. A typical cybersecurity attorney [17]. Figure p. 83,92, 104