RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.
REPORT

I. INTRODUCTION

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States (U.S.). It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

II. CYBERSECURITY THREATS -- BACKGROUND

The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. Cyber-criminals exploit weaknesses in software and operating platforms, the domain name system, and mobile and web-based applications. They conduct successful social engineering through phishing attacks, social media, email, and various applications. Malware can quickly morph, change security controls, lurk in systems undetected, download other malware, and exfiltrate data undetected.

An organization-wide cybersecurity program with defined controls based on risk categorizations reflecting the operational impact and magnitude of harm of a cyber incident can mitigate risk to a considerable degree. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper security planning and implemented appropriate security safeguards.

In today’s digital world, threats to data and information systems are found almost everywhere a computer, server, smart phone, thumb drive, or other electronic device is operating (including the cloud). Many organizations provide access to their networks to business partners and entrust their data and business functions to outsourcing and cloud providers, creating additional risks. The proliferation of mobile devices and wireless technologies that enable mobile commerce and a continually expanding array of applications—more than 1.5 million—also present vulnerable points in the flow of sensitive data in computer networks.

Security is only as strong as its weakest link. Failed security has resulted in thousands of data breaches that have led to the loss or compromise of millions of personally identifiable records, as well as the theft of classified information, valuable intellectual property and trade secrets, and the
compromise of critical infrastructure. The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual.

The protection of one of the most valuable and vulnerable assets of all organizations—its information—is not only vitally important, but it also avoids the high costs associated with cybercrime, including forensic investigations and data breach notification; the loss of confidential, classified, and proprietary data; reputational damage; loss of public confidence; and in the case of business, drops in stock price, and loss of market share and trust. Breaches also have resulted in the disclosure of closely-held government information, and businesses have faced regulatory fines and investigations, civil damage actions, administrative proceedings, and criminal indictments. The first- and third-party losses associated with security incidents are rising, and cybersecurity is now one of the top risks organizations must manage.

**Sensitive Data At Risk**

There are many types of sensitive data that are targeted by cyber-criminals or subject to unauthorized access, use, disclosure, or sabotage by insiders. They include personally identifiable information (PII), personal health information (PHI), and financial records, confidential and proprietary business data, intellectual property and trade secrets, research data, privileged legal documents, and classified information (including sensitive national security information). There is a vibrant market for these data, and all organizations—regardless of size—should consider themselves at risk.

The sensitive personal data being amassed by companies and governments is staggering. Inexpensive storage has enabled companies to collect and store large amounts of data and retain it far longer than they would have if it were in paper. “Big data,” the term applied to the collection of massive amounts of data that can be correlated, analyzed, and parsed for targeted advertising and strategic business purposes, creates rich targets for cyber-criminals. PII that can be used for fraud is being collected and often stored by organizations unprotected, putting many Americans at risk. On its website, the Internal Revenue Service (IRS) indicates that it “has seen a significant increase in refund fraud that involves identity thieves who file false claims for refunds by stealing and using someone's Social Security number.”

Another aspect of the problem is illustrated by the dependence of American society on electronic transactions and e-commerce, which has fueled data breaches in all industry sectors. Failed security has resulted in massive data breaches of millions of personally identifiable records. The recent data breaches of leading retail companies and credit bureaus have caught the attention of the public, politicians, and law enforcement. The success of these breaches, however, has also

---

created a “me too” among cyber-criminals eager to capture their own trove of data. Risks will increase with the “Internet of Things,” as the Internet becomes the backbone for appliances, gadgets, and operational aspects of daily life. Many of the most personal aspects of people’s lives will be documented and transmitted over the Internet, subject to interception or theft.

Protecting the Nation’s Critical Infrastructure

The national and economic security of the United States depends on the reliable functioning of critical infrastructure: cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation’s security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company’s bottom line. It can drive up costs and impact revenue. It can harm an organization’s ability to innovate and to gain and maintain customers.5


Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, issued in February 2013, advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. Comprehensive cybersecurity programs are essential for critical infrastructure organizations, and following appropriate security frameworks and standards is central to achieving a strong cybersecurity posture and resilience. The electric sector, for example, voluntarily agreed to comply with cybersecurity requirements promulgated by the North American Electric Reliability Corporation and the Federal Energy Regulatory Commission (NERC/FERC).

The National Institute of Standards and Technology (NIST) recently published the Framework for Improving Critical Infrastructure Cybersecurity, and mapped the Framework to other accepted security frameworks and standards.

Law Firms Are Targets of Cyber Attacks

The threat of cyber attacks against law firms is growing. Lawyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices. There are many reasons for hackers to target the information being held by law firms. They collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery.

The data and information kept by law firms are largely protected by the attorney-client privilege and/or the work product doctrine, as well as by various legal ethics requirements. Thus, lawyers and law firms should implement an appropriate cybersecurity program to protect confidential and sensitive information.

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. The FBI has issued warnings to firms and held a meeting in early 2012 with approximately 200 law firms in New York City to discuss the risk of breaches and theft of client data. A cybersecurity firm that helps organizations secure their networks against threats and resolve computer security incidents estimated that 80 major law firms were breached in 2011 alone.

The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals (2013) provides threat information, practical guidance and strategies to lawyers and law firms of all sizes, and explores the relationship and legal obligations between lawyers and clients when a cyber-attack occurs. Amendments to the ABA Model Rules of Professional Conduct (Model Rules) adopted in 2012 provide that a lawyer’s duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology (Comment [8] to Model Rule 1.1). Further, to enhance the protection of client confidential information, Model Rule 1.6 (Confidentiality) provides that 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.” The touchstone regarding lawyers’ obligations under Model Rules 1.1 and 1.6 is reasonableness. What is reasonable depends on the circumstances. With regard to data security, the Comments to Model Rule 1.6 provide lawyers with a nonexclusive list of factors designed to help them assess the reasonableness of their actions.

III. CYBERSECURITY PROGRAM—FRAMEWORKS AND STANDARDS

There are a number of accepted frameworks and standards that can serve as a reference for developing, implementing, and maintaining an appropriately-tailored cybersecurity program. Some of these well-known frameworks and standards include:

- Information Technology Infrastructure Library (ITIL), http://itil-officialsite.com

• International Society of Automation (ISA), http://www.isa.org
• ISACA, COBIT, http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
• National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS), http://csrc.nist.gov
• Carnegie Mellon University Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), http://cert.org/octave
• U.S. Nuclear Regulatory Commission, nrc-stp.ornl.gov/slo/regguide571.pdf
• The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

These references are generally consistent, and a number of the provisions in the various security frameworks and standards map to one another. Thus, it is less important which framework or standard an organization might choose to follow and more important that it undertakes the key activities of a cybersecurity program.

A cybersecurity program is comprised of a series of activities. These activities include, for example: governance by boards of directors and/or senior management; development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training.

Due to the nature of the threat environment, certain activities in a cybersecurity program are ongoing. Continuous monitoring and log analysis are designed to provide data that can provide early detection of threats. To maintain a proactive security posture, potential threats should be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address cybersecurity threats and risks in a timely, disciplined, and structured fashion.

Privacy compliance requirements should be incorporated into the cybersecurity program. In addition, an effective cybersecurity program requires trained personnel to evaluate the security impact of actual and proposed changes to the system, assess security controls, correlate and analyze security-related information, and provide actionable communication of the security status across all levels of the organization.

Administrative, technical, organizational and physical controls help ensure the confidentiality, availability, and integrity of digital assets. Such controls should be carefully determined,
implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems, which can also be useful for private sector organizations.10

Many organizations are undertaking some of the required cybersecurity activities, but not others, and some activities may be performed without all the critical inputs. In such cases, the resulting cybersecurity program could have gaps and deficiencies and associated risks that may adversely affect the organization’s operations, financial bottom line, and compliance. To help protect against massive data breaches or loss of confidential/proprietary data, organizations—whether private or public—should continually work to assess and improve their security posture, in light of the most recent guidance and recommendations on cybersecurity programs.

Small Organizations

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical. Small organizations, including small law firms and solo practitioners, can prioritize key cybersecurity activities and tailor them to address the specific risks that have been identified. For example, NIST has provided guidance on information security for small businesses.11 Similarly, the U.S. Department of Health and Human Services (HHS) has accorded flexibility in its HIPAA Security Series guidance for the needs of small covered entities.12

IV. RISK-BASED ASSESSMENT—AN ACCEPTED BUSINESS PROCESS

Organizational risk can include many types of risk (e.g., management, investment, financial, legal liability, safety, logistics, supply chain, and security risk). Security risks related to the operation and use of information systems is just one of many types of organizational risk. This Resolution focuses on one aspect of a comprehensive enterprise risk management program—operational and IT/cybersecurity risk.

Risk assessments inform decision-makers and support the risk management process by identifying: (i) relevant threats to the organization or threats directed through third party entities; (ii) vulnerabilities both internal and external to the organization; (iii) the impact (i.e., harm) to the organization and individuals that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a categorization of risk according to the degree of risk and magnitude of harm to the organization flowing from the threat or vulnerability if it occurred.

Cybersecurity is based on a systematic assessment of risks that are present in a particular operating environment. Ensuring the confidentiality, integrity, and availability of digital assets is fundamental to their protection. Risk assessments are undertaken to identify gaps and deficiencies in a cybersecurity program due to operational changes, new compliance requirements, an altered threat environment, or changes in the system architecture and technologies deployed.

Risk assessments are the basis for the selection of appropriate security controls and the development of remediation plans so that risks and vulnerabilities are reduced to a reasonable and appropriate level. The principal goal of the organization’s risk management process should be to protect the organization and its ability to perform its mission, not just to protect its IT assets.

Risk assessment is not new to most businesses. It is a fundamental business process that many have been following since at least 1977 when Congress enacted the requirement in the Foreign Corrupt Practices Act of 1977 (FCPA), 15 U.S.C. §§ 78dd-1, et seq., that public companies have internal controls. Nearly all rely on the COSO Framework to comply with the internal control reporting requirements under the FCPA and the Sarbanes-Oxley Act of 2002, PL 107-204, 116 Stat 745. The framework, issued in 1992 and updated in 2013, is designed to assist companies in structuring and evaluating controls that address a broad range of risks. It is geared to the achievement of three important objectives—operations (operational and financial reporting goals, and safeguarding assets from loss, the objective of an effective cybersecurity program), reporting (financial and non-financial), and compliance (with laws and regulations).

Risk assessments for publicly-traded companies are addressed in the Securities and Exchange Commission (SEC) guidance on Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents.

Examples of cybersecurity risk management frameworks and standards include:

- **ISO/IEC 27005:2011: Information Security Risk Management.** It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the implementation of information security based on a risk management approach.

- **ISO/IEC 31000:2009: Risk Management–Principles and Guidelines.** This document is intended to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. It can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

- **Managing Information Security Risk, Organization, Mission, and Information System View,**

---

NIST Spec Pub 800-39 (March 2011)\textsuperscript{17} and \textit{Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach}, NIST Spec Pub 800-37 Rev. 1 (February 2010).\textsuperscript{18} These publications provide guidance for developing an integrated, organization-wide process for managing risk that includes the activities of security categorization; security control selection, implementation, and assessment; information system authorization; and security control monitoring.

- \textbf{Critical Sectors—DHS Infrastructure Risk Management Approach.}\textsuperscript{19} This guidance provides a useful approach to critical infrastructure risk management utilizing a risk management framework enunciated by DHS. It is designed to be applied to all threats and hazards, including cyber incidents, natural disasters, man-made safety hazards, and acts of terrorism, although different information and methodologies may be used to understand each. Risk information allows partners, from facility owners and operators to federal agencies, to prioritize their risk management efforts.

- \textbf{DOE Electricity Subsector Cybersecurity Risk Management Process (RPM).}\textsuperscript{20} The electricity subsector increasingly relies on digital technology to reduce costs, increase efficiency, and maintain reliability during the generation, transmission, and distribution of electric power. Managing cybersecurity risk is critical to achieving their strategic goals and objectives, including reliability, resiliency, security, and safety. Issued by the Department of Energy in conjunction with NIST and NERC, this guidance is designed to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks.

\section{V. CYBERSECURITY PROGRAM—CYBER RESPONSE PLANS}

Incident response is the practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future reference. Fully developed and tested incident response plans and business continuity/disaster recovery (BC/DR) plans are components of a cybersecurity program. Organizations should be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Response plans, policies, and procedures should be able to accommodate the full array of threats, not just data breaches.

Incident response plans involve stakeholders across an organization, including IT, security, legal, finance, operational units, human resources, and procurement. The individuals should be identified and their roles and responsibilities defined. Communication with and coordination among stakeholders is an important aspect of an incident response plan. This includes the identification of who within an organization should be responsible for communicating with

employees, customers, and other key groups (e.g., investors). It would also include plans for
appropriate external communications, such as with first responders, forensic investigation
experts, Computer Emergency Response Teams (CERTs), Information Sharing and Analysis
Centers (ISACs), regulators, communications providers, and outside counsel.

If litigation is anticipated, adequate documentation and evidentiary procedures for incident
response can be very important. This advance planning can help to ensure that valuable
tracking and tracing data and evidence of what happened within a system are preserved and
secured and chain of custody is documented.

For many organizations, adequate incident response planning is a compliance requirement. For
example, those organizations subject to the Federal Information Security Management Act
(FISMA), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-
Bliley Act (GLBA), or state data breach laws.

Resources are available to assist organizations in understanding the key components of incident
response. NIST, for example, has published an excellent guide, the Computer Security Incident
Incident Response Teams.

Business Continuity Management—The other critical cyber response plan for a cybersecurity
program is a business continuity/disaster recovery plan. Although they are commonly lumped
together as BC/DR, there are separate processes for business continuity and disaster recovery. A
cybersecurity incident that is initially handled under an incident response plan may cause a
business interruption that requires implementation of business continuity procedures. Thus, each
plan should be drafted and tested for such circumstances to ensure a smooth and efficient
response and continuity of operations.

Certain critical infrastructure sectors have BC/DR requirements. NERC, for example, has
requirements for BC/DR in its required standards, and it conducts ongoing work regarding
continuity of operations and resiliency of electricity grids. These activities help these companies
stay abreast of threats and develop, implement, and maintain sophisticated BC/DR plans.

VI. INFORMATION SHARING

Sharing threat information regarding cyber incidents with others, such as law enforcement,
community emergency response teams (CERTs), information sharing and analysis centers

23 See, e.g., Cyber Attack Task Force, Final Report, accepted by NERC Board of Trustees, May 9, 2012, available at
http://www.nerc.com/docs/cip/catf/12-CATF_Final_Report_BOT_clean_Mar_26_2012-Board%20Accepted%200521.pdf; Severe Impact Resilience Task Force, Final Report, accepted by NERC Board of
Board_Accepted.pdf.
(ISACs), business partners, and public sector cyber officials who could benefit from the knowledge, helps advance cyber defenses and resiliency in other organizations. An attack on any organization may impact others, or it may be targeted at a particular activity or business process, such as point-of-sale systems or control processes. The sharing of threat information can substantially improve the ability of other organizations to respond to a similar attack. It also expands the knowledge base about threats and effective mitigation measures.

Many organizations have not thought through what external assistance they might need when responding to incidents. Establishing relationships with external organizations—such as FBI InfraGard, ISACs, CERTs, and industry cyber groups—regarding cyber threats can be an important defensive measure for any organization. Such organizations are usually open to receiving information in an anonymized or sanitized fashion, if desired, by the entity providing the information.

It is important that organizations identify what data they might share, determine with whom they would share it and in what form, and consider any legal ramifications associated with the data or sharing it with third parties. Although some have raised concerns that antitrust constraints may arise with information sharing, the U.S. Department of Justice (DOJ) has indicated a willingness to provide letters of exception, if requested, to enable cyber information sharing. On April 14, 2014, DOJ joined with the Federal Trade Commission (FTC) and issued a joint “Antitrust Policy Statement on Sharing of Cybersecurity Information,” which clarifies the issue:

Through this Statement, the Department of Justice’s Antitrust Division (the “Division”) and the Federal Trade Commission (the “Commission” or “FTC”) (collectively, the “Agencies”) explain their analytical framework for information sharing and make it clear that they do not believe that antitrust is—or should be—a roadblock to legitimate cybersecurity information sharing.

VII. EXISTING ABA POLICY

In recent years, the ABA House of Delegates and Board of Governors have adopted several policies regarding cybersecurity and lawyers’ use of technology, and the proposed Resolution is consistent with those existing ABA policies. These ABA policies include the following:

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firms, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations. The complete Resolution and Report are available at:

24 Lawyers, law firms, and organizations and entities authorized to provide legal services should take into consideration any ethical constraints that may apply to client records, and any legal restrictions applicable to records under seal, grand jury information, classified information, etc.
Policy Adopted by the ABA Board of Governors (November 2012)

The ABA's Board of Governors approved a policy in November 2012 comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force. The complete Resolution and Report are available at:

http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf


Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality. Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.

Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

The Resolutions and related Reports are available at:

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_105b.authcheckdam.pdf

http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc
VIII.  CONCLUSION

This Resolution is intended to call attention to the importance of appropriate cybersecurity programs for all organizations. These issues are linked directly to our Nation’s economic and national security. The principles and concepts discussed in this Resolution and Report can help organizations, including law firms, understand and address cybersecurity threats and risks.

Respectfully Submitted,

Judith Miller
Harvey Rishikof
Co-Chairs, ABA Cybersecurity Legal Task Force

August 2014
1. **Summary of Resolution(s).**

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

2. **Approval by Submitting Entities.**

The Cybersecurity Legal Task Force approved the Resolution on May 6, 2014.

The Section of Science & Technology Law voted to co-sponsor this Resolution by email vote of the Section Council (in accordance with the Section Bylaws) on May 6, 2014.

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 consistent with, and would build upon, several existing ABA policies, including the following:

Resolution 118, Adopted by the House of Delegates at the 2013 Annual Meeting in San Francisco (August 2013)

*This Resolution condemns intrusions into computer systems and networks utilized by lawyers and law firm, urges federal, state, and other governmental bodies to examine and amend existing laws to fight such intrusions, and makes other related recommendations.*

14
Policy Adopted by the ABA Board of Governors (November 2012)

The ABA’s Board of Governors approved a policy comprised of five cybersecurity principles developed by the ABA Cybersecurity Legal Task Force.

* * *


Resolution 105A amends the black letter and Comments to Model Rule 1.0 (Terminology), the Comments to Model Rule 1.1 (Competence) and Model Rule 1.4 (Communication), and the black letter and Comments to Model Rule 1.6 (Confidentiality of Information) and Model Rule 4.4 (Respect for Rights of Third Parties) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and confidentiality.

Resolution 105B amends the black letter and Comments to Model Rules 1.18 and 7.3, and the Comments to Model Rules 7.1, 7.2 and 5.5 of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding lawyers’ use of technology and client development.

Resolution 105C amends the Comments to Model Rule 1.1 (Competence) and Model Rule 5.5 (Unauthorized Practice of Law; Multijurisdictional Practice of Law), and the title and Comments to Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistants) of the ABA Model Rules of Professional Conduct dated August 2012, to provide guidance regarding the ethical implications of retaining lawyers and nonlawyers outside the firm to work on client matters (i.e., outsourcing).

5. What urgency exists which requires action at this meeting of the House?

The Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual. It is clear that all organizations—whether private or public sector—should take action to strengthen their security posture.

The only effective defense is a fully-implemented cybersecurity program with controls based on operational criteria and magnitude of harm and risk categorization. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization had undertaken proper cybersecurity planning and implemented appropriate security safeguards.

6. Status of Legislation. (If applicable)
7. **Brief explanation regarding plans for implementation of the policy, if adopted by the House of Delegates.**

The Resolution will be distributed to various private and public sector organizations, and other stakeholders in order to alert them to the ABA’s newly-adopted policy and to encourage them to take action consistent with the ABA policy.

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, Section of Environment, Energy and Resources, 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)**

    Lucy Thomson, Livingston PLLC,
    Washington, D.C.
    lucythomson1@mindspring.com
    (703) 798-1001

    Jody Westby, Global Cyber Risk, Washington, D.C.
    westby@globalcyberrisk.com
    (202) 337-0097

    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
12. Contact Name and Address Information. (Who will present the report to the House?)

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
EXECUTIVE SUMMARY

1. Summary of the Resolution

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. It encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected. This Resolution and Report are intended to educate organizations and heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

Recognizing that small businesses, small law firms and solo practitioners have varying financial and human resources available to them, the components of a cybersecurity program should be flexible and their implementation should be practical.

2. Summary of the Issue that the Resolution Addresses

This Resolution addresses cybersecurity issues that are critical to the national and economic security of the U.S. The threat environment today is highly sophisticated, and massive data breaches are occurring with alarming frequency. The consequences of a cyber incident or data breach can have a disturbing impact on the victim, whether a business, organization, government entity, or an individual. It is thus appropriate to encourage all organizations—whether private or public—to develop, implement and maintain an appropriate cybersecurity program. In many cases, data breaches or other types of cyber incidents could have been prevented or detected early and the risks of the incident mitigated if the organization or entity had undertaken proper cybersecurity planning and implemented appropriate security safeguards.

2. Please Explain How the Proposed Policy Position Will Address the Issue

Through this Resolution, the ABA highlights the importance of cybersecurity plans for private and public sector organizations as a matter of sound governance and risk management. This Resolution and Report will educate organizations, heighten their sensitivity to cybersecurity risks, and help them effectively evaluate their own specific risks and respond on behalf of their organization. The Resolution and Report do not define any obligations pursuant to laws or rules, including applicable lawyers’ rules of professional conduct.

4. Summary of Minority Views

This Resolution and report have been revised in response to input received from several ABA entities. No minority views have come to our attention with respect to the revised report.