AMERICAN BAR ASSOCIATION

CYBERSECURITY LEGAL TASK FORCE
SECTION OF SCIENCE & TECHNOLOGY LAW

REPORT TO THE HOUSE OF DELEGATES

RESOLUTION

RESOLVED, That the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate security program, including:

(1) conducting regular assessments of the threats, vulnerabilities, and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems; and

(2) implementing appropriate security controls to address the identified threats, vulnerabilities, and risks, consistent with the types of data and systems to be protected and the nature and scope of the organization;

FURTHER RESOLVED, That the American Bar Association encourages these organizations to develop and test a response plan for possible cyber attacks, including disclosure of data breaches, notification of affected individuals, and the recovery and restoration of disrupted operations; and

FURTHER RESOLVED, That the American Bar Association encourages these organizations to (1) engage in partnerships or cooperative relationships, where appropriate, to address the problem of cyber attacks by sharing information on cyber threats, and (2) develop points of contact and protocols to enable such information sharing.

REPORT

I. INTRODUCTION

This Resolution addresses security issues that are critical to the national and economic security of the United States (U.S.). It calls for private and public sector organizations[1] to address the security of their digital assets through an organization-wide security program that includes regular assessments of the threats and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems, and (2) the development and implementation of an appropriate security program to address the identified threats, vulnerabilities, and risks. The activities comprising a security program should be undertaken in accordance with accepted security frameworks and standards and be consistent with the types of data and systems to be protected and the nature and scope of the organization.

The Resolution also urges these organizations to develop and test a response plan for possible cyber attacks and engage in partnerships or cooperative relationships, where appropriate, to address the problem of cyber attacks by sharing information about cyber threats.

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.

II. CYBERSECURITY THREATS

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 security 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.

[1] This includes law firms and organizations authorized to provide legal services.

109

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. Many organizations provide access to their networks to business partners and entrust their data and business functions to outsource 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.[2] 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.

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. This includes 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.[3] 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."[4]

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.[5]

---

[2] White House, Cyberspace Policy Review, pages 1-2, 17, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[3] For example, a Vietnamese national was indicted recently for allegedly participating in an international scheme to steal and sell hundreds of thousands of Americans' PII though various websites he operated. *United States v. Ngo*, No. 13-crm-1116 (D. N.H. 2013), *available at* http://www.justice.gov/opa/pr/2013/October/13-crn-1116.html.

[4] IRS Criminal Investigation Targets Identity Theft Refund Fraud, February 2013, *available at* http://www.irs.gov/uac/Newsroom/IRS-Criminal-Investigation-Targets-Identity-Theft-Refund-Fraud-2013.

[5] *See.* Thomson, Lucy L., *Data Breach and Encryption Handbook* (ABA 2011), chapter 5, pages 57-85.

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. [6]

The U.S. Department of Homeland has designated the following 17 government and private industry sectors as critical infrastructure: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials and Waste, Transportation, and Water and Wastewater Systems. The private sector owns the vast majority of the nation's critical infrastructure and key resources—about 85 percent.

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 security programs are essential for critical infrastructure organizations, and following appropriate security frameworks and standards is central to achieving a strong security 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

Law firms are businesses and should take special care to ensure that they have a strong security posture and a well-implemented security program. The data and information kept by law firms

[6] NIST *Framework for Improving Critical Infrastructure Cybersecurity*, (February 12, 2014) Executive Summary, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

are largely protected by the attorney-client privilege and/or the work product doctrine, as well as by various legal ethics requirements.

The threat of cyber attacks against law firms is growing. Lawyers and law offices 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.

Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad. [7] 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.[8] 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.[9]

The *ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* (2013) provides practical threat information, 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. Lawyers and law offices have a responsibility to protect confidential records from unauthorized access and disclosure, whether malicious or unintentional, by both insiders and hackers. Amendments to the black letter and comments to the *ABA Model Rules of Professional Conduct* (Model Rules) adopted in 2012 explicitly 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."

III. SECURITY PROGRAM—FRAMEWORKS AND STANDARDS

There are a number of accepted frameworks and standards for developing, implementing, and maintaining a security program. Some of these well-known standards include[10]:

[7] Michael Riley and Sophia Pearson, China-Based Hackers Target Law Firms to Get Secret Deal Data, *available at* http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.
[8] Mike Mintz, "Cyberattacks on Law Firms—A Growing Threat," *Martindale.com*, Mar. 19, 2012, http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat.
[9] Mandiant Intelligence Center Report, APT1: Exposing One of China's Cyber Espionage Units, page 20, *available at* http://www.mandiant.com.
[10] Westby, Jody R., "Cybersecurity and Law Firms: A Business Risk," *Law Practice Magazine*, Vol. 39, No. 4, *available at* http://www.americanbar.org/publications/law_practice_magazine/2013/july-august/cybersecurity-law-firms.html.

- International Organization of Standardization (ISO), the 27000 series[11], http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- 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
- Payment Card Industry Security Standards Council (PCI SSC), https://www.pcisecuritystandards.org/security_standards/documents.php
- National Institute of Standards and Technology (NIST) Special Publication 800 (SP-800) series and Federal Information Processing Standards (FIPS), http://csrc.nist.gov
- Information Security Forum (ISF) Standard of Good Practice for Information Security, https://www.securityforum.org/?page=publicdownload2011sogp
- Carnegie Mellon University Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), http://cert.org/octave
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP), nerc.com/page.php?cid=2|20
- 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

Fortunately, they are generally consistent, and a number of the requirements in the various security frameworks and standards map to one another. Thus, it is less important which framework or standard an organization follows and more important that it undertakes all of the key activities of a security program.

An organization-wide security program is comprised of a series of activities, including governance by boards of directors and senior executives; development of security strategies and 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. The foregoing is not an exhaustive list.

Due to the nature of the threat environment, certain activities in a security program are ongoing. Continuous monitoring and log analysis are a critical part of an organization-wide risk management, and are designed to provide meaningful, actionable intelligence and reporting that can provide early detection of threats. To maintain a highly proactive security posture, potential threats must be investigated and targeted attacks detected in advance or addressed as they occur. The objective is to address the multitude of security threats and risks in a timely, disciplined, and structured fashion.

[11] Given the cost and effort required to obtain and maintain ISO 270001 certification, this may not be appropriate for small organizations, particularly where the risks are not great and the benefit achieved would be minimal.

To properly support an organization's risk management framework, privacy compliance requirements also must be incorporated into the security program. In addition, an effective security program requires a team of 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.

The determination of security controls is one of the most important activities of a security program. Effective security programs have administrative, technical, organizational and physical controls to help ensure the confidentiality, availability, and integrity of digital assets. Such controls must be carefully determined, implemented, and enforced. NIST has published extensive guidance on the selection of controls for government systems, which is equally appropriate for all organizations.[12]

The problem, however, is that many organizations are undertaking some of the required security activities, but not others, and some activities are performed without all the critical inputs. Therefore, the resulting security program has gaps and deficiencies and associated risks that impact the organization's operations, financial bottom line, and compliance is not adequately managed. In part, this is due to (a) a lack of attention at the top of many organizations, (b) a failure to assign key roles and responsibilities for privacy and security, and (c) deficient funding for security personnel, training, and program activities.

To protect against massive data breaches, it is clear that all organizations–whether private or public–must take immediate action to strengthen their security posture.

Small Organizations

Recognizing that small law offices and solo practitioners may lack the financial resources of larger firms, the components of a security program are flexible and their implementation must be practical and determined based upon the types of data and systems to be protected, the nature and scope of the organization, its compliance requirements, and system architecture. Small organizations, including small law offices and solo practitioners, will need to create a security program that prioritizes key security activities and is tailored to address the specific risks that have been identified. NIST has recognized that for some small organizations, "the security of their information, systems, and networks might not be a high priority, but for their customers, employees, and trading partners it is very important."[13] 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.[14]

---

[12] *See, e.g., Security and Privacy Controls for Federal Information Systems and Organizations,* National Institute of Standards & Technology, Special Pub 800-53, Rev. 4, Apr. 2013, *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[13] NIST Interagency Report 7621, *Small Business Information Security: The Fundamentals,* 2009, was published to assist small business management to understand how to provide basic security for their information, systems, and networks, *available at* http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

[14] *See, Security Standards: Implementation for the Small Provider, available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf.

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 components of organizational risk that senior executives address as part of their ongoing risk management responsibilities. This Resolution focuses on one aspect of a comprehensive enterprise risk management program—operational and IT/cyber 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.

Risk assessments are an essential element of a security program. 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. A risk assessment may be used to identify gaps and deficiencies in a security 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 companies. It is a fundamental business process they 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.[15]. 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), reporting (financial and non-financial), and compliance (with laws and regulations). Safeguarding organizational assets, including the confidentiality, integrity and availability of sensitive personal data and computer networks, from theft or fraud by hackers and malicious insiders is at the core of what an effective security program is designed to do.

---

[15] The Committee on Sponsoring Organizations of the Treadway Commission ("COSO"), an initiative of several groups with an interest in effective internal control, *available at* http://www.coso.org.

109

Risk assessment is necessary for publicly-traded companies to meet Securities and Exchange Commission (SEC) guidance on *Disclosure by Public Companies Regarding Cybersecurity Risks and Cyber Incidents*.[16]

Examples of cybersecurity risk management frameworks and standards include:

- ISO/IEC 27005:2011: *Information Security Risk Management.*[17] 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*.[18] 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)[19] and *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).[20] 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.

- *Critical Sectors—DHS Infrastructure Risk Management Approach.*[21] 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.

- *DOE Electricity Subsector Cybersecurity Risk Management Process* (RPM).[22] 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

[16] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[17] http://www.iso.org/iso/catalogue_detail?csnumber=56742.
[18] http://www.iso.org/iso/catalogue_detail?csnumber=43170.
[19] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.
[20] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.
[21] U.S. Department of Homeland Security, *Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach*, http://www.dhs.gov/sites/default/files/publications/NIPP%202013%20Supplement_Executing%20a%20CI%20Risk%20Mgmt%20Approach_508.pdf.
[22] http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.

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.

V. SECURITY 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 plans are critical components of a security program. Organizations must be prepared if a cyber attack or data breach occurs or if an event interrupts their operations. Thus, response plans, policies, and procedures must be able to accommodate the full array of threats, not just data breaches.

Incident response plans must involve stakeholders across an organization, including IT, security, legal, finance, operational units, human resources, and procurement. The incident response team should be identified and their roles and responsibilities defined. The communication with and coordination among stakeholders is one of the most important aspects of an incident response plan. This includes the identification of who within an organization should be responsible for communicating with external stakeholders, investors, employees, customers, and other key groups. External stakeholders include 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 are very important. This ensures valuable tracking and tracing data and evidence of what happened within a system are preserved and secured and chain of custody is documented. Advance planning and the advice of a crisis communications expert can be invaluable in keeping a cybersecurity incident from becoming a disaster.

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

There are ample resources available to assist organizations in understanding the key components of incident response. NIST, for example, has published an excellent guide, the *Computer Security Incident Handling Guide,*[23] and Carnegie Mellon has issued the *Handbook for Computer Security Incident Response Teams.*[24]

Business Continuity Management—The other critical cyber response plan for a security 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

[23] *Computer Security Incident Handling Guide,* NIST Spec Pub 800-61, Rev. 2 (Aug. 2012), *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911736.
[24] *Handbook for Computer Security Incident Response Teams,* Carnegie Mellon University, Software Engineering Institute, *available at* http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305.

plan must 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.[25]

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 (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 all 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 improves the knowledge base about threats and effective mitigation measures.

Many companies have not thought through their comprehensive incident response or developed cyber response plans, much less thought about how they might share threat information. Establishing relationships with external organizations–such as FBI Infragard, ISACs, CERTs, and industry cyber groups–regarding cyber threats is 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 to whom they would share it and in what form, and consider any legal ramifications associated with the data or sharing it with third parties.[26] 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")

[25] *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 Trustees, May 9, 2012, *available at* http://www.nerc.com/comm/OC/SIRTF%20Related%20Files%20DL/SIRTF_Final_May_9_2012-Board_Accepted.pdf.

[26] Lawyers, law firms, and organizations and entities authorized to provide legal services must 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.

(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.[27]

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, and would build upon, 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:

http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf

* * *

Resolution 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

* * *

Resolutions 105 A, B and C, Adopted by the House of Delegates at the 2012 Annual Meeting in Chicago (August 2012).

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.

[27] Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information, *available at* http://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

The 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 complete Resolutions and the 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

It is imperative that all organizations–private sector companies and other organizations, government departments and agencies, and professional firms such as legal, accounting, engineering, and consulting entities–develop, implement, and maintain an organization-wide security program in accordance with accepted security frameworks and standards. Today, too many organizations and entities–including critical infrastructure companies–have completed some activities within a security program, but not all, making them easy targets for sophisticated cyber-criminals. The lack of a disciplined process for the selection of security controls and ongoing reviews are two of the most serious gaps in security programs. Likewise, many organizations do not devote adequate funding to address known gaps and deficiencies in their security programs or to ensure that their organizations have well-developed plans to enable them to respond adequately to incidents and maintain continuity of business operations.

Through this Resolution, the ABA stresses the importance of security programs for all organizations as a matter of sound governance and risk management and as an imperative that is linked directly to our nation's economic and national security. Cybersecurity has moved beyond the realm of technical personnel; the maintenance of a security program, including the components stressed in this Resolution, is a responsibility that all senior executives, business owners, attorneys, general counsels, compliance officers, and government officials should embrace.

109

Respectfully Submitted,

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

August 2014

GENERAL INFORMATION FORM

Submitting Entity: ABA Cybersecurity Legal Task Force

Co-sponsoring Entity: Section of Science & Technology Law

Submitted By: Judith Miller and Harvey Rishikof, Co-Chairs,
ABA Cybersecurity Legal Task Force

1. Summary of Resolution(s).

This Resolution addresses security issues that are critical to the national and economic security of the U.S. It calls for all private and public sector organizations to address the security of their digital assets through the development, implementation, and maintenance of an organization-wide security program that includes (1) regular assessments of the threats and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems, and (2) implementation of appropriate security controls to address the identified threats, vulnerabilities, and risks. All activities comprising a security program should be undertaken in accordance with accepted security frameworks and standards and they should be consistent with the types of data and systems to be protected and the nature and scope of the organization, its compliance requirements, and system architecture.

The Resolution also encourages these organizations to develop and test a response plan for possible cyber attacks, and engage in information sharing partnerships or cooperative relationships, where appropriate, to address the problem of cyber attacks by sharing information about cyber threats..

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.

* * *

Resolution 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.

* * *

Resolutions 105 A, B and C, Adopted by the House of Delegates at the 2012 Annual Meeting in Chicago (August 2012).

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.

The 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 security 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–must take immediate action to strengthen their security posture.

The only effective defense is a fully-implemented security 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 security planning and implemented appropriate security safeguards.

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.

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
Washington, D.C. 20036
(202) 288-2013 (cell)
rishikofh@me.com

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 calls for all private and public sector organizations to address the security of their digital assets through the development, implementation, and maintenance of an organization-wide security program that includes (1) regular assessments of the threats and risks to their data, applications, networks, and operating platforms, including those associated with operational control systems, and (2) implementation of appropriate security controls to address the identified threats, vulnerabilities, and risks. All activities comprising a security plan should be undertaken in accordance with accepted security frameworks and standards, and they should be consistent with the types of data and systems to be protected and the nature and scope of the organization, its compliance requirements, and system architecture.

The Resolution also urges these organizations to develop and test a response plan for possible cyber attacks, and engage in information sharing partnerships or cooperative relationships, where appropriate, to address the problem of cyber attacks by sharing information about cyber threats..

2. **Summary of the Issue that the Resolution Addresses**

This Resolution addresses security 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–must take immediate action to strengthen their security posture.

The only effective defense is a fully-implemented security program with security 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 or entity had undertaken proper security planning and implemented appropriate security safeguards.

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

Through this Resolution, the ABA stresses the importance of security plans for all private and public sector organizations as a matter of sound governance and risk management and as an imperative that is linked directly to our nation's economic and national security. Cybersecurity has moved beyond the realm of technical personnel; the maintenance of a security plan, including the components stressed in this Resolution, is a responsibility that all senior executives, business owners, attorneys, general counsels, compliance officers, and government officials should embrace.

4. **Summary of Minority Views**

No minority views have come to our attention.