

Chapter 11 and Cybersecurity: The Inevitable Collision



April A. Wimberg
Moderator
Dentons



John G. Loughnane
Panelist
Nutter McClennen & Fish LLP



Kyle W. Miller
Panelist
Dentons



Elizabeth Vandesteeg
Panelist
Levenfeld Pearlstein, LLC

January 19, 2022

Introductions And Welcome

Scenario 1

You engage a new debtor client and through the intake the client discloses that one of the big issues that the company has recently faced was a “cyber attack”.

Scenario 2

You are Debtor's counsel to a heavy machinery dealer/retailer that is currently in a chapter 11 bankruptcy. The Debtor's DIP financing has recently been approved, you are looking toward drafting a plan and the client calls to state that they were just notified that "a security incident occurred" and they need advice as to what to do next.

Scenario 3

You are Debtor's counsel to a regional hospital and have had your 363 sale process approved, and now you are getting ready for an auction. Two days before the auction, the client calls and says their systems are completely locked out and the company has a \$5M ransom note.

Final Q & A

The background is a solid blue color. On the right side, there are three overlapping circles of different shades of blue, creating a modern, abstract design.

Appendix 1

Information Security Programs

Developing an Information Security Program (ISP)

- What is information security?
 - Refers to processes and methodologies designed and implemented to protect print, electronic, or any other form of information or data, including –
 - Confidential, private, and sensitive information; or
 - Data derived from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption

Developing an Information Security Program (ISP), cont.

- What is an Information Security Program (ISP)?
 - A memorialized set of the company's information security policies, guidelines and procedures
 - Objective is to assess risk, monitor threats, and mitigate cyber security attacks

Developing an Information Security Program (ISP), cont.

- Who needs an ISP?
 - Every company regardless of size
 - Whether or not you deal with PII, your data could still be the target of an attack
 - Your own financial records, key information, or other confidential information could be an attractive target for attackers as they could potentially sell or manipulate in other ways to make a profit

3 Key Components of an Effective ISP

- Threat and vulnerability management
 - Designed to mitigate the risk of an information security breach and meet compliance with regulatory requirements
 - Should cover -
 1. Program governance
 2. Threat management
 3. Vulnerability management

Elements of an Effective ISP

- Purpose
- Scope
- Information security objectives
- Confidentiality, accessibility, and integrity of data
- Authority and access control policy
- Classification of data
- Data support and operations
- Security awareness sessions
- Responsibilities and duties of personnel
- Relevant laws

ISP Purpose

- Establish a general approach to information security
- Detect and forestall the compromise of information security
 - i.e. misuse of data, networks, computer systems and applications
- Protect reputation of the company with respect to its ethical and legal obligations
- Recognize the rights of customers
 - i.e. providing effective mechanism for responding to complaints

ISP Scope

- An effective ISP will cover –
 - All data
 - Programs
 - Systems
 - Facilities
 - Personnel, and
 - Other tech infrastructure

ISP Objectives/Goals

- Companies should have a defined ISP objective(s)
 - Helps measure success and failure of ISP
- Information security systems are deemed to safeguard 3 main objectives –
 - Confidentiality
 - Integrity
 - Availability

ISP Objectives/Goals, cont.

- A well-defined ISP mission statement will include -
 - Company's main function
 - What is it that your security team does for the company?
 - Your primary customers
 - Who is it that your team primarily serves?
 - Protecting the products and services that make up the revenue of your business
 - The geographic location in which you operate, if relevant

ISP Authority and Access Control Policy

- Typically, a security policy has a hierarchical pattern -
 - Senior staff - may have enough authority to decide on what data can be shared and with whom
 - Junior staff - usually bound not to share the little amount of information they have unless explicitly authorized
 - Policies governing senior employees may not be the same policy governing junior employees
 - ISP should address every basic position in the organization with specifications that will clarify their authoritative status

ISP Classification of Data

- Data can have different value and thus may impose separation and specific handling regimes/procedures for each kind of data
- Information classification system is commonly sorted as:
 - High risk class
 - Confidential class
 - Public class

ISP Classification of Data, cont.

- High risk class - generally data protected by state and federal legislation
 - Information covered under The Data Protection Act, HIPAA, FERPA
 - Financial;
 - Payroll; and
 - Personnel (privacy requirements).
- Confidential class - not protected under law, but should be protected against unauthorized disclosure
- Public class - information freely distributed

ISP Security Awareness

- The knowledge and attitude members of the company possess for protection of the information assets of a company
- Providing employees training could help provide employees with information regarding how to collect/use/delete data, maintain data quality, records management, confidentiality, privacy, appropriate utilization of IT systems, correct usage social networking, etc.

ISP Policies & Procedures

- Overall, a company should focus on creating policies and procedures relating to:
 - Data governance and classification
 - Access controls
 - Capacity and performance planning
 - Systems and network security
 - Systems and network monitoring
 - Systems and application development
 - Physical security and environmental controls
 - Risk assessment
 - Incident response
 - Personnel training

Appendix 2

Counsel's Role Across the System's Development Lifecycle (SDLC)



THE WHITE HOUSE
WASHINGTON

TO: Corporate Executives and Business Leaders

FROM: Anne Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology

SUBJECT: What We Urge You To Do To Protect Against The Threat of Ransomware

DATE: June 2, 2021

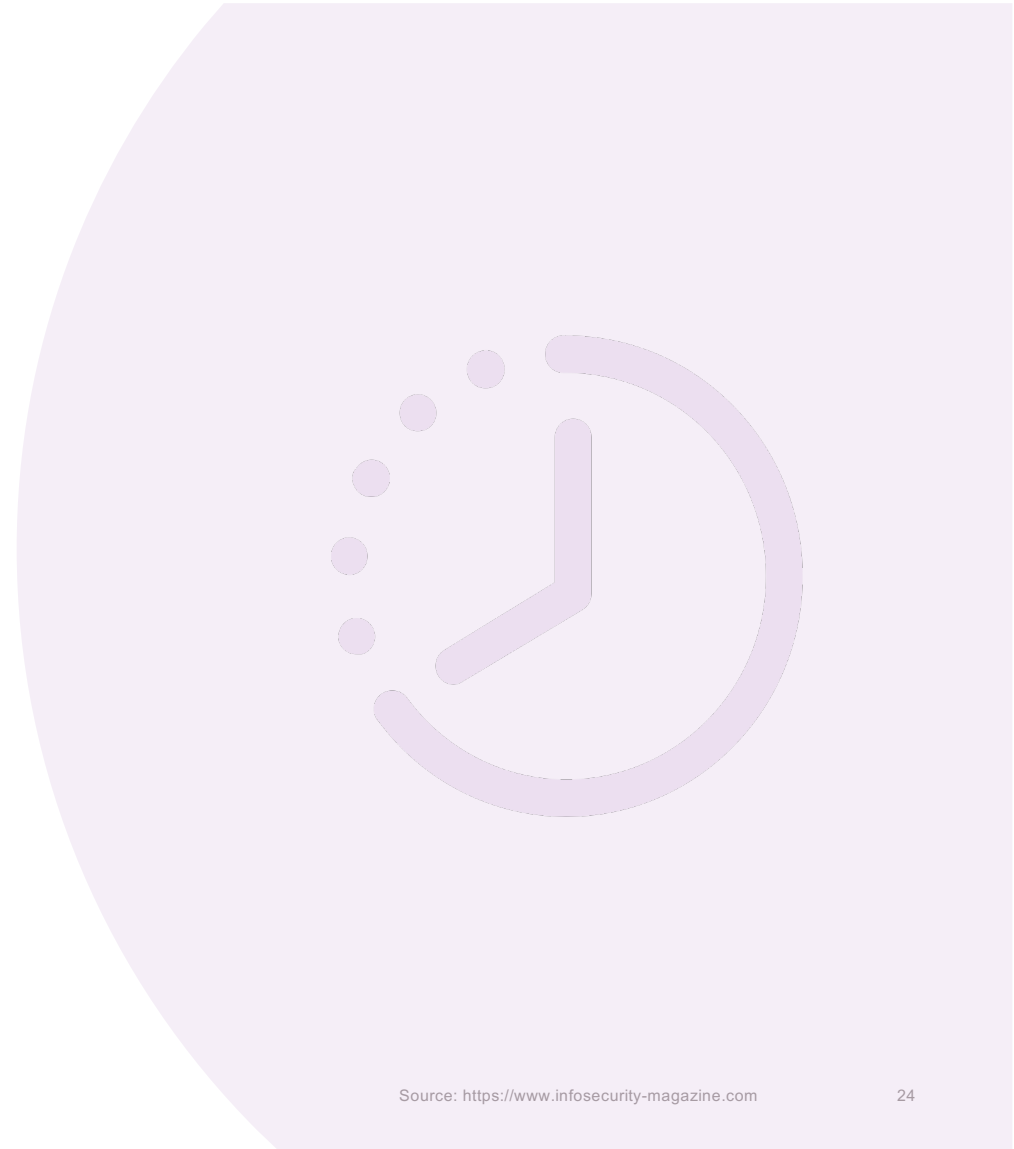
The number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks – both private and public sector – is a top priority of the President's.

Under President Biden's leadership, the Federal Government is stepping up to do its' part, working with like-minded partners around the world to disrupt and deter ransomware actors. These efforts include disrupting ransomware networks, working with international partners to hold countries that harbor ransomware actors accountable, developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds.

The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. But there are immediate steps you can take to protect yourself, as well as your customers and the broader economy. Much as our

In 2020

- Ransomware increased by 435% over 2019
- 1 Ransomware victim every 10 seconds
- 75% of all victim companies were running up to date endpoint protection
- Researchers estimate \$6 Billion paid to attackers
- First reported death due to ransomware attack





U.S. Department
OF
HEALTH & HUMAN SERVICES

NIST Special Publication 800-66 Revision 1


NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

**An Introductory
Guide for Implementing
Health Insurance and
Accountability (HIPAA) Security
Requirements**

Matthew Scholl, Kevin
Joan Hash, Pauline Bo
Carla Dancy Smith, and
others

October 2008

Computer Security Division
Information Technology
National Institute of Standards and Technology
Gaithersburg, MD 20899


U.S. Department of Commerce
Carol M. Galligan, Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

INFORMATION SECURITY

HIPAA Administrative Safeguards

45 CFR
(Unofficial Version, a)

Administrative Safeguards

4.1. Security Management Process (§ 164.308(a)(1))

HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.

Key Activities	Description	Sample Questions
1. Identify Relevant Information Systems	<ul style="list-style-type: none"> Identify all information systems that house EPHI. 	<ul style="list-style-type: none"> Are all hardware and software for which the organization

4.3. Workforce Security (§ 164.308(a)(3))

HIPAA Standard: Implement policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information.

Physical Safeguards

4.10. Facility Access Controls (§ 164.310(a)(1))⁶⁴

HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Key Activities	Description	Sample Questions
1. Conduct an Analysis of Existing Physical Security Vulnerabilities ^{61, 62}	<ul style="list-style-type: none"> Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities. Assign degrees of significance to each vulnerability identified and ensure that proper access is allowed. Determine which types of facilities require access controls to safeguard EPHI, such as: <ul style="list-style-type: none"> Data Centers Peripheral equipment locations IT staff offices Workstation locations. 	<ul style="list-style-type: none"> If reasonable and appropriate, do nonpublic areas have locks and cameras? Are workstations protected from public access or viewing? Are entrances and exits that lead to locations with EPHI secured? Do policies and procedures already exist regarding access to and use of facilities and equipment? Are there possible natural or man-made disasters that could happen in our environment? Do normal physical protections exist (locks on doors, windows, etc., and other means of preventing unauthorized access)?
2. Identify Corrective Measures ^{63, 66}	<ul style="list-style-type: none"> Identify and assign responsibility for the measures and activities necessary to correct deficiencies and ensure that proper access is allowed. Develop and deploy policies and procedures to ensure that repairs, upgrades, and /or modifications are made to the appropriate physical areas of the facility while ensuring that proper access is allowed. 	<ul style="list-style-type: none"> Who is responsible for security? Is a workforce member other than the security official responsible for facility/physical security? Are facility access control policies and procedures already in place? Do they need to be revised? What training will be needed for employees to understand the policies and procedures? How will we document the decisions and actions? Are we dependent on a landlord to make physical changes to meet the requirements?

⁶⁰ Note: See also Section 4.10, *HIPAA Standard: Facility Access Controls* and Section 4.14, *HIPAA Standard: Access Controls*.

⁶¹ This key activity may be performed as part of the risk analysis implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process*.

⁶² See Key Activity 4.10.3, *Develop a Facility Security Plan*. This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.

⁶³ See Section 4.11, *HIPAA Standard: Workstation Use*.

⁶⁴ See Section 4.7, *HIPAA Standard: Contingency Plan*.











⁶⁵ This key activity may be performed as part of the risk management implementation specification. See Section 4.1, *HIPAA Standard: Security Management Process*.

⁶⁶ See Key Activity 4.10.3, *Develop a Facility Security Plan*. This activity and all associated bullets in the Description and Sample Questions are part of the facility security plan implementation specification.

⁶⁷ See Section 4.2, *HIPAA Standard: Assigned Security Responsibility*.

⁶⁸ See Section 4.5, *HIPAA Standard: Security Awareness and Training*.
















Section 500.2. Cybersecurity Program

- (a)  Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.
- (b)  The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:
- (1)  Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;
 - (2)  use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;
 - (3)  detect Cybersecurity Events;
 - (4)  respond to identified or detected Cybersecurity Events to mitigate any negative effects;
 - (5)  recover from Cybersecurity Events and restore normal operations and services; and
 - (6)  fulfill applicable regulatory reporting obligations.
- (c)  A Covered Entity may meet the requirements of this Part by adopting a cybersecurity program maintained by an Affiliate, provided that the Affiliate's cybersecurity program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of this Part.
- (d)  All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Adopted, *New York State Register* March 1, 2017/Volume XXXIX, Issue 09, eff. 3/1/2017

23 NYCRR 500.2

Section 500.3. Cybersecurity Policy

- (a)  Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:
- (1)  information security;
 - (2)  data governance and classification;
 - (3)  asset inventory and device management;
 - (4)  access controls and identity management;
 - (5)  business continuity and disaster recovery planning and resources;
 - (6)  systems operations and availability concerns;
 - (7)  systems and network security;
 - (8)  systems and network monitoring;
 - (9)  systems and application development and quality assurance;
 - (10)  physical security and environmental controls;
 - (11)  customer data privacy;
 - (12)  vendor and Third Party Service Provider management;
 - (13)  risk assessment; and
 - (14)  incident response.

Adopted, *New York State Register* March 1, 2017/Volume XXXIX, Issue 09, eff. 3/1/2017

23 NYCRR 500.3

Gramm-Leach-Bliley

§314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

Children's Online Privacy Protection Act

(b) Regulations

(1) In general

Not later than 1 year after October 21, 1998, the Commission shall promulgate under section 553 of title 5 regulations that—

(D) require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

§312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

California Consumer Privacy Act

(1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of [Section 1798.81.5](#), is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

- (A)** To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.
- (B)** Injunctive or declaratory relief.
- (C)** Any other relief the court deems proper.

EU Cybersecurity Regulation

- GDPR Article 32 – Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Savidge v. Pharm-Save, Inc.

- Dispute between employees and an employer that allegedly inadvertently disclosed confidential employee information in a cyber-attack, the Court dismissed causes of action based on (1) Invasion of Privacy; (2) Negligence Per Se; and (3) Intentional Infliction of Emotional Distress. Savidge v. Pharm-Save, Inc., No. 3:17-CV-00186-TBR, 2017 WL 5986972 (W.D. Ky. Dec. 1, 2017).
- After Plaintiffs amended their complaint with revised causes of action the Court dismissed the additional causes of (1) Misappropriation of Trade Secrets; (2) Conversion; (3) Trespass to Chattels; and (4) Bailment. Savidge v. Pharm-Save, Inc., No. 3:17-CV-186-CHB, 2020 WL 265206 (W.D. Ky. Jan. 17, 2020).
- The *only* causes that survive the Motion to Dismiss stage are negligence and breach of implied contract.
- The Court noted of negligence, as applied to the alleged cyberattack, that the company must observe “such care as a reasonably prudent person would exercise under the circumstances.”

Industry Standards

- Industry standards and customs are important part of demonstrating reasonableness.
 - Childress v. Kentucky Oaks Mall Co., No. 5:06CV-54-R, 2007 WL 2772299, at *4 (W.D. Ky. Sept. 20, 2007)
 - Silverpop Sys. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016)

NIST 800 Series

- Fed
- Offi

Security and Information Systems

NIST SP 800-53, Rev. 5

SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND INFORMATION

NIST SP 800-53, Rev. 5

54

NIST SP 800-53, Rev. 5

55

IR-6 INCIDENT REPORTING

Control:

- Require personnel to report suspected capability within [Assignment: organ b].
- Report incident information to [Assig b].

Discussion: The types of incidents reported designated reporting authorities reflect a policies, standards, and guidelines. Incident effectiveness assessments, security requirement technology products.

Related Controls: [CM-6](#), [CP-2](#), [IR-5](#), [IR-5](#).

Control Enhancements:

- INCIDENT REPORTING | [AUTOMATED REPORTING](#)
Report incidents using [Assignment: organization].
Discussion: The recipients of incident mechanisms include email, posting of incident response tools and program.
Related Controls: [IR-7](#).
- INCIDENT REPORTING | [VULNERABILITY](#)
Report system vulnerabilities associated organization-defined personnel or organization.
Discussion: Reported incidents that organizational personnel including system agency information security officers, and the risk executive (function). The actions to address the discovered system.
Related Controls: None.

- INCIDENT REPORTING | [SUPPLY CHAIN](#)
Provide incident information to the organizations involved in the supply system components related to the incident.
Discussion: Organizations involved in system integrators, manufacturers, resellers. Entities that provide supply Security Council (FASCI). Supply chain information technology products, system distribution processes, or warehouse information to share and consider the about supply chain incidents, including root cause of an incident.
Related Controls: [IR-8](#).

References: [FASCI-18](#), [41 CFR 201](#), [USC](#)

- TRANSMISSION OF SECURITY AND PRIVACY
Verify the integrity of transmitted se

Discussion: Part of verifying the integrity and privacy attributes that are associated with an unauthorized manner. Unauthorized result in a loss of integrity for transmission.

Related Controls: [AU-10](#), [SC-8](#).

- TRANSMISSION OF SECURITY AND PRIVACY
Implement anti-spoofing mechanism attributes indicating the successful a

Discussion: Some attack vectors operate system to intentionally and malicious system. The alteration of attributes the security functions are in place and open.

Related Controls: [SI-3](#), [SI-4](#), [SI-7](#).

- TRANSMISSION OF SECURITY AND PRIVACY
Implement [Assignment: organization] and privacy attributes to transmit te

Discussion: Cryptographic mechanism privacy attribute binding to transmit information.

Related Controls: [AC-16](#), [SC-12](#), [SC-13](#).

References: [OMB A-130](#).

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATION

Control:

- Issue public key certificates under an obtain public key certificates from an organization.
- Include only approved trust anchors in organization.

Discussion: Public key infrastructure (PKI) organizational systems and certificates related application-specific time services. In crypt anchor is an authoritative source (i.e., a certificate derived. A root certificate for a PKI system certificate store maintains a list of trusted

Related Controls: [AU-10](#), [IA-5](#), [SC-12](#).

Control Enhancements: None.

References: [SP 800-32](#), [SP 800-57-1](#), [NIST](#)

SC-18 MOBILE CODE

Control:

- Define acceptable and unacceptable mobile code.
- Authorize, monitor, and control the use of mobile code.

- DEVELOPER TESTING AND EVALUATION | [STATIC CODE ANALYSIS](#)

Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

Discussion: Static code analysis provides a technology and methodology for security reviews and includes checking for weaknesses in the code as well as for the incorporation of libraries or other included code with known vulnerabilities or that are out-of-date and not supported. Static code analysis can be used to identify vulnerabilities and enforce secure coding practices. It is most effective when used early in the development process, when each code change can automatically be scanned for potential weaknesses. Static code analysis can provide clear remediation guidance and identify defects for developers to fix. Evidence of the correct implementation of static analysis can include aggregate defect density for critical defect types, evidence that defects were inspected by developers or security professionals, and evidence that defects were remediated. A high density of ignored findings, commonly referred to as false positives, indicates a potential problem with the analysis process or the analysis tool. In such cases, organizations weigh the validity of the evidence against evidence from other sources.

Related Controls: None.

- DEVELOPER TESTING AND EVALUATION | [THREAT MODELING AND VULNERABILITY ANALYSES](#)

Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:

- Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];
- Employs the following tools and methods: [Assignment: organization-defined tools and methods];
- Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and
- Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].

Discussion: Systems, system components, and system services may deviate significantly from the functional and design specifications created during the requirements and design stages of the system development life cycle. Therefore, updates to threat modeling and vulnerability analyses of those systems, system components, and system services during development and prior to delivery are critical to the effective operation of those systems, components, and services. Threat modeling and vulnerability analyses at this stage of the system development life cycle ensure that design and implementation changes have been accounted for and that vulnerabilities created because of those changes have been reviewed and mitigated.

Related Controls: [PM-15](#), [BA-3](#), [BA-5](#).

- DEVELOPER TESTING AND EVALUATION | [INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE](#)

(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and

CHAPTER THREE

PAGE 157

ISO/EIC 27000 Series



Standards About us News Taking part **Store** EN

ICS > 35 > 35.030

ISO/IEC 27000:2018

Information technology — Security techniques — Information security management systems — Overview and vocabulary

The electronic version of this International Standard can be downloaded from the ISO/IEC Information Technology Task Force (ITTF) web site.

ABSTRACT

[PREVIEW](#)

ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document

- cover commonly used terms and definitions in the ISMS family of standards;
- do not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining new terms for use.

BUY THIS STANDARD

FORMAT

LANGUAGE

PDF + EPUB + REDLINE

English

PAPER

English

CHF **166**

BUY

CIS Controls

- The Center for Internet Security is a nonprofit organization that aids entities in their cybersecurity programs.
- Best known for its Multi-State Information Sharing and Analysis Center (MS-ISAC) which helps state and local governments prevent and respond to cybersecurity threats.
- Publishes its Critical Security Controls (CIS Controls) to guide the implementation of organization's cybersecurity programs.

- 18 Controls are:

1. Inventory and Control of Enterprise Assets	10 Malware Defenses
2. Inventory and Control of Software Assets	11. Data Recovery
3. Data Protection	12. Network Infrastructure Management
4. Secure Configuration of Enterprise Assets and Software	13. Network Monitoring and Defense
5. Account Management	14. Security Awareness and Skills Training
6. Access Control Management	15. Service Provider Management
7. Continuous Vulnerability Management	16. Application Software Security
8. Audit Log Management	17. Incident Response Management
9. Email Web Browser and Protections	18. Penetration Testing

California Data Breach Report 2012-2015

- 1) The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.

Kamala D. Harris, Attorney General
California Department of Justice

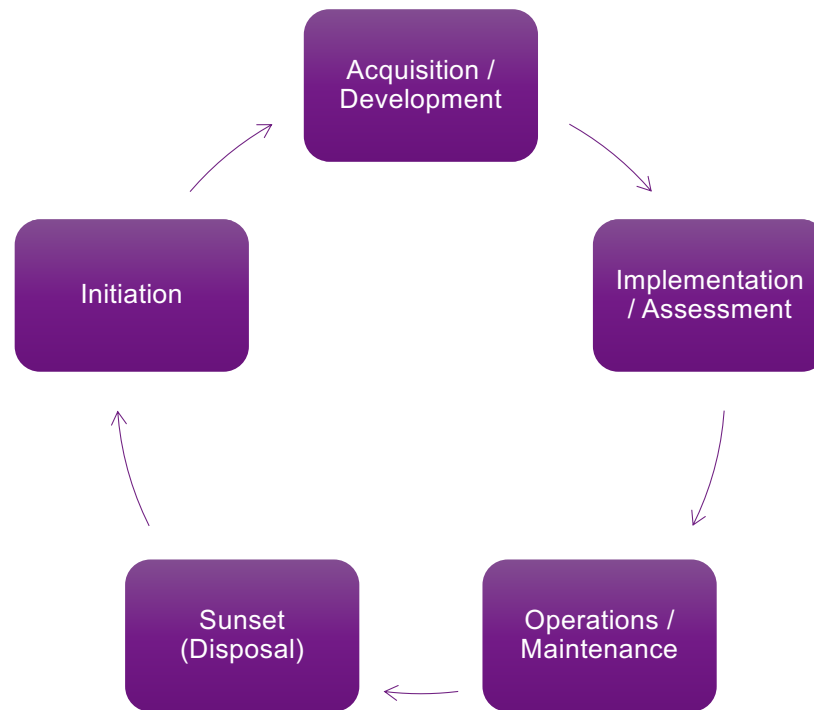
February 2016

Mathematical Formula

- In 1947, Judge Learned Hand attempted to make the reasonable person standard more systematic by finding liability in negligence under his now famous formula: If the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: *i.e.*, whether B less than PL. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).
- In February 2021, the Sedona Conference updated the *Carroll Towing* formula for the purpose of cybersecurity as follows.

$$B_2 - B_1 < (P \times H)_1 - (P \times H)_2.$$

Systems Development Life Cycle



Initiation

- Organization recognizes the need for a system and documents its purpose.
- Identify key security roles required to develop system.
- Identify the key stakeholder responsible for the system's security.
- The information the system will process is evaluated for security requirements, and all stakeholders should have a common understanding of the security considerations.
- Counsel should ensure corporate policies are in place to guide subsequent standards, procedures, and guidelines.
- Counsel should review information categorization to ensure it is appropriate under applicable regulation.

Initiation

- Statutory scheme for data classification:
 - GLBA — Financial information
 - HIPAA— PHI
 - FERPA — Educational records
 - COPPA — PII of children under 13
- Standards for data classification:
 - NIST 800-53 – Based on “Impact Level”

HIGH	Severe or catastrophic adverse effect
MODERATE	Serious adverse effect
LOW	Limited adverse effect

- ISO27k - A.8.2 requires classification, labeling, and handling of data based on legal requirements, value, and sensitivity.

Acquisition / Development

- System constructed.
- Conduct risk assessments.
- Develop security plans.
- Develop testing of security features to ensure system functions as intended
- Counsel should perform gap analysis on all security documentation and ensure compliance with company security policies.
- Counsel negotiates contracts necessary to develop system.

Implementation / Assessment

- Receive approval to operate the system
- Reviews and tests performed.
- Formally Operate the System.

Operations / Maintenance

- System is in place and operating.
- Modifications to the system are developed and tested.
- Hardware and software components are added or replaced.
- Performance of system is continuously monitored to ensure compliance with security requirements.
- Change management procedures are observed.

Incident Response

- Organization should respond based on its Incident Response Plan.
- Counsel should run investigation like other internal investigations.
- Counsel should engage necessary third parties under new engagements.
- Counsel should manage forensic investigators to ensure quality investigation to inform legal analysis.
- Counsel should understand underlying technology.
- Counsel will determine if incident amounts to a legal breach with notification requirements.

Sunset / Disposal

- System discarded.
- Develop plans for destruction of information.
 - Review contracts containing disposal information.
 - Review regulations with secure destruction requirements.

Recent Regulatory Actions

- December 2020 Poland's Personal Data Protection Office imposed a fine of €250,000 on a company that had data stolen on 140,699 clients.
- April 2021, the US Supreme Court unanimously curbed the FTC's ability to impose financial penalties for unreasonable cybersecurity.
- This year the New York Department of Financial Services (NYDFS) entered into a consent order with a company for \$1.5 million when a standard examination uncovered an unreported email compromise and a lack of required periodic risk assessments.

The Cybersecurity Attorney: Counsel's Role In The Systems Development Lifecycle

Kyle W. Miller

Kyle W. Miller is an attorney on the Dentons Global Data Privacy and Cybersecurity team and holds a Master of Science in Applied Information Technology from Bellarmine University. Prior to law school he served as Manager of Network Administration and Security for a Healthcare Data Analytics company. Kyle's practice includes Security Incident Response Investigations, pre and post-incident counsel, and data privacy counsel.

Cybersecurity attorneys routinely field questions from clients relating to their cybersecurity posture. Some questions relate to evaluating security solutions that range from minimal costs to hundreds of thousands of dollars, with security features corresponding to their price. Others relate to determining when a forensic firm is necessary for an incident investigation and when it is acceptable to rely on in-house IT personnel. Others relate to corporate policies that some stakeholders push for security and others object to as too cumbersome. All of these questions, and many others organizations seek counsel on, relate to the degree to which companies must protect their information and systems, what we attorneys would call the duty of care. Most questions from clients reveal the same underlying truth, organizations do not easily grasp how their cybersecurity posture may lead to legal liability.

When advising companies in this space it is important to keep several facts in mind. First, all connected systems have attack vectors that may be exploited by malicious actors. Second, businesses are looking to counsel to help understand the legal risks in their security posture. Third, the legal standards courts and legislatures impose on cybersecurity programs are, in a vacuum, so vague as to be meaningless to many organizations and technology professionals. Attorneys must understand how the law is applied to technology in order to advise clients of their risks, build robust and sufficient cybersecurity programs, respond appropriately to security incidents, and defend organizations in regulatory and civil litigation.

The Legal Standard

Companies have an obligation to implement reasonable cybersecurity practices when unauthorized access, use, or disclosure of information can harm others. The simple negligence standard is easy to state, but more difficult to implement.

Courts in Kentucky and throughout the nation recognize a company's duty to implement reasonable cybersecurity practices. In a recent dispute between employees and an employer that allegedly inadvertently disclosed confidential employee information in a cyber-attack, the Court dismissed causes of action based on (1) Invasion of Privacy; (2) Negligence Per Se; and (3) Intentional Infliction of Emotional Distress.¹ After Plaintiffs amended their complaint with revised causes of action the Court dismissed the additional causes of (1) Misappropriation of Trade Secrets; (2) Conversion; (3) Trespass to Chattels; and (4) Bailment.² The *only* causes that survived the Motion to Dismiss stage are negligence and breach of implied contract. The Court noted of negligence, as applied to the alleged cyberattack, that the company must observe "such care as a reasonably prudent person would exercise under the circumstances." In dismissing the eight other causes of action the court aligned itself with the legal norm of reasonableness without adding other legal theories to the company's actions.

Statutes that impose a duty related to cybersecurity often rely on the common law fallback of reasonableness. For example, the Children's Online Privacy Protection Act (COPPA) directs the Federal Trade Commission to promulgate regulations that require website operators "to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." 15 USCS § 6502. In promulgating those regulations the FTC provided the following, limited, guidance: The operator must establish and maintain reasonable procedures to protect

¹ Savidge v. Pharm-Save, Inc., No. 3:17-CV-00186-TBR, 2017 WL 5986972 (W.D. Ky. Dec. 1, 2017).

² Savidge v. Pharm-Save, Inc., No. 3:17-CV-186-CHB, 2020 WL 265206 (W.D. Ky. Jan. 17, 2020).

the confidentiality, security, and integrity of personal information collected from children. 16 CFR 312.8. Even highly regulated industries are hardly in better shape. For example organizations in the financial industry are commanded to develop information security programs that are “appropriate to [their] size and complexity” and that are “reasonably designed to achieve the objectives” of the Gramm Leach Bliley Act (GLBA). 16 CFR 314.3. In Kentucky, state agencies and nonaffiliated third parties must implement “reasonable security and breach investigation procedures” with guidance from relevant state departments. KRS 61.932.

Yet, attorneys provide little value to clients by simply telling them to behave reasonably. Who within an organization determines what is reasonable? An IT professional may feel differently than the CEO, or a member of the board of directors, or a customer. Instead, counsel must understand the threat landscape and the best practices and technology that mitigate those threats. Attorneys must also understand the sensitivity of the data that organizations hold. Finally, attorneys must understand their clients’ business and how to help them find a path forward that mitigates risk without placing an undue burden on the company.

Industry Standards

Industry standards and customs are an important part of proving an organization acted reasonably in litigation.³ Attorneys counseling companies must understand the standards to which those companies endeavor to adhere, and be ready to make recommendations should a company be missing best practices. There are many accepted standards that could be helpful in designing a cybersecurity program, including the following.

NIST 800 Series

The Federal Information Security Management Act (FISMA) tasks the National Institute of Standards and Technology (NIST) with developing standards, guidelines, methods, and techniques for providing information security for federal agencies. NIST publishes these safeguards, and others, in its NIST 800 Series documents. Though designed for federal agencies, NIST 800 series publications are the foundation for many organizations’ cybersecurity programs because they are freely available and implemented and maintained by the federal government. However, the NIST publications are not as popular outside of the US and multinational corporations are unlikely to use them as they will want a uniform security framework across all offices. Important publications for attorneys to understand are NIST 800-53, which provides security and privacy controls for information systems and organizations and NIST 800-100 which is an information security handbook for managers.

ISO/EIC 27000 Series

Often referred to as “ISO27K” this series is published jointly by the International Organization for Standardization and the International Electrotechnical Commission. As the names of the publishing organizations imply, these documents are implemented internationally or by US companies with an international presence or within the regulatory purview of an international regulator. These publications are not freely available, but subject to strict license after purchasing the publications with Swiss Francs. Still, their prevalence across many industries mandates attorneys to be familiar with them. Important publications for attorneys to understand are ISO/EIC 27001 which provides requirements for information security systems and ISO/IEC 27003 which provides guidance on the same.

Center for Internet Security – Critical Security Controls

The Center for Internet Security is a nonprofit organization that aids entities in their cybersecurity programs. It is best known for its Multi-State Information Sharing and Analysis Center (MS-ISAC) which helps state and local governments prevent and respond to cybersecurity threats. It also publishes its

³ *Childress v. Kentucky Oaks Mall Co.*, No. 5:06CV-54-R, 2007 WL 2772299, at *4 (W.D. Ky. Sept. 20, 2007); *Silverpop Sys. v. Leading Mkt. Techs., Inc.*, 641 F. App’x 849, 852 (11th Cir. 2016)

Critical Security Controls (CIS Controls) to guide the implementation of organization's cybersecurity programs. In 2014, then California Attorney General Kamala D. Harris issued the California Data Breach Report that found the CIS Controls "identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all [the CIS Controls] that apply to an organization's environment constitutes a lack of reasonable security."⁴ Therefore organizations that must comply with California law would do well to map their policies and procedures to the 20 CIS Controls to demonstrate reasonableness.

A Mathematical Formula

While the standards and guidelines often provide a framework organizations may use to build their security program, it can still be difficult to determine if any specific safeguard or control would be reasonable for an organization to implement. In 1947, Judge Learned Hand attempted to make the reasonable person standard more systematic by finding liability in negligence under his now famous formula: If the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: *i.e.*, whether B less than PL.⁵

In February, 2021, the Sedona Conference updated the Carroll Towing formula for the purpose of cybersecurity as follows.⁶

$$B_2 - B_1 < (P \times H)_1 - (P \times H)_2.$$

The Sedona Conference adopted the Carroll Towing variables but swapped L for H to mean magnitude of harm. Subscript 1 relates to the security controls in place at the time of an incident and subscript 2 relates to an alternative control the company could have implemented to prevent the harm that occurred. The formula, in plain English, states that an organization's security controls are unreasonable when additional controls would burden the company less than they would benefit a person adversely affected by the harm caused by the lack of the additional control.

If you think through the formula for a hypothetical client it is easy to see where the complexity lies. The existing and proposed burdens should be relatively easy to calculate. The probability and magnitude of harm variables, however, require a full risk analysis. This analysis should determine what harm is contemplated, how it can be avoided or mitigated, and what the resulting damages would be. Attorneys should not merely guess at the magnitude of harm and the probability that the harm will materialize. Instead, systemic analysis with the organization should yield educated predictions. To facilitate, many organizations including NIST, ISO, and others have risk assessment methodologies which can help professionals come to reasonable inputs.⁷

Applying the Law

The resources above provide tools necessary to advise clients on their obligations related to cybersecurity. By way of example, we can look at some recent widespread attacks that have raised questions from many of our clients. In the last few months hundreds of thousands of organizations have been impacted by zero day attacks leveraging vulnerabilities in critical business infrastructure. First, attackers planted a vulnerability in the popular SolarWinds IT management appliance. SolarWinds appears to have unknowingly pushed the exploit out to its clients via a regular update, which then allowed attackers to gain access and control over wide swaths of the victim's infrastructure. Second, attackers exploited a series of vulnerabilities in on-premise Microsoft Exchange servers that permitted attackers to run malicious code on the victim's machine, including creating backdoor access.

⁴ California Department of Justice, *California Data Breach Report* (2016) available at <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf>

⁵ *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

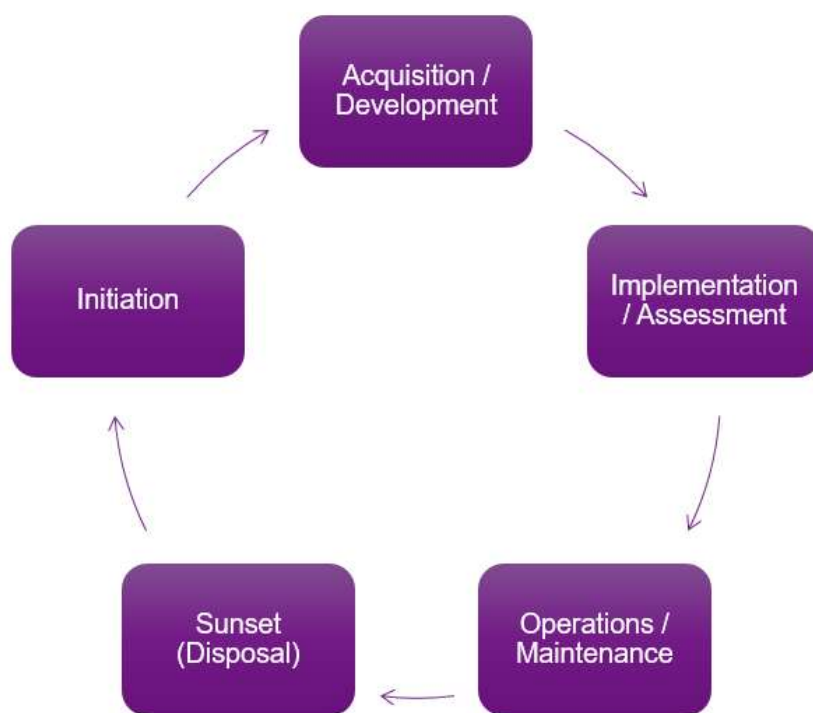
⁶ The Sedona Conference, *Commentary on a Reasonable Security Test*, 22 SEDONA CONF. J. 345 (forthcoming 2021) available at https://thesedonaconference.org/publication/Commentary_on_Reasonable_Security_Test.

⁷ See, eg. NIST SP 800-30; ISO/EIC 27005.

Zero day attacks are a unique threat in that there is very little an organization can do to prevent them. Even still, a company must implement reasonable practices to prevent harm to others. By any standard, once an organization is aware of a security event that compromises core infrastructure, it must respond to and mitigate the event.⁸ The organization's ability to appropriately respond is determined by the security regime it puts in place prior to the event. It should have response processes and procedures in place, guidelines on how to analyze and respond to threats, and mitigation procedures for update and patch management. Though an organization cannot prevent zero day attacks, it can position itself to timely respond once the vulnerability and remediation is publicized. In the case of the Microsoft Exchange attack, organizations that have not patched their systems are falling victim to an increasing array of attacks as new threat actors are reverse engineering the exploit to attack unpatched systems. Using the Sedona Formula, the burden of deploying a patch is very low, as they are developed by the makers of the affected hardware and software. The probability of harm is high as these vulnerabilities are publicized and new threat actors are working to leverage them before companies deploy the critical fix. The magnitude of harm is dependent on the sensitivity of the information an organization holds in its systems. It is easy to see the formula demands quickly patching the systems.

Pre-incident, attorneys can be valuable in reviewing cybersecurity programs to ensure companies are in position to respond to such attacks when they occur, thereby reducing potential legal liability. Post-incident, attorneys provide value in facilitating investigations and managing legal exposure. Attorneys that are well-versed in the evolving legal standards, industry standards, and threat landscape can become a highly valuable asset to a company's cybersecurity team.

The Systems Development Lifecycle⁹



Initiation Phase

⁸ See, for example NIST 800-53 IR 4; ISO/EIC 27001:2013, A.12.2.1, A.16.1.5; and CSC 18.

⁹ Radack, S. (2009), The System Development Life Cycle (SDLC), ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=902622 (Accessed April 2, 2021).

In this phase organizations recognize the need for a system and document the system's purpose. The organization should identify key security roles required to develop system, including the key stakeholder responsible for the system's security. The organization must evaluate and categorize any information the system will process and map that categorization to applicable security requirements. All stakeholders should understand the security considerations for the system.

Counsel should review security documentation to ensure compliance with company policies. Counsel should also review information categorization to ensure it is appropriate under applicable regulation. This requires monitoring any relevant statutory and regulatory scheme for data classification in addition to any contractual requirements. If the organization is mapping their policies to an industry standard it should follow that standard's guidelines for data classification. For example, the NIST 800-53 instructs mapping to three levels of classification:

HIGH	Severe or catastrophic adverse effect
MODERATE	Serious adverse effect
LOW	Limited adverse effect

Acquisition / Development Phase

In this phase the system is constructed. Organizations should conduct risk assessments related to the data that will be processed by the system. Further, the organization should develop security plans specifically tailored to the system. Using these risk assessments and security plans, organizations should develop testing protocols and metrics of security features to ensure the system functions as intended.

Additionally, counsel should perform gap analysis on all security documentation and ensure compliance with company security policies. In this phase counsel negotiates contracts necessary to develop the system. In some instances the *entire* system is acquired, either custom built or off the rack. In either case counsel must be involved at all phases to ensure the contract for the system or its components accurately reflects the intentions and risk profiles of the parties.

Implementation / Assessment

In this phase management and legal give formal approval to operate the system. The reviews and tests built in previous phases are performed on the final system that will go live. When the tests are sufficiently passed the system is implemented.

Counsel should review its previously created tests to ensure ongoing compliance. Counsel should also define critical "no-go" conditions that will prevent deployment if security standards are not met.

Operations / Maintenance

In this phase the system is in production and operating. The organization should ensure any modifications to the system are developed and tested. Hardware and software components will be added or replaced. Performance of the system is continuously monitored to ensure compliance with security requirements. When any material change is made the organization should ensure change management procedures are observed.

If security is breached and there is an incident, the organization should respond according to its incident response plan. Counsel should initiate an investigation as it would other internal investigations. If third parties are necessary for the investigation, they should be retained by counsel under new engagements. Forensic investigators must provide accurate details to inform counsel's legal analysis. Critically, counsel should understand underlying technology so it can effectively manage the investigation. Once counsel has the details of the incident it will determine if incident amounts to a legal breach with notification requirements.

Sunset / Disposal

In this phase the system is discarded. The organization must develop plans for destruction of information. Counsel should review contracts containing disposal information as well as regulations with secure destruction requirements.

Recent Cybersecurity Enforcement Actions

2020 saw the first penalties for unreasonable cybersecurity practices under the GDPR article 32. Poland's Personal Data Protection Office imposed a fine of €250,000 on a company that had data stolen on 140,699 clients.¹⁰

In April, 2021, the US Supreme Court unanimously curbed the FTC's ability to impose financial penalties for unreasonable cybersecurity.¹¹

In 2021 the New York Department of Financial Services (NYDFS) entered into a consent order with a company for \$1.5 million when a standard examination uncovered an unreported email compromise and a lack of required periodic risk assessments.¹²

¹⁰ Order (in Polish), available at <https://uodo.gov.pl/decyzje/DKN.5130.1354.2020>; machine translation available at https://gdprhub.eu/index.php?title=UODO_-_DKN.5130.1354.2020.

¹¹ AMG Capital Mgmt., LLC v. FTC, 141 S. Ct. 1341 (2021).

¹² NYDFS Consent order, available at https://www.dfs.ny.gov/system/files/documents/2021/03/ea20210303_residential_mortgage_0.pdf.

BY ELIZABETH B. VANDESTEEG

Technology and Legal Ethics: A User's Manual (Part I)

Editor's Note: *This new column addresses the wide-ranging issues of data security and privacy fundamentals, including ethical considerations, for the restructuring professional. Those interested in contributing for this column should contact Ms. Vandesteeg at evandesteeg@sfggh.com.*



**Coordinating Editor
Elizabeth B.
Vandesteeg**
Sugar Felsenthal Grais
& Helsinger, LLP
Chicago

Lisa Vandesteeg is chair of the Litigation and Dispute Resolution Group of Sugar Felsenthal Grais & Helsinger LLP in Chicago. Her practice includes bankruptcy, commercial litigation, business disputes and privacy and data-security issues. She is a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. A 2017 ABI "40 Under 40" honoree, she serves as an associate editor for the ABI Journal.

Once upon a time, certain attorneys embraced the view that being a Luddite¹ was a point of pride; they had practiced in paper for decades, and new-fangled technology was unnecessary to provide top-notch service to their clients. This worldview has ever-decreasing adherents, as technology has reached into nearly every facet of the practice of law. Not only is facility with technology a practical business requirement to adequately serve clients, it is now also an ethical requirement imposed upon attorneys in most states. Standard rules of professional conduct mandate that attorneys both take reasonable steps to keep the client data that they hold secure and provide notice to clients should there be an unauthorized disclosure of such data.

For bankruptcy attorneys, the implications of these standards are particularly far-reaching. While commercial litigators and their transactional counterparts might be privy to confidential data, it is likely that such information will be discrete and related solely to the dispute or deal at issue. There will be only a few parties involved, and the process will not require public disclosures beyond limited public filings.

On the other hand, bankruptcy is a process that requires comprehensive disclosures and involves numerous parties. Bankruptcy attorneys, particularly those representing corporate debtors, might find themselves responsible for an entire company's data, including all financial, proprietary and employee information. They must understand the types of potentially sensitive information in their possession and the proper ways to safeguard it from unauthorized access or disclosure.

This article is the first in a two-part series discussing the fundamentals of the intersection of cybersecurity and ethics for bankruptcy attorneys. This article discusses the key ethical rules in the realm of technology and data security. The second article, which will appear in a later issue, will pro-

vide guidance as to the best practices with respect to securing and transferring client data as part of information-security programs for law firms, as well as the necessary steps that law firms must take to notify clients in the event of a data breach and loss of client information.

Technological Competence: The Cornerstone of Cyber Ethics

Any attorney's first and most important ethical duty to clients is to provide competent legal representation. Model Rule 1.1 of the American Bar Association's (ABA) Model Rules of Professional Conduct² requires that such "competent representation" to a client include the requisite legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.³

An attorney's ability to provide that competent representation includes a requirement of technological facility. Specifically, Comment 8 to Model Rule 1.1 requires an attorney to keep abreast of "the benefits and risks associated with relevant technology."⁴ With this addition, the Model Rule's definition of "competency" now mandates that attorneys maintain both a substantive knowledge of law *and* proficient skills with the ever-evolving technology available to attorneys and clients.

In the seven years since the ABA adopted Comment 8 to Model Rule 1.1, 38 states have included similar requirements in their ethical rules.⁵ For attorneys, achieving and maintaining a certain level of technological proficiency is simply no longer optional.⁶

What to Do?

Technology invades nearly every province of legal practice — from the use of timekeeping and

1 A "Luddite" is defined as someone "who is opposed to especially technological change." Merriam-Webster Dictionary, available at merriam-webster.com/dictionary/Luddite (last visited Jan. 7, 2020).

2 The ABA Model Rules of Professional Conduct were adopted by the ABA House of Delegates in 1983 and serve as models for the ethics rules of most U.S. jurisdictions. Some variation has been adopted by all 50 states.

3 Model Rules of Prof'l Conduct R. 1.1 (2019).

4 Model Rules of Prof'l Conduct R. 1.1, cmt. 8 (2019) (adopted in 2012).

5 At the time of this article, 11 states have yet to enact versions of Comment 8 in their rules of professional responsibility or otherwise recognize the technological competence duty: Alabama, Alaska, Georgia, Hawaii, Maine, Maryland, Mississippi, Nevada, New Jersey, Oregon and South Dakota. While one of the remaining states, California, has not formally adopted the change to its rules of professional conduct, it has issued an ethics opinion expressly acknowledging the technological competence duty in the context of e-discovery in litigation. State Bar of Calif. Standing Comm. Prof'l Responsibility and Conduct Formal Op. No. 2015-109 (2015).

6 At least two states, Florida and North Carolina, now mandate not only technological competence, but also technology training as part of their continuing legal education programs.

continued on page 49

Cyber-U: Technology and Legal Ethics: A User's Manual (Part I)

from page 12

billing software to the redaction required of e-filers to e-discovery, and from vetting vendors for security compliance to training staff and attorneys on recognizing security risks. The complex relationship between new technological opportunities and the accompanying risks can create a confusing landscape for attorneys.

For example, the use of third-party service providers, such as cloud-based document-management and storage companies, might benefit an attorney in the form of increased efficiency in moving away from paper records. However, that attorney must monitor how those service providers secure and store client data. The widespread availability of public wireless networks also provides attorneys with the chance to check email and perform work remotely from nearly any location, but such networks also bring heightened risk of exposing client data to bad actors who monitor and intercept internet traffic on those networks.

How, then, do attorneys comply with this requirement for technological competence? “Competence” in technology cannot be satisfied by merely hiring qualified IT personnel and considering the matter solved. The Model Rules make it clear that attorneys must educate themselves on both the risks and benefits of technology, either through self-study (*e.g.*, by attending continuing legal education seminars, such as those offered at ABI conferences), associating with knowledgeable individuals in their law practice, or otherwise receiving training on relevant technology.⁷

Attorneys must know enough about the new technology they use to perform legal services to ensure that they are compliant with their professional responsibilities to keep client information confidential and secure. An attorney using new technology without learning how to operate it safely is running afoul of the fundamental ethical obligations.

Confidentiality: Lock It Up

While technology may have changed the means by which attorneys maintain and transmit sensitive information, the duty of confidentiality remains unchanged. Model Rule 1.6 prohibits an attorney from revealing “information relating to the representation of a client” unless such client gives informed consent, or the disclosure is “impliedly authorized” or otherwise permitted.

Attorneys are ethically required to make “reasonable efforts” to prevent inadvertent or unauthorized disclosure of — or unauthorized access to — information relating to the representation of a client (or former client).⁸ Attorneys can take some comfort in knowing that the Model Rules provide that unauthorized access or inadvertent disclosure of client information “does not constitute a violation of paragraph (c) [of Model Rule 1.6] if the lawyer has made reasonable efforts to prevent the access or disclosure.”⁹

In typical lawyerly fashion, the “reasonable efforts” standard is a fuzzy one, and the determination of whether efforts are indeed reasonable is a fact-specific inquiry. Relevant factors include the sensitivity of the information, the risk of disclosure without additional precautions, the cost of extra measures, the difficulty of adding safeguards, and whether more safeguards adversely affect the lawyer’s ability to represent the client.¹⁰

The onus is also on an attorney to analyze and determine any appropriate safeguards regarding the transmission of confidential information. The Model Rules specify that this does not necessarily require the use of special security measures (such as encrypting every email), but prompt lawyers to consider whether special security measures are warranted with respect to particularly sensitive information or material protected by law or confidentiality agreements.¹¹

Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information.

What to Do?

The “reasonable efforts” standard requires an informed and delicate balancing act. Attorneys must implement strong data-security practices in order to safeguard client data and comply with ethical responsibilities. However, at the same time, attorneys must take into account both the actual cost of additional security measures (technological or otherwise), and also the potential adverse impact of such security on the lawyer’s ability to practice law. For example, while requiring encryption of every document in a firm’s database might make the data extremely secure, it would also create a practical inability for attorneys to efficiently perform work.

This standard requires attorneys to be well-versed enough in technological matters to appropriately assess what security measures are sufficient and when. For example, “reasonable efforts” for an attorney dealing with an individual client’s personal or financial data may involve encrypting any email providing that information to another recipient or arranging for an alternative means of secure transmission. For example, an attorney representing a corporation seeking to sell its assets pursuant to § 363 of the Bankruptcy Code should perform due diligence on the cloud-based document-hosting service that might be used as the data room to confirm that it has sufficient security safeguards in place. Attorneys must also be aware of and avoid common and well-known data

7 Model Rules of Prof’l Conduct R. 1.1, cmts. 1, 6, 8 (2019). See, *e.g.*, *James v. Nat’l Fin. LLC*, No. 8931-VCL, 2014 WL 6845560 (Del. Ch. Dec. 5, 2014) (discussing competence as requirement of Pennsylvania and Delaware rules of professional conduct in the context of e-discovery violations).

8 Model Rules of Prof’l Conduct R.1.6(c) and cmt. 20 (2019) (adopted in 2012).

9 Model Rules of Prof’l Conduct R. 1.6, cmt. 18 (2019).

10 *Id.* See, *e.g.*, State Bar of Ariz. Ethics Op. 09-04 (2009) (discussing standards for electronic access to client files).

11 Model Rules of Prof’l Conduct R. 1.6, cmt. 19 (2019).

continued on page 50

Cyber-U: Technology and Legal Ethics: A User's Manual (Part I)

from page 49

security risks, such as the use of unsecured wireless networks in coffee shops and airports, and instead use a secured wireless network to communicate with clients.

Supervisory Responsibilities

Attorneys are required to not only be competent in their own legal practice but also be responsible for the actions taken by those under their supervision.

Junior Attorneys

Partners and other supervisory attorneys are required to “make reasonable efforts” to ensure that the firm has in effect measures “giving reasonable assurance” that all lawyers in the firm conform to the ethical rules. A supervising attorney must also make “reasonable efforts” to ensure that junior lawyers adhere to the ethical rules.¹²

When considering those responsibilities in the context of technology and data security, senior attorneys must instruct junior attorneys on the responsibility to safeguard client data. Supervisory attorneys must provide training (ideally as part of and in compliance with a holistic information-security program) on critical security issues, including using care when emailing recipients outside the firm; avoiding the use of public unsecured wireless networks; and properly securing devices containing client data such as mobile phones, tablets and laptops. Partners cannot turn a blind eye when they see junior lawyers failing to take such precautions, or they risk ethical violations themselves.

Nonlawyer Employees and Vendors

Similarly, lawyers are responsible for overseeing nonlawyers employed or retained by, or associated with, a lawyer. This rule contemplates the oversight responsibilities triggered by an attorney’s use of both nonlawyer employees within a firm and service providers outside the firm, and requires an attorney to take “reasonable efforts” (there is that fuzzy standard again!) to ensure that services are provided in a manner that is compatible with the lawyer’s professional obligations.¹³

Law firms regularly employ nonlawyers, including paralegals, secretaries or law clerks. A lawyer must give such assistants “appropriate instruction and supervision” concerning the ethical aspects of their employment, “particularly regarding the obligation not to disclose information relating to the representation of a client.”¹⁴

Attorneys also frequently make use of external vendors in legal practice, such as investigators, expert witnesses, e-discovery vendors and cloud-based services for hosting

firm and client data. For bankruptcy practitioners, this might also include third parties such as claims and noticing agents.

What to Do?

What do these supervisory responsibilities require on a practical level? Read in tandem with the competence required of Model Rule 1.1 and the need to safeguard client confidences in Model Rule 1.6, these supervisory responsibilities require attorneys to know enough about technology and data security to appropriately hire and supervise junior attorneys, nonlawyers and service providers.

An attorney may not simply hire any vendor they hear about without first investigating that vendor’s particular data-security practices and confirming that the vendor stores and transmits any data it handles in a manner that is compatible with that attorney’s professional obligations. “Reasonable efforts” to ensure that an external vendor is performing its work in a manner compatible with the lawyer’s professional obligations should include consideration of such factors as “the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.”¹⁵

Similarly, there is no way for an attorney to avoid ethical responsibilities by blaming a breach on an assistant who may have clicked on a bad email link or responded to a fraudulent request for a wire transfer. Attorneys, particularly supervisory attorneys such as partners, should implement an information-security program to ensure that proper supervision and standards are in place in order to comply with ethical responsibilities. An attorney should also provide training to staff members in areas such as email security awareness, proper procedures for sending and receiving wire transfers, procedures for storing and destroying client documents and data, and protocols for sending client data outside the firm.

Conclusion

Technological competence and appropriate data-security measures are no longer a problem that can be outsourced to IT. Attorneys must train themselves, their employees and their vendors in the use of reasonable, situation-specific safeguards for client data and other sensitive information. This is not only a prudent business move, but it is also required by ethical rules in most states. With proper training and oversight, attorneys can comply with these ethical rules and ensure the security of client data. **abi**

¹² Model Rules of Prof’l Conduct R. 5.1 (2019).

¹³ Model Rules of Prof’l Conduct R. 5.3 (2019).

¹⁴ Model Rules of Prof’l Conduct R. 5.3, cmt. 2 (2019).

¹⁵ Model Rules of Prof’l Conduct R. 5.3, cmt. 3 (2019). *See, e.g.*, Ill. State Bar Assoc. Advisory Op. No. 16-06 (2016) (discussing “reasonable efforts” to employ when selecting and hiring cloud computing vendor).

Copyright 2020

American Bankruptcy Institute.

Please contact ABI at (703) 739-0800 for reprint permission.

BY ELIZABETH B. VANDESTEEG

Technology and Legal Ethics: A User's Manual (Part II)

Editor's Note: *Part I of this article was published in the February 2020 issue.*



**Coordinating Editor
Elizabeth B.
Vandesteege**
*Sugar Felsenthal Grais
& Helsinger LLP
Chicago*

Lisa Vandesteege is chair of the Litigation and Dispute Resolution Group at Sugar Felsenthal Grais & Helsinger LLP in Chicago. Her practice includes bankruptcy, commercial litigation, business disputes and privacy and data security issues. Ms. Vandesteege is a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. A 2017 ABI "40 Under 40" honoree, she serves as an associate editor for the ABI Journal.

As was discussed in Part I,¹ use of technology has become a vital and inescapable component of the practice of law. Society's now-ubiquitous reliance on technology has required the legal industry to augment the ethical standards that attorneys must uphold in order to maintain fundamental protections for their clients and their clients' information. These ethical standards are applicable to all attorneys equally, but they are particularly relevant for bankruptcy attorneys, who are custodians of a host of personally identifiable information (PII)² and other sensitive and confidential information.

Part II of this article will focus on the specific ethical obligations and practical standards set forth in two recent American Bar Association (ABA) ethics opinions governing the storage and transmittal of client data, as well as the necessary steps that lawyers and firms must take to protect against, and notify clients of, any unauthorized access to client information.

Securing Communication of Protected Client Information

On May 11, 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R, "Securing Communication of Protected Client Information." Acknowledging that law firms are high-quality targets of hackers, the purpose of Formal Opinion 477R was to address "how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world."³

The ABA's conclusion is that "[a] lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access." How, then, should one determine what steps are "reasonable" to prevent unauthorized access to client information? Formal Opinion 477R expressly

states that it is "beyond the scope" of the opinion to expressly dictate what may constitute "reasonable steps" to protect client data, but it provides the following "considerations as guidance":

1. *Understand the nature of the threat:* A lawyer must consider the sensitivity of the client's information and whether the information is at a higher risk for cyberattack (e.g., trade secret or financial information); higher-risk scenarios require greater efforts to protect.⁴

2. *Understand how client confidential information is transmitted and where it is stored:* A lawyer must understand the law firm's technological landscape in terms of how electronic communications are created, where client data is stored, and how and by whom the data can be accessed.⁵

3. *Understand and use reasonable electronic security measures:* A lawyer should understand the various options that exist to protect electronic information and implement appropriate measures to protect client data and communications. This could include the use of secure internet access methods (secure Wi-Fi or virtual private network); complex passwords; firewalls; anti-malware/antivirus software; regular security patches and updates; encryption; and multifactor authentication.⁶

4. *Determine how electronic communications about clients' matters should be protected:* A lawyer and client should discuss what levels of security will be required for electronic communications, recognizing that communications might be at varying levels of sensitivity and could require different degrees of protection.⁷

5. *Label clients' confidential information:* A lawyer should mark client communications as "privileged and confidential" in order to put any unintended recipient on notice of the intent for the communication to remain confidential.⁸

6. *Train lawyers and nonlawyer assistants in technology and information security:* Applying ABA Model Rules 5.1 and 5.3, lawyers must establish policies regarding, and train employees on the use of, secure methods of communication with clients and reasonable measures for the storage of and access to client data and communications.⁹

1 Elizabeth B. Vandesteege, "Technology and Legal Ethics: A User's Manual (Part I)," XXXVIX ABI Journal 2, 12, 49-51, February 2020, available at abi.org/abi-journal (unless otherwise specified, all links in this article were last visited on Feb. 26, 2020).

2 PII is defined as "[a]ny information about an individual, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linkable to an individual, such as medical, educational, financial, and employment information." "Personally Identifiable Information," IAPP Resource Center, available at iapp.org/resources/article/personally-identifiable-information.

3 ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477R, at 2 (2017).

4 *Id.* at 6.

5 *Id.*

6 *Id.* at 6-7.

7 *Id.* at 7-8.

8 *Id.* at 8.

9 *Id.* at 9.

7. *Conduct due diligence on vendors providing communication technology:* A lawyer must take reasonable steps to analyze potential vendors who will be involved in the transmittal or storage of client data or communications. Lawyers should consider reference checks and vendor credentials; vendor security policies and hiring practices; use of confidentiality agreements; and availability of legal fora in the event of violations of the vendor agreement.¹⁰

From the perspective of a cybersecurity attorney, these “considerations” are the framework of a basic information security program. The creation and implementation of a thoughtful and deliberate information security program, as evidenced by and set forth in a written information security policy evidencing its terms, is a best practice that every law firm should follow. Simply put, an information security policy is a company’s documented statement of rules and guidelines that need to be followed with respect to the security of company data. For a law firm, an information security policy should expressly apply to client data, and it should detail the administrative, physical and technical safeguards in place to provide reasonable protection of client information.

Lawyers’ Obligations After an Electronic Data Breach or Cyberattack

Data loss and hacking are now commonly discussed in terms of “when” and not “if.” Even an attorney who has taken reasonable steps to protect client data and communications may well nonetheless be the target of a cybersecurity incident or data breach involving client information. How should an attorney ethically handle and respond to such an event?

On Oct. 17, 2018, the ABA Ethics Committee issued Formal Opinion 483, “Lawyers’ Obligations After an Electronic Data Breach or Cyberattack.” Formal Opinion 483 “picks up where Opinion 477R left off, and discusses an attorney’s ethical obligations when a data breach exposes client confidential information.”¹¹ It sets forth both obligations related to the detection of and response to a cybersecurity incident, as well as specific notice requirements to clients.

For purposes of Formal Opinion 483, a data breach occurs when “material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired.”¹² But not every data breach will result in an ethical violation — only those where “a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.”¹³

Reasonable Efforts to Prevent a Data Breach

In the first instance, lawyers have an obligation to monitor for data breaches.¹⁴ They must monitor firm technology and resources connected to the internet, as well as external

data sources and external vendors who might access or provide services involving client data.

Lawyers and law firms should also proactively develop a detailed incident response plan (IRP) before a breach occurs, so that appropriate and coordinated steps might be taken immediately thereafter.¹⁵ While every lawyer’s IRP should be tailored to fit their office’s or firm’s specific practice, the fundamental goal of any IRP is to appropriately handle an incident through (1) preparation; (2) detection and analysis; (3) containment, eradication and recovery; and (4) post-incident activity.¹⁶

As part of the preparation phase, it is important to draft the IRP as a simple standalone document. It should designate and provide contact information for team members and their backups (a “breach response team”), together with the specific roles that each member will play in the event of a security incident, and at every stage of the incident.¹⁷ Best practices then encourage the breach response team to engage in “tabletop exercises” in order to test and practice the IRP procedures before a security incident happens.

After taking prompt action to contain and eradicate the breach, a lawyer is ethically obligated to “make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer’s clients.”¹⁸ The extent of such efforts, whether through restoration of existing systems or through implementation of new technology, will depend on the specific circumstances of the breach. Unless the lawyer or firm is trained in this area, it is best to outsource this process to trained experts to ensure complete recovery and prevent further breaches.

Attorneys must then make reasonable efforts to determine what actually occurred during the data breach. Ethical standards governing post-breach investigations require that the lawyer have enough information to both confirm that the breach has in fact been contained and evaluate the extent, if any, to which client data was accessed or lost.¹⁹ In addition, the post-breach investigation should be extensive enough to determine how the breach occurred in order to patch any and all vulnerable access points.

Obligations to Provide Notice of Data Breach

The Model Rules of Professional Conduct require that a lawyer must “keep the client reasonably informed about the status of a matter” and “shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”²⁰ Formal Opinion 483 interprets these rules to impose an ethical obligation on a lawyer to communicate with current clients about a data breach.²¹

Current clients are entitled to notification when a data breach occurs that involves, or likely involves, material client

10 *Id.* at 9-10.

11 ABA Comm. on Ethics and Prof’l Responsibility, Formal Op. 483, at 2 (2018) (“ABA Formal Op. 483”).

12 *Id.* at 4. It is important to note that this definition is applicable only to determining whether attorneys have ethical obligations arising out of the applicable ABA Model Rules and Formal Opinions. This definition is not the one that might be applicable should a loss of client information also trigger notification requirements under various state or federal data-breach-response laws.

13 ABA Formal Op. 483 at 5-6.

14 *Id.* at 4-6.

15 *Id.* at 6 (citing Jill D. Rhodes & Robert S. Litt, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals* (2d ed. 2018)).

16 Nat’l Inst. of Standards and Tech., *Computer Security Incident Handling Guide*, at 21-45 (2012), available at nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

17 ABA Formal Op. 483 at 6-7 (citing Steven M. Puiszis, “Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning,” *The Prof’l Lawyer*, Vol. 24, No. 3 (November 2017)).

18 *Id.* at 7.

19 *Id.* at 7-8.

20 Model Rules of Prof’l Conduct R. 1.4(a)(3) and 1.4(b) (2019).

21 ABA Formal Op. 483 at 10-12.

continued on page 64

confidential information.²² Upon disclosing a breach to a client, a lawyer must provide enough information for the client to make an informed decision about what to do next, if anything, with respect to the present representation. This means that a lawyer must disclose to the client not only the occurrence of, but also the extent of, the unauthorized access to or disclosure of the confidential client information. Lawyers should be prepared to advise the client regarding the breach response plan, the efforts being taken to recover the client information, and any additional measures being implemented to increase data security and prevent future breaches.²³

Finally, and apart from ethical obligations, if a data breach involves unauthorized access to PII, whether of clients or others, a lawyer must examine potential notification obligations under various state and federal laws. All 50 states have adopted breach-notification laws, with differing definitions of “protected information” and “breach,” and differing standards for scope and requirements of notice.²⁴

²² As a matter of legal ethics, this notification obligation does not extend to former clients “in the absence of a black-letter provision requiring such notice.” Rather, lawyers are encouraged either to reach a specific agreement with the client about how to handle electronic information post-representation, or to adopt a general document-retention policy to reduce overall the amount of information retained of former clients. ABA Formal Op. 483 at 13.

²³ ABA Formal Op. 483 at 14-15.

²⁴ *Id.* at 15 (citing to Nat'l Conference of State Legislatures, Security Breach Notification Laws (Sept. 29, 2018), available at [ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx](https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx)).

Conclusion

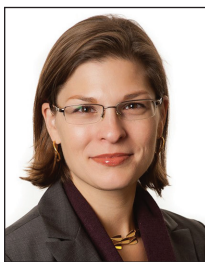
Lawyers are individuals governed by ethical obligations with respect to the confidential information entrusted to them by their clients. However, law firms are businesses, with the goal of making a profit for the partners or shareholders, and the interests of individual lawyers and the businesses they work for can sometimes conflict.

Fortunately, there is great overlap between best business practices and legal ethical obligations with respect to data security. To check both boxes, lawyers and their firms should be very deliberate in creating and implementing an information security program that appropriately protects a firm's most valuable asset: its clients' information and communications. This can only be done if lawyers take the necessary time to familiarize themselves with the technologies they use, implement set standards for how client data will be stored and accessed (through the use of a written information security policy), install preventive measures to protect against breaches, and know what to do if/when a breach occurs (through the use of an incident response plan). Failing to follow this protocol risks inviting otherwise-avoidable liability that can threaten a lawyer's practice and reputation. **abi**

BY ELIZABETH B. VANDESTEEG

Technology and Legal Ethics

Remote Work Considerations (Part III)



Coordinating Editor
Elizabeth B. Vandesteeg
Levenfeld Pearlstein,
LLC; Chicago

Lisa Vandesteeg is a partner in the Financial Services and Restructuring Group of Levenfeld Pearlstein, LLC in Chicago. She is also a Certified Information Privacy Professional for the U.S. Private Sector, as qualified by the International Association of Privacy Professionals. In addition, Ms. Vandesteeg is an associate editor for the ABI Journal and a 2017 ABI "40 Under 40" honoree.

One are the days when attorneys could take an “as needed” approach to technology. The legal industry has long accepted that the pervasive and ever-changing nature of technology — not to mention its many benefits — means it is an integral part of the practice of law. Attorneys also need to understand and adjust the ethical standards that the profession must uphold in order to maintain fundamental protections for their clients and their clients’ information. As discussed in Part I of this series,¹ ethical standards are applicable to all attorneys equally, but they are particularly relevant for bankruptcy attorneys, who are custodians of a host of personally identifiable information (PII) and other sensitive and confidential information. Part II² focused on the specific ethical obligations and practical standards set forth in two recent American Bar Association (ABA) ethics opinions — Formal Opinions 477R³ and 483⁴ — which govern the storage and transmittal of client data, as well as the necessary steps that lawyers and firms must take to protect against, and notify clients of, any unauthorized access to client information.

In Part III, the article will discuss Formal Opinion 498,⁵ the ABA’s most recent ethics opinion, which was released in March 2021. This opinion takes a fresh look at the latest technological advances and changes to the ways that attorneys practice law in a remote-work environment, and provides guidance on how to navigate the heightened cybersecurity risks attorneys face in that remote environment.

Legal Practice and Ethical Obligations Extend Beyond Brick-and-Mortar Offices

Formal Opinion 498 begins by acknowledging that lawyers’ legal practices are not confined to their business offices, nor is there a requirement for them to have a brick-and-mortar office:

A lawyer’s virtual practice often occurs when a lawyer at home or on-the-go is working from a location outside the office, but a lawyer’s practice may be entirely virtual

because there is no requirement in the Model Rules that a lawyer have a brick-and-mortar office. Virtual practice began years ago but has accelerated recently, both because of enhanced technology (and enhanced technology usage by both clients and lawyers) and increased need.

Ethics rules apply regardless of where an attorney practices, whether virtually or not. Given the reality of a largely remote legal industry over the course of the COVID-19 pandemic (and the high likelihood of ongoing remote legal work) the ABA issued Formal Opinion 498 to identify and clarify certain rules that are specifically implicated and especially critical with a virtual office.

Competence, Diligence and Communication

Formal Opinion 498 points to Model Rules 1.1, 1.3 and 1.4,⁶ which address lawyers’ core ethical duties of competence, diligence and communication with their clients, with a reminder that these duties apply regardless of whether interactions are face-to-face or virtual. As mentioned in Part II of this series, Formal Opinion 477R expressly states that it is “beyond the scope” of the ABA Formal Opinion to expressly dictate what may constitute “reasonable steps” to protect client data, but it provides various factors and considerations as guidance. Formal Opinion 498 reiterates that, as noted in Formal Opinion 477R, lawyers must employ a “fact-based analysis” to various factors to “guide lawyers in making a ‘reasonable efforts’ determination.” Formal Opinion 498 also states that “[w]hether interacting face-to-face or through technology, lawyers must ‘reasonably consult with the client about the means by which the client’s objectives are to be accomplished; ... keep the client reasonably informed about the status of the matter; [and] promptly comply with reasonable requests for information....’”⁷ Thus, lawyers should have plans in place to ensure responsibilities regarding competence, diligence, and communication are being fulfilled when practicing virtually.”

Confidentiality

Pursuant to Model Rule 1.6, the obligation of client confidentiality persists regardless of whether

1 Elizabeth B. Vandesteeg, “Technology and Legal Ethics: A User’s Manual (Part I),” XXXIX *ABI Journal* 2, 12, 49-51, February 2020, available at abi.org/abi-journal.

2 Elizabeth B. Vandesteeg, “Technology and Legal Ethics: A User’s Manual (Part II),” XXXIX *ABI Journal* 4, 24-25, 64, April 2020, available at abi.org/abi-journal.

3 See ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017).

4 See ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 (2018).

5 See ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 498 (2021).

6 Model Rules of Prof’l Conduct, R. 1.1, R. 1.3 and R. 1.4.

7 Model Rules of Prof’l Conduct, R. 1.4(a)(2)-(4).

continued on page 48

Cyber-U: Technology and Legal Ethics: Remote Work Considerations

from page 12

an attorney has a physical or virtual legal practice. Formal Opinion 498 reminds attorneys, that “[a]t all times, but especially when practicing virtually, lawyers must fully consider and implement reasonable measures to safeguard confidential information and take reasonable precautions when transmitting such information.”

Supervision

Formal Opinion 498 reiterated that supervising attorneys have an obligation to ensure that attorneys on their team are also abiding by these rules, even in a remote-work environment. This means that attorneys must ensure that paralegals, assistants and other professionals working on client matters have access to technology that safeguards client information. Moreover, attorneys must take steps to oversee the other members of their team to ensure compliance with the rules, use of technological safeguards and proper instruction of the rules and safeguards. Formal Opinion 498 also specifically recommended “routine communication and other interaction ... to discern the health and wellness of the lawyer’s team members.”

Best Practices and Technologies for Use in Virtual Practices

Formal Opinion 477R noted that a “lawyer has a variety of options to safeguard communications, including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network [VPN], or another secure internet portal), using unique complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software.” Formal Opinion 498 specifically addresses some best practices and potential technological solutions that exist in managing virtual practices, including these six avenues.

Technology Systems

Although attorneys might not consider managing technology systems part of their job description, this is simply a required undertaking in a remote-work environment, both as a firm and as individual practitioners. The ethics rules make clear that attorneys (and their firms) have an obligation to carefully review the terms of their hardware and software agreements to ensure that these systems are adequately protecting client confidentiality. Formal Opinion 498 specifically reminds lawyers to take steps to prevent unauthorized access to confidential information, advising lawyers to “be diligent in installing any security-related updates and using strong passwords, antivirus software, and encryption.” While this is a best practice in all circumstances, it is especially important to monitor in the remote-work environment when

firm-owned devices may remain off the controlled network for extended periods of time.

In a remote-work environment, lawyers need to be more vigilant about risks in their home/work environment. Home routers should be secured, and lawyers should consider using VPNs when outside the office network. As technology evolves, updates to these systems might be necessary as well.

The complex relationship between technological advances and the accompanying risks can create a confusing landscape for attorneys, and the unique circumstances of the COVID-19 pandemic have exacerbated these complexities.

Accessing Client Files

Lawyers must take care to use systems that allow them to remotely access client files and protect this information from possible data loss. For many firms and attorneys, a reputable cloud-storage service is the best option, with data regularly backed up and accessible in the event of a data loss. Lawyers and law firms should also have a data-breach policy and communications plan in place should a data loss or breach occur.

In addition, the opinion reiterated Formal Opinion 477R’s clarifications on document and data exchange, stating that “lawyers’ virtual-document and data-exchange platforms should ensure that documents and data are being appropriately archived for later retrieval and that the service or platform is and remains secure. For example, if the lawyer is transmitting information over email, the lawyer should consider whether the information is and needs to be encrypted (both in transit and in storage).”

Virtual Meetings

Many lawyers have relied on virtual meeting platforms, such as Zoom and Microsoft Teams, to meet with clients and team members, especially over the past 12-18 months, while many law firms have operated remotely. Formal Opinion 498 reminds lawyers that access to accounts and meetings should only be through strong passwords, and all recordings and transcripts should be secured and only used with client consent.

Smart Speakers

Attorneys should disable the listening capability of devices or services in the home office, such as smart speakers, virtual assistants and other listening-enabled devices (e.g., Siri and Alexa), while communicating about client matters. This is important to appropriately mitigate against unintended, unauthorized access to attorney/client privileged communications.

Supervision of Technology Use and Virtual Offices

For many attorneys working remotely, a “home office” might be nothing more than a table in a bedroom or kitchen not separated from the rest of the home by a closed door. Nonetheless, attorneys always must be diligent about maintaining privilege and should take care to ensure that client-related meetings and information cannot be overheard or seen by others in the household, office or other remote location, or by other third parties.

Formal Opinion 498 noted that supervision of the firm’s bring-your-own-device policy is particularly important. If lawyers or law firm professionals will be using their own devices “to access, transmit, or store client-related information,” the policy must ensure that security is tight, that a lost or stolen device may be remotely wiped, that client-related information cannot be accessed by others (including family members), and that client-related information will be adequately and safely archived and available for subsequent retrieval.

Technology Vendors and Other Third Parties

Attorneys’ obligation to protect client confidentiality also extends to vendors and third parties. Formal Opinion 498 states that lawyers should consider the use of a confidentiality agreement with their technology vendors and other third-party providers to protect client information. This, again, is a best practice regardless of whether the legal practice is in person or remote.

Limitations on Virtual Legal Practice

Formal Opinion 498 acknowledges that virtual practice and technology have limitations. For example, lawyers must make sure that trust-accounting rules, which vary significantly across states, are followed, regardless of whether they have a virtual legal office. In addition, lawyers and law firms must be able “to write and deposit checks, make electronic transfers, and maintain full trust-accounting records while practicing virtually.” Lawyers should also “make and maintain a plan to process the paper mail, to docket correspondence and communications, and to direct or redirect clients, prospective clients, or other important individuals who might attempt to contact the lawyer at the lawyer’s current or previous brick-and-mortar office.” If a lawyer will not be available at their physical office, there must be signage indicating this information.

Conclusion

The complex relationship between technological advances and the accompanying risks can create a confusing landscape for attorneys, and the unique circumstances of the COVID-19 pandemic have exacerbated these complexities. However, one thing remains certain: Competence in technology cannot simply be outsourced, and attorneys’ ethical obligations cannot be minimized. The Model Rules — and the ABA’s recent opinions — make it clear that attorneys must educate themselves on the ever-changing risks and the benefits of technology. **abi**

Copyright 2021
American Bankruptcy Institute.
Please contact ABI at (703) 739-0800 for reprint permission.

Faculty: Chapter 11 and Cybersecurity: The Inevitable Collision

John G. Loughnane, CIPP is a partner in the Corporate and Transactions Department of Nutter McClennen & Fish LLP in Boston and has more than 25 years of experience focused on growing and restructuring companies. He works with clients entering into business, intellectual property and real estate transactions (such as financings, licensings and acquisitions) to help structure and close durable deals, and he helps clients navigate a range of business obstacles, including issues involving the potential or actual financial distress of other parties. Mr. Loughnane specializes in advising on restructurings, recapitalizations, going-concern sales and liquidations occurring both in and out of court. He has worked with corporate debtors, investors, secured parties, unsecured parties, official creditors' committees, trustees, vendors, licensors/licensees, landlords, employees, officers, directors and buyers. Mr. Loughnane has taken on leadership roles in the American Bar Association (ABA) (Steering Committee member, Legal Technology Resource Center), ABI (co-chair of its Mediation Committee and former co-chair of its Emerging Industries and Technology Committee) and the Turnaround Management Association (TMA) (Trustee of TMA Global and past president of its Northeast Chapter). He is also an active member of the Boston Bar Association and co-chaired its Bankruptcy Section. The impact of the accelerating pace of digital transformation on the important issues of privacy and security led Mr. Loughnane to earn the Certified Information Privacy Professional (CIPP/US) designation from the International Association of Privacy Professionals (IAPP). He speaks and writes regularly on a variety of commercial topics, including dealing effectively with disruption in negotiating, structuring and enforcing deals. Following law school, Mr. Loughnane clerked for Hon. Ronald R. Lagueux of the U.S. District Court for the District of Rhode Island. He is admitted to practice in Massachusetts and New York, and before the U.S. Court of Appeals for the First Circuit and the U.S. Supreme Court. Mr. Loughnane received his A.B. from the College of the Holy Cross and his J.D. with honors from the George Washington University Law School.

Kyle W. Miller is Of Counsel with Dentons in Louisville, Ky., and an attorney in the firm's global Data Privacy and Cybersecurity group. His practice builds on his career as a cybersecurity professional to assist clients with needs related to cybersecurity, data privacy, intellectual property and technology. Mr. Miller counsels clients across all phases of their systems development lifecycle. He drafts and assesses organizations' cybersecurity programs, performing gap and risk assessments under applicable information security frameworks and standards. He also crafts and leads cybersecurity tabletop exercises to test and practice organizations' cybersecurity programs. Mr. Miller drafts and implements data-privacy programs that are compliant with domestic

and global legal regimes. He has experience reviewing and negotiating technology contracts, including data rights and transfer agreements, and he handles trade secret, trademark and other intellectual property disputes. Mr. Miller has experience as cybersecurity incident and disclosure counsel for organizations ranging from small businesses to global corporations. He coordinates with forensic investigators to assist victims of cyberattacks in mitigating and recovering from damage caused by malicious actors, and he crafts regulatory and consumer disclosures related to these cybersecurity incidents as necessary. Prior to law school, Mr. Miller managed network administration and information security for a health care data analytics company, gaining experience in risk-management, data privacy, security-incident response and regulatory compliance. He received his undergraduate degree in political science from the University of Louisville, his M.S. in applied information technology from Bellarmine University, and his J.D. from Vanderbilt University Law School, where he founded the Law and Technology Society. As a law student, Mr. Miller helped plan Nashville's 2nd Annual Data Monetization Conference as well as an award-winning Legal Hackathon. He also clerked for the U.S. Attorney's Office, focusing on the areas of health care fraud, white-collar crime and computer crime prosecution.

Elizabeth B. Vandesteeg, CIPP is a partner in the Financial Services & Restructuring Group at Levenfeld Pearlstein, LLC in Chicago, where she focuses on identifying risk exposure and mitigating liability for clients, with a concentration in the areas of bankruptcy, creditors' rights, commercial litigation, and data security and privacy. She represents secured creditors, debtors, unsecured creditors, creditors' committees, landlords and shareholders in bankruptcy courts throughout U.S., as well as clients in civil litigation in federal and state courts. Her passion is helping clients identify and resolve potential problems related to creditors' rights, troubled businesses, bankruptcy and workouts, and business disputes. Ms. Vandesteeg is a Certified Information Privacy Professional for the U.S. Private Sector by the International Association of Privacy Professionals, and she advises clients on cybersecurity and privacy compliance and regulatory issues. She also guides clients in developing and implementing information security programs that are reasonable and appropriate for their specific business needs and risks, as well as advising them in responding to data breaches, and was instrumental in launching the *ABI Journal's* Cyber U column. Previously, Ms. Vandesteeg was with Sugar Felsenthal Grais & Helsinger LLP, where she was a partner and member of the firm's Executive Committee. She also is a member of ABI's 2017 inaugural class of "40 Under 40." Ms. Vandesteeg received her B.A. from Columbia University and her J.D. from Boston College.

April A. Wimberg is a partner at Dentons Bingham Greenbaum in Louisville, Ky., and has commercial and bankruptcy litigation experience. Her representations include creditors, committees, debtors, trustees and other interested parties involved in litigation arising out of corporate insolvencies. She also has assisted organizations in wind-down operations, serving as a receiver and advisor. Ms. Wimberg has experience obtaining temporary restraining orders, injunctions and writs in matters where assets are at risk of being concealed or diminished. Her representations include a wide array of industries, including coal, hemp, health care, retail, tobacco, manufacturing and

commercial real estate. Prior to joining the firm, Ms. Wimberg spent 10 years working on Wall Street and in corporate strategy for *Fortune* 50 companies, where she gained experience in reviewing loan transactions and identifying business issues in litigation and opportunities with distressed assets. She received her B.A. in political science in 2000 from the University of Kentucky and her J.D. in 2013 from the University of Louisville.