AMERICAN BAR ASSOCIATION

ADOPTED BY THE HOUSE OF DELEGATES

AUGUST 12-13, 2013

RESOLUTION

RESOLVED, That the American Bar Association condemns unauthorized, illegal governmental, organizational and individual intrusions into the computer systems and networks utilized by lawyers and law firms;

FURTHER RESOLVED, That the American Bar Association urges federal, state, local, territorial, and tribal governmental bodies to examine, and if necessary, amend or supplement, existing laws to promote deterrence and provide appropriate sanctions for unauthorized, illegal intrusions into the computer networks utilized by lawyers and law firms;

FURTHER RESOLVED, That the American Bar Association urges the United States government to work with other nations and organizations in both the public and private sectors to develop legal mechanisms, norms and policies to deter, prevent, and punish unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms;

FURTHER RESOLVED, That while the American Bar Association supports governmental actions, policies, practices and procedures to combat these unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms, the ABA opposes governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court and bar regulation and oversight of lawyers and the legal profession; and

FURTHER RESOLVED, That the American Bar Association urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice, and also comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.

REPORT

I. Introduction

This Report explains the American Bar Association's ("ABA") resolution regarding the growing problem of intrusions into the computer systems and networks utilized by lawyers and law firms. It notes the alarming rise of attacks on these electronic systems and networks and the recent rise of nation states as significant actors in hacking activities over the past decade. The Report also condemns these unauthorized, illegal intrusions and urges governmental bodies at all levels—federal, state, local, territorial, and tribal—to examine, and if necessary, amend or supplement existing laws to deter and punish these intrusions but only in a manner that respects and protects client confidentiality, the broader confidential lawyer-client relationship, and traditional state court regulation and oversight of lawyers and the legal profession. Further, the Report notes the different measures available to combat hacking, including diplomatic and law enforcement tools, legislation, and regulatory measures. This Report also underscores the importance of protecting confidential client information, the attorney-client privilege, and other core legal principles. Finally, the Report describes the ethical rules and professional obligations of lawyers and law firms implicated by information security breaches. This includes the lawyer's obligation to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice. It also includes the lawyer's obligation to comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity. Overall, the Resolution builds upon the several ABA Resolutions passed by the House of Delegates and Board of Governors relating to information security and client confidentiality.

Moreover, it is the expectation of the Task Force that there will be additional resolutions on cyber dealing with the issues of privacy, legal and illegal intrusions, and government responsibilities. This resolution does not address U.S. government activities authorized by law in the national security realm.

II. Background

A. Increasing Cyber Attacks on Lawyers and Law Firms

As American businesses and government agencies become increasingly reliant upon electronic communications, they grow more vulnerable to information security attacks. Such attacks are increasingly sophisticated and target critical infrastructure and national security assets as well as personal information. Criminals, terrorists, and nation states all see potential gains from attacking information systems. These threats to highly sensitive information trigger concerns from the national security community, privacy advocates, and industry leaders alike.

The Director of the National Security Agency estimates that the United States loses $250 billion each year due to cyber-espionage and other malicious attacks on information systems.[1] Confidentiality, integrity, and availability are the three cornerstone goals that every data security program is designed to achieve. Malicious attacks exploiting security vulnerabilities take a number of forms. A common attack affecting "availability" and information access is a "distributed denial of service" ("DDoS") attack, whereby servers are overwhelmed when malicious attackers flood the bandwidth or other resources of the targeted system with external communications requests. Attacks on "integrity" cause improper modification of information by inserting, deleting, or changing existing data. In an attack affecting "confidentiality," an eavesdropper can gain access to sensitive data whenever it leaves a secure area or is transmitted in an unsecure fashion (i.e., unencrypted).

New and increasingly elaborate methods are being developed for accessing confidential information. By using "phishing" or "spear phishing" attacks, intruders attempt to acquire information, such as login credentials. Masquerading as a trustworthy entity in an electronic communication, they entice users to open an e-mail attachment or click on a link to a website containing malicious software that will infect a network's computers and report sensitive information back to the intruders.[2] These programs often remain undetected for months.[3]

Attacks on confidential information held in private systems and networks can pose a direct threat to the economic and national security interests of the United States as well as the security of individuals and companies. Data collected by government agencies and by private information security experts over the past half-decade indicate a serious rise in state-sponsored hacking activities.[4] "Attribution" techniques—which allow investigators to detect where cyber attacks originate—have improved, and information security experts have linked many recent attacks on private organizations to state-sponsored actors.[5] A 2013 National Intelligence Estimate identified state-sponsored hacking as a chief threat to the country's economic competitiveness.[6] The report represents the consensus view of the United States intelligence community and describes a wide range of sectors that have been the focus of hacking over the past five years, including the financial, information technology, aerospace, and automotive sectors.[7]

---

[1] Keith Alexander, Dir., Nat'l Sec. Agency, & Commander, U.S. Cyber Command, Speech at the American Enterprise Institute: Cybersecurity and American Power (Jul. 9 2012), *available at* http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/.

[2] MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[3] *Id.*

[4] OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE (Oct. 2011).

[5] MANDIANT APT1, *supra* note 2; *See also* JAMES R. CLAPPER, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 2-3 (Mar. 12, 2013) ("State and non-state actors increasingly exploit the Internet to achieve strategic objectives.").

[6] Ellen Nakashima, *U.S. said to be target of massive cyber-espionage campaign*, WASH. POST, (Feb. 10, 2013), http://articles.washingtonpost.com/2013-02-10/world/37026024_1_cyber-espionage-national-counterintelligence-executive-trade-secrets.

[7] *Id.*

As security experts in aggressively targeted sectors have ramped up security efforts, the information security firm Mandiant reports that state-sponsored hackers have broadened their sights to include outside vendors and the business partners of high-value targets.[8] Mandiant's comprehensive report on information security in the private sector points to an increase in attacks on the computer systems and networks of firms engaging in outsourced tasks, such as information technology, human resources, financial, and legal services.[9]

Because law firms work with thousands of clients across numerous industry sectors, cyber intruders see law firms as lucrative storehouses of sensitive information.[10] Companies seek counsel when they are engaged in deeply sensitive and highly expensive matters, which tend to generate information that is potentially of great value to third parties. Financial details concerning a merger or acquisition can give any interested outside entity an advantage in future negotiations. Similarly, lawyers have access to details about an organization's inner workings in the midst of litigation. Such information enables competitors to assess the financial stability of an organization and gain other tactical information. Furthermore, a firm's litigation strategy is often outlined in various intra-firm communications. These documents provide significant advantage to opposing parties or interested third parties when computer systems or networks are successfully breached.

Law enforcement authorities in the United States, Canada, and the UK have all noted the rise in threats to law firm information systems. In November 2011, the Federal Bureau of Investigation ("FBI") convened 200 large law firms in New York City to urge them to review their cybersecurity policies. In 2012, the Director General of the British MI-5 informed the 300 largest companies in the UK that their information was as likely to be stolen from the computers of their attorneys and international consultants as from their own. The FBI does not track individual breaches or keep statistics on the types of businesses attacked, but a 2012 Mandiant report estimated that 80% of the 100 largest United States law firms were subject to successful data breaches by malicious intruders in 2011 alone.[11]

B. A Threat to Attorney-Client Confidentiality

Consistent with its commitment to client protection, the ABA is committed to defending the confidentiality of lawyer-client communications against these new threats. Protecting confidences is imperative for both ethical and practical reasons. Preservation of client confidentiality is widely recognized as fundamental to the ability of lawyers to successfully represent their clients' interests. Clients must be secure in their ability to share confidential information with their lawyers, and the preservation of the confidentiality of lawyer-client communications is crucial to public confidence in the legal system. The legal profession, the

---

[8] MANDIANT, M-TRENDS 2012: AN EVOLVING THREAT (2012), *available at* https://www.mandiant.com/resources/m-trends/.
[9] *Id.*
[10] Jessica Seah, *China Hacking Report Raises Alarms at Law Firms*, THE ASIAN LAWYER (Feb. 25, 2013), http://www.law.com/jsp/article.jsp?id=1202589420933&slreturn=20130319060101.
[11] Michael A. Riley, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG NEWS (Jan. 31, 2012), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

legal system, and foreign and domestic actors should not ignore this important facet of the attorney-client relationship.

The involvement of nation states in targeting confidential legal information is particularly troubling. Basic principles of due process and even human rights may be violated when confidential communications are breached by such intrusions. As protectors of the rule of law and the integrity of those who practice law, the ABA and the United States legal community condemn such intrusions and the organizations and nations engaged in this conduct.

III. A Strong United States and International Response

Widespread intrusions into the computer systems and networks of law firms deeply threaten clients, the legal profession and our system of justice. The United States has acknowledged that private actors and foreign governments disregard this essential aspect of legal representation when they systemically steal information, threaten access to information, or improperly modify information to the disadvantage of clients. The ABA urges the United States government and international community to speak out against these intrusions and to counter them with decisive action. In addition, the ABA urges not just the federal government, but state, local, territorial, and tribal governmental bodies as well, to examine, and if necessary, amend or supplement, any existing laws as may be necessary to deter and punish those who launch these unauthorized, illegal intrusions into the computer systems and networks of lawyers and law firms.

A. Importance of Protecting Client Confidences

Preserving the confidentiality of the attorney-client relationship is a bedrock principle of the American Bar Association. However, widespread security breaches expose client confidences and erode trust. This in turn jeopardizes the ability of lawyers to carry out their critical role in the legal system. The obligation of lawyers to maintain confidentiality, a fiduciary duty of the highest order, is expressed in the common law, the applicable rules of professional conduct, the attorney-client privilege and the work product doctrine.

1. Confidentiality, the Attorney-Client Privilege and the Work Product Doctrine

The fiduciary duty of confidentiality of an agent, particularly a lawyer, vis-à-vis the lawyer's client, has historical roots in the common law. It remains a common law duty, but today it is also codified in the rules of professional conduct of every jurisdiction in the United States, in essentially the same form as one finds it in the ABA Model Rules of Professional Conduct ("Model Rules").[12] The duty of confidentiality, which applies to any voluntary act by a lawyer, is extremely broad in its Model Rule incarnation, protecting all information relating to the representation, even if that information has been otherwise disclosed in public documents. The Model Rules provide narrow exceptions that permit, but do not require, lawyer disclosure of confidential client information. Such exceptions include but are not limited to when the lawyer

[12] *See* ABA MODEL RULES OF PROFESSIONAL CONDUCT (2013), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.

reasonably believes disclosure is necessary to prevent reasonably certain death or serious bodily harm, to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial financial injury to another and for which the client has used or is using the lawyer's services, to consult with another lawyer about the lawyer's compliance with the Rules, and to comply with other law or a court order.[13]

The attorney-client privilege is the oldest common law privilege for confidential communications, dating to 16th century England. It is a privilege whose underlying purpose is to enable persons to seek and lawyers to provide candid legal advice through unfettered communication between lawyer and client without fear that those communications will be disclosed to others. The availability of the privilege is considered indispensable to effective lawyer advocacy on behalf of clients in every representation, both before tribunals and elsewhere. In a landmark case regarding attorney-client privilege, the Supreme Court noted "full and frank communication between attorneys and their clients" also "promote[s] broader public interests in the observance of law and administration of justice."[14]

Attorney-client communications are generally only privileged if the communication was for the purpose of enabling the client to secure legal assistance and was made outside the presence of third parties. Some exceptions to the privilege include communications unrelated to the representation, non-legal advice, and advice in furtherance of an illegal activity.[15] The privilege is also lost if the client knowingly waives the privilege on informed consent.[16] However, the attorney-client privilege cannot be lost simply because a government agency or other third party claims they need to know the client's communications with a lawyer. If this exception were adopted, clients could not know whether their communications would be privileged in advance. As a result, clients would likely withhold crucial facts from their lawyers and fail to receive the advice they need to conform their conduct to the law.

The work product doctrine protects the work product of an attorney developed in anticipation of litigation.[17] Like the attorney-client privilege, the doctrine is rooted in ensuring effective legal representation by preventing the exposure of certain lawyer work product material to adversaries. However, the doctrine's main purpose is to allow the lawyer to thoroughly prepare for litigation. Thus, while not all attorney-client privileged communications are work product (because they do not occur in anticipation of litigation), work product is in a certain sense broader because it covers communications with non-clients as well as clients, if undertaken in anticipation of litigation. Another key difference is that both the attorney and client may claim ownership of the work product while the attorney-client privilege belongs solely to the client.[18]

2. Confidentiality Obligations in Cyberspace

---

[13] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2013).
[14] *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).
[15] *See Clark v. U.S.*, 289 U.S. 1, 15 (1933); *U.S. v. Bob*, 106 F.2d 37, 40 (2d Cir. 1939).
[16] *See U.S. v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358-59 (D. Mass. 1950).
[17] EDNA EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE, 391-465 (4th ed. 2001).
[18] *Id.*, at 490.

Recent technological advances create new and unique legal challenges. The American Bar Association is already providing leadership and guidance on protecting client information from cybersecurity breaches and balancing important policy goals.[19] Lawyers have a responsibility to develop and maintain systems that will effectively secure client information and firm computer networks. Lawyers must also dedicate themselves to staying competent in cybersecurity to better represent clients who are victims of cybercrimes.

The legal profession has historically provided leadership and played an essential role in preserving legal rights and, ultimately, the rule of law. The complexity and severity of cybersecurity threats only make the legal profession's involvement more necessary. In August 2005, the ABA House of Delegates unanimously approved Resolution 111, which broadly addressed attorney-client principles. The resolution reaffirmed the preservation of the attorney-client privilege and work product doctrine as central to maintaining the confidential lawyer-client relationship. The key public benefits can be summarized as follows:

1. Promoting voluntary legal compliance.
2. Encouraging client candor.
3. Ensuring effective client advocacy.
4. Ensuring access to justice.
5. Promoting efficiency in the American adversarial legal system.

The principles of the attorney-client privilege and work product doctrine must be protected in the context of cyber intrusions. However, lawyers must also develop policies that strike the right balance between client-attorney confidentiality and necessary access to protected information. The client information implicated in a law firm cyber intrusion may be relevant in attempting to determine the perpetrator who exposed the privileged information in the first place. Reconciling these competing objectives will require thoughtful debate and patience from the legal community.

B. Potential Government Actions to Reduce Cyber Intrusions

The United States government has an obligation to help protect the computer systems and networks of American companies and citizens from unlawful intrusion. In order to combat the new and significant threats of cyber attacks, the government should evaluate a full spectrum of law enforcement, military, diplomatic, intelligence, and economic measures to pressure cyber-espionage actors into stopping their attacks. This Report notes a number of tools that United States authorities may consider, including increased investigations to hold hackers accountable, high-profile diplomatic actions, economic sanctions, and use of visa authority.

1. Renewed Focus on Investigations

Government criminal and civil investigations should use law enforcement and intelligence authorities to penetrate hacker networks. Litigants and lawyers who participate in or abet cyber intrusions should also be sanctioned and prosecuted. Such conduct by lawyers should also be

---

[19] *See e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. & R. 1.6(c) (2013) (as adopted in August 2012).

subject to review by lawyer disciplinary authorities. The United States Department of Justice ("DOJ") prosecutes cyber-espionage primarily through the National Security Division and the Criminal Division's Computer Crime and Intellectual Property Section. DOJ should prioritize and devote more resources to cybercrime, including attacks on law firms.[20] For example, DOJ's National Security Division may begin indicting suspected state-sponsored hackers, in part as a deterrent strategy. Although nation states are not likely to turn over their citizens to the United States for criminal prosecution, the specific legal action makes it more difficult for a hacker's state-sponsor to deny a problem exists. The action would give the United States additional leverage in diplomatic negotiations. The indictments would also have the benefit of discouraging suspected hackers from traveling freely because foreign governments could easily turn them over to United States law enforcement.[21]

The United States could reemphasize mutual international assistance for investigatory powers under the Convention on Cybercrime.[22] In 2001, the Convention of the Council of Europe codified international best practices for legal frameworks protecting against cybercrime.[23] The United States has both signed and ratified the Convention.[24] Article 25 states "parties should afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data."[25] As a practical matter, this principle of active cooperation remains extremely relevant to the world of cyber-espionage.

Cyber intrusion investigations would also greatly benefit from domestic public-private cooperation. Since private companies are frequent victims of cybercrimes, they often possess the motivation and creativity to bolster the government's efforts. In particular, the private sector could supplement the government's relative lack of financial resources. This may include using a private investigator in place of a government investigator.[26] A compromised company can also volunteer information on the cyber intruder's nature, goals, tactics, and potential vulnerabilities.

2. Diplomatic Responses

The United States should lead a multinational coalition of countries that have been major targets of cyber attacks to discourage such attacks, including those against lawyers and law

---

[20] *See The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012), *available at* http://www.steptoecyberblog.com/2012/11/02/the-hackback-debate/.
[21] Siobhan Gorman, *U.S. eyes pushback on China hacking*, WALL ST. J. (Apr. 22, 2013), http://online.wsj.com/article/SB10001424127887324345804578424741315433114.html.
[22] COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME (Nov. 11, 2001) E.T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Apr. 22, 2013).
[23] *Id.;* David Satola & Henry L. Judy, *Towards A Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, 37 WM. MITCHELL L. REV. 1745, 1791 (2011).
[24] Satola, *supra* note 23, at 1772-73.
[25] CONVENTION ON CYBERCRIME, *supra* note 22.
[26] Testimony of Stewart Baker, *The Department of Homeland Security: An Assessment of the Department and a Roadmap for its Future*, House Homeland Security Committee 112th Congress (Sep. 20, 2012).

firms.[27] Using a collaborative approach through bilateral and multilateral diplomacy, the U.S. should encourage development of an international code of conduct to combat cyber intrusions. At his January 2013 nomination hearing, Secretary of State John Kerry mentioned the need to "engage in cyber diplomacy and cyber negotiations and try to establish rules of the road that help us to be able to cope" with the challenges of foreign hackers.[28]

When cooperation is not feasible, the United States should take a firmer diplomatic tone with nation states implicated in attacks on the computer systems and networks of American law firms. "The international community cannot tolerate such activity from any country," said National Security Advisor Thomas Donilon regarding cyber intrusions in March 2013 remarks to the Asia Society.[29] With proper attribution, the international community could bring negative publicity to state-sponsored hackers. This in turn could persuade specific countries and private companies to raise complaints with the offending nation state. Along those lines, the United States government should continue to press cyber-espionage actors at the highest levels of diplomacy. All state-sponsors of cyber attacks should recognize the urgency of the problem and acknowledge the need to prevent widespread cybercrimes. The United States can encourage these nation states to conduct their own investigations, prioritize domestic anti-hacking enforcement, and expose the individuals responsible for specific intrusions.

3. Other Government Sanctions and Tools

The United States government could also consider serious measures such as economic sanctions or asset forfeitures against those involved in cyber intrusions, or the strategic use of visa authority vis-à-vis foreign nationals. The Treasury Department's Office of Foreign Assets Control ("OFAC") administers sanctions against targeted foreign actors.[30] OFAC accomplishes key national security goals by imposing controls on transactions and freezing assets under United States jurisdiction.[31] OFAC's legal authority derives from presidential national emergency powers and specific legislation.[32] Many of the sanctions are based on United Nations resolutions and other international mandates. The Computer Fraud and Abuse Act ("CFAA") also authorizes the criminal forfeiture of any personal property or interest in personal property derived from illegal

---

[27] Dean Cheng, *Chinese Cyber Attacks: Robust Response Needed*, Heritage Foundation Issue Brief #3861 (Feb. 23, 2013), http://www.heritage.org/research/reports/2013/02/chinese-cyber-attacks-robust-response-needed.

[28] Testimony of John Kerry, *Hearing on the Nomination of John Kerry to be Secretary of State*, Senate Foreign Relations Committee 112th Congress (Jan. 24, 2013).

[29] Thomas Donilon, National Security Advisor to the President, Remarks at the Asia Society: The United States and the Asia-Pacific in 2013 (Mar. 11, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

[30] *Office of Foreign Assets Control*, TREASURY.GOV, (last accessed May 3, 2013), http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

[31] *Id.*

[32] *See* 50 U.S.C. § 1702 (a)(1)(B), (C) (2012) (granting authority to the President to declare an economic emergency and then impose sanctions).

activity.[33] Additionally, the Obama administration has proposed amending the CFAA to include a civil forfeiture provision.[34]

Visas too could be used either as a carrot or a stick. At the Attorney General's discretion, DOJ can issue S-5 criminal informant visas to foreign nationals possessing "critical reliable information concerning a criminal organization."[35] Meanwhile, the Department of Homeland Security has the authority to adopt a policy of denying or canceling visas to individuals involved in cyber-espionage, including researchers.[36]

C. Protecting Client Confidentiality During Investigations

Confidential client information should be protected during any cyber intrusion investigation, consistent with ethics rules and to prevent the erosion of the attorney-client privilege and work product doctrine. Assisting such government investigations is important, but law enforcement should seek ways to conduct investigations without breaching confidentiality. If private investigators are going through compromised computer systems and networks instead of government investigators, they too must take steps to avoid disclosing the client's information. Guidelines should also ensure client confidences are not used in unrelated investigations, unless the privilege or work product protection is waived by the client's consent. Privileged and confidential client information from law firm systems and networks should not be permitted to be used in prosecutions or civil enforcement cases against the client and third parties. This protection should also extend to government agency inquiries related to intelligence or national security.

Government efforts to combat cyber attacks should comport with ABA's long-standing commitment to the principle of attorney-client confidentiality. Both parties suffer when the foundation of the attorney-client relationship is threatened. The exposure of information to government agencies or private parties creates a chilling effect on client-attorney communication and reduces client candor. Such exposure also discourages voluntary legal compliance and information-sharing in cybercrime investigations. This is especially problematic as companies conducting internal investigations increasingly rely on law firms' attorney-client privilege.[37]

IV. Ethical and Professional Obligations for Computer Security

The wealth of confidential data maintained in lawyers' computers and information systems faces substantial and very real security risks.[38] It is critical for all lawyers to understand and

---

[33] *See* 18 U.S.C. § 1030 (i)(A),(B) (2012).
[34] Testimony of Richard Downing, *Cyber Security: Protecting America's New Frontier*, House Judiciary Subcommittee on Crime, Terrorism and Homeland Security 112th Congress (Nov. 15, 2011).
[35] KARMA ESTER, CONG. RESEARCH SERV., RS21043, IMMIGRATION: S VISAS FOR CRIMINAL AND TERRORIST INFORMANTS (2005), *available at* http://www.fas.org/sgp/crs/terror/RS21043.pdf.
[36] *See e.g.*, 8 U.S.C. § 1184(b); Geoff Dyer, *US seeks cyber espionage crackdown*, FINANCIAL TIMES (Mar. 28, 2013), http://www.ft.com/cms/s/0/f2adc696-97cc-11e2-97e0-00144feabdc0.html#axzz2QrxFlXSV.
[37] Christopher Matthews, *Law firms tout cybersecurity cred,* WALL ST. J. (Mar. 31, 2013), http://online.wsj.com/article/SB10001424127887324883604578394593108673994.html.
[38] RANDY J. CURATO, CYBER LAWYERING DATA MANAGEMENT AND SECURITY: A LAW FIRM MANAGEMENT GUIDE 14 (Dec. 2012).

address these risks to ensure they comply with their legal, ethical, and regulatory obligations to safeguard client data.[39] The ABA Model Rules of Professional Conduct provide guidance to lawyers regarding their ethical obligations about preventing the unauthorized disclosure of and unauthorized access to confidential client information and responding to a breach should it occur. This Resolution, in the final Further Resolved clause, reminds lawyers and law firms of the importance of reviewing and complying with applicable ethics rules and also other law that governs their conduct in the cybersecurity context.

A. Protection of Information Systems

There are two main duties implicated in the protection of confidential client information from inadvertent disclosure or unauthorized access: (1) the duty of competence under Model Rule 1.1, and (2) the duty of confidentiality under Model Rule 1.6.

1. Duty of Competence: Model Rule 1.1[40]

Model Rule 1.1 provides that a lawyer shall provide "competent representation" to a client. This requires "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[41] In August 2012, the House of Delegates adopted amendments to the Comments to Model Rule 1.1 at the recommendation of the ABA Commission on Ethics 20/20 to highlight the importance of technology to legal practice. Comment [8] to Model Rule 1.1 now states that a lawyer "should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."[42] The amendment does not impose new obligations on lawyers.[43] Rather, it is intended to highlight the growing significance of technology to legal practice and emphasize a lawyer's responsibility to stay informed.[44]

The duty is not necessarily for lawyers to become technological experts, but to ensure that they understand the impact of technology on the activities of a client or law firm. Technical proficiency implicates not only adequate protection of confidential information, but providing adequate advice to clients on technological matters including protection of the client's own data.

The Report of ABA Ethics 20/20 Commission explaining the amendment noted that a lawyer should understand the basic features of relevant technology, such as how to create an electronic document and how to use email, in order to ensure clients receive competent and

---

[39] Jon M. Garon, *Technology Requires Reboot of Professionalism and Ethics for Practitioners*, 16 J. INTERNET L. 3 (2012).
[40] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2013).
[41] Garon, *supra* note 39.
[42] CURATO, *supra* note 38.
[43] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. [8] (2013).
[44] Garon, *supra* note 39; Matt Nelson, *New changes to Model Rules a wake-up call for technologically challenged lawyers*, INSIDE COUNSEL (Mar. 13, 2013), http://www.insidecounsel.com/2013/03/28/new-changes-to-model-rules-a-wake-up-call-for-tech.

efficient legal services.[45] Some suggest that the level of knowledge a lawyer should obtain will depend on factors such as the types and sensitivity of data collected by the lawyer or law office in each particular area of practice.

Attorneys have an obligation to safeguard information relating to clients. This may include approaching information security as a process, understanding the limitations in attorneys' competence, obtaining appropriate assistance, continuing security training and awareness, and reviewing technology, threats, and available security options as they evolve over time.[46] Flexibility is required to allow obligations to grow and develop alongside technological advancement.

Many law firms and lawyers already rely on IT to assist them in relevant technology and training. Lawyers who do not do so already may want to consult with technological experts to ensure that they are adequately keeping pace with rapidly changing technology and related security threats.[47] Additionally, law firms might benefit by increasing the number of nonlawyers devoted to safeguarding information and training attorneys in how to prevent accidental disclosure or unauthorized access.

2. Duty of Confidentiality: Model Rule 1.6[48]

A lawyer has an ethical duty to take reasonable measures to protect a client's confidential information from unauthorized access and disclosure. Under Model Rule 1.6, lawyers must take "reasonable precautions" to safeguard "information relating to the representation of a client."

The ABA amended Model Rule 1.6 in August 2012 to require that this duty extend to client information in computers and information systems. New paragraph (c), states, "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[49] However, an inadvertent disclosure or breach alone does not constitute a violation of the rule if reasonable precautions have been taken. Notably, the new black letter Rule and Comment did not change any ethical obligations. It simply made the prevailing understanding of the obligations explicit and clear in light of new technology.

Defining the "reasonable precautions" lawyers must take to protect data poses a challenge. The specific administrative, technical, or physical safeguards required for a client's information will vary from situation to situation. Additionally, what is "reasonable" will change as technology

---

[45] ABA Commission on Ethics 20/20 Introduction and Overview (May 7, 2012), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf.

[46] David G. Ries, *Cybersecurity for Attorneys: Understanding the Ethical Obligations*, LAW PRACTICE TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html.

[47] *Id.*

[48] MODEL RULES OF PROF'L CONDUCT R. 1.6 (2013).

[49] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2013).

changes. Comment [18] provides guidance as to what is "reasonable" by identifying some of the factors that would dictate heightened security and require greater precaution.[50] These standards include the:

1. Sensitivity of the information
2. Likelihood of disclosure if additional safeguards are not used
3. Cost of using additional safeguards
4. Difficulty of using the safeguards
5. Extent to which the safeguards adversely affect the ability to represent the client (e.g., by making a device or important piece of software excessively difficult to use).[51]

Lawyers may develop greater clarity and specificity with individual clients through contractual agreements and waivers. Indeed, Comment [18] states that a client may require the lawyer to use special security measures beyond the requirements of Rule 1.6, or may waive certain security measures that would otherwise be required by the Rule.[52] Comment [19] includes a similar provision. These provisions should be utilized to avoid uncertainty. Significantly, many state bar ethics opinions have indicated that lawyers and law firms should obtain informed consent from the client prior to utilizing any cloud computing or third-party online hosts of confidential client information.[53] Accordingly, these types of agreements may already be relatively common practice for many lawyers and law firms.

Confidentiality also implicates Model Rule 5.3, which provides that lawyers with managerial authority in a law firm must take steps to ensure that all firm employees, including nonlawyers, handle data and use technology in a manner that reasonably safeguards client information. Further, Comment [3] to Rule 5.3 extends the obligation beyond firm staff to vendors and other nonlawyers outside the firm.[54] Many incidences of hacking occur through offsite vendors or the personal computers of employees. In response, lawyers and law firms could develop internal policies and training as part of the "reasonable" precautions utilized to safeguard confidential information and prevent liability.

---

[50] CURATO, *supra* note 38, at 14.
[51] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2013).
[52] CURATO, *supra* note 38, at 15.
[53] *See e.g.*, Massachusetts Bar Ass'n., Ethics Op. 12-03 (2012), *available at* http://www.massbar.org/publications/ethics-opinions/2010-2019/2012/opinion-12-03; Pennsylvania Bar Ass'n., Formal Op. 2011-200 (2011), *available at* http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf; New Hampshire Bar Ass'n., Advisory Op. 2012-13/4 (2012), *available at* http://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp; New York State Bar Ass'n Comm. on Prof'l Ethics, Advisory Op. 842 (2010), *available at* http://www.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&template=/CM/ContentDisplay.cfm&ContentID=140010; Vermont Bar Ass'n., Advisory Op. 2010-6 (2010). *See also* JOHN M. BARKETT, ETHICAL CHALLENGES ON THE HORIZON: CONFIDENTIALITY, COMPETENCE AND CLOUD COMPUTING (2011), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac2013/sac_2013/36_the_ethical.authcheckdam.pdf.
[54] CURATO, *supra* note 38, at 14.

Lawyers should keep informed of state and federal laws governing information security. Comment [18] to Model Rule 1.6 notes that whether a lawyer is required to take additional steps to comply with other laws that govern data privacy is beyond the scope of the Rule. However, there is a burgeoning body of privacy and breach notification laws that apply to lawyers, as well as those who store or transmit electronic information. Lawyers should familiarize themselves and comply with these laws.

B. Legal and Ethical Duties Triggered by a Security Breach

With respect to client communications, when there is a breach of confidentiality, a lawyer may have a duty to disclose that breach under the Model Rules. The ethical obligations of lawyers to disclose breaches to a client are set forth in Model Rule 1.4. Model Rule 1.4 generally discusses a lawyer's duty to communicate with his or her client. Rule 1.4(a) requires keeping the client "reasonably informed about the status of the matter."[55] Rule 1.4(b) states that a "lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[56] Though not explicitly stated, these provisions indicate that in certain circumstances lawyers might have an ethical obligation to provide notice to a client when confidential information relating to the client is compromised.

The general standard for Rule 1.4 is that a lawyer must keep clients informed about material developments. Therefore, lawyers must tell clients that a breach occurred when it is material to their case. However, the scope of the duty to inform remains under review. For example, in 2009, the Illinois State Bar Association took the position that a lawyer may be obligated to disclose a breach to its client "if it is likely to affect the position of the client or the outcome of the client's case."[57] However, other state bars have either specifically declined to issue direct opinions or have issued opinions that have no clear standard.[58]

Some of the ambiguity associated with determining when a material breach has occurred can be mitigated by provisions in Rule 1.4 that require obtaining "informed consent."[59] As part of good practice, a lawyer may want to inform clients of the technology and security practices they utilize so that clients can make informed decisions. Lawyers may also want to provide specialized instructions to clients regarding how a breach or possible breach of confidential information will be handled.[60] By obtaining informed consent in advance, lawyers and law firms can craft specific terms regarding what constitutes a material breach and when clients will be informed of a breach. Notably, certain legal and regulatory requirements may be stricter than the ethical rules. Thus, it is important that lawyers ensure that consent agreements are in accordance with state and federal laws.

---

[55] MODEL RULES OF PROF'L CONDUCT R. 1.4 (2013); Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning-Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 228-30 (2011).
[56] *Id.*
[57] BARKETT, *supra* note 53.
[58] *Id.,* at 14.

[59] MODEL RULES OF PROF'L CONDUCT R. 1.4 (2013).
[60] Trope & Hughes, *supra* note 55, at 229 (2011).

Beyond their ethical duties, lawyers may be subject to legal or regulatory requirements for breach notification.[61] Forty six (46) states as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws that require any business in possession of certain sensitive personal information about a covered individual to disclose a breach of that information to the person(s) affected. The first federal data breach notification law covers health care.[62] Furthermore, a breach may affect entities and individuals who are not clients. This means that lawyers' legal obligations may not be limited to information relating to their clients.

V. Conclusion

Information security represents an increasingly important issue for the legal profession. Sophisticated hacking activities on private computer systems and networks, including on those utilized by lawyers and law firms, have increased dramatically over the last decade. These information security breaches expose clients, their lawyers, and society at large to significant economic losses. Further, these breaches undermine the legal profession as a whole by threatening client confidentiality, the attorney-client privilege, and the broader confidential lawyer-client relationship. As the national representative of the legal profession, the ABA should play a leading role in urging the United States and other governmental bodies to discourage, prevent, and punish malicious intrusions into lawyer and law firm computer systems and networks, but only in a fashion that protects these core legal principles and traditional state court regulation and oversight of lawyers and the legal profession. The ethical rules have long imposed certain professional obligations on lawyers and law firms to protect confidential information from breaches, but as technology advances, the legal profession must adapt to meet the demands of clients and ensure that cornerstones of the profession, such as confidentiality, remain intact.

Respectfully submitted,

Judith Miller and Harvey Rishikof
Co-Chairs, Cybersecurity Legal Task Force
August 2013

---

[61] LUCY THOMSON, DATA BREACH AND ENCRYPTION HANDBOOK (ABA 2011).
[62] National Conference of State Legislatures, State Security Breach Notification Laws, *available at* http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx; 42 U.S.C. § 17931, 78 FR 5642 (Jan. 25, 2013).

GENERAL INFORMATION FORM

Submitting Entity: Cybersecurity Legal Task Force

Submitted By: Judith Miller and Harvey Rishikof, Co-Chairs

1. Summary of Resolution(s).

   This Resolution condemns unauthorized, illegal intrusions by governments, organizations, and individuals into the computer systems and networks utilized by lawyers and law firms; urges federal, state, and other governmental bodies to examine and, if necessary, amend existing laws to fight such intrusions; urges the United States government to work with other nations and organizations in both the public and private sectors to deter, prevent, and punish such intrusions; supports governmental measures to combat such intrusions while opposing governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court regulation of lawyers; urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice; and urges lawyers and law firms to comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.

2. Approval by Submitting Entity.

   May 7, 2013

3. Has this or a similar resolution been submitted to the House or Board previously?

   No.

4. What existing Association policies are relevant to this Resolution and how would they be affected by its adoption?

   The proposed Resolution is consistent with and builds upon the cybersecurity principles previously developed by the Task Force and adopted by the Board of Governors in November 2012, especially Principle 3 ("Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.") and Principle 4 ("Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.") (*see* Board of Governors resolution adopted in November 2012). The proposed Resolution is also consistent with ABA Model Rule of Professional Conduct 1.6 ("Confidentiality of Information"), which prohibits lawyers from revealing confidential client information unless the client gives informed consent or one or more narrow

exceptions apply. In addition, the Resolution is generally consistent with and would build upon other existing ABA policies (1) supporting the attorney-client privilege and the work product doctrine and opposing governmental policies, practices, or procedures that would erode those protections (*see* Resolution 111, adopted August 2005), and (2) opposing new federal agency regulations on lawyers engaged in the practice of law where the effect would be to undermine the confidential lawyer-client relationship, the attorney-client privilege, or traditional state court regulation of lawyers (*see* Board of Governors resolution adopted in October 2009).

5. If this is a late report, what urgency exists which requires action at this meeting of the House?

   Not applicable.

6. Status of Legislation. (If applicable)

   Not applicable.

7. Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates.

   In consultation with the ABA Governmental Affairs Office, Task Force leaders would prepare letters to Congress and/or comment letters to relevant federal agencies, and may meet with congressional and agency staff to urge adoption of legislations or regulations consistent with the Resolution. Task Force leaders may also reach out to law firms, bar associations, other legal groups, and the courts in order to educate them about the growing problem of unauthorized, illegal intrusions into the computer systems and networks utilized by lawyers and law firms and to help them devise practical ways to protect confidential client information from such intrusions.

8. Cost to the Association. (Both direct and indirect costs)

   None.

9. Disclosure of Interest. (If applicable)

   Not applicable.

10. Referrals.

    The proposed Resolution and Report has been sent to the Chairs and staff liaisons of each ABA Section, Division, Task Force, Standing Committee and Commission represented in the ABA Cybersecurity Legal Task Force. They are: Section of Administrative Law, Business Law, Center for Professional Responsibility, Criminal Justice Section, Section of Individual Rights and Responsibilities, International Law, Law Practice Management Section, Litigation, Science and Technology Law,

Special Committee on Disaster Response and Preparedness, Standing Committee on Law and National Security, Standing Committee on Technology and Information Systems, State and Local Government Law, Tort, Trial and Insurance Practice and Public Utility, Communications and Transportation Law.

11. Contact Name and Address Information. (Prior to the meeting. Please include name, address, telephone number and e-mail address)

Stewart Baker
Partner, Steptoe & Johnson
1330 Connecticut Avenue, NW
Washington, DC 20036
(202) 429-6402
sbaker@steptoe.com

Judith Miller
Co-Chair, ABA Cybersecurity Legal Task Force
1050 Connecticut Avenue, N.W., Suite 400
Washington, D.C. 20036
(202) 341-8127 (cell)
Judith.miller3@gmail.com

Harvey Rishikof
Co-Chair, ABA Cybersecurity Legal Task Force
1050 Connecticut Avenue, N.W., Suite 400
Washington, D.C. 20036
(202) 288-2013 (cell)
rishikofh@me.com

Holly McMahon
Staff Director
ABA Cybersecurity Legal Task Force
1050 Connecticut Avenue, N.W., Suite 400
Washington, D.C. 20036
(202) 662-1035
Holly.mcmahon@americanbar.org

12. Contact Name and Address Information. (Who will present the report to the House? Please include name, address, telephone number, cell phone number and e-mail address.)

Judith Miller
Co-Chair, ABA Cybersecurity Legal Task Force
1050 Connecticut Avenue, N.W., Suite 400
Washington, D.C. 20036
(202) 341-8127 (cell)
Judith.miller3@gmail.com

118

Harvey Rishikof
Co-Chair, ABA Cybersecurity Legal Task Force
1050 Connecticut Avenue, N.W., Suite 400
Washington, D.C. 20036
(202) 288-2013
rishikofh@me.com

EXECUTIVE SUMMARY

1. Summary of the Resolution

This Resolution condemns unauthorized, illegal intrusions by governments, organizations, and individuals into the computer systems and networks utilized by lawyers and law firms; urges federal, state, and other governmental bodies to examine and, if necessary, amend existing laws to fight such intrusions; urges the United States government to work with other nations and organizations in both the public and private sectors to deter, prevent, and punish such intrusions; supports governmental measures to combat such intrusions while opposing governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, the confidential lawyer-client relationship, or traditional state court regulation of lawyers; urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information and keeping clients reasonably informed that are set forth in the Model Rules of Professional Conduct, as amended in August 2012 and as adopted in the jurisdictions applicable to their practice; and urges lawyers and law firms to comply with other applicable state and federal laws and court rules relating to data privacy and cybersecurity.

2. Summary of the Issue that the Resolution Addresses

As American businesses and government agencies become increasingly reliant upon network communications, they grow more vulnerable to information security attacks. These attacks increasingly target both citizen information and national security assets. Criminals, terrorists, and nation states all see potential gains from attacking information systems. These threats to highly sensitive information trigger concerns from the national security community, privacy advocates, and industry leaders alike, and seriously threaten client confidentiality.

3. Please Explain How the Proposed Policy Position will Address the Issue

By adopting the proposed Resolution, the ABA will be able to play a leading role in urging the United States government and other governmental bodies to examine, and if necessary, amend or supplement existing laws in order to discourage, prevent, and punish malicious intrusions into lawyer and law firm computer systems and networks, but only in a fashion that protects client confidentiality, the attorney-client privilege, the larger confidential lawyer-client relationship, and traditional state court regulation and oversight of lawyers and the legal profession.

4. Summary of Minority Views

The Cybersecurity Legal Task Force is unaware of any minority views.