St. Mary's Journal on Legal Malpractice & Ethics

Volume 14 | Number 1 Article 5

1-9-2024

Cyber Security: A Lawyer's Ethical Duty

Meagan Folmar

COMMENT

*Meagan Folmar**

Cyber Security: A Lawyer's Ethical Duty

CONTENTS

***Author.** St. Mary's University School of Law 2023. The Author would like to thank family and friends for being steadfast supporters. The Author would like to thank her Comment Editor Araseli Garza and her faculty advisor Professor Bob Summers, J.D. for all the helpful feedback and critiques during the writing of this Comment. The Author would like to thank the *St. Mary's Legal Malpractice & Ethics* Board and the Staff Writers for their assistance and feedback during the editing process. The Author hopes this Comment drives thoughtful and meaningful changes to best serve clients in the future.

I. INTRODUCTION

The world today is unrecognizable from the world of the past. Technology has changed virtually every facet of modern-day living, and society has undergone a complete metamorphosis from life as we knew it twenty years ago. It has played an important role in various aspects of civilization, such as war, culture, quality of living, and medical advancements. Also, technology has influenced the application, interpretation, and development of the law. Due to the prominence of technology in society, cyber security is no longer a thing of the future; it is here today, and it must be dealt with now.

Consider the world in which we live: employers deposit currency to employees electronically, cell phone applications digitally transfer money, credit cards are used for practically every monetary transaction, Zoom is used to administer education to students, important government applications are performed online, almost everyone uses a phone to communicate, sensitive personally identifiable information is electronically stored, and the average person relies on critical infrastructure to survive. The fact that the average person is reliant on critical infrastructure is troubling because this infrastructure is also dependent on technology to function. This reliance upon technology presents a troubling vulnerability that could easily be exploited by malicious actors. Additionally, this illustrates a high likelihood that average Americans across the country will suffer devastating consequences if they lose access to necessary resources provided by critical infrastructure, such as access to food, electricity, clean water, or emergency services.

Such ramifications that would result from exploiting these weaknesses would likely have critical effects on the United States. The United States' status as a first world country, leader of the free world, and haven of peace to people around the globe would then naturally be threatened. This realization—one which is grounded on genuine vulnerabilities and realistic threats—has not been lost on government officials in leadership positions. Recognizing how heavily the United States relies on critical infrastructures for daily life, which, as stated previously, is dependent upon technology that is highly vulnerable to cyber-attacks, former Secretary of Defense Leon Panetta warned of a "[C]yber Pearl Harbor" in 2012.[1] Over a decade

1. *See* Leon Panetta, Sec'y of Def., U.S. Dep't of Def., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012),

has passed since this warning, and yet, any successful cyber-attack on these vulnerable critical infrastructures could still devastate life as we know it in the United States.[2]

There are many factors that contribute to why cyber vulnerabilities are so prevalent in the United States and extremely dangerous to her inhabitants and allies. One of the main issues that this Comment will explore in depth below is the lack of ethical standards for lawyers in relation to cyber security. Ethical standards for lawyers related to the field of cyber security, also known as cyber ethics, are woefully insufficient in the rapidly advancing field of technology. In short, the legal profession has not acted ethically in its approach with cyber security, and it is time to hold lawyers accountable in this long-ignored ethical duty. Numerous factors have played a role in this problem, but a key reason for its manifestation lies in the fundamental differences between the legal field and technological professions.

Not only is cyber security constantly evolving but its evolution progresses at a faster rate than the law—which is reliant upon tradition and precedent—can keep up with.[3] Legislation has passed in various fields of society, which serves to demonstrate how pervasive cyber security affects all aspects of life. These categories include—but are not limited to—banking requirements,[4] enforcing accountability standards on computer services providers,[5] instituting obligations on financial institutions,[6] making endeavors to protect critical infrastructure,[7] addressing new constitutional

---

http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (emphasizing the danger of a catastrophic cyber-attack and the need for cyber leadership).

2. *See* RICHARD J. CAMPBELL, CONG. RSCH. SERV., R45312, ELECTRIC GRID CYBERSECURITY 1, 17 (2018) (remarking how vital electricity is to the functioning of modern life and its vulnerability to cyber-attacks).

3. *See* ERIC A. FISCHER, CONG. RSCH. SERV., R42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW OF MAJOR ISSUES, CURRENT LAWS, AND PROPOSED LEGISLATION 1, 2 (2014) (showing the United States lacks an overarching framework legislation for cyber security).

4. *See* 15 U.S.C.A. § 1681 (West) (noting how the banking system depends on fair and accurate reporting and requiring consumer reporting agencies to implement reasonable procedures to protect consumer information).

5. *See* 47 U.S.C.A. § 230 (West 2018) (enforcing obligations on computer services with notification requirements of parental controls).

6. *See* Gramm–Leach–Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (mandating financial institutions to inform clients of their information-sharing practices and protect their sensitive data).

7. *See* Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (facilitating efforts to protect national critical infrastructure from cyber threats).

questions,[8] liability relating to cyber bullying,[9] deciding the legality of secretly taped conversations,[10] using artificial intelligence,[11] and implementing standards for safeguarding health information.[12]

Cyber security has also found its way in the court system based on innovative legal issues and courts have long needed to address the impact cyber security has had on existing laws, such as cyber harassment,[13] cyber vandalism,[14] data breaches,[15] and breach of contract claims.[16] It is important to note decisions by courts often describe these kinds of cases with adjectives like "fantastic"[17] or "speculative."[18] It is not uncommon for courts to regularly dismiss motions or claims that have some cyber security component. Such descriptions and holdings by courts to dismiss or deny

8. *See* U.S. CONST. amend. I (requiring freedom of speech which extends to the cyber domain).

9. Natasha Rose Manuel, *Cyber-Bullying: Its Recent Emergence and Needed Legislation to Protect Adolescent Victims*, 13 LOY. J. PUB. INT. L. 219, 246–47 (2011) (discussing the legal complexity of cyber bullying and constitutional concerns).

10. *See generally* CHARLES DOYLE, CONG. RSCH. SERV., R42650, WIRETAPPING, TAPE RECORDERS, AND LEGAL ETHICS: AN OVERVIEW OF QUESTIONS POSED BY ATTORNEY INVOLVEMENT IN SECRETLY RECORDING CONVERSATION 1 (2012) (discussing attorney ethics with complicated issue of secretly recording conversations legally).

11. *See generally* LAURIE A. HARRIS, CONG. RSCH. SERV., IF10608, OVERVIEW OF ARTIFICIAL INTELLIGENCE 1 (2017) (demonstrating the pervasive use of artificial intelligence in the modern world, including its effect on the legal and cyber security sector).

12. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (preventing fraud and abuse and protecting patient health information).

13. *See* Brune v. Takeda Pharms. U.S.A., Inc., No. 1:18CV298-LG-RHW, 2019 WL 3323511, at *1 (S.D. Miss. July 24, 2019) (dismissing plaintiff's claim of cyber harassment).

14. *See* Cobb v. Consunji, No. C-11-02496 DMR, 2011 WL 6813221, at *1–2, 7 (N.D. Cal. Dec. 28, 2011) (granting defendant's motion to dismiss plaintiff's claim of cyber-attacks on his computer and cyber vandalism on his home network).

15. *See In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1320 (N.D. Ga. 2019) (holding plaintiffs' claim asserting their private information was compromised from a data breach from the defendant's knowledge of their severe cyber security deficiencies was recognized under Georgia law); *see also* LabMD Inc. v. Boback, 47 F.4th 164, 173 (3d Cir. 2022) (dealing with cyber security practices and data leak of confidential patient information).

16. *See* Orbital Eng'g, Inc. v. Buchko, 578 F. Supp. 3d 727, 733 (W.D. Pa. 2022) (denying an expert's opinions on cyber security industry standards with breach of contract claim under Federal Rules of Evidence).

17. *See* Hensley v. Agorapulse, Inc., No. 3:20-CV-01539-HZ, 2022 WL 3586715, at *2 (D. Or. Aug. 18, 2022) (dismissing plaintiff's fantastic claims of identity theft, cyberterrorism, and cyberstalking).

18. *See* Lake v. Hobbs, No. CV-22-00677-PHX-JJT, 2022 WL 3700756, at *12 (D. Ariz. Aug. 26, 2022) (holding the plaintiffs lacked standing but noting the precious right to vote and holding no injury in fact with claims asserting how voting machines are hackable).

cyber security related claims, defenses, and evidence,[19] may be indicative of a pervasive, institution-wide problem of lawyers not understanding how cyber security works or cyber security's real-world legal impact.

The dichotomy between cyber security and the legal profession is a unique problem which has extensive ramifications for a few different reasons. As a highly specialized field, cyber security may be misunderstood by lawyers who may not comprehend the full effects cyber security has on daily life, its impact on interpreting laws, and the long-ago arisen ethical duties of lawyers across the legal profession. Lawyers hold a position of power in society[20] as they act as representatives for clients who have been harmed in some way, whether that involves representing plaintiffs, prosecutors, defense counsels, or general advisors for companies. To be more specific, lawyers have an ethical responsibility to represent their clients effectively, maintain the best interests of their clients, and safeguard their clients' sensitive information. Cyber security has existed for years, but the legal industry has not kept up with their duty to act competently. Despite this fact, there is a gross deficiency in the legal profession where fiduciaries and protectors of the people have not been acquiring the necessary knowledge to maintain basic competency to effectively represent their clients.

An effective solution to this problem is for state bar associations and the American Bar Association (ABA) to create an ethical cyber security culture and to enforce standards on both aspiring lawyers and practicing lawyers to follow. They can effectuate these imperative objectives by implementing changes for both practicing lawyers and law students. First, these bar associations can best target practicing lawyers by updating their professional responsibility rules and requiring continuing legal education courses related to cyber security. On the other side, they can best target law students by mandating law schools to provide a cyber security course for all law students as a prerequisite for graduation, updating the Multistate Professional Responsibility Examination, and adding cyber security as a new subject on the Uniform Bar Examination.

19. *See* FED. R. EVID. 1101 (demonstrating how the Federal Rules of Evidence apply to various federal courts, cases, and proceedings).

20. *See* JENNIFER E. MANNING, CONG. RSCH. SERV., R46705, MEMBERSHIP OF THE 117TH CONGRESS: A PROFILE 2 (2022) (showing how law is among the top three professions of the 117th Congress).

II. BACKGROUND

As modern society has astronomically advanced due to technological developments, an emphatic ethical duty has arisen for lawyers to be educated in basic cyber security. The process of becoming a lawyer already requires advanced, specialized education; likewise, cyber security is an advanced, specialized field that takes years for technology specialists to master. To be clear, this Comment is not advocating for lawyers to become experts in two complicated, specialized fields. This Comment simply demonstrates the importance of lawyers having basic cyber security literacy and advocates for state bars and the ABA to instill an ethical legal culture in relation to cyber security. Technology and cyber security pervade every area of life;[21] globalization of the world has fundamentally changed how lawyers should apply laws and how they should ethically behave.

Lawyers are leaders in ethics and policy in this nation, which is illustrated by the fact that the legal field dominates as one of the top three careers of legislators before being elected to office.[22] Despite the changed world we live in and the importance of cyber security in a modern society, there has noticeably lacked an express duty for lawyers to have cyber ethics and enforcement standards related to cyber security.[23] Lawyers must be held responsible for obtaining basic knowledge in cyber security due to the sensitivity of personal information lawyers keep in their possession, and the reliance clients have on lawyers to protect their information and advocate for them to the best of their ability. It is up to regulatory organizations—such as the state bars and the ABA—to take official action to create ethical cyber security rules and guidelines for how lawyers should act.

III. ANALYSIS

A. State Bars and the American Bar Association must create and enforce ethical

21. *See* Laurel S. Terry, *Transnational Legal Practice (United States)*, 47 YEAR IN REV. 499, 499–501 (2013) (explaining the developments of transnational law and explaining how the legal market has sustained fundamental changes due to globalization and technology).

22. *See* MANNING, *supra* note 20, at 2 (showing how law is among the top three professions of the 117th Congress).

23. *See* Kathleen E. Lang, *Computer Network Security and Cyber Ethics*, 2 J. HIGH TECH. L. 1, 1–2 (2003) (stressing the need for a legal framework to handle living in a cyber society and developing legal processes to protect users while addressing cyber ethics).

cyber standards on lawyers

Ethics is a key component of the legal profession because of lawyers' unique roles in society and their special responsibilities to clients.[24] In the widely used Black's Law Dictionary, ethics is defined as:

> 1. A system of moral tenets or principles; the collective doctrines relating to the ideals of human conduct and character. 2. The study of behavior as judged by moral right and wrong, including the sources, principles, and enforcement of behavioral standards.[25]

Legal ethics in the Black's Law Dictionary is defined as:

> The standards of professional conduct applicable to members of the legal profession within a given jurisdiction. Ethical rules consist primarily of the ABA Model Rules of Professional Conduct and the earlier ABA Model Code of Professional Responsibility, together with related regulatory judgments and opinions. The Model Rules of Professional Conduct have been enacted into law, often in a modified form, in most states.[26]

Nowhere in either of these definitions that are contained in this highly influential legal dictionary is the mention of cyber security or a lawyer's ethical duties in relation to cyber security. Discussion and implementation of ethics, particularly legal ethics, has been around for centuries with two conflicting theories of thought:

> Two old and antagonistic traditions of thought shape the modern field of legal ethics . . . influenced the design of the American republic . . . that have been a part of our public life ever since. Our view of the legal profession . . . is the product of a similarly unstable combination of elements drawn from these two traditions . . . . Just as it is impossible to assign one tradition of thought, the republican or contractarian, a decisive priority in the political system our founders created, it is likewise impossible to say which of these contains the truth about legal ethics. . . . That is because legal ethics is not taught in

24. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS intro. (Am. L. Inst. 2000) (reflecting how ethical lawyers are driven by professional ideals and showing how lawyers have special moral, professional, and legal responsibilities for justice as officers of the court and representatives of clients).

25. *Ethics*, BLACK'S LAW DICTIONARY (11th ed. 2019).

26. *Legal Ethics*, BLACK'S LAW DICTIONARY (11th ed. 2019).

> isolation. It is taught to students who are also studying other subjects . . . even though it may not be an explicit topic of discussion in these courses.[27]

The history, influences, and discussion of differing thoughts of ethics and legal ethics illustrate the increasing complexities and moral ethical dilemmas in modern times. Regardless of whether lawyers follow the republican or contractarian ethical systems of thought, ethical legal cyber security standards and principles still apply to all forms of practice. This fact is particularly relevant nowadays and has only become more prevalent with the rise, dominance, and permanence of cyber security. For example, consider the cyber vulnerabilities of critical infrastructures and the steady increase of cyber warfare between countries around the globe.[28] The conduct of war has evolved with the advancement of cyber warfare, so too must the rules of ethics evolve to meet this change. The need for lawyers to understand cyber security in this context becomes even more critical when considering the importance of properly advising governments when to engage an enemy who is utilizing interconnected computer systems and how to avoid inadvertently breaching legal obligations when responding to cyber-attacks. The need for cyber literacy and ethical education is particularly relevant to lawyers in the private sector who advise companies how to legally respond to cyber-attacks.[29]

Ethics is also significantly affected by a world that grows smaller and more digitized with each passing day.[30] While the United States' legal culture places a strong emphasis on tradition and precedent, the United States also has a long history of leading efforts in legal ethics on a global scale.[31] However, some laws passed by Congress have been insufficient and a truly effective solution rests with regulatory organizations like state bars and the

27. *See* Anthony T. Kronman, *The Fault in Legal Ethics*, 122 DICK. L. REV. 281, 281, 291, 294 (2017) (discussing the origins and influences of legal ethics).

28. *See* JENNIFER K. ELSEA, CONG. RSCH. SERV., LSB10709, WAR CRIMES: A PRIMER 1 (2022) (discussing war crimes and international armed conflict and demonstrating relevance of cyber legal ethics in modern times with increasing information warfare).

29. *See* KRISTIN FINKLEA, CONG. RSCH. SERV., R42547, CYBERCRIME: CONCEPTUAL ISSUES FOR CONGRESS AND U.S. LAW ENFORCEMENT 11–12 (2015) (illustrating the different concerns and goals of law enforcement and the private sector in response to a cyber incident).

30. *See* Terry, *supra* note 21, at 372 (2017) (examining how global developments have affected legal ethics in the United States).

31. *See* MICHAEL A. WEBER, CONG. RSCH. SERV., IF10861, GLOBAL HUMAN RIGHTS: MULTILATERAL BODIES & U.S. PARTICIPATION 1 (2018) (showing the United States' leading role in composing comprehensive human rights and fundamental freedoms in international treaties in the aftermath of World War II).

ABA. Lawyers should obviously show great deference to any legislation passed by Congress. However, lawyers should not wait long periods of time for specific statutes to become binding law, nor should they solely rely on Congress—a conglomerate of lawyers and non-lawyers—to set forth ethical standards of legal practice. As a heavily self-regulated profession,[32] it is the responsibility of lawyers themselves and regulatory legal organizations who understand the demands and duties of legal practice to set forth enforceable standards for ethical conduct. Cyber security has existed for years, and yet, lawyers have not been meeting their ethical duty of acquiring this necessary knowledge. To illustrate, law firms are gold mines for hackers and are major targets for cyber-attacks. Law firms of all locations, practice areas, and sizes face a serious risk of cyber-attacks due to the sensitive information and money that they hold.[33] Despite being an obvious target for malicious actors and attacks, elemental cyber security standards, such as the use of email encryption, have noticeably lacked.[34]

State bars and the ABA play a vital role in establishing an ethical cyber security culture in the United States' legal field, given their legal influence and regulatory authority over practicing attorneys. For example, lawyers who do not obey the ethical standards of conduct set forth by their state bars are subject to discipline and potential disbarment. State bars have individual ethical standards, but many states utilize common themes, such as using an objective reasonableness standard to evaluate whether a lawyer's conduct is considered ethical.[35] The ABA, unlike the state bars, has a national legal focus with significant influence on the development of legal

32. *See* L. PAIGE WHITAKER, CONG. RSCH. SERV., LSB10278, CONTINUING LEGAL EDUCATION: WHAT'S REQUIRED AND OPPORTUNITIES FOR MEMBERS AND STAFF TO SATISFY THOSE REQUIREMENTS 1 (2019) (explaining how attorneys are members of a self-regulated profession).

33. *Cybersecurity for Law Firms: What Legal Professionals Should Know*, A.B.A. (Dec. 29, 2022), https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity-for-law-firms/ [https://perma.cc/S8G2-TSMD].

34. *See* Karen Painter Randall & Steven A. Kroll, *Getting Serious About Law Firm Cybersecurity*, 300-JUN N.J. LAW. 54, 55 (2016) (showing how law firms have experienced many data breaches, advocating an ethical duty for law firms to take an active approach to cyber security, and demonstrating how only 35% of lawyers use encryption when sending emails).

35. *See* James M. McCauley, *Professional Responsibility*, 43 U. RICH. L. REV. 255, 264 (2008) (discussing ethical standards of lawyers in Virginia, including measuring actions under an objective reasonableness standard).

and ethical standards.[36] Due to their power and widespread influence, state bars and the ABA must implement and enforce ethical rules of cyber conduct for all lawyers.

The first section of this Comment advocates for two concrete suggestions that state bar associations and the ABA can adopt to meet this ethical duty. The first suggestion is to update the Model Rules of Professional Conduct and the second is to require annual legal education units related to cyber security. Years have passed since government officials have recognized the catastrophic impact that cyber-vulnerabilities pose to the United Sates.[37] Over a decade has come and gone since former U.S. Secretary of Defense Panetta warned of a "[C]yber Pearl Harbor," but as will be explained in more detail below, this warning has been shouted hopelessly into the abyss without effective ethical response by a profession that prides itself on its impeccable morality.[38] One solution to this national problem and moral imperative for the practice of law is for state bars and the ABA to implement and enforce an ethical cyber security culture.

1. Update the Model Rules of Professional Conduct

The Model Rules of Professional Conduct (Model Rules) are rules created by the ABA to serve as a model for ethical standards of conduct on lawyers in the United States. Scholars have argued for decades that updates need to be made to the Model Rules.[39] A few cyber security related comments have been added to various rules, but these additions have proven to be insufficient.[40] There may be concerns about changing the language of the Model Rules themselves due to the need for stability and years of precedent

36. *See ABA Timeline*, A.B.A., https://www.americanbar.org/about_the_aba/timeline/ [https://perma.cc/KNR7-HFXY] (showing a timeline of the ABA, including when the ABA implemented standards for education and admission of lawyers into the practice of law).

37. *See* Panetta, *supra* note 1 (emphasizing the danger of a catastrophic cyber-attack and the need for cyber leadership).

38. *Panetta Warns of 'Cyber Pearl Harbor'*, ASS'N U.S. ARMY (Apr. 26, 2022), https://www.ausa.org/news/panetta-warns-cyber-pearl-harbor [https://perma.cc/UJM4-RHJB]; *see* WHITAKER, *supra* note 32, at 1(explaining how attorneys are members of a self-regulated profession).

39. *See* Michelle Grant, *Legislative Lawyers and the Model Rules*, 14 GEO. J. LEGAL ETHICS 823, 827–828, 833 (2001) (arguing how the Model Rules are insufficient for legislative lawyers who have special responsibilities to the integrity of creating law and reinforcing how legislative lawyers must diligently advocate for their clients).

40. *See* John G. Loughnane, *2019 Cybersecurity*, A.B.A. (Oct. 16, 2019), https://www.americanbar.org/groups/law_practice/publications/techreport/abatechreport2019/cybersecurity2019/ [https://perma.cc/TWL5-PR3X] (illustrating some efforts made by ABA to meet cyber security ethical demands).

before making such a change.[41] However, innovation must be made and is long past due.[42] The framework of classic ethics[43] has evolved with our now globalized world,[44] even if professional rules have yet to evolve to effectively meet these needs. The following proposals might be met with disapproval, but Model Rule 1.6 was controversial when first implemented, and it is now ingrained in how lawyers ethically interact with clients.[45] Dissenters may argue that cyber security literacy should be limited to lawyers who work in fields related to technology, but cyber security naturally encompasses all areas of law. No lawyer can escape this ethical duty.[46] Law firms, due to their nature of carrying sensitive client information, are common targets for cyber criminals seeking to exploit that information.[47]

There are three main Model Rules that must be updated to include cyber security ethical standards: Model Rule 1.1,[48] Model Rule 1.3,[49] and Model Rule 1.6.[50] Given how cyber security pervades all aspects of modern life, the ability of lawyers to provide competent representation, act reasonably and diligently, and protect client information is implicated.

41. *See* Sissela Bok, *Can Lawyers Be Trusted?*, 138 U. PA. L. REV. 913, 914–15 (1990) (discussing controversy when Model Rule 1.6 was adopted and strict interpretations of lawyer responsibilities).

42. *See* William D. Henderson, *Three Generations of U.S. Lawyers: Generalists, Specialists, Project Managers*, 70 MD. L. REV. 373, 374 (2011) (determining the importance of innovation for legal successes and economic prosperity).

43. *See* Stephen R. Galoob & Su Li, *Are Legal Ethics Ethical? A Survey Experiment*, 26 GEO. J. LEGAL ETHICS 481, 484–90 (2013) (debating competing legal ethical theories and comparing them to ordinary morality).

44. *See* Joseph Z. Fleming, *E-Ethics*, SV039 ALI-CLE 1265 (2014) (defining e-ethics as recognizing legal changes resulting from instantaneous communication and pointing out electronic ethics issues).

45. *See* Bok, *supra* note 41, at 915–16 (discussing controversy when Model Rule 1.6 was adopted and strict interpretations of lawyer responsibilities).

46. *See* Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 23–24 (2010) (showing how new developments in technology affect attorneys' ability to safeguard client confidentiality and discussing arising questions, such as whether liability should attach to lawyers who send documents with hidden sensitive information).

47. *See* Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 AM. U. L. REV. 1243, 1250 (2013) (emphasizing the devastating cyber threats the public and private sectors are facing and explaining how law firms are targets for insidious attacks since they are centers to sensitive information and secrets).

48. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.1 (AM. BAR ASS'N 2023) (requiring lawyers to be competent).

49. *See id.* R. 1.3 (requiring lawyers to act with reasonable diligence).

50. *See id.* R. 1.6 (requiring lawyers not to reveal client information without consent).

First, cyber security affects a lawyer's ethical duty to be competent while representing a client.[51] Model Rule 1.1 states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[52]

Competence does not come with a comprehensive set of strict rules, nor does it remain stagnant over time or vary based on geographic location or area of practice.[53] Because the internet is engrained in the functionality of daily life, cyber security naturally affects a lawyer's competence.[54] As a result, it is imperative for lawyers to have cyber literacy so they can understand real-world cyber risks to properly advise clients.[55] It is essential for lawyers to be competent, lest the client suffer damages for her lawyer's ineptitude.[56] As mentioned above, a few Comments that bear some relation to cyber security have been added:

> Comment 8 to Model Rule 1[.1] makes clear, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." Clearly, the duty of competency requires cyber security considerations.[57]

---

51. *See id.* R. 1.1 (requiring lawyers to be competent).

52. *Id.*

53. *See* Emile Loza, *Attorney Competence, Ethical Compliance, and Transnational Practice*, 52 ADVOC. 28, 28 (2009) (demonstrating how a small town from Idaho is affected by globalized legal practice and arguing how globalization demands change for how attorneys practice and evolving standards for competence).

54. *See* JACOB A. STEIN & ANDREW M. BEATO, THE LAW OF LAW FIRMS § 9:3 (2d ed. 2021) (describing how the Internet has become essential to legal practice and different permissible conduct of lawyers with different mediums of communication); *see also* MODEL RULES OF PROF'L. CONDUCT R. 1.1 (requiring lawyers to be competent).

55. *See* James A. Johnson, *Insuring Against Cybercrime-Know the Risks*, 91-MAY N.Y. ST. B.J. 14, 15 (2019) (showing the importance of lawyers to understand cyber risks to properly advise clients); *see also* MODEL RULES OF PROF'L. CONDUCT R. 1.1 (requiring lawyers to provide competent representation).

56. *See* ROBERT C. LOWE, 1 LA. PRAC. DIVORCE § 2:2 (2022) (describing how disciplinary rules are required for attorneys to follow and damages for legal malpractice are available for clients who have suffered from attorney's conduct from failing to provide reasonable competence).

57. *See* Loughnane, *supra* note 40 (illustrating some efforts made by ABA to meet cyber security ethical demands); *see also* MODEL RULES OF PROF'L. CONDUCT R. 1.1 cmt. 8 (listing out Comments added to Model Rule 1.1).

Comment 8 to Model Rule 1.1 states that lawyers "should keep abreast of changes in the law . . . including the benefits and risks . . . with relevant technology."[58] This language is passive and vague, allowing for too much leeway to require truly ethical legal cyber security conduct and does not "[c]learly . . . require[] cyber[]security considerations" as argued.[59] This language passively encourages lawyers to familiarize themselves with some cyber security changes so long as it remains "relevant," but the Rule does not actively advocate for lawyers to educate themselves in the realm of cyber security related to the practice of law.[60] Telling lawyers that they "should" stay afloat is not the same as requiring lawyers to take responsibility for their cyber security literacy.[61] Comment 8 must be updated with proactive language. For example, to maintain competence—with the necessary prerequisites of maintaining knowledge and skill—all lawyers must educate themselves on laws passed and widely accepted cyber security and technological industry practices.

There is a significant distinction between the current and proposed Rule—namely, the difference between mandatory and permissive language. One significant difference is the use of the word "should"[62] versus the use of the word "must." The use of the word "should"[63] connotates optional acquiescence; in other words, lawyers may continue utilizing poor cyber security hygiene, which places their clients and firms at risk. Adopting the word "must" in the Model Rules is an entirely different matter altogether. It would hold American lawyers accountable for their cyber education and cyber security practices. Additionally, "benefits and risks of . . . relevant technology"[64] leaves considerably more room for argument in court

58. Loughnane, *supra* note 40.

59. *Id.*

60. *See id.* (illustrating some efforts made by ABA to meet cyber security ethical demands).

61. *See id.* (explaining how "[the] opinion does not set forth a mandated form of incident response plan[,]" but rather gives discretion to how individual professionals decide to conform to the Model Rules).

62. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.1 cmt. 8 ("To maintain the requisite knowledge and skill, a lawyer *should* keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.") (emphasis added).

63. *See id.* ("To maintain the requiste knowledge and skill, a lawyer *should* . . . .") (emphasis added).

64. *See* Loughnane, *supra* note 40 (emphasizing how Comment 8 to Rule 1.1 clarifies a duty of competency in cyber security ethics).

proceedings or malpractice settlements to excuse poor cyber security practices, as opposed to lawyers following the intent and purpose of rules passed to protect clients. To be clear, this Comment is not suggesting that lawyers are generally unethical or only follow explicit, mandatory guidance. However, years of inaction have passed. It is long past time to make lawyers act ethically in relation to cyber security, considering its ramifications on clients and modern-day life.

Second, cyber security affects a lawyer's ethical obligation to act with reasonable diligence.[65] Model Rule 1.3 states a "lawyer shall act with reasonable diligence and promptness in representing a client."[66] This rule naturally reflects every lawyer's moral duty to look after their clients' interests.[67]

> [T]he ideal of moral purity—the ideal that one's life should be lived in fulfillment of the most demanding moral principles, and not just barely within the law . . . . Does the lawyer whose conduct and choices are governed only by the traditional conception of the lawyer's role, which these positive rules reflect, lead a professional life worthy of moral approbation, worthy of respect—ours and his own?[68]

The requirement to diligently pursue clients' interests should not be a limited rule with narrow interpretations; it must necessarily be interpreted broadly and encompass lawyers' ethical duties related to the cyber realm.[69] No lawyer, no law firm, and no client exists on an island.[70] Cyber security should and must be considered alongside legal due diligence obligations.[71] Reasonable steps must be taken to safeguard sensitive client information and perform damage control, particularly after a data breach, which

65. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.3 (requiring lawyers to act with reasonable diligence).

66. *Id.*

67. *See* Charles Fried, *The Lawyer as Friend: The Moral Foundations of the Lawyer-Client Relation*, 85 YALE L.J. 1060, 1066 (1976) (showing how lawyers advance their clients' interests as their dominant purpose).

68. *Id.* at 1061.

69. *See* Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, 50 U. MICH. J.L. REFORM 859, 879 (2017) (emphasizing the future of due diligence in a modern world and arguing for a wider view where enterprise risk management merges with cyber security).

70. *See id.* at 860 (illustrating the future risk management concerns and ethical duties that will relate to cyber security).

71. *See id.* at 879 (stating how "despite growing recognition as to the scale and scope of the multifaceted cyber threat facing firms, many . . . are thinking of due diligence too narrowly").

companies routinely fail to do.[72] Hackers have repeatedly revealed and exploited vulnerabilities in the government and private sector for years.

A more concerning development is that even where companies have data breach incident response plans, those plans are often ill-advised and approved by executives who may or may not have acted negligently or without any regard for how their actions deliberately put their companies at risk.[73] In the case of a discovered data breach, unresolved ethical duties arise, such as whether a lawyer should advise the company to pay ransoms in the event of cyber extorsion.[74] The failure to take reasonable steps may be indicative of a sub-standard ethical cyber security culture, which can be remedied by implementing institution-wide ethical cyber security standards in the legal field.[75] Acting ethically and responsibly must be a lawyer's top priority;[76] it is thus common sense to require all lawyers to maintain basic cyber security knowledge. Consequently, it is a moral imperative for state bars and the ABA—due to their power to regulate all lawyers within their chain of command—to implement an ethical cyber security culture in the legal profession.

Lastly, cyber security affects a lawyer's relationship with clients and a lawyer's ethical duty to protect their client's information, absent informed consent from the client or certain other limited circumstances.[77] Model Rule 1.6 states that: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or . . . permitted by paragraph (b)."[78]

---

72. *See* Roland L. Trope, *When Incident Response Goes Awry: Cybersecurity Developments*, 74 BUS. LAW. 229, 233 (2019) (showing the legal and ethical issues of when general counsel needs to provide guidance when businesses are subject to cyber extortion while demonstrating how major companies fail to take reasonable steps in the event of a breach).

73. *See id.* at 231–33 (describing Uber's ill-advised missteps that occurred in the event of cyber extortion).

74. *See id.* at 237 (showing the legal and ethical issues that arise when general counsel needs to provide guidance when businesses are subject to cyber extortion).

75. *See* Thomas R. Tinder, *Legal Ethics*, 30 W. VA. LAW., Aug. 2004, at 1 (showing how lawyers commit ethical legal violations with lack of diligence and reinforcing how legal ethics is the most important responsibility).

76. *See id.* ("Acting ethically and professionally is the most important activity in which every State Bar member is involved.").

77. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.6(a) (requiring lawyers not to reveal client information without consent).

78. *Id.*

Lawyers act as the gatekeepers of their clients' personal information and are vulnerable sources that hackers routinely target.[79] This vulnerability is particularly important from a legal standpoint since cyber-crimes have recently reached epic proportions around the world, with damages estimated to have accumulated over $400 billion annually.[80] Cyber security insurance policies have been offered in recent years.[81] While cyber security related insurance policies may be a good alternative for companies who do everything they can to prevent a breach but fail to do so,[82] it should not be a lawyer or a law firm's first recourse when dealing with cyber security related issues. Cyber security related insurance policies should not be a law firm's primary means to protect its client information because insurance is, by nature, a reactive measure.

Instead, lawyers in both the public and private sectors must take proactive action by educating themselves in basic cyber security literacy to best prevent data breaches in the first place. For example, lawyers who do not understand basic cyber security might unintentionally disclose their clients' data in violation of Rule 1.6.[83] Deciding whether a lawyer is acting ethically while interacting with clients depends on various circumstances. These unintentional disclosures of sensitive client information can result from lawyers acting in a way that compromises their clients' data,[84] such as failing to follow bare minimum cyber security precautions that lead to insecure data communications. Disclosure of client information can also occur when lawyers, lawyers' agents, clients, or clients' agents communicate by using social media platforms.[85] With every new generation increasingly using social media, lawyers should expect more outreach from potential clients who utilize these platforms. For example, consider a lawyer who communicates with a client through private messages on Facebook and a lawyer who responds to a client's message by making a public post on

79. Dan Zureich & William Graebe, *Cybersecurity: The Continuing Evolution of Insurance and Ethics*, 82 DEF. COUNS. J. 192, 192–93 (2015).

80. *Id.*

81. *Id.* at 196.

82. *See id.* at 196–97(explaining the different types of cyber insurance policies and how they insure against losses related to a data breach of cyber-attack).

83. Alyssa A. Johnson & Mollie T. Kugler, *Protect your Firm from Collateral Damage*, 61 No. 10 DRI FOR DEF. 56, 56 (2019).

84. *See* Kenzie Schott Cardella, *Getting Hacked: It's Only a Matter of Time*, 68 LA. B.J. 114, 114 (2020) (emphasizing "an attorney's ethical obligation when it comes to protecting client data").

85. *See* Lisa McGrath, *How to Avoid Ethical Violations When Using Social Media*, 61 ADVOC. 30, 31–32 (2018) (comparing lawyers' ethical responsibilities in relation to social media).

TikTok. It is also important to consider what technology the lawyer used when communicating with a client to determine if they may be acting unethically. A lawyer who drafts important client documents with sensitive data on a computer may, or may not, act more ethically than a lawyer using an old iPad. Or, consider a lawyer who casually works at their local coffee shop and uses the shop's public network (or those who fail to use email encryptions or Virtual Private Networks) to send sensitive emails. Additionally, the use or lack of basic cyber security safeguards are significant factors in determining ethical or professional legal behavior.[86]

> Comment 18 sets forth factors to be "considered in determining the reasonableness of the lawyer's efforts include . . . the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients . . . ."[87]

Comment 18 to Rule 1.6 is better drafted than Comment 8 to Rule 1.1.[88] This is in part because Rule 1.6(c) uses the word "shall,"[89] denoting mandatory action. This Rule could also implement additional remarks or minor edits to emphasize the need for an explicit reference to cyber security related action. For example, additional factors might include:

1) The likelihood of harm to the client if the lawyer and the lawyer's agents do not utilize accepted cyber security practices.

2) The likelihood of unauthorized disclosure or interception of any communication related to representation (including, but not limited to, using public networks, not using Virtual Private Networks, not using encryption, etc.).

3) The importance of using and implementing physical and cyber security safeguards.

4) The lack of cyber security safeguards used by other lawyers, subordinates, or superiors inside or outside the law firm, government

86. *See* Shackelford et al., *supra* note 69, at 365–66 (demonstrating how few businesses are making necessary safeguards to protect private data and promote cyber security).

87. Loughnane, *supra* note 40.

88. *See id.* (comparing Comment 18 to Comment 8, illustrating inadequate Comment drafting of knowing cyber security as a necessary prerequisite to a lawyer's duty to be competent).

89. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.6 (requiring lawyers not to reveal client information without consent).

agency, solo practice, etc. and how the actions of other lawyers do not excuse the individual lawyer's responsibility of using acceptable cyber security practices.

The current factors of this Rule are important and emphasize real-world concerns, such as the cost and difficulty of implementing safeguards.[90] The problem with the current list is that it tilts towards excusing improper cyber security hygiene, which only further perpetuates the problem. None of the current factors mention the effect on the client, and by emphasizing costs over utility, the client will ultimately be the one who is harmed by the legal industry's failure to implement and maintain acceptable cyber security practices.

This Comment is not advocating for every single law company, from solo companies to mammoth-sized law firms, to rigorously adopt and apply the most expensive and cutting-edge cyber security safeguards and mechanisms, or to apply such strict cyber security standards where a lawyer's services are rendered ineffective. Such an idea would likely bankrupt many companies that provide invaluable services to their communities, and constantly changing computer systems and safeguards would prove more futile than helpful. The client would then suffer harm from lawyers who could not effectively provide legal services. The most important takeaway from this discussion is that all law companies and government agencies must utilize accepted cyber security factors to best serve their clients without citing to "cost" and "difficulty" as excuses to not implement acceptable cyber security practices.[91]

Implementing ethical standards and enforcing disciplinary penalties on lawyers who fail to meet their basic responsibilities to their clients would effectively create an ethical legal cyber security culture. For example, the Texas Disciplinary Rules of Professional Conduct serve as a model for ethical conduct to promote public safety, assist Texas-licensed lawyers in making ethical decisions, and explain the consequences of violating these standards.[92] Other states, such as Virginia, have adopted and codified

90. *See id.* R. 1.6 cmt. 17, 18 (demonstrating the current list of factors related to disclosure of confidential information and safeguards).

91. *See id.* (demonstrating the current list of factors related to disclosure of confidential information and safeguards).

92. *See* Gaines West et al., *Ethics and Administrative Law: How the Proposed Amendments to the Texas Rules of Professional Conduct May Impact Administrative Proceedings*, 11 TEX. TECH ADMIN. L.J. 305, 307 (2010) (discussing how the Texas Disciplinary Rules of Professional Conduct acts as a model of ethical

similar rules for regulating the ethical conduct of Virginia-licensed lawyers by utilizing objective standards for evaluating ethical legal conduct.[93] However, as state and national rules currently stand, uncertainty remains.[94]

> Although every state is free to adopt its own ethical rules, most states have adopted a version of the Model Rules of Professional Conduct . . . . To date, [fifty-one] states have adopted a version of the Model Rules . . . .[95]

The importance of the ABA and the Model Rules of Professional Conduct cannot be understated. ABA requirements are extremely important due to their significant influence on the national stage; aspiring lawyers will face noteworthy obstacles being admitted to a state bar to practice law if they do not attend an ABA accredited law school or meet other ABA related requirements.[96] As demonstrated and analyzed above, the national deficiency in cyber security ethics can be partially remedied by updating the Model Rules to reflect the evolution of ethics and the need for cyber-ethical lawyers in modern-day life.[97]

2. Create ethical legal education units specifically for cyber security

This Comment also advocates for state bars and the ABA to require practicing lawyers to take additional annual legal education courses to remain in good standing in their admitted jurisdiction(s). These continuing legal education courses would exclusively focus on cyber security practices and related ethical conduct. This suggestion would act in tandem with the argument that state bars and the ABA must update their ethical rules of conduct so lawyers would receive continual training on cyber security to help them understand their respective duties and responsibilities. By

behavior with the objective of promoting public protection, providing guidance, and explaining disciplinary standards for attorneys who do not comply with these standards).

93. McCauley, *supra* note 35, at 263–64 (discussing ethical standards of lawyers in Virginia, including measuring actions under an objective reasonableness standard).

94. *See* JOHN K. VILLA, 1 CORPORATE COUNSEL GUIDELINES § 3:2 (2022) (discussing how genuine questions of ethics for corporate counsel remain and illustrating how severe the consequences are of not obeying disciplinary rules).

95. *Id.*

96. *See* Terry, *supra* note 21, at 466–89 (examining the influences and evolution of legal ethics in the United States for the past century while discussing how the ABA "required law schools to teach [legal ethics]" and Model Rules of Professional Conduct to maintain accreditation).

97. *See id.* (stating how state bars and the ABA changed legal ethics requirements and rules over time to fit the current need).

implementing both suggestions, instead of picking one suggestion over the other, state bars and the ABA would then effectively create an ethical cyber security culture while providing guidance and assistance so lawyers can meet these duties.

Annual legal education units are essential for creating and maintaining an ethical cyber culture.[98] Obligatory legal education units have already been employed by state bars across the country with an emphasis on professional responsibility.[99] Common categories that are the subject of continuing education units due to their high ethical importance, include malpractice, managing offices, prejudice, and professionalism.[100] If these subjects are considered important enough for annual training, then subjects such as cyber security and cyber ethics can only be deemed essential and must be included as a separate category for annual legal education units.

Consider how rapidly the field of cyber security evolves on a day-to-day basis, how it effects everyday life, how interconnected and cyber-dependent systems are around the world,[101] and how devastating the implications of poor cyber security practices could have on clients and the functioning of modern-day life as discussed above. Consequently, it is only common sense and morally relevant to include cyber security as a subject for obligatory annual continuing education courses that lawyers must study to maintain good standing in their admitted jurisdiction(s).[102] Without ethical standards, legal community practices, and official guidance, questionable legal actions can result.[103] It is important for lawyers to understand that legal ethics is not stagnant; it is a living, breathing organism that evolves with never-ending societal changes and demonstrates how all lawyers should behave to meet the needs of current times.[104]

---

98. *See* Marcia L. Proctor, *Continuing Education in Professional Responsibility*, 77 MICH. B.J. 678, 678–79 (1998) (discussing the importance of legal education units).

99. *See id.* at 678–80 (explaining how state bars require professional responsibility and mandatory legal education to develop ethical lawyers).

100. *See id.* at 678–79 (listing areas of focus for annual ethical development).

101. *See* Nicholas Tsagourias, *Cyberwar: Law and Ethics for Virtual Conflicts*, 110 AM. J. INT'L L. 609, 611–12 (2016) (explaining how prevalent cyber security vulnerabilities are in our global world).

102. *See id.* at 610–11 (discussing how cyber security vulnerabilities are morally relevant).

103. *See* Michael L. Fox, *To Tell or Not to Tell: Legal Ethics and Disclosure after Enron*, 2002 COLUM. BUS. L. REV. 867, 885–87 (2002) (discussing the changing field of legal ethics in the United States in the aftermath of questionable legal activities and studying ethical developments of the Model Rules, ALI's Restatement, and a couple states' ethical rules).

104. *See id.* (exploring the evolution of rules of legal ethics in the quest to effectively provide standardization and guidance to lawyers confronted with a myriad of challenges).

The continuing legal education requirements for lawyers vary from state to state, with each state bar specifying a different total number of required hours. For example, Missouri requires lawyers to acquire three credit hours from designated programs and activities related to legal ethics.[105] Three credit hours may not sound like a lot of time, but even requiring as few as three hours every year can make a vast difference in implementing an ethical culture in the legal community.[106] This difference positively benefits clients while reducing the likelihood of legal malpractice,[107] particularly when you consider the importance of understanding cyber security and the moral imperative for lawyers to understand cyber ethics. New challenges and ethical dilemmas naturally arise over time, especially with how rapidly cyber security evolves.[108] These fast-paced changes are best addressed in the annual legal education courses, which will likely reduce the likelihood of legal malpractice.[109] These are but a few of the reasons why it is imperative for state bars and the ABA to ensure every lawyer's knowledge is up to date with current standards.[110]

This Comment's first argument is to set forth suggestions to resolve the legal industry's woeful lack of an enforceable and ethical cyber security system. This argument takes a two-pronged approach that advocates for both suggestions to work in tandem to address the underlying issues pervading this critical problem. First, state bar associations and the ABA should update their rules of professional responsibility, particularly updating the current language, the subsequent comments, and taking a broader interpretation for Model Rule 1.1, Model Rule 1.3, and Model Rule 1.6. Cyber security and specific cyber security related concerns and practices must explicitly be added and addressed.

105. Nathan A. Rosen, *Legal Ethics Research for Missouri Lawyers*, 51 J. MO. B. 233, 233 (1995).

106. *See id.* (stating the presumed impact of providing and requiring lawyers to take annual legal education credits).

107. *Id.* at 236.

108. *See id.* at 233 (demonstrating why annual legal and ethical classes are necessary for modern lawyers)

109. *See id.* (requiring law students and attorneys to complete legal ethics training to reduce instances of malpractice).

110. *See* Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 485, 492 (2015) (discussing various challenges of cyber security and states' duties "inherent in human rights law and in international humanitarian law," as well as with those who have been impacted by cyber incidents).

The second suggestion for this two-pronged approach is to create legal education units that exclusively cover cyber security related subjects. These cyber security courses can be administered from state-accredited classes that lawyers must pass to remain in good standing within their jurisdiction(s) of practice. Utilizing one approach only increases the effectiveness of the other. It reinforces to all lawyers the importance of having basic cyber security literacy and acting ethically in this globalized world where no one can escape the effects of cyber security. As a result, implementing both suggestions simultaneously will properly address this national concern and implement a truly ethical cyber security culture.

B. State Bars and the American Bar Association must create and enforce ethical standards on law students and law schools

While it is imperative to enforce cyber security ethical standards on practicing lawyers, the two-pronged approach offered in the first argument is not alone enough to comprehensively implement an ethical cyber security legal culture. The two-pronged approach is essential in developing an ethical cyber security culture for practicing lawyers. However, to truly resolve this national issue and implement this ethical culture, state bars and the ABA must go back further than simply targeting currently practicing lawyers. A truly ethical cyber security culture can only be effectuated by teaching and enforcing these standards at the beginning of an aspiring lawyer's legal journey. Creating ethical lawyers and implementing an ethical legal culture requires teaching cyber security and cyber security ethics to aspiring lawyers while they are in law school.

Creating ethical lawyers by targeting law students can be accomplished in several ways. The following three proposals should be implemented altogether to truly develop an ethical cyber security culture. This objective can be accomplished by requiring law schools to teach a cyber security ethics class to maintain their accreditation with the ABA. Also, the regulatory organizations must update the Multistate Professional Responsibility Examination and the Uniform Bar Examination, which law school graduates must pass to become licensed attorneys.

1. Require a cyber security ethical class for law schools to maintain accreditation

To properly create a cyber security culture in the legal field, it is not enough to implement and enforce ethical standards on practicing lawyers.

It is also necessary to target law schools and students to build an ethical culture from the ground up. For such an essential topic that has not received proper ethical and scholarly attention for years, law schools need an incentive to implement these changes. One way to accomplish this objective is for the ABA to require law schools to provide a cyber security legal ethics course before students are eligible to graduate. It is important to note that this Comment is not advocating for the ABA to require students to take advanced cyber security classes or to recruit professors who are renowned cyber security experts. Advanced cyber security classes designed for computer science students are not necessary; in fact, this would be a gross overcorrection to the current problem the United States' legal profession has been promulgating for years. Similar to cyber security, the study of law is already a complicated subject that requires years of specialized education. The distinction hinges on the complexity of the cyber security course offered. It is essential for law schools to teach a *basic* cyber security literacy course that covers industry best practices and ethical cyber standards relevant to the legal profession.[111]

While essential and practical to prepare law students for real-world practice, it is important to note that requiring law schools to administer cyber security related classes could pose some difficulties that should be recognized for proper implementation. Unlike the law, with its long history of emphasizing precedent, cyber security evolves rapidly. Due to how quickly cyber security evolves, it has historically been considered a subject of secondary importance by lawyers. Cyber security's prevalence towards the world, legal interpretation, and lawyers' ethics makes this subject important. It is time to move this topic to the forefront of concern.[112]

This apathetic attitude is the antithesis of the culture needed to address the weight of responsibility that lawyers possess and their moral duty to act ethically. It is long past time for lawyers to truly understand how cyber threats heavily influence lawyers' actions, affect their law firm's brand and

111. *See* Raymond L. Panneton, *Cyber Security Awareness for Lawyers by Henry Dalziel and David Willson Elsevier, Inc.*, 54 HOUS. LAW., Oct. 12, 2016, at 42 (emphasizing the importance of lawyers having cyber security awareness and providing a basic cyber security education pertinent to legal services, not advocating to make lawyers technology experts) (emphasis added).

112. *See id.* (showing complications, complexities, and apathetic legal attitudes of implementing cyber security).

effectiveness, and pose great harm to their clients.[113] Amongst basic cyber security tenets, there are important concepts where cyber security and the law intersect. For example, law students must understand how liability from cyber space could be imposed on states, lawyers, and clients.[114]

In a globalized world, where cyber space affects state and individual conduct in virtually every form, it is essential for law students—the precursor for practicing lawyers—to understand how liability is imposed to properly advise their clients and determine accountability in cyber space.[115] The law of torts, for example, is no longer confined to the world of the living, where people and objects physically interact.[116] Questions of negligence, causation, accountability, intent, and harm—while more difficult to ascertain in cyber space—nonetheless apply and are highly relevant in the world of cyber space where cyber-attacks and cyber negligence result in cyber torts.[117] Issues of liability related to cyber space hacks, operations, and attacks are prevalent in this sub-field of commonly practiced law, particularly when considering malicious cyber-attacks that cross transnational boundaries.[118]

As discussed in the first argument, cyber security definitively impacts a lawyer's duty of competence and affects their duty of confidentiality to protect their clients' information. Physically locking up files or notes containing personal or otherwise sensitive client information is not sufficient anymore. Any sort of information that is collected with the assistance of technology throughout the course of a lawyer's representation or stored digitally after that representation has concluded will likely result in an unauthorized disclosure of that client's confidential information by malicious actors.[119] It is essential for law students to understand the significance of such actions and subsequent liability that would likely result before becoming licensed lawyers. Additionally, cyber security can impact a lawyer's or law firm's reputation, a fact that is important to illustrate to law

113. *See id.* (advocating for lawyers to change their attitudes and take ethical cyber action and showing the impact on law brands and client representation).

114. *See* Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 572 (2018) (advocating to impose liability on states for cyber torts to decrease harm and compensate victims).

115. *See id.* at 573 (showing how liability could be imposed on groups).

116. *See id.* (explaining how the law of torts apply to the realm of cyber space).

117. *See id.* (showing complex tort questions in relation to cyber security).

118. *Id.*

119. *See* MODEL RULES OF PROF'L. CONDUCT R. 1.6 (requiring lawyers not to reveal client information without consent).

students before they begin practicing in the real world where clients can be harmed by a lawyer's failure to apply basic cyber security principles.[120]

Requiring law schools to provide a cyber ethics class that students must take before being eligible to graduate is an appropriate measure to promote a culture of ethical accountability, and it is an effective response to help resolve this national issue.[121] For example, if the legal profession as a whole has a renowned reputation for cyber security literacy and enforcing ethical standards of practice, this reputation could better serve clients and may even deter many cyber-attacks. While there may be disagreements about whether the ABA should require law schools to provide a cyber ethics class, there is precedent of the ABA requiring law schools to provide certain classes to maintain their accreditation.[122] In today's globalized world, where cyber security pervades every aspect of life, a cyber security ethics class should be deemed essential for aspiring lawyers.[123] This suggestion is appropriate from legislative, judicial, and ethical standpoints. Targeting law students can become one facet of a multi-layered, ethical cyber deterrence approach that aligns with what the United States has been attempting to implement for years.[124]

Law students educated in cyber ethics will best serve the judicial system when state and federal trial courts confront disputed facts that have strong cyber-related components.[125] This will allow attorneys—with the assistance of their student clerks and interns—to argue issues effectively before judges and juries who determine outcomes of cases.[126] When cyber-related cases reach appellate courts, well-trained law student interns can provide

120. *See* William J. Wernz, *Confidentiality Rules in the Age of Social Media a Historical Perspective*, 75 BENCH & BAR MINN. 24, 25 (2018) (discussing how social media and online rating services have vital impacts on fundamental values of confidentiality and lawyers' reputation).

121. *See* CHRIS JAIKARAN, CONG. RSCH. SERV., R47011, CYBERSECURITY: DETERRENCE POLICY 9–10 (2022) (deterring individuals is an effective response and bringing accountability in cyber space is essential).

122. *See ABA Timeline*, *supra* note 36 (showing a timeline of the ABA, including when the ABA implemented standards for education and admission of lawyers into the practice of law).

123. *See* Loza, *supra* note 53, at 28 (demonstrating how a small town from Idaho is affected by globalized legal practice and arguing how globalization demands change for how attorneys practice and evolving standards for competence).

124. *See* JAIKARAN, *supra* note 121, at 9–10 (deterring individuals is an effective response and bringing accountability in cyber space is essential).

125. *See Hensley*, No. 3:20-CV-01539-HZ, 2022 WL 3586715, at *2 (dismissing plaintiff's fantastic claims of identity theft, cyberterrorism, and cyberstalking).

126. *Id.*

invaluable legal research and analysis to the judges. Finally, as discussed in depth above, lawyers have an emphatic ethical duty to have basic cyber security literacy in order to act ethically and to best advise their clients.[127] The sooner law school students learn and understand these vital principles—particularly if taught in a formal setting as a prerequisite to graduate—the better off they will be as practicing lawyers. The entire legal sector will then benefit by having competent legal professionals and clients will be better off with their cyber-ethical lawyers.

2. Update the Multistate Professional Responsibility Examination

A second suggestion for state bars and the ABA to effectively target law students is by updating the Multistate Professional Responsibility Examination (MPRE) to specifically address ethical concerns regarding cyber security. The MPRE is a nationally administered exam designed to test an aspiring lawyer's ethical knowledge.[128] Law students must pass this test in an overwhelming majority of states to be eligible for admittance into their respective state bars.[129] The MPRE was implemented as a result of the creation of ethical rules, evolution of bar examinations, and updates in law school accreditation standards.[130] The MPRE does not reflect an individual's ethical code, but it does reflect a national need for legal professionals to have clear, written standards of ethics.[131] However, the exam's effectiveness at testing aspiring lawyers' ethical knowledge has been questioned for years.[132]

Bar leaders in the 1960s recognized the importance of having an effective legal ethics code in a time of great social change, which, in turn, spurred the need for change in legal and ethical standards.[133] Life in the 2020s, like life in the 1960s, is a time of great change calling for an update in standards to

127. *See* Johnson, *supra* note 55, at 14 (showing the importance of lawyers to understand cyber risks to properly advise clients).

128. *See* Paul T. Hayden, *Putting Ethics to the (National Standardized) Test: Tracing the Origins of the MPRE*, 71 FORDHAM L. REV. 1299, 1299 (2003) (examining the origins of the MPRE which tests bar applicants on their understanding of ethics and its historical significance).

129. *See id.* (explaining the importance and prevalence of the MPRE in state bars across the country).

130. *Id.* at 1301–02.

131. *See* Leslie C. Levin, *The MPRE Reconsidered*, 86 KY. L.J. 395, 405–07 (1998) (showing how the MPRE theoretically reflects national ethical standards).

132. *See id.* at 402–03 (critiquing the MPRE's effectiveness and arguing to improve it by highlighting rules most needed to know for real practice).

133. *See id.* at 399–400 (showing the historical context for the development and implementation of the MPRE).

meet the demands of modern-day practice once again. The MPRE can be improved by adding subjects related to cyber security. Requiring such an addition would be an improvement since aspiring lawyers will undoubtedly encounter cyber security related legal issues. This suggestion is not one born of idealism. It is merely a recognition of the historical development of the MPRE and the need for updates in a time where the world is rapidly changing, like in the 1960s.[134] No law student or practicing attorney can escape cyber security issues, particularly considering ethical questions of conduct in relation to cyber security, that will inevitably arise throughout one's legal career.

A critical issue where ethical cyber security practice is demanded involves the private sector's impact on the United States' critical infrastructure.[135] Much of the United States' "critical infrastructure is owned and operated by the private sector."[136] These critical infrastructures include—but are not limited to—electricity, healthcare, and energy sectors, which illustrates how important it is for lawyers working in oil and gas to understand cyber security just as much as a lawyer specializing in national security law.[137] A particular note of concern is a 2020 report that evaluated cyber security in oil and gas, a subset of the energy critical infrastructure sector, which found major cyber security deficiencies throughout many enterprises.[138]

Cyber security also significantly effects the financial sector, where various financial institutions are commonly subjected to data breaches.[139] In 2019, First American Financial had a breach that compromised 885 million files with social security numbers, driver's licenses, and other information.[140] Such a compromise of personal information raises critical privacy concerns.

134. *See id.* at 409 (suggesting updates for rules most needed for aspiring lawyers to know for real practice).

135. *See* BRIAN E. HUMPHREYS, CONG. RSCH. SERV., IF12061, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE: COUNTERING RUSSIAN AND OTHER NATION-STATE CYBER THREATS 1 (2022) (showing how interconnected the private sector is with critical infrastructure).

136. *Id.*

137. *See id.* (demonstrating how federal initiatives for cyber threats often depend on the private sector because an abundance of the United States' critical infrastructure is operated by the private sector).

138. *See id.* (demonstrating critical concerns on modern-day life if cyber security vulnerabilities in critical infrastructures are exploited).

139. *See* ANDREW P. SCOTT & PAUL TIERNO, CONG. RSCH. SERV., IF11717, INTRODUCTION TO FINANCIAL SERVICES: FINANCIAL CYBERSECURITY 1 (2022) (explaining the impact of cyber security in relation to financial services).

140. *See id.* (providing an example of real-world impacts from a financial breach).

Additionally, breaches of financial institutions raise other concerns, such as people losing the livelihood they depend on to survive, the lack of financial substitutes after a breach, and the loss of confidence in the market, which could spur further economic harm.[141] As demonstrated above, the need for cyber-ethical educated lawyers is not limited to lawyers who specialize in technological fields; lawyers working for insurance companies, lawyers who specialize in financial work, and even tax lawyers clearly need to have basic cyber education and ethical cyber values.

It is important to note that adding cyber security as a subject to the MPRE, while necessary, may pose some difficulties for implementation. There are many different types of cyber incidents, such as espionage, terrorism, and other crimes.[142] The classification of these different types of cyber incidents varies based on the actor's motivation.[143] Understanding a cyber actor's motivation is important because of the way a cyber incident is conducted and knowing the reason why it is performed affects who and what will be targeted. For example, a financial institution should be warier of and prepare for cyber-crimes since criminals may have a major profit motivation for conducting cyber-crimes.[144] On the other hand, general counsel for government agencies would likely be more concerned with cyber terrorism based on politically motivated cyber actors.[145] Thus, a lawyer who is advising a financial company would likely have different legal and ethical concerns for their clients as opposed to lawyers advising other types of clients. Consequently, the drafters of the MPRE should avoid umbrella terms, such as "cyber incident," and be very clear in their questions on what is happening, who the target is, and any applicable motivations.[146] It is ultimately very important for the MPRE drafters themselves to understand the different types of cyber incidents, the cyber questions they are constructing, cyber-ethical conduct, and to be cognizant on how they phrase questions regarding these topics to ensure a correct answer.

Despite potential difficulties drafters may encounter while updating the MPRE and drafting appropriate cyber-ethical questions, it is still extremely

141. *See id.* (explaining the impact of cyber security in relation to economic harm).

142. *See* FINKLEA, *supra* note 29, at 1(defining cyber incidents and the varying types of cyber-attacks).

143. *See id.* (showing differences between various types of cyber incidents).

144. *See id.* (showing the importance of understanding the different kinds of cyber incidents and their different targets for exploitation).

145. *See id.* (explaining why certain lawyers should be concerned with cyber terrorism).

146. *See id.* (showing how cyber definitions have differing meanings and connotations).

important to add cyber ethics as a prominent subject on the exam. Cyber ethics is essential for the future of the legal industry and for building an ethical cyber security legal culture. Adding this subject to the MPRE is an important step in a positive direction towards an ethical cyber security culture where lawyers around the United States will take this subject more seriously.

3. Update the Uniform Bar Examination

The Uniform Bar Examination (UBE) is the final step in determining who is eligible to become a licensed lawyer. The UBE tests several selected topics deemed important for aspiring lawyers to know, and based on the aforementioned discussion, it can only be considered crucial that cyber security is added as a subject on the exam.[147] The UBE stands as the gatekeeper for aspiring lawyers; it is the final hurdle law school graduates must pass before becoming licensed and admitted into a jurisdiction for legal practice.[148] The UBE, like the MPRE, has received criticism for similar reasons.[149] Both examinations have been criticized for testing a narrow range of topics, as opposed to testing real-world skills lawyers must possess to become competent in actual practice.[150] The main purpose of the UBE is to "protect the public from incompetent new lawyers," but instead focuses remain on "rais[ing] the passing score on the bar exam rather than to examine and address the public's actual concerns."[151]

The UBE differs from the MPRE because the UBE exam is designed to measure an aspiring lawyer's competence.[152] It was developed as a tool to create uniform licensing like other highly regulated professional industries—such as the medical field[153]—and has been adopted in a myriad of

147. *See* Andrea A. Curcio, *A Better Bar: Why and How the Existing Bar Exam Should Change*, 81 NEB. L. REV. 363, 364 (2002) (arguing how the bar exam and law schools focus on testing certain knowledge while ignoring needed skills competent lawyers need).

148. *See id.* at 365 (explaining how important the bar is to obtain legal licensing).

149. *See id.* at 364–65 (showing how the bar has received criticism for years).

150. *See id.* (explaining some of the specific criticisms the bar has received since implementation).

151. *Id.*

152. *See* Hayden, *supra* note 55, at 1305–06 (examining the origins of the MPRE which tests bar applicants on their understanding of ethics and its historical significance).

153. Marsha Griggs, *Building a Better Bar Exam*, 7 TEX. A&M L. REV. 1, 4 (2019).

jurisdictions throughout the United States.[154] While it may be an update to antecedent bar examinations, the UBE has still received criticism for similar reasons of past bars, in addition to new concerns.[155] To become a more effective examination that tests essential real-world knowledge, the UBE needs to test basic cyber security knowledge.

There may be concerns expressed about adding additional testable subjects or broadening the UBE since it is already considered a difficult test to pass. However, if the true purpose of the UBE is to "protect the public from incompetent new lawyers,"[156] then adding cyber security as a subject on the examination will surely meet this objective. Cyber security, unlike some other subjects tested on the bar exam, will affect every area of practice aspiring lawyers will encounter. Cyber security is unique to other UBE subjects because it cannot be escaped since the cyber realm has bled into virtually every aspect of law and life.

As discussed above, it is incredibly important for lawyers to obtain cyber security knowledge and utilize cyber ethics. Both of these topics are imperative objectives that regulatory organizations, like state bars and the ABA, must implement. The constant changes in cyber security and cyber ethics naturally affect a lawyer's competence, requiring lawyers to continually update their knowledge in these subjects. The inclusion of these topics as part of a national, legal framework for ethics will serve a utilitarian purpose for testing competence, and "protect[ing] the public from incompetent new lawyers" who do not understand the pervasive impact cyber security has on the law, ethical conduct, and likelihood of success of client's cases.[157] Adding cyber security as a subject on the UBE will address some concerns and criticisms the UBE has received for years. Considering the ethical responsibility of all lawyers to understand cyber security and to act ethically in relation to cyber security, it is only common sense to add cyber security as a testable subject on the UBE as a true test of minimum competence.

154. *See* Susan Henricks, *The Uniform Bar Examination is Coming to Texas a Preliminary Look at What Will be Covered*, 82 TEX. B.J. 340, 340 (2019) (showing how the Texas Bar Examination will adopt the UBE accepted by thirty-four other United States jurisdictions).

155. *See* Griggs, supra note 152, at 4–5 (examining the UBE as a tool to test uniform codes and bringing uniform licensing like in the medical profession).

156. Curcio, supra note 147, at 366

157. *See id.* (arguing how the bar exam and law schools focus on testing certain knowledge while ignoring needed skills competent lawyers need).

IV. CONCLUSION

This Comment has demonstrated the importance of cyber security and cyber ethics in today's world. Our society has long grown dependent on technology, not just as a convenient way to communicate or to simplify complicated matters, but as a matter of survival for average Americans. Naturally, cyber security has had a vital impact on the legal sector, even if the legal community has not generally recognized it. Cyber security has been an essential, albeit ignored, fundamental factor to determine if lawyers have met their professional obligations. This Comment has shown how cyber security and cyber ethics are essential as matters of competence for representing clients, influencing precedent as officers of the court, and basic morality to step up and do the right thing in a time when one successful hack can indefinitely darken the world.

There are very serious and realistic threats in the cyber realm that pose critical issues from national and judiciary standpoints, and this Comment has offered a comprehensive framework with multiple prongs that can solve this problem. This pervasive problem is not—as many might argue—limited to lawyers who work exclusively in technology related fields. Cyber security affects all major areas of life, from personal standpoints, legal standpoints, and basic survival standpoints. Even lawyers who work in oil and gas cannot break away from this inescapable fact. As leaders in legislative and judicial branches of government, representatives of clients with ethical duties and special responsibilities, and officers of the court, lawyers must finally recognize their ethical duty to have cyber security literacy and action. This Comment has suggested an effective multi-faceted approach with multiple solutions to resolve this problem.

The first argument targets practicing lawyers. This argument heavily relies on addressing the need for updating official ethical standards imposed on practicing lawyers. Included with these proposals are modifications to the current language of ethical standards for lawyers' competence, diligence, and duties to clients. State bar associations and the ABA are regulatory organizations that are best situated to effectuate these long-needed changes and to meet this imperative objective. Cyber security's related troubling concerns and potentially devastating impact on life in the United States has existed for years, but little has woefully been done.

This national and judiciary problem has existed for years without lawyers—as officers of the court, leaders in the law, and members of a self-regulated profession—acting to meet their evolved ethical responsibilities.

It is long past time for state bars and the ABA to implement and enforce ethical standards on lawyers in relation to cyber security. These regulatory organizations can enforce ethical cyber standards for practicing lawyers by updating their respective rules of ethical conduct and by requiring acceptable cyber-ethical conduct in line with industry standards. Additionally, state bars and the ABA can include cyber ethics as a required component for annual continuing legal education courses practicing lawyers must take to remain in good standing with the jurisdiction(s) they are admitted in to practice law. This two-pronged approach is designed to be implemented simultaneously to truly implement an ethical culture with one suggestion reinforcing the effectiveness of the other.

The second argument focuses on targeting law students who are aspiring legal professionals who have yet to be licensed as practicing lawyers. It is essential for law students to understand how cyber security affects ethical courses of actions and other commonly intersecting aspects of law. Not only will this course of action best create future cyber-ethical lawyers, but it will also impact cases and appellate decisions when cyber-ethical students assist attorneys and judges as interns. State bars and the ABA can implement an ethical culture from the bottom-up by requiring law schools to administer a cyber ethics class for students to take as a prerequisite for graduation in order to maintain their accreditation with the ABA, requiring cyber ethics as a testable subject on the MPRE, and adding cyber security as a testable subject on the UBE.

The sooner aspiring lawyers learn cyber security and cyber-ethical concepts and understand their ethical duties, the better positioned practicing lawyers, courts, and clients will be in the long run. Insidious threats exist in cyber space, which should naturally affect how lawyers conduct themselves. A dire warning of devastation was in fact given over a decade ago, but that warning was shouted into the abyss, without those wielding their unique influence to act and implement a cohesive framework to best keep ahead on this issue.

This fact is particularly relevant when considering the importance of lawyers' role in society as leaders in developing and interpreting law affecting hundreds of millions of American citizens throughout the United States. This is also relevant due to how heavily clients rely on their lawyers. Lawyers have a duty to act competently, responsibly, and ethically. These duties demand nothing less than for lawyers to have cyber security literacy and cyber ethics because these skills could easily mean the difference between a client losing everything and injustice prevailing in the halls of liberty.

Yesterday was the time to act. Now is the time to take responsibility, fix the mistakes of the past, and enact crucial ethical standards to develop a truly ethical cyber security culture so lawyers can ethically represent their clients.