CONTINUING LEGAL EDUCATION

ALBANY LAW SCHOOL
CENTER FOR CONTINUING LEGAL EDUCATION

Legal Ethics in an Age of Technology

January 24, 2022

80 NEW SCOTLAND AVENUE
ALBANY, NEW YORK 12208-3494
TEL: 518-472-5888 FAX: 518-445-2303
WWW.ALBANYLAW.EDU/CLE

Legal Ethics in an Age of Technology

January 24, 2023

Sponsored by:

ALBANY LAW SCHOOL

CENTER FOR CONTINUING LEGAL EDUCATION

and

City of New York
Administrative Judicial Institute

Legal Ethics in the Age of Technology

January 24, 2022

SPEAKER BIOGRAPHY

ANTONY HAYNES Associate Dean for Strategic Initiatives; Director of Cybersecurity and Privacy Law; Associate Professor of Law joined Albany Law School in December 2015. He has extensive litigation experience in the intellectual property, securities, and criminal defense areas.

He served as an associate at the law firm Quinn Emanuel Urquhart & Sullivan, LLP, in Washington, D.C., and before that at Williams & Connolly LLP, in Washington, D.C.

Prior to practicing law, Antony was an Assistant Professor of Computer Science at the U.S. Air Force Academy, where he taught courses in programming, developed the Academy's Information Assurance curriculum, and created the intercollegiate Cyber Defense Exercise. He has extensive experience with a host of software and hardware technologies, including Cisco routers, Motorola microprocessors, TCP/IP networking protocols, SQL databases, and web-based programming. He developed an on-line survey-system for the Department of Epidemiology at a major university.

After the Air Force Academy he was an associate at Chatham Financial Corporation, Capital Markets, Kennett Square, Pa., where he led a company-wide software effort, wrote financial software and coordinated technical developers.

He is a distinguished graduate of the U.S. Air Force Academy, where he was recognized as the top computer science graduate. He received his M.S. in Computer Science from the University of Illinois at Urbana/Champaign, where his thesis focused on machine learning and expert systems.

He is an entrepreneur who leverages his background in computer science, technology, business and the law to advise startup companies. In addition to advising startups, he has spent time acquiring and growing companies.

AWS Customer Agreement | Last Updated: February 25, 2022 | See What's Changed

This AWS Customer Agreement (this "Agreement") contains the terms and conditions that govern your access to and use of the Service Offerings (as defined below) and is an agreement between the applicable AWS Contracting Party specified in Section 14 below (also referred to as "AWS," "we," "us," or "our") and you or the entity you represent ("you" or "your"). This Agreement takes effect when you click an "I Accept" button or check box presented with these terms or, if earlier, when you use any of the Service Offerings (the "Effective Date"). You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into this Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity. Please see Section 14 for definitions of certain capitalized terms used in this Agreement.

1. Use of the Service Offerings.

1.1 Generally. You may access and use the Services in accordance with this Agreement. Service Level Agreements and Service Terms apply to certain Service Offerings. You will comply with the terms of this Agreement and all laws, rules and regulations applicable to your use of the Service Offerings.

1.2 Your Account. To access the Services, you must have an AWS account associated with a valid email address and a valid form of payment. Unless explicitly permitted by the Service Terms, you will only create one account per email address.

1.3 Third-Party Content. Third-Party Content may be used by you at your election. Third-Party Content is governed by this Agreement and, if applicable, separate terms and conditions accompanying such Third-Party Content, which terms and conditions may include separate fees and charges.

2. Changes.

2.1 To the Services. We may change or discontinue any of the Services from time to time. We will provide you at least 12 months' prior notice if we discontinue material functionality of a Service that you are using, or materially alter a customer-facing API that you are using in a backwards-incompatible fashion, except that this notice will not be required if the 12 month notice period (a) would pose a security or intellectual property issue to us or the Services, (b) is economically or technically burdensome, or (c) would cause us to violate legal requirements.

2.2 To the Service Level Agreements. We may change, discontinue or add Service Level Agreements from time to time in accordance with Section 12.

3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. You may specify the AWS regions in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the AWS regions you select. We will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to any government or third party or (b) move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, we will give you notice of any legal requirement or order referred to in this Section 3.2. We will only use your Account Information in accordance with the Privacy Notice, and you consent to such usage. The Privacy Notice does not apply to Your Content.

4. Your Responsibilities.

4.1 Your Accounts. Except to the extent caused by our breach of this Agreement, (a) you are responsible for all activities that occur under your account, regardless of whether the activities are authorized by you or undertaken by you, your employees or a third party (including your contractors, agents or End Users), and (b) we and our affiliates are not responsible for unauthorized access to your account.

4.2 Your Content. You will ensure that Your Content and your and End Users' use of Your Content or the Service Offerings will not violate any of the Policies or any applicable law. You are solely responsible for the development, content, operation, maintenance, and use of Your Content.

4.3 Your Security and Backup. You are responsible for properly configuring and using the Service Offerings and otherwise taking appropriate action to secure, protect and backup your accounts and Your Content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Your Content from unauthorized access and routinely archiving Your Content.

4.4 Log-In Credentials and Account Keys. AWS log-in credentials and private keys generated by the Services are for your internal use only and you will not sell, transfer or sublicense them to any other entity or person, except that you may disclose your private key to your agents and subcontractors performing work on your behalf.

4.5 End Users. You will be deemed to have taken any action that you permit, assist or facilitate any person or entity to take related to this Agreement, Your Content or use of the Service Offerings. You are responsible for End Users' use of Your Content and the Service Offerings. You will ensure that all End Users comply with your obligations under this Agreement and that the terms of your agreement with each End User are consistent with this Agreement. If you become aware of any violation of your obligations under this Agreement caused by an End User, you will immediately suspend access to Your

Content and the Service Offerings by such End User. We do not provide any support or services to End Users unless we have a separate agreement with you or an End User obligating us to provide such support or services.

5. Fees and Payment.

5.1 Service Fees. We calculate and bill fees and charges monthly. We may bill you more frequently for fees accrued if we suspect that your account is fraudulent or at risk of non-payment. You will pay us the applicable fees and charges for use of the Service Offerings as described on the AWS Site using one of the payment methods we support. All amounts payable by you under this Agreement will be paid to us without setoff or counterclaim, and without any deduction or withholding. Fees and charges for any new Service or new feature of a Service will be effective when we post updated fees and charges on the AWS Site, unless we expressly state otherwise in a notice. We may increase or add new fees and charges for any existing Services you are using by giving you at least 30 days' prior notice. We may elect to charge you interest at the rate of 1.5% per month (or the highest rate permitted by law, if less) on all late payments.

5.2 Taxes. Each party will be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that party upon or with respect to the transactions and payments under this Agreement. All fees payable by you are exclusive of Indirect Taxes, except where applicable law requires otherwise. We may charge and you will pay applicable Indirect Taxes that we are legally obligated or authorized to collect from you. You will provide such information to us as reasonably required to determine whether we are obligated to collect Indirect Taxes from you. We will not collect, and you will not pay, any Indirect Tax for which you furnish us a properly completed exemption certificate or a direct payment permit certificate for which we may claim an available exemption from such Indirect Tax. All payments made by you to us under this Agreement will be made free and clear of any deduction or withholding, as may be required by law. If any such deduction or withholding (including but not limited to cross-border withholding taxes) is required on any payment, you will pay such additional amounts as are necessary so that the net amount received by us is equal to the amount then due and payable under this Agreement. We will provide you with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Agreement.

6. Temporary Suspension.

6.1 Generally. We may suspend your or any End User's right to access or use any portion or all of the Service Offerings immediately upon notice to you if we determine:

> (a) your or an End User's use of the Service Offerings (i) poses a security risk to the Service Offerings or any third party, (ii) could adversely impact our systems, the Service Offerings or the systems or Content of any other AWS customer, (iii) could subject us, our affiliates, or any third party to liability, or (iv) could be fraudulent;

(b) you are, or any End User is, in breach of this Agreement;

(c) you are in breach of your payment obligations under Section 5; or

(d) you have ceased to operate in the ordinary course, made an assignment for the benefit of creditors or similar disposition of your assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding.

6.2 Effect of Suspension. If we suspend your right to access or use any portion or all of the Service Offerings:

(a) you remain responsible for all fees and charges you incur during the period of suspension; and

(b) you will not be entitled to any service credits under the Service Level Agreements for any period of suspension.

7. Term; Termination.

7.1 Term. The term of this Agreement will commence on the Effective Date and will remain in effect until terminated under this Section 7. Any notice of termination of this Agreement by either party to the other must include a Termination Date that complies with the notice periods in Section 7.2.

7.2 Termination.

(a) Termination for Convenience. You may terminate this Agreement for any reason by providing us notice and closing your account for all Services for which we provide an account closing mechanism. We may terminate this Agreement for any reason by providing you at least 30 days' advance notice.

(b) Termination for Cause.

(i) By Either Party. Either party may terminate this Agreement for cause if the other party is in material breach of this Agreement and the material breach remains uncured for a period of 30 days from receipt of notice by the other party. No later than the Termination Date, you will close your account.

(ii) By Us. We may also terminate this Agreement immediately upon notice to you (A) for cause if we have the right to suspend under Section 6, (B) if our relationship with a third-party partner who provides software or other technology we use to provide the Service Offerings expires, terminates or requires us to change the way we provide the software or other technology as part of the Services, or (C) in order to comply with the law or requests of governmental entities.

7.3 Effect of Termination.

(a) Generally. Upon the Termination Date:

(i) except as provided in Section 7.3(b), all your rights under this Agreement immediately terminate;

(ii) you remain responsible for all fees and charges you have incurred through the Termination Date and are responsible for any fees and charges you incur during the post-termination period described in Section 7.3(b);

(iii) you will immediately return or, if instructed by us, destroy all AWS Content in your possession; and

(iv) Sections 4.1, 5, 7.3, 8 (except Section 8.3), 9, 10, 11, 13 and 14 will continue to apply in accordance with their terms.

(b) Post-Termination. Unless we terminate your use of the Service Offerings pursuant to Section 7.2(b), during the 30 days following the Termination Date:

(i) we will not take action to remove from the AWS systems any of Your Content as a result of the termination; and

(ii) we will allow you to retrieve Your Content from the Services only if you have paid all amounts due under this Agreement.

For any use of the Services after the Termination Date, the terms of this Agreement will apply and you will pay the applicable fees at the rates under Section 5.

8. Proprietary Rights.

8.1 Your Content. Except as provided in this Section 8, we obtain no rights under this Agreement from you (or your licensors) to Your Content. You consent to our use of Your Content to provide the Service Offerings to you and any End Users.

8.2 Adequate Rights. You represent and warrant to us that: (a) you or your licensors own all right, title, and interest in and to Your Content and Suggestions; (b) you have all rights in Your Content and Suggestions necessary to grant the rights contemplated by this Agreement; and (c) none of Your Content or End Users' use of Your Content or the Service Offerings will violate the Acceptable Use Policy.

8.3 Intellectual Property License. The Intellectual Property License applies to your use of AWS Content and the Services.

8.4 Restrictions. Neither you nor any End User will use the Service Offerings in any manner or for any purpose other than as expressly permitted by this Agreement. Neither you nor any End User will, or will attempt to (a) reverse engineer, disassemble, or decompile the Services or AWS Content or apply any other process or procedure to derive the source code of any software included in the Services or AWS Content (except to the extent applicable law doesn't allow this restriction), (b) access or use the Services or AWS Content in a way intended to avoid incurring fees or exceeding usage limits or quotas, or (c) resell the Services or AWS Content. The AWS Trademark Guidelines apply to your use of the AWS Marks. You will not misrepresent or embellish

the relationship between us and you (including by expressing or implying that we support, sponsor, endorse, or contribute to you or your business endeavors). You will not imply any relationship or affiliation between us and you except as expressly permitted by this Agreement.

8.5 Suggestions. If you provide any Suggestions to us or our affiliates, we and our affiliates will be entitled to use the Suggestions without restriction. You hereby irrevocably assign to us all right, title, and interest in and to the Suggestions and agree to provide us any assistance we require to document, perfect, and maintain our rights in the Suggestions.

9. Indemnification.

9.1 General. You will defend, indemnify, and hold harmless us, our affiliates and licensors, and each of their respective employees, officers, directors, and representatives from and against any Losses arising out of or relating to any third-party claim concerning: (a) your or any End Users' use of the Service Offerings (including any activities under your AWS account and use by your employees and personnel); (b) breach of this Agreement or violation of applicable law by you, End Users or Your Content; or (c) a dispute between you and any End User. You will reimburse us for reasonable attorneys' fees, as well as our employees' and contractors' time and materials spent responding to any third party subpoena or other compulsory legal order or process associated with third party claims described in (a) through (c) above at our then-current hourly rates.

9.2 Intellectual Property.

(a) Subject to the limitations in this Section 9, AWS will defend you and your employees, officers, and directors against any third-party claim alleging that the Services infringe or misappropriate that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(b) Subject to the limitations in this Section 9, you will defend AWS, its affiliates, and their respective employees, officers, and directors against any third-party claim alleging that any of Your Content infringes or misappropriates that third party's intellectual property rights, and will pay the amount of any adverse final judgment or settlement.

(c) Neither party will have obligations or liability under this Section 9.2 arising from infringement by combinations of the Services or Your Content, as applicable, with any other product, service, software, data, content or method. In addition, AWS will have no obligations or liability arising from your or any End User's use of the Services after AWS has notified you to discontinue such use. The remedies provided in this Section 9.2 are the sole and exclusive remedies for any third-party claims of infringement or misappropriation of intellectual property rights by the Services or by Your Content.

(d) For any claim covered by Section 9.2(a), AWS will, at its election, either: (i) procure the rights to use that portion of the Services alleged to be infringing; (ii) replace the alleged infringing portion of the Services with a non-infringing alternative; (iii) modify the alleged infringing portion of the Services to make it non-infringing; or (iv) terminate the allegedly infringing portion of the Services or this Agreement.

9.3 Process. The obligations under this Section 9 will apply only if the party seeking defense or indemnity: (a) gives the other party prompt written notice of the claim; (b) permits the other party to control the defense and settlement of the claim; and (c) reasonably cooperates with the other party (at the other party's expense) in the defense and settlement of the claim. In no event will a party agree to any settlement of any claim that involves any commitment, other than the payment of money, without the written consent of the other party.

10. Disclaimers.

THE SERVICE OFFERINGS ARE PROVIDED "AS IS." EXCEPT TO THE EXTENT PROHIBITED BY LAW, OR TO THE EXTENT ANY STATUTORY RIGHTS APPLY THAT CANNOT BE EXCLUDED, LIMITED OR WAIVED, WE AND OUR AFFILIATES AND LICENSORS (A) MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR THE THIRD-PARTY CONTENT, AND (B) DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED OR EXPRESS WARRANTIES (I) OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, (II) ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, (III) THAT THE SERVICE OFFERINGS OR THIRD-PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, AND (IV) THAT ANY CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR ALTERED.

11. Limitations of Liability.

WE AND OUR AFFILIATES AND LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICE OFFERINGS, OR, (III) WITHOUT LIMITING ANY OBLIGATIONS UNDER THE SERVICE LEVEL AGREEMENTS, ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; (B) THE COST OF

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF OR ACCESS TO THE SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, EXCEPT FOR PAYMENT OBLIGATIONS UNDER SECTION 9.2, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY UNDER THIS AGREEMENT WILL NOT EXCEED THE AMOUNT YOU ACTUALLY PAY US UNDER THIS AGREEMENT FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE. THE LIMITATIONS IN THIS SECTION 11 APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

12. Modifications to the Agreement.

We may modify this Agreement (including any Policies) at any time by posting a revised version on the AWS Site or by otherwise notifying you in accordance with Section 13.10; provided, however, that we will provide at least 90 days' advance notice in accordance with Section 13.10 for adverse changes to any Service Level Agreement. Subject to the 90 day advance notice requirement with respect to adverse changes to Service Level Agreements, the modified terms will become effective upon posting or, if we notify you by email, as stated in the email message. By continuing to use the Service Offerings after the effective date of any modifications to this Agreement, you agree to be bound by the modified terms. It is your responsibility to check the AWS Site regularly for modifications to this Agreement. We last modified this Agreement on the date listed at the end of this Agreement.

13. Miscellaneous.

13.1 Assignment. You will not assign or otherwise transfer this Agreement or any of your rights and obligations under this Agreement, without our prior written consent. Any assignment or transfer in violation of this Section 13.1 will be void. We may assign this Agreement without your consent (a) in connection with a merger, acquisition or sale of all or substantially all of our assets, or (b) to any affiliate or as part of a corporate reorganization; and effective upon such assignment, the assignee is deemed substituted for AWS as a party to this Agreement and AWS is fully released from all of its obligations and duties to perform under this Agreement. Subject to the foregoing, this Agreement will be binding upon, and inure to the benefit of the parties and their respective permitted successors and assigns.

13.2 Entire Agreement. This Agreement incorporates the Policies by reference and is the entire agreement between you and us regarding the subject matter of this Agreement. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between you and us, whether written or verbal, regarding the subject matter of this Agreement (but does not supersede prior commitments to purchase Services such as Amazon EC2 Reserved Instances). We will not be bound by, and specifically object to, any term, condition or other provision that is

different from or in addition to the provisions of this Agreement (whether or not it would materially alter this Agreement) including for example, any term, condition or other provision (a) submitted by you in any order, receipt, acceptance, confirmation, correspondence or other document, (b) related to any online registration, response to any Request for Bid, Request for Proposal, Request for Information, or other questionnaire, or (c) related to any invoicing process that you submit or require us to complete. If the terms of this document are inconsistent with the terms contained in any Policy, the terms contained in this document will control, except that the Service Terms will control over this document.

13.3 Force Majeure. We and our affiliates will not be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, electrical or power outages, utilities or other telecommunications failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

13.4 Governing Law. The Governing Laws, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between you and us. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

13.5 Disputes. Any dispute or claim relating in any way to your use of the Service Offerings, or to any products or services sold or distributed by AWS will be adjudicated in the Governing Courts, and you consent to exclusive jurisdiction and venue in the Governing Courts, subject to the additional provisions below.

> (a) If the applicable AWS Contracting Party is Amazon Web Services, Inc., Amazon Web Services Canada, Inc., Amazon Web Services Korea LLC or Amazon Web Services Singapore Private Limited, the parties agree that the provisions of this Section 13.5(a) will apply. Disputes will be resolved by binding arbitration, rather than in court, except that you may assert claims in small claims court if your claims qualify. The Federal Arbitration Act and federal arbitration law apply to this Agreement, except that if Amazon Web Services Canada, Inc. is the applicable AWS Contracting Party the Ontario Arbitration Act will apply to this Agreement. There is no judge or jury in arbitration, and court review of an arbitration award is limited. However, an arbitrator can award on an individual basis the same damages and relief as a court (including injunctive and declaratory relief or statutory damages), and must follow the terms of this Agreement as a court would. To begin an arbitration proceeding, you must send a letter requesting arbitration and describing your claim to our registered agent Corporation Service Company, 300 Deschutes Way SW, Suite 304, Tumwater, WA 98501. The arbitration will be conducted by the American Arbitration Association (AAA) under its rules, which are available at www.adr.org or by calling 1-800-778-7879. Payment of filing, administration and arbitrator fees will be governed by the AAA's rules. We will reimburse those fees for claims totaling less than $10,000 unless the arbitrator determines the claims are frivolous. We will not seek attorneys' fees

and costs in arbitration unless the arbitrator determines the claims are frivolous. You may choose to have the arbitration conducted by telephone, based on written submissions, or at a mutually agreed location. We and you agree that any dispute resolution proceedings will be conducted only on an individual basis and not in a class, consolidated or representative action. If for any reason a claim proceeds in court rather than in arbitration we and you waive any right to a jury trial. Notwithstanding the foregoing we and you both agree that you or we may bring suit in court to enjoin infringement or other misuse of intellectual property rights.

(b) If the applicable AWS Contracting Party is Amazon Web Services South Africa Proprietary Limited, the parties agree that the provisions of this Section 13.5(b) will apply. Disputes will be resolved by arbitration in accordance with the then-applicable rules of the Arbitration Foundation of Southern Africa, and judgment on the arbitral award must be entered in the Governing Court. The Arbitration Act, No. 42 of 1965 applies to this Agreement. The arbitration will take place in Johannesburg. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties.

(c) If the applicable AWS Contracting Party is Amazon AWS Serviços Brasil Ltda., the parties agree that the provisions of this Section 13.5(c) will apply. Disputes will be resolved by binding arbitration, rather than in court, in accordance with the then-applicable Rules of Arbitration of the International Chamber of Commerce, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in the City of São Paulo, State of São Paulo, Brazil. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information. The Governing Courts will have exclusive jurisdiction for the sole purposes of (i) ensuring the commencement of the arbitral proceedings; and (ii) granting conservatory and interim measures prior to the constitution of the arbitral tribunal.

(d) If the applicable AWS Contracting Party is Amazon Web Services Australia Pty Ltd, the parties agree that the provisions of this Section 13.5(d) will apply. Disputes will be resolved by arbitration administered by the Australian Center for International Commercial Arbitration (“ACICA”) in accordance with the then-applicable ACICA Arbitration Rules, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in Sydney, Australia. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information.

(e) If the applicable AWS Contracting Party is Amazon Web Services New Zealand Limited, the parties agree that the provisions of this Section 13.5(e) will apply. Disputes will be resolved by arbitration administered by the New Zealand Dispute Resolution Centre ("NZDRC") in accordance with the then-applicable Arbitration Rules of NZDRC, and judgment on the arbitral award may be entered in any court having jurisdiction. The arbitration will take place in Auckland, New Zealand. There will be three arbitrators. The fees and expenses of the arbitrators and the administering authority, if any, will be paid in equal proportion by the parties. The parties agree that the existence of and information relating to any such arbitration proceedings will not be disclosed by either party and will constitute confidential information.

13.6 Trade Compliance. In connection with this Agreement, each party will comply with all applicable import, re-import, sanctions, anti-boycott, export, and re-export control laws and regulations, including all such laws and regulations that apply to a U.S. company, such as the Export Administration Regulations, the International Traffic in Arms Regulations, and economic sanctions programs implemented by the Office of Foreign Assets Control. For clarity, you are solely responsible for compliance related to the manner in which you choose to use the Service Offerings, including your transfer and processing of Your Content, the provision of Your Content to End Users, and the AWS region in which any of the foregoing occur. You represent and warrant that you and your financial institutions, or any party that owns or controls you or your financial institutions, are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the Specially Designated Nationals List and Foreign Sanctions Evaders List of the U.S. Department of Treasury, and the Entity List of the U.S. Department of Commerce), the European Union or its Member States, or other applicable government authority.

13.7 Independent Contractors; Non-Exclusive Rights. We and you are independent contractors, and this Agreement will not be construed to create a partnership, joint venture, agency, or employment relationship. Neither party, nor any of their respective affiliates, is an agent of the other for any purpose or has the authority to bind the other. Both parties reserve the right (a) to develop or have developed for it products, services, concepts, systems, or techniques that are similar to or compete with the products, services, concepts, systems, or techniques developed or contemplated by the other party, and (b) to assist third party developers or systems integrators who may offer products or services which compete with the other party's products or services.

13.8 Language. All communications and notices made or given pursuant to this Agreement must be in the English language. If we provide a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

13.9 Confidentiality and Publicity. You may use AWS Confidential Information only in connection with your use of the Service Offerings as permitted under this Agreement. You will not disclose AWS Confidential Information during the Term or at any time

during the 5-year period following the end of the Term. You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of AWS Confidential Information, including, at a minimum, those measures you take to protect your own confidential information of a similar nature. You will not issue any press release or make any other public communication with respect to this Agreement or your use of the Service Offerings.

13.10 Notice.

(a) To You. We may provide any notice to you under this Agreement by: (i) posting a notice on the AWS Site; or (ii) sending a message to the email address then associated with your account. Notices we provide by posting on the AWS Site will be effective upon posting and notices we provide by email will be effective when we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address then associated with your account when we send the email, whether or not you actually receive the email.

(b) To Us. To give us notice under this Agreement, you must contact AWS by facsimile transmission or personal delivery, overnight courier or registered or certified mail to the facsimile number or mailing address, as applicable, listed for the applicable AWS Contracting Party in Section 14 below. We may update the facsimile number or address for notices to us by posting a notice on the AWS Site. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided registered or certified mail will be effective three business days after they are sent.

13.11 No Third-Party Beneficiaries. Except as set forth in Section 9, this Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to this Agreement.

13.12 U.S. Government Rights. The Service Offerings are provided to the U.S. Government as “commercial items,” “commercial computer software,” “commercial computer software documentation,” and “technical data” with the same rights and restrictions generally applicable to the Service Offerings. If you are using the Service Offerings on behalf of the U.S. Government and these terms fail to meet the U.S. Government’s needs or are inconsistent in any respect with federal law, you will immediately discontinue your use of the Service Offerings. The terms “commercial item” “commercial computer software,” “commercial computer software documentation,” and “technical data” are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

13.13 No Waivers. The failure by us to enforce any provision of this Agreement will not constitute a present or future waiver of such provision nor limit our right to enforce such provision at a later time. All waivers by us must be in writing to be effective.

13.14 Severability. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect. Any invalid or unenforceable portions will be interpreted to effect and intent of the original portion. If such construction is not possible, the invalid or unenforceable portion will be severed from this Agreement but the rest of the Agreement will remain in full force and effect.

13.15 Account Country Specific Terms. You agree to the following modifications to the Agreement that apply to your AWS Contracting Party as described below:

(a) If the applicable AWS Contracting Party is Amazon Web Services Australia Pty Ltd, the parties agree as follows:

If the Services are subject to any statutory guarantees under the Australian Competition and Consumer Act 2010, then to the extent that any part of this Agreement is unenforceable under such Act, you agree that a fair and reasonable remedy to you will be limited to, at our election, either: (i) supplying the Services again; or (ii) paying for the cost of having the Services supplied again.

(b) If the applicable AWS Contracting Party is Amazon Web Services Japan G.K., the parties agree as follows:

(i) The following sentence is added at the end of Section 8.5 (Suggestions):

“The foregoing assignment includes the assignment of the rights provided under Article 27 (Rights of Translation, Adaptation, etc.) and Article 28 (Right of the Original Author in the Exploitation of a Derivative Work) of the Copyright Act of Japan, and you agree not to exercise your moral rights against us, our affiliates or persons who use the Suggestions through the consent of us or our affiliates.”

(ii) The following sentences are added at the end of Section 11 (Limitation of Liability):

“THE DISCLAIMER OR THE DAMAGES CAP IN THIS SECTION MAY NOT BE APPLIED TO DAMAGES CAUSED BY EITHER PARTY’S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT IF SUCH DISCLAIMER OR THE DAMAGES CAP ARE DEEMED AGAINST PUBLIC POLICY UNDER ARTICLE 90 OF THE CIVIL CODE. IN THAT EVENT, THE SCOPE OF THE DISCLAIMER SHALL BE NARROWLY CONSTRUED IN SUCH MANNER AND THE DAMAGES CAP MAY BE INCREASED BY SUCH MINIMUM AMOUNT SO THAT THE DISCLAIMER OR THE DAMAGES CAP HEREUNDER WOULD NOT BE DEEMED AGAINST PUBLIC POLICY UNDER ARTICLE 90 OF THE CIVIL CODE.”

14. Definitions.

“Acceptable Use Policy” means the policy located at http://aws.amazon.com/aup (and any successor or related locations designated by us), as it may be updated by us from time to time.

“Account Country” is the country associated with your account. If you have provided a valid tax registration number for your account, then your Account Country is the country associated with your tax registration. If you have not provided a valid tax registration, then your Account Country is the country where your billing address is located, except if you have a credit card associated with your AWS account that is issued in a different country and your contact address is also in that country, then your Account Country is that different country.

“Account Information” means information about you that you provide to us in connection with the creation or administration of your AWS account. For example, Account Information includes names, usernames, phone numbers, email addresses and billing information associated with your AWS account.

“API” means an application program interface.

“AWS Confidential Information” means all nonpublic information disclosed by us, our affiliates, business partners or our or their respective employees, contractors or agents that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential. AWS Confidential Information includes: (a) nonpublic information relating to our or our affiliates or business partners’ technology, customers, business plans, promotional and marketing activities, finances and other business affairs; (b) third-party information that we are obligated to keep confidential; and (c) the nature, content and existence of any discussions or negotiations between you and us or our affiliates. AWS Confidential Information does not include any information that: (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been known to you at the time of your receipt from us; (iii) is received from a third party who did not acquire or disclose the same by a wrongful or tortious act; or (iv) can be shown by documentation to have been independently developed by you without reference to the AWS Confidential Information.

“AWS Content” means Content we or any of our affiliates make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; Documentation; sample code; software libraries; command line tools; proofs of concept; templates; and other related technology (including any of the foregoing that are provided by our personnel). AWS Content does not include the Services or Third-Party Content.

"AWS Contracting Party" means the party identified in the table below, based on your Account Country. If you change your Account Country to one identified to a different AWS Contracting Party below, you agree that this Agreement is then assigned to the new AWS Contracting Party under Section 13.1 without any further action required by either party.

Account Country	AWS Contracting Party	Facsimile	Mailing Address

Australia	Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	N/A	Level 37, 2-26 Park NSW, 2000, Austra
Brazil*	Amazon AWS Serviços Brasil Ltda.	N/A	A. Presidente Jusce 2.041, Torre E - 18 Floors, Vila Nova C Paulo, Brasil
Canada	Amazon Web Services Canada, Inc.	N/A	120 Bremner Blvd, Toronto, Ontario, M
Japan	Amazon Web Services Japan G.K.	N/A	1-1, Kamiosaki 3-c Shinagawa-ku, Tok Japan
New Zealand	Amazon Web Services New Zealand Limited	N/A	Level 5, 18 Viaduct Auckland, 1010, Ne
Singapore	Amazon Web Services Singapore Private Limited	N/A	23 Church Street, # Singapore 049481
South Africa	Amazon Web Services South Africa Proprietary Limited	206-266-7010	Wembley Square 2, Road, Gardens, Cap South Africa
South Korea	Amazon Web Services Korea LLC	N/A	L12, East tower, 23 Gangnam-gu, Seou Republic of Korea
Any country within Europe, the Middle East, or Africa (excluding South Africa) ("EMEA")**	Amazon Web Services EMEA SARL	352 2789 0057	38 Avenue John F. 1855, Luxembourg
Any country that is not listed in this table above.	Amazon Web Services, Inc.	206-266-7010	410 Terry Avenue N Seattle, WA 98109- U.S.A.

*Brazil is your Account Country only if you have provided a valid Brazilian Tax Registration Number (CPF/CNPJ number) for your account. If your billing address is located in Brazil but you have not provided a valid Brazilian Tax Registration Number (CPF/CNPJ number), then Amazon Web Services, Inc. is the AWS Contracting Party for your account.

**See https://aws.amazon.com/legal/aws-emea-countries for a full list of EMEA countries.

“AWS Marks” means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its affiliates that we may make available to you in connection with this Agreement.

“AWS Site” means http://aws.amazon.com (and any successor or related site designated by us), as may be updated by us from time to time.

“AWS Trademark Guidelines” means the guidelines and trademark license located at http://aws.amazon.com/trademark-guidelines/ (and any successor or related locations designated by us), as they may be updated by us from time to time.

“Content” means software (including machine images), data, text, audio, video or images.

“Documentation” means the user guides and admin guides (in each case exclusive of content referenced via hyperlink) for the Services located at http://aws.amazon.com/documentation (and any successor or related locations designated by us), as such user guides and admin guides may be updated by AWS from time to time.

“End User” means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account. The term “End User” does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than under your account.

"Governing Laws" and “Governing Courts” mean, for each AWS Contracting Party, the laws and courts set forth in the following table:

AWS Contracting Party	Governing Laws	Governing Courts
Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891)	The laws of New South Wales	The courts of New So
Amazon AWS Serviços Brasil Ltda.	The laws of Brazil	The courts of the City State of São Paulo
Amazon Web Services Canada, Inc.	The laws of the Province of Ontario, Canada and federal laws of Canada applicable therein.	The provincial or fede located in Toronto, O
Amazon Web Services EMEA SARL	The laws of the Grand Duchy of Luxembourg	The courts in the distr Luxembourg City
Amazon Web Services, Inc.	The laws of the State of Washington	The state or Federal c County, Washington
Amazon Web Services Japan G.K.	The laws of Japan	The Tokyo District C

Amazon Web Services Korea LLC	The laws of the State of Washington	The state or Federal c County, Washington
Amazon Web Services New Zealand Limited	The laws of New Zealand	The courts of New Ze
Amazon Web Services Singapore Private Limited	The laws of the State of Washington	The state or Federal c County, Washington
Amazon Web Services South Africa Proprietary Limited	The laws of the Republic of South Africa	The South Gauteng H Johannesburg

"Indirect Taxes" means applicable taxes and duties, including, without limitation, VAT, Service Tax, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

"Intellectual Property License" means the separate license terms that apply to your access to and use of AWS Content and Services located at https://aws.amazon.com/legal/aws-ip-license-terms (and any successor or related locations), as may be updated from time to time.

"Losses" means any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees).

"Policies" means the Acceptable Use Policy, Privacy Notice, the Site Terms, the Service Terms, the AWS Trademark Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into this Agreement, but does not include whitepapers or other marketing materials referenced on the AWS Site.

"Privacy Notice" means the privacy notice located at http://aws.amazon.com/privacy (and any successor or related locations designated by us), as it may be updated by us from time to time.

"Service" means each of the services made available by us or our affiliates, including those web services described in the Service Terms. Services do not include Third-Party Content.

"Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time. The service level agreements we offer with respect to the Services are located at https://aws.amazon.com/legal/service-level-agreements/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time.

“Service Offerings” means the Services (including associated APIs), the AWS Content, the AWS Marks, and any other product or service provided by us under this Agreement. Service Offerings do not include Third-Party Content.

“Service Terms” means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms (and any successor or related locations designated by us), as may be updated by us from time to time.

“Site Terms” means the terms of use located at http://aws.amazon.com/terms/ (and any successor or related locations designated by us), as may be updated by us from time to time.

“Suggestions” means all suggested improvements to the Service Offerings that you provide to us.

“Term” means the term of this Agreement described in Section 7.1.

“Termination Date” means the effective date of termination provided in accordance with Section 7, in a notice from one party to the other.

“Third-Party Content” means Content made available to you by any third party on the AWS Site or in conjunction with the Services.

“Your Content” means Content that you or any End User transfers to us for processing, storage or hosting by the Services in connection with your AWS account and any computational results that you or any End User derive from the foregoing through their use of the Services. For example, Your Content includes Content that you or any End User stores in Amazon Simple Storage Service. Your Content does not include Account Information.

The Ethical Duties of Technology Competence and Reasonable (Cyber) Security

The rapidly evolving area of cybersecurity means that many attorneys can no longer take an ostrich-like approach to data breaches. Simply hoping an incident never happens in your practice is no longer realistic when two-thirds of law firms have suffered data breaches.[1] Even major law firms like Cravath and Weil Gotshal have suffered significant compromises of client data.[2] The massive data breach of Panamanian law firm Mossack Fonesca resulted in the exposure of hundreds of wealthy clients' tax avoidance schemes to international scrutiny.[3] The American Bar Association (ABA) and state bar associations have also created ethical guidelines requiring each attorney have technological competence and maintain reasonable (cyber) security. Attorneys should be extremely concerned that they have not taken adequate steps to establish their technology competence and reasonable security because they could face reputation damage, legal malpractice and negligence claims, and fines and sanctions for client data breaches.

I. Ethical Duty of Technology Competence

A majority of states, including New York, have adopted an attorney ethical duty of technology competence.[4] The foundation of an attorney's duty of competence lies in Rule 1.1, which has stated since 1983 that "[a] lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[5] In 2015, New York adopted Comment [8] to Rule 1.1, which clarifies that the scope of the duty of competence includes technology: "To maintain the requisite knowledge and skill, a lawyer should . . . *keep abreast of the benefits and risks associated with technology* the lawyer uses to provide services to clients or to store or transmit confidential information . . . ." (emphasis added).[6]

Antony K. Haynes
Albany Law School
Associate Dean For
Strategic Initiatives And
Information Systems
Executive Director Shaffer
Law Library
Director Cybersecurity &
Privacy Law
Assistant Professor Of Law
ahaynes@albanylaw.edu

Practicing attorneys have faced difficulties demonstrating basic competency in respect to technology and these difficulties have led to unfavorable outcomes for their clients. For example, one law firm inadvertently posted a link to a client's Claims File to the internet, leading the magistrate judge in the case to waive any attorney-client privilege or work-product protection over information contained in the file.[7] In another matter, an attorney did not understand that e-discovery software could not show more than a limited number of records on a single computer screen and as a result inadvertently produced documents containing the financial records of tens of thousands of Wells Fargo's customers.[8] These cases illustrate the basic principle that attorneys have a duty to understand how the technology they use works.

Nevertheless, it can be difficult to determine what constitutes a minimum standard of care for technology competence. One suggestion is that technology competence includes facility with performing basic Microsoft Word processing tasks. Attorneys may wish to assess whether the legal practitioners in their office are able to accept/turn-off track changes, cut & paste, replace text, format fonts and paragraphs, fix footers, insert hyperlinks, apply/modify styles, insert/update cross-references, insert page breaks, insert non-breaking spaces, clean document properties; and create comparison documents (i.e., a redline).[9] Beyond this, maintaining technology competence requires attorneys to have a colleague, staff member of consultant to help the attorney "keep abreast of the benefits and risks associated with technology."[10]

II. Ethical Duty of Reasonable (Cyber) Security

Applying technology competence to client confidentiality results in an attorney ethical duty of reasonable (cyber) security. While New York courts have not yet adopted ABA Model Rule 1.6 Comment [18], there is an emerging standard for what constitutes reasonable cyber security. This emerging standard requires attorneys demonstrate "reasonable efforts" by applying several non-exclusive factors as well as to take certain minimal steps for cybersecurity. Attorneys can also look to industry standards, such as those put forth by the Center for Internet Security (CIS) Critical Security Controls for a standard for reasonable cyber security.

A. Rule 1.6 Commentary

Under both New York and the Model Rule 1.6(c), a lawyer must act competently to protect client confidential information and both the New York and ABA versions of Rule 1.6 apply a "reasonableness" standard.[11] The ABA has indicated that a data breach in and of itself does not constitute a violation of Rule 1.6(c)'s requirement to preserve client confidences as long as "the lawyer has made reasonable efforts to prevent access or disclosure."[12] Attorneys should consider, in making a reasonableness determination, several factors:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards

THE ETHICAL DUTIES OF TECHNOLOGY COMPETENCE AND REASONABLE (CYBER) SECURITY (continued)

Continued from page 14

adversely affect the lawyer's ability to represent clients.[13]

In Comments to its version of Rule 1.6, Virginia has emphasized that "[p]erfect online security and data protection is not attainable. … What is 'reasonable' is determined in part by the size of the firm."[14] Furthermore, attorneys should review and address several practices:

- Periodic staff security training and evaluation programs, including precautions and procedures regarding data security;
- Policies to address departing employee's future access to confidential firm data and return of electronically stored confidential data;
- Procedures addressing security measures for access of third parties to stored information;
- Procedures for both the backup and storage of firm data and steps to securely erase or wipe electronic data from computing devices before they are transferred, sold, or reused;
- The use of strong passwords or other authentication measures to log on to their network, and the security of password and authentication measures; and
- The use of hardware and/or software measures to prevent, detect and respond to malicious software and activity.[15]

B. Industry Standards

Along with the Rule 1.6 commentary, a good place to start with establishing reasonable cybersecurity is the CIS controls. In 2016, California listed these controls as a minimum standard of care for reasonable cyber security for companies doing business in California.[16] CIS has indicated that the first five controls will "[e]liminate the vast majority of your organization's vulnerabilities":

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Security Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Continuous Vulnerability Assessment and Remediation
- Controlled Use of Administrative Privileges.[17]

While the legal profession is still coming to grips with the impact of technology on legal practice, Albany Law School (ALS) stands at the forefront of helping educate and train attorneys to gain technology competence and establish reasonable cybersecurity. ALS offers seminars, courses, certificates and degree programs around technology and innovation, including the nation's first fully online LLM specializing in cybersecurity and data privacy. Courses offered online include cybersecurity law and policy, cyberspace law, privacy law, cybersecurity frameworks, cybercrime, cyber war, global data protection, supply chain cybersecurity, and healthcare compliance. Upcoming Albany County Bar Association (ACBA) CLEs offered by ALS will address the intersection of technology and the law, including the ethical duties of technology competence and reasonable security. ●

Antony K. Haynes is an Associate Dean and Assistant Professor at Albany Law School, where he directs the Cybersecurity and Privacy Law Program. Email him at ahayn@albanylaw.edu.

1 *Law Firm Cyber Security Scorecard* – Q1 2017, LogicForce 7 (2017), http://marketing.logicforce.com/acton/attachment/21751/f-0058/1/-/-/-/-/lf_cyber_security_scorecard_060317.pdf.

2 Nicole Hong and Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, Wall St. J. (Mar. 29, 2016, 9:14 AM), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

3 Julie Sobowale, 6 *Major Law Firm Hacks in Recent History*, A.B.A. J. (Mar. 2017), http://www.abajournal.com/magazine/article/law_firm_hacking_history.

4 Robert Ambrogi, *28 States Have Adopted Ethical Duty of Technology Competence*, LawSites (last updated Sept. 5, 2017), https://www.lawsites-blog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html.

5 N.Y. Rules of Prof'l Conduct r. 1.1(a) (amended 2017).

6 *Id.* at cmt. 8.

7 Harleysville Ins. Co. v. Holding Funeral Home, Inc., No. 1:15CV00057, 2017 WL 1041600, at *8 (W.D. Va. Feb. 9, 2017) (finding "the posting of the Claims File to the internet waived any attorney-client privilege or any work-product protection over the information contained in the file"), objections sustained in part and overruled in part, No. 1:15CV00057, 2017 WL 4368617 (W.D. Va. Oct. 2, 2017) (reversing the relevant findings of the magistrate judge and finding no waiver of attorney-client privilege or of any work-product protection).

8 Christine Simmons, *Lawyer's 'Inadvertent' E-Discovery Failures Led to Wells Fargo Data Breach*, Law.com (Jul. 26, 2017, 7:13 PM), https://www.law.com/sites/almstaff/2017/07/26/lawyers-inadvertent-e-discovery-failures-led-to-wells-fargo-data-breach/.

9 *What Is The Legal Technology Assessment?* Procertas, https://www.procertas.com/offerings/legal-technology-assessment/ (last visited Jan. 19, 2018). Simply assuming that younger attorneys will automatically understand technology is not an effective strategy as one one-third of law students could perform these word-processing tasks on their first attempt. Darth Vaughn and Casey Flaherty, *Tech Comes Naturally to 'Digital Native' Millennials? That's a Myth*, A.B.A. J. (Oct. 13, 2016, 8:30 AM), http://www.abajournal.com/legalrebels/article/tech_comes_naturally_to_digital_native_millennials_thats_a_myth.

10 *See*, e.g., Va Rules of Prof'l Conduct r. 1.6(d) cmt. 20 (amended 2016) ("To comply with this Rule, a lawyer does not need to have all the required technology competencies. The lawyer can and more likely must turn to the expertise of staff or an outside technology professional.").

11 *Compare* N.Y. Rules of Prof'l Conduct r. 1.6(c) (amended 2017) ("A lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client" (emphasis added)) *with* Model Rules of Prof'l Conduct R. 1.6 (Am. Bar Ass'n 2013) (requiring a lawyer "shall make *reasonable efforts* to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client" (emphasis added)).

12 Model Rules of Prof'l Conduct r. 1.6 cmt. 18 (Am. Bar Ass'n 2013).

13 *Id.*

14 Va Rules of Prof'l Conduct r. 1.6(d) cmt. 20.

15 *Id.* cmt. 21.

16 Kamala D. Harris, *California Data Breach Report*, Cal. Dep't of Just. 30 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.

17 *CIS Controls*, Center for Internet Security, https://www.cisecurity.org/controls/ (last visited Jan. 19, 2018).

THE LAW FIRM GUIDE TO

Cybersecurity

Avoiding Damage and Disclosure
Within Your Practice

Reprinted with Permission from the
Washington State Bar Association

WASHINGTON STATE
BAR ASSOCIATION

The Law Firm Guide to
CYBERSECURITY
Avoiding Damage and Disclosure in Your Practice

WASHINGTON STATE
BAR ASSOCIATION

The Law Firm Guide to Cybersecurity
Avoiding Damage and Disclosure in Your Practice

Product of the WSBA's Practice Management Assistance Program

www.wsba.org/pma

1325 4th Avenue, Suite 600, Seattle, WA 98101-2539

If you have any questions about this resource, please contact us at pma@wsba.org or schedule a consultation at www.wsba.org/consult.

REPRODUCTION

DISCLAIMER

The Washington State Bar Association (WSBA) provides this guide for informational purposes only; the WSBA does not warrant the information provided with regard to accuracy or any other purpose. No endorsement is intended. The information contained herein does not constitute legal advice or legal opinions.

You are responsible for ensuring your own legal and ethical compliance. Any use of the materials herein is not a defense against discipline, a malpractice claim, or other legal proceeding. This guide does not modify the rules, statutes, and regulations set by the federal government, state legislature, Washington Supreme Court, or the Bylaws and policies of the WSBA, or confer any additional rights.

050520-v1

Contents

Introduction

CYBERSECURITY MAY FEEL LIKE the last item on a long list of considerations for running your law firm and practicing law. What you may not realize is that your firm is vulnerable right now, as you read this, if you have not incorporated basic best practices to guard data and information.

The goal of this guide is to help you understand the issues and trends affecting law firms, and to provide simple, practical resources for you to safeguard yourself and your clients.

In discussing cybersecurity, this guide will cover the common issues and risks for law firms with the use of technology. Generally, the technology tools discussed here are recommended—or even necessary—to effectively practice in today's legal marketplace. However, if you do not know what the best practices are for using these technology tools, you could be putting your practice, and your clients, at risk.

Learning Objectives

This resource will cover these topics:

- Your professional obligations for cybersecurity
- Common misconceptions about technology
- Best practices for securing documents and information

Is This Guide for Me?

WHAT IT INVOLVES:

Cybersecurity is a broad term that generally refers to the protection of systems and information connected to the Internet.

WHAT COULD GO WRONG:

Hackers are increasingly targeting law firms because they can become a one-stop shop for a variety of sensitive documents and information. There is also a growing trend of "ransomware," where a hacker encrypts firm files so that they are inaccessible, and then demands a ransom in exchange for restoring access to the files.[1]

YOU'RE VULNERABLE IF:

- You use the same password for everything.
- You don't know what "phishing" means.
- You transmit confidential documents or Personally Identifiable Information (PII) without safeguards.[2]
- Your clients do the above.

WHAT YOU CAN DO:

- Encrypt files and information
- Use a secure messaging system
- Follow best practices in information management ■

---

[1] For a discussion of cyber attack trends for small businesses, see Patrick Thielen and Dave Charlton, *Cyber Attack Inevitability: The Threat Small & Midsize Businesses Cannot Ignore,* CHUBB (2019) (available at https://www.chubb.com/us-en/_assets/doc/2019_01.31_cyber_whitepaper_chubb_r3.pdf).

[2] "PII" is Personal Identifiable Information, , which is any information about an individual including (1) 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 (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. See: Erika McCallister, Tim Grance, & Karen Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" ES1, NIST, available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Your Professional Obligations for Cybersecurity

THE UNDERLYING PRINCIPLES of professional responsibility apply to a modern law office. If you are using mobile devices or cloud services, you have these fundamental responsibilities:

1. **Protect Confidentiality.** You have a general duty to keep all client information confidential.[3] This guide will discuss various ways that digital information can be vulnerable to disclosure, and you need ensure that you are preserving confidentiality in a digital environment.

2. **Competency.** Under your obligation to provide competent representation one thing you are required to do is keep yourself apprised of changes in technology.[4]

3. **Supervise Your Staff.**[5] This is true regardless of your connection to the Internet, but you have a responsibility to adequately supervise your staff. In terms of cybersecurity, this means that you should make sure they are following best practices (see discussion in following sections). It also means that you should be aware of any devices that are being used to access or store client data.

For more information about your ethical responsibilities, contact the WSBA Ethics Line at (800) 945-9722 and refer to WSBA Advisory Opinions 201601 and 2215. ■

---

[3] See RPC 1.6 (or, for Limited License Legal Technicians (LLLTs), LLLT RPC 1.6); RPC 1.15A (or, for Limited License Legal Technicians (LLLTs), LLLT RPC 1.15A).

[4] See RPC 1.1, Comment 8 (or, for LLLTs, LLLT RPC 1.1).

[5] See RPC 5.1, 5.2, 5.3 and 5.10. For LLLTs, see the LLLT RPC 5.1, 5.2, and 5.3.

Get Into the Cloud ... Safely

Cloud-Computing Explained

THE TERM "CLOUD COMPUTING" is a term that encompasses different types of computing resources (such as applications, storage) that are made available by a service provider for convenient, on-demand network access. Although "cloud" implies something magical or ethereal, cloud computing is generally just a form of service that leverages large, centralized data centers for those computing resources. Examples of cloud computing include Amazon AWS, Google Docs, and Microsoft Office 365. Many companies providing services to attorneys offer cloud services.

A common type of cloud service is **Cloud Storage**. Cloud storage is a simple way to "store, access, and share data over the Internet."[6] In other words, it is a method of storing data electronically so that the data is accessible anytime, from anywhere. When you use a cloud-storage service, instead of using your computer's hard drive or a networked server that you have to maintain, you pay a company to store that data on its servers. Examples of cloud storage include OneDrive for Business, Google Drive for Business, and Dropbox.

Some lawyers believe they are not using cloud services. But, if you have an email address that you access through a web browser or an app which ends with a domain address such as outlook.com, gmail.com, you are most likely already using the Cloud for your email data. You are also using the cloud if you use any kind of web application for which the data is not stored on your drive, or a local copy is stored on your hard drive but syncs with a copy stored at a hosted service data center. (This includes most practice management software, project management apps like Trello, and web-based budgeting software like QuickBooks Online).

[6] AMAZON WEB SERVICES, What is Cloud Storage? (https://aws.amazon.com/what-is-cloud-storage/)

Provided you are selecting a vendor with adequate security practices, cloud storage is an excellent way to improve your efficiency and ensure that you are protecting files from inadvertent destruction.

Often, attorneys who do not utilize cloud services (or who think they do not utilize cloud services) are worried about security and confidentiality. That is a reasonable concern, since WSBA members have an explicit duty to maintain confidentiality as well as a duty of technology competency.[7] However, cloud storage could be one of the most secure options for most solo and small firm attorneys, so long as you understand the Service Level Agreement, Terms of Service, and Privacy Policy of your hosted service providers; keep yourself apprised of the trends in the industry; and take adequate efforts to ensure you are following best practices. ■

[7] For more information, review WSBA Advisory Opinions **2215 (2012)** and **201601 (2016)**.

Key Considerations for Secure Data Management

USING A CLOUD SERVICE (as opposed to storing data on your own server or hard drive) may be an ideal security option for solo and small-firm practitioners.[8] In selecting a cloud service, there are a few key considerations. You also should incorporate these principles regardless of whether you use the cloud or rely on your own storage.

You're Still Responsible for Local Security

Even when you use Cloud or hosted services, you are still responsible for the security of your local devices and your portion of the network you use to connect to your Internet Service Provider (ISP), such as Frontier, Comcast, or CenturyLink.

If you work from home or share a physical office with other lawyers in a different firm, then you should have a firewall and use the firewall to separate your networks into separate virtual local area networks (vLAN). A firewall is a device or program that controls the flow of network traffic between two networks or a device and a network that employ differing security postures.[9] For example, a hardware firewall is often installed between the Internet, and a local area network in a home of office. Consider the case where an attorney practices from their home. Their ISP is Comcast, so they have a cable modem. The attorney could install a firewall to the cable modem, and then have a network with the firm devices (desktops and computers) isolated on it; and a separate network for other devices, such as the Smart TVs, and other non-work devices.

---

[8] In rare cases, your practice area may require an exception. Because cloud storage means that data is stored on a third-party's servers, you may want to avoid using a cloud service if you need to be concerned about government surveillance of some kind. This would be an exceptional case and you should consult with a technology expert to devise a protocol that will work for you.

[9] Karen Scarfone, Paul Hoffman, "Guidelines on Firewalls and Firewall Policy," ES-1, NIST, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.

Keep Your Systems Updated

You need to ensure that the operating system on your devices is up-to-date with the latest security patches. For example, if you use a Windows Computer you should be running a supported version of Windows (typically Windows 10). If you are using a Mac, you should be running the latest version of macOS. If you access the hosted services from mobile devices such as a smartphone or tablet, they should be running the latest version of the relevant OS.

Some people fail to update the latest security patches because they believe it makes the computer system slower or less efficient. Sometimes, patches do create temporary computing errors. However, those security patches are critical for addressing known vulnerabilities on your devices, so you should always take advantage of available security upgrades.

Use an Anti-Malware Program

Malware is malicious code that is, unbeknownst to the user, inserted into another program with the intent to destroy your data, run malicious programs, or otherwise compromise the confidentiality, integrity, or availability of your data and devices.[10] Windows 10 includes anti-malware software built in (Windows Defender), and third-party anti-malware solutions are available for macOS and Android systems.

Encrypt Wherever You Can

Data you are saving needs to be encrypted. Encryption is a process to secure data from prying eyes.[11] At its most basic level, encryption is a way of making it difficult and time-consuming for unwanted parties to gain access to information. It works by taking information and encoding it so the information is gibberish to anyone who does not have the encryption "key."

---

[10] Murugiah Souppaya, Karen Scarfone, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops,"vii, NIST, available at **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf**.

[11] David G. Ries, Sharon D. Nelson & John W. Simek, Encryption Made Simple for Lawyers (2012).

Your computer's hardware configuration may allow you to easily encrypt your hard drive. For example, Apple users can use FileVault to encrypt everything on their computer.[12] The similar protection on Windows devices is provided by BitLocker.[13] Encrypting your hard drive is a critical first step.

Encryption in Transit

For cloud services such as document storage and email, most if not all such services provide encryption **in transit**. This means that while data is transmitted over the Internet, the information is encrypted and protected from third-party view. If you are using cloud services you need to understand the Service Level Agreement (SLA) and Terms of Service to ensure you know whether or not data is encrypted in transit, and what steps if any you must take to enable such encryption.

Encryption at Rest

Once data is transmitted to the cloud (the service provider's servers) the data may be decrypted to be stored on the vendor's servers. This means that data is viewable to anyone who has access to those servers, including any hackers that gain access (however unlikely that may be). For optimal security, make sure that any cloud service you use offers encryption in transit, but also encryption **at rest**.[14] This means that the information is encrypted as it sits on the cloud vendor's servers. Understand whether that is offered standard, or if you need to opt in to that in the software settings.[15] As of this writing, Google Drive for Business, Dropbox, and Microsoft OneDrive for Business are vendors that offer encryption in transit and at rest.

---

[12] See generally *"Use FileVault to encrypt the startup disk on your Mac"* Apple, available at **https://support.apple.com/en-us/HT204837.**

[13] Chris Hoffman, *How to Enable Full-Disk Encryption on Windows 10*, How-To Geek (Jan. 11, 2017) (**http://bit.ly/2x3P3Vq**)

[14] If you serve a client population that is especially vulnerable in the case of government subpoenas, etc. (such as immigrants) you need to be more concerned about data encryption than most attorneys and you may want to consider a zero-knowledge service. Please contact the Practice Management Assistance program (**www.wsba.org/consult**) to discuss.

[15] See Sharon Nelson & Jim Calloway, *The Cloudy Ethics of Cloud Computing*, THE DIGITAL EDGE (Aug. 29, 2018 Legal Talk Network) (**http://bit.ly/2N8x9ea**).

Encrypting Email

Unfortunately encrypting your email is not straightforward. While some email services allow you to encrypt messages between you and the recipient, it can reduce the convenience of using traditional email services. If you arrange it with your client in advance, you can take simple steps like require a password to view communications. If the password becomes known by a third party, they would have access to your communications.

The simplest approach for secure messaging is to limit your email use to sharing information not highly sensitive. If you are transmitting documents or information that contains things like attorney-client confidential communications, Personally Identifiable Information (PII) (birthdates, social security numbers, addresses, bank account numbers, etc.) or trade secrets and non-public information, you should choose a different method to transmit that information.

Methods of Transmitting Sensitive Information Securely

- For sensitive information, you can either utilize secure email settings (e.g. Gmail allows you to set a password for individual emails you send), or you can use secure messaging services.
- For communicating between you and your client, one of the easiest ways to use secure messaging is to utilize client portals in practice management software. Usually your client would have to enter a unique username and password before they can view correspondence or documents from you.
- For sharing with third parties (outside counsel, experts, etc.) you can use password-protection on files to ensure that only individuals with the password can view the data.

Encourage your clients to adopt best practices for managing the electronic information related to their case. That means making sure they use good, unique passwords for their email or accounts, and setting up their devices so they are not vulnerable if their phone is lost or stolen.

Restrict Remote Access

One of the appealing features of cloud services is that you can access your data from anywhere with an Internet or data connection. Cloud services also make it easy to collaborate with your co-workers and share files externally.

Because cloud services make it easier for you to access data from anywhere, it also becomes easier for a third party to access your data from their own device. This is not a defect of the cloud service. Instead, it is dependent on the access controls you put in place for your accounts and devices.

The ability to access information from anywhere gives you greater flexibility, but it also may cause you to expose client information. This is especially true when you use public wireless connections to access the Internet (such as working in a coffee shop or on an airplane).[16] Public WiFi is still considered "public" and "unsecured" even if you receive a password to connect to the Internet (such as a guest code at your hotel).

When your device accesses public WiFi the data that is being shared over the Internet becomes vulnerable to third-party snooping.[17] **Virtual Private Networks (VPNs)** work by creating an encrypted tunnel so that the information traveling over the Internet is protected from view by other people on that public WiFi network.[18] You should install a VPN on any device that you use to access public WiFi. You should try to select a VPN that does not log any information that passes through it. This means you should likely avoid "free" VPN services which may be ad-based or may collect your user data, instead opting to pay for the VPN software.

---

[16] Steven Petrow, *I Got Hacked Mid-Air While Writing an Apple-FBI Story,* USA Today (Feb. 24, 2016) (**https://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720/**)

[17] This includes calls made over WiFi: see Tian Xie, et. al., *The Dark Side of Operational Wi-Fi Calling Service*s, available at: **https://www.egr.msu.edu/~mizhang/papers/2018_CNS_WiFiCalling.pdf**.

[18] Tom Mighell, *Keeping Communications Confidential with a VPN,* LAW PRACTICE DIVISION (September/October 2017) (**http://dashboard.mazsystems.com/webreader/51548?page=32**); Megan Zavieh, *VPN: A Simple Step Toward Cybersecurity,* ATTORNEY AT WORK (Apr. 12, 2018) (**https://www.attorneyatwork.com/vpn-simple-step-toward-cyber-security/**).

The second thing you need to implement is something called **remote wipe** for any mobile device (smart phones, laptops, etc.) that has access to firm data or client information. Remote wipe allows you to delete files and information from a device even if you have lost physical access to it. So for example, if you lose your phone on the bus, you can wipe the data before anyone can access it. Any device you use (or your employees use) should be able to be wiped remotely. Otherwise, those devices should not be permitted to hold, or connect to applications that hold, client information (including email).

Require Two-Factor Authentication

The next step in your security protocols is to make sure you are protecting the login process with two-factor authentication. Two-factor authentication (also sometimes called "multi-factor authentication" or "two-step verification") is utilizing at least two separate mechanisms for confirming your identity before you can gain access to the account.

Usually two-factor authentication means you have to (1) enter your password, and (2) verify your identify by doing something like answering a secret question, or entering a code that is texted to your phone. You can also use an authenticator app on your phone.

Most service providers will allow two-factor authentication, and you should always opt-in to two-factor authentication when that is an option. If employees have access to client data or information on their mobile devices, they should have to utilize two-factor authentication, preferably using phones securely locked with either their fingerprint or with complex passwords.

Cloud Service Checklist

For a checklist to select a cloud service provider, visit **www.wsba.org/guides**. Because technology changes constantly, you should keep yourself apprised of changing Service Level Agreements, Terms of Service, Privacy Policies, and industry standards, and ensure that the service you use is meeting those standards.

Use Best Practices for Passwords

The recommended practices for passwords have changed. This is because (1) technology advances all the time and (2) people follow similar patterns, such as using pop culture references, that make passwords vulnerable.[19] In June 2017, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) provided guidance for password creation.[20] Here are key takeaways:

1. **Long Passwords Required.** Password length is the primary factor of password strength. If your password is too short, it is vulnerable to brute force attacks (when an attacker tries many passwords or phrases hoping to guess correctly). Most people create passwords of 8–12 characters in length. Importantly, an advanced intruder can crack an eight-character password in about six hours.[21] To make your passwords less vulnerable, you should use passwords, or pass phrases, that are 25 characters long (or as long as you can depending on the password restrictions set by the vendor).
2. **"Password" is a Terrible Password.** At this point, most people know that it is a terrible idea to use the word "password" within your actual password. However, even if you do not do that, you may still include common patterns or words easily guessed.[22] For best results, do not use common dictionary words in your password and never use the name of your firm or the hosted service itself. It is better to use words or phrases uniquely relevant to you, and are not readily available from public records (e.g. your children's names, birthdates, your address, etc.).

---

[19] See https://www.wired.com/2016/05/password-tips-experts/ quoting a CEO of a password management company. You should avoid pop culture references, regardless of the length of your password.

[20] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Digital Identity Guidelines* (June 2017) (https://pages.nist.gov/800-63-3/sp800-63b.html#appA). See also Samantha Raphelson, *Forget Tough Passwords: New Guidelines Make It Simple,* NATIONAL PUBLIC RADIO (Aug. 14, 2017) (https://n.pr/2CFmIKh)

[21] See the calculator widget by Better Buys at https://www.betterbuys.com/estimating-password-cracking-times/.

[22] For examples, check out Cara McGoogan, *The world's most common passwords revealed: Are you using them?,* THE TELEGRAPH (Jan. 16, 2017) (https://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/) and WIKIPEDIA, *List of the most commons passwords* (last updated Sept. 7, 2018) (https://en.wikipedia.org/wiki/List_of_the_most_common_passwords).

3. **Don't Repeat Yourself.** Every password you use should be unique. That means you should not use the same password for multiple accounts or services. The reason for this is that it makes it easy for someone to gain access across your various accounts if they just have one log-in obtained by a breach or other method. Every password is the opportunity to add a locked door. Do not duplicate the key.
4. **Don't Force Changes in Password.** Recent studies show that constantly changing passwords may cause more problems than it prevents. Some systems force the use of a new password every 60 days. If you are following the first three recommendations, you may wish to stop forcing or frequently changing your password or the passwords of your employees.[23]

Passwords should be used not only for applications and for software, but also on the devices you use to access those applications and software. This includes your computer, laptop or tablet, and mobile devices. Otherwise, third parties could access your data and files stored locally without even needing your web passwords.[24]

[23] See generally, "Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903— Dropping the password expiration policies", available at **https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/**.

[24] Most cloud services will store data "locally" on your devices, meaning that data is downloaded from the Internet onto your device so that you can access it even when you are not connected to the Internet. When you are connected to the Internet, your device will transmit data back and forth with the cloud service.

▶ *Password Managers*

If you follow the above advice, it will be difficult (if not impossible) to keep track of these passwords and actually remember them all. Fortunately, you can use an encrypted password manager that will allow you to securely keep track of your passcodes using one primary password. Examples include Keychain, LastPass, and 1Password. For more, check out:

- Chris Hoffman, *Why You Should Use a Password Manager, and How to Get Started,* HOW-TO GEEK (Dec. 12, 2016) (**https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/**)
- Eric Limer, *You Should Be Using a Password Manager*, POPULAR MECHANICS (May 24, 2017) (**https://www.popularmechanics.com/technology/security/a26629/use-password-manager/**)
- Cara McGoogan, *Is it safe to use a password manager?*, THE TELEGRAPH (Apr. 4, 2017) (**https://www.telegraph.co.uk/technology/0/safe-use-password-manager/**)

Some password managers integrate with MFA devices or keys, which provide additional protection, including using biometrics. For example, Google and Yubico make specialized USB-like devices which integrate with password managers.[25] ■

[25] For examples, check out Google Titan, available at: **https://cloud.google.com/titan-security-key/** or Yubico key available at **https://yubico.com**.

Special Case: IoT Devices

AN IoT (Internet Of Things) DEVICE is any appliance, gadget, accessory, or other physical item that connects to the Internet.[26] Examples of IoT devices include:

- **IoT wearables** such as smart watches or step counters.
- Virtual assistant services and hardware such as the Amazon Echo and Google Home.
- Home monitoring equipment such as a nanny cam or pet camera.

An IoT device for your practice can help you run a more efficient law office. For example, you can use a Virtual Assistance service to help you track your time, complete tasks, and more. But if you use an IoT device (whether at home or at work) you may be opening yourself up to cybercrimes:

- An IoT wearable can allow data access if it is lost or stolen.[27]
- Innocuous devices like smart lightbulbs and coffeemakers can expose your Wi-Fi password.[28]
- Some devices are monitored by the service provider and could create logged data subject to subpoena or create issues related to confidentiality and attorney-client privilege.

---

[26] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, Forbes (Mar. 13, 2014) (https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#100450dc1d09)

[27] Kirk McElhearn, *Apple Watch Security and Privacy Tips*, INTEGO (Jan. 10, 2018) (https://www.intego.com/mac-security-blog/apple-watch-security-and-privacy-tips/)

[28] Dan Goodin, *Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords*, ARS TECHNICA (July 7, 2014) (https://arstechnica.com/information-technology/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/); Steve Ranger, *The spy on the corner of your desk: Why the smart office is your next security nightmare*, ZDNet (Mar. 1, 2018) (https://www.zdnet.com/article/the-spy-on-the-corner-of-your-desk-why-the-smart-office-is-your-next-security-nightmare/)

If you are using an IoT device within the scope of your practice (whether at the office or at home when you work remotely), you need to make sure your devices are set up securely and that you are using them consistent with the best practices described here. That means that you use unique and strong passwords (see **"Use Best Practices for Passwords" on page 12**) for each device and prioritize services that use robust encryption. Again, it is necessary to fully understand the Service Level Agreement, Terms and Service, and Privacy Policies for all such devices.

In addition, because IoT devices are especially vulnerable to malicious attacks, also take these precautions:

1. **Just Say No:** if an IoT device you are considering does not allow you to update its software or firmware, or change the password, avoid purchasing it.[29]
2. **Separate Your Network:** Your Internet network can be compartmentalized so guests using your WiFi do not get access to the main network.[30] Similarly, create a separate network for your IoT devices.[31]
3. **Limit BYOD at Work:** Besides your own devices, if you have employees you also need to consider what devices they are bringing to work, and what devices they are using to review or access firm data. Your employment agreement should set out guidelines for staff.

■

[29] Rob Marvin, *The 5 Worst Hacks and Breaches of 2016 and What They Mean for 2017,* PC MAG (Jan. 7, 2017) (**https://www.pcmag.com/article/350793/the-5-worst-hacks-and-breaches-of-2016-and-what-they-mean-fo**).

[30] Bradley Mitchell, *Setting Up and Using a Guest Wi-Fi Network,* LIFEWIRE (Mar. 19, 2019) (**https://www.lifewire.com/guest-network-for-home-tutorial-818204**).

[31] Mark Dacanay, *Common Sense Security Tips for IoT in the Office,* GLOBALSIGN BLOG (Apr. 24, 2018) (**https://www.globalsign.com/en/blog/cybersecurity-tips-for-office-iot/**)

Special Case: Email Phishing

PHISHING IS A CYBERCRIME in which a hacker poses as a legitimate institution or person to "lure" someone into providing sensitive information such as passwords, bank account information, etc.[32] Hackers can also pose as a legitimate sender to lure a recipient to open a file or web link that causes malware to be downloaded to the computer (also known as a "malicious link").[33]

Lawyers are vulnerable to these schemes because most people are not using basic best practices for email security, and hackers know that law firms are a prime target for hacking. For example, a hacker may gain access to a client's account, and then masquerade as your client mislead you and your staff. into misdirecting settlement funds to a different bank account.

Don't Take the Bait

Before you click a link or download a file you receive via email, make sure it is what it purports to be. Here is an example phishing email:

I tried sending you this doc earlier but noticed the failure delivery so had to re-send it securely.

Kindly view below:

116Kb

PDF <https://smarturl.it/8vaw26> | Preview <https://smarturl.it/8vaw26>

Download <https://smarturl.it/8vaw26>

[32] PHISHING.ORG, *What is Phishing?* (Accessed Sept. 12, 2018) (**http://www.phishing.org/what-is-phishing**).

[33] Michigan State University, College of Engineering, *How to Recognize a Malware Email* (Accessed Sept. 12, 2018) (**https://www.egr.msu.edu/decs/security/how-recognize-malware-email**).

The message was followed by a signature block from a WSBA member that looked valid—it had his WSBA number, his address, his phone, etc. However, the recipient was not expecting any documents from this person, and the format and phrasing was somewhat unusual. If you receive an email like this, these are all warning signs that should prompt you to call the sender to make sure they actually transmitted a message to you. Here, the member's email account had been compromised and a third party was using it to send phishing emails.

To protect yourself from similar issues:

1. **Make Sure They Are Who They Say They Are.** Some phishing schemes rely on tricking you into believing the sender is coming from a trusted domain, when in fact there are clues to suggest otherwise. Check the sender's email address (not just the display name) and look for inconsistencies in the domain name. For example, instead of "@becu.org" the sender's domain might be "@becu-company.com."

2. **Give Unexpected Items More Scrutiny.** Before you click on a link or open an attachment you received, make sure you consider whether it was something you were expecting. If not, call the sender on the phone (do not verify by email!) to confirm that the document or link is authentic. Unsolicited invitations to view or access a document may be phishing schemes.

3. **Inspect Links.** A hyperlink has two elements: the text displayed (what you see on the screen), and the actual URL (web) address you will be directed to when you click the link. For example, if you are viewing these materials electronically, hover your mouse over **this link** until you see the text of the URL address. It is also possible to create a link that displays one address, but directs you somewhere else (e.g. **https://www.wsba.org/pma)**. Never click a link you have not inspected first.

4. **Disable Macros and Protect Files.** This is an easy step you can take right now. For all of your Microsoft Office products, make sure that your settings are set so that (1) macros are disabled and (2) documents from the Internet are opened in "protective view."[34]

5. **Don't Give Identifiers Away.** Some phishing schemes may ask you to respond to an email with your sensitive information like your social security number, or answers to your secret questions. Do not provide sensitive information unless you have verified the authenticity of the service provider and the data is remitted securely.[35] ■

[34] Specific steps for these items will vary depending on your software. You can find information on how to do this within the Help resources in your program, or you can contact us for assistance at pma@wsba.org.

[35] For more information about verifying the security of the website (e.g. checking the SSL certificate), see Joyce Tammany, *How Can I Tell If a Website Is Safe? Look For These 5 Signs,* SITELOCK (Aug. 24, 2018) (https://www.sitelock.com/blog/is-this-website-safe/).

TL;DR[36]

WHETHER OR NOT you realize it, you probably are already using cloud services. With any technology or electronic information, the RPCs require you to: (1) protect the confidentiality of client information, (2) supervise your staff's use and access to that information and (3) stay apprised of technology changes that impact your ability to competently provide legal services. ■

[36] A shorthand notation summarizing the content of the materials.

Glossary

Term/Acronym	Definition
BYOD	"Bring Your Own Device" refers to employees using personal devices (computers, phones, etc.) to connect to workplace Internet or access firm data.
Cloud Computing	Broad term that encompasses different types of computing resources (such as applications, storage) that are made available by a service provider for convenient, on-demand network access
Cloud Storage	The method of storing, accessing, and sharing data over the Internet.
Encryption	A process of securing data that makes it more difficult for third parties to gain access to the data. Data can be encrypted as it is sent or received over the Internet (encryption "in transit") or while it is stored (encryption "at rest").
Internet of Things (IoT)	Any appliance, gadget, accessory, or other physical item that connects to the Internet. Includes IoT Wearables, such as smart watches.
ISP	Internet Service Provider; your ISP is the company that you pay for Internet access.

Macro	A sequence of computing instructions recorded as a single step. The concept is that you can automate routine or tedious steps for greater efficiency, but malicious actors can also record macros that will harm your computer or cause a data breach.
Malicious Link	A hyperlink or attached file that, when clicked or opened, will cause malware to be downloaded to the user's computer.
Malware	Malicious code that is, unbeknownst to the user, inserted into another program with the intent to destroy your data, run malicious programs, or otherwise compromise the confidentiality, integrity, or availability of your data and devices
Password Manager	A software program that securely stores password and account information.
Remote Wipe	A method of deleting data from a device that you do not have physical access to.
Two-Factor Authentication	Requiring two or more methods of verification before access is permitted. Also called "multi-factor authentication" (MFA) or "two-step verification."
URL	Uniform Resource Locator; better known as a "web address" or "web link."
VPN	Virtual Private Networks (VPNs) create an encrypted tunnel so that the information you send or receive over the Internet is protected from view by other people connected to the same WiFi network.

Additional Resources

Frequently Asked Questions

- *I use Apple devices. Do I need anti-malware?*

Yes. Although most malware targets the Windows operating system, bad actors are developing malicious code that targets the mac operating system as well.

- *Is it okay to use a cloud-based service?*

With some exceptions, cloud computing may be a very secure option for you if you follow best practices for cybersecurity.

WSBA Member Resources

For more information and assistance from the WSBA, consider these resources:

- **Free Lending Library:** Borrow from a selection of 400 books. You can register immediately online and start placing holds. Titles will be shipped to you automatically. Visit **www.wsba.org/library** to get started.
- **Free Consultations:** You can speak with an advisor in the Practice Management Assistance program for personalized advice regarding your law firm business management. Visit **www.wsba.org/consult** to get started.
- **Free Ethics Help:** You can speak to WSBA staff regarding questions of ethical obligations and your professional responsibility. The phone number is (800) 945-9722.
- **Discounts on Software and Services:** Through the Practice Management Discount Network, WSBA members receive discounts on a menu of software and services to help you improve your practice and client service delivery. Visit **www.wsba.org/discounts** to learn more.

For more resources, visit **www.wsba.org/MemberSupport**. ■

WASHINGTON STATE
BAR ASSOCIATION

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents[1]

Version 2.0 (September 2018)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to a cyber incident can be critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* a data breach incident, ransomware attack, or other cyber incident occurs.

The Cybersecurity Unit originally published this "best practices" document to help organizations prepare a cyber incident response plan and, more generally, to better equip themselves to respond effectively and lawfully to a cyber incident. This updated version includes additional incident response considerations, including ransomware, information sharing pursuant to the Cybersecurity Information Sharing Act of 2015, cloud computing, and working with cyber incident response firms. It distills lessons learned by federal investigators and prosecutors and input from private sector companies that have managed cyber incidents. It includes advice on preventing cyber incidents, as well as advice on working effectively with law enforcement. Like its predecessor, it was drafted primarily for smaller organizations and their legal counsel; however, it may be useful for larger organizations with more experience in handling cyber incidents as well.

I. Steps to Take *Before* a Cyber Intrusion or Attack Occurs

Having well-established plans and procedures in place for managing and responding to cyber intrusions and attacks is a critical first step toward being prepared to weather a cyber incident. Such pre-planning can help organizations limit damage to their computer networks, minimize work stoppages, expedite mitigation efforts, and enhance the ability of law enforcement to identify and apprehend perpetrators. Organizations should take the steps outlined below before

[1] The guidance contained in this document is intended to help organizations and investigators prevent, mitigate, and respond to cyber incidents; however, it may not apply to all organizations or in every situation. Therefore, failure to take all of the proposed steps or implement all of the measures discussed herein should not be interpreted *per se* as unreasonable or negligent conduct. In addition, this document confers no rights or remedies and does not have the force of law. *See United States v. Caceres*, 440 U.S. 741 (1979). It is also not intended to have any regulatory effect.

a cyber incident occurs.

A. Educate Senior Management about the Threat

Organizations are increasingly aware of the threat posed by cyber incidents such as data breaches and ransomware attacks and the potential cost of inadequately preparing for them. But ensuring that an organization is prepared to manage the risk posed by cyber threats requires a common understanding throughout the organization of the nature, scope, and severity of the threat. In particular, an organization's senior management, board of trustees, and any other governing body responsible for making resource decisions and setting priorities should be aware of how cyber threats can disrupt an organization, compromise its products, impair customer confidence and relations, and otherwise cause costly damage.

Regular briefings about existing and emerging cyber threats and appropriate risk management strategies are one way of keeping senior management informed. Cyber incident preparedness exercises (which are discussed further below) can be another valuable educational tool.

B. Identify Your "Crown Jewels"

The cost and difficulty of protecting an entire enterprise from all manner of cyber threats can be overwhelming. Accordingly, an organization should prioritize its cybersecurity efforts. Different organizations have different mission-critical needs. For some organizations, even a short-term disruption in email service will have a devastating impact on operations. Other organizations may not be so dependent on email to conduct their business, but they may suffer significant harm if certain intellectual property is stolen. For others, the ability to guarantee the integrity and security of the data they store and process is the essential service that must be protected. Before formulating a cyber incident response plan, an organization should first determine which of its data, assets, and services warrants the greatest protection.

Prioritizing the protection of an organization's "crown jewels" and assessing how to manage the risk associated with protecting them are important first steps toward preventing the type of catastrophic harm that can result from a cyber incident. The Cybersecurity Framework produced by the National Institute of Standards and Technology (NIST) provides excellent, free guidance on risk-management planning and policies that provide a prioritized, flexible, and cost-effective approach to protecting critical networks. The NIST Cybersecurity Framework has been widely adopted and can be easily integrated into risk management and incident response planning.[2]

[2] NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2018), https://www.nist.gov/cyberframework.

Properly assessing risk is important. It is the key to setting effective cybersecurity priorities. When assessing risk, an organization should evaluate threats that stem from the use of contractors, service providers, and other outside agents that host an organization's data and/or have access to its network, data, or resources (e.g., third-party vendors, law firms, and clearinghouses). An organization's data is only as secure as its greatest point of vulnerability, and that vulnerability might belong to a third party.

C. Have an Actionable Plan in Place … Now!

Organizations should have a plan in place for handling computer intrusions, data breaches, and other cyber incidents before they occur; yet many still lack a formal cyber incident response plan.[3] During a cyber incident, an organization's management and other personnel should be focused on containing the incident, mitigating the harm, and collecting and preserving vital information that will help them assess the nature and scope of the incident and the potential source of the threat. An organization should not be creating emergency procedures or considering response options for the first time while in the midst of a cyber incident. Any decisions regarding incident response that can be made beforehand should be captured in the plan to save valuable time during an incident.

The plan should be "actionable," meaning it should: provide specific, concrete procedures to follow in the event of a cyber incident; be up-to-date; include timelines for the completion of critical tasks; and identify key decision makers. At a minimum, the plan should address, or at least provide a process for addressing, the following considerations:

- Who has decision-making responsibility for different elements of an organization's cyber incident response, including public communications, implementing security and mitigation measures, engaging with law enforcement, and resolving legal questions;
- How to contact critical personnel at any time, day or night, and how to proceed if critical personnel are unreachable or unavailable;
- What mission-critical data, networks, assets, or services should receive prioritized attention during an incident;
- How to contact and interact with other parties who host the organization's affected data and services (e.g., cloud storage service providers or commercial data centers);
- How to contact the organization's retained incident response firm or otherwise obtain incident response assistance, if needed;

[3] PONEMON INSTITUTE, THIRD ANNUAL STUDY ON THE CYBER RESILIENT ORGANIZATION (2018), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55015655USEN&. (finding that 77% of respondents lacked a formal incident response plan).

- When and how to restore backed-up data, including measures for insuring the integrity of backed-up data before restoration;
- What criteria will be used to determine whether data owners, customers, or partner organizations need to be notified if their data or networks may have been illegally accessed; and
- When and how to notify law enforcement and/or other government entities.

Once an incident response plan is prepared, all personnel with incident response roles, particularly anyone with a role in making technical, operational, or managerial decisions during an incident, should keep it close at hand. While under normal circumstances it may be most efficient to make the plan available in electronic form on the organization's network, have hard copies readily available in case a cyber incident—for instance, a ransomware attack[4]—renders an organization's online resources inaccessible.

Familiarity with the incident response plan should be ingrained through regularly conducted exercises. Staging regular exercises has the auxiliary benefit of ensuring the plan is kept up-to-date as inevitable personnel changes occur within an organization.

Exercises can take a variety of forms—from full-blown real-time enactments of incidents to discussions of scenarios explored in a "tabletop" setting. They need not require major time investments. Regardless of the format, it is valuable to perform exercises regularly to make sure communications channels and emergency processes remain up-to-date and familiar. Such exercises should be designed to verify that necessary lines of communication exist, decision-making roles and responsibilities are well understood, technology that may be needed during an actual incident is available and likely to be effective, and personnel have a common understanding of how the organization will handle an emergency. Deficiencies and gaps identified during an exercise should be noted for speedy resolution.

D. Engage with Law Enforcement Before an Incident

Organizations should establish a relationship with their local offices of federal law enforcement agencies long before they suffer a cyber incident. Having a point-of-contact and a pre-existing relationship with law enforcement will ease any subsequent contact if an organization later needs law enforcement assistance. It will also help establish a relationship that fosters bi-

[4] "Ransomware" is malware designed to make data or a device inaccessible, often by encrypting data stored on the device or locking a device's keyboard, until a ransom is paid. Federal departments and agencies have published guidance for Chief Information and Chief Information Security Officers with advice regarding how to avoid and mitigate ransomware attacks. *See, e.g.*, FEDERAL BUREAU OF INVESTIGATION, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

directional information sharing that is beneficial both to potential victim organizations and law enforcement.

As discussed in detail in the next section on responding to a cyber incident, federal law enforcement has focused on improving its outreach to and support of organizations facing cyber threats. At headquarters and in the local field offices throughout the country, law enforcement has dedicated agents and resources to building better lines of communications and instituting policies and practices that better serve victims of cyber attacks and intrusions.

The principal federal law enforcement agencies responsible for investigating criminal violations of the federal Computer Fraud and Abuse Act are the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (Secret Service). Both agencies conduct regular outreach to private sector companies and other organizations likely to be targeted for intrusions and attacks. Such outreach occurs mostly through the FBI's InfraGard chapters and the Cyber Task Forces in each of the FBI's 56 field offices, and through the Secret Service's nationwide network of Electronic Crimes Task Forces. Organizations will find responsive federal law enforcement nearby, regardless of where they are located.

Federal law enforcement is also a valuable source of cyber threat information that can help prevent a cyber incident. The FBI and Secret Service often develop and share cyber threat information through collaboration with information sharing and analysis organizations, other government agencies, non-governmental organizations, and private sector organizations. In partnership with DHS, the FBI publishes Private Industry Notifications (PINs), which provide contextual information about ongoing or emerging cyber threats, and FBI Liaison Alert System (FLASH) reports, which provide technical indicators gleaned through investigations or intelligence. Similarly, in partnership with DHS, federal law enforcement publishes joint products, such as Joint Analysis Reports (JARs) and Joint Technical Advisories (JTAs) that furnish additional cyber threat intelligence. Such products are available to members of InfraGard and Secret Service's Electronic Crimes Task Forces.

E. Have Appropriate Workplace Policies in Place

Because institutionalized familiarity with the organization's plan for addressing a cyber incident can expedite response time and save critical minutes, hours, or even days of recovery time, an organization should adopt internal policies and rules that will help ensure that its personnel are familiar with the incident response plan. For instance, the procedures for responding to a cyber incident can be integrated into routine personnel training.

Some personnel policies can also prevent cyber threats and mitigate potential damage. For

example, promptly revoking the computer credentials of terminated employees—particularly system administrators and information technology staff—can prevent a spiteful ex-employee from damaging a former employer's network or data. An organization that has already adopted such policies should also ensure that they are enforced.

F. Institute Basic Cybersecurity Procedures

Of course, every organization should adopt and maintain commonsense cybersecurity practices. Such practices can be found in guidance and white papers that are readily available from government and private sector sources. However, in law enforcement's experience, certain cybersecurity measures have outsized security benefits.

For instance, the majority of intrusions are conducted using known software vulnerabilities. Therefore, a reasonable patch management program will help prevent many attempted intrusions. Likewise, access controls and network segmentation that appropriately limit the availability of data—particularly information considered to be an organization's "crown jewels"—can minimize the consequences of a breach, regardless of whether the breach is attributable to an insider threat or remote computer intrusions. While not infallible, reasonable password management programs and use of multi-factor authentication can thwart rudimentary password-cracking efforts. In addition, some type of perimeter defense, such as a firewall, can help detect common cyber threats. These are basic cybersecurity measures that may not thwart more sophisticated criminals; however, they are effective against an array of commonly used exploits.

Regardless of the nature of the cyber threat, server logs are typically critical to ascertaining the cause and origin of a cyber incident. A criminal investigation, as well as an internal investigation or audit, will likely rely on log data. Consequently, an organization should enable logging on all its servers and configure them to maintain copies of logs for as long as practicable.[5]

G. Procure Appropriate Cybersecurity Technology and Services Before an Incident Occurs

Ideally, organizations will acquire or have ready access to the technology and services they will need to respond to and recover from cyber incidents. Depending on an organization's resources, the types of assets it wants to protect, and the nature of the cyber threats it needs to counter, this may mean procuring cybersecurity services such as intrusion detection capabilities, data loss prevention technologies (e.g., backups), and/or traffic filtering or scrubbing services.

[5] Ideally, an organization should conduct "informational level logging" (i.e., logging of "normal" events, such as traffic passing through a firewall instead of just traffic that generates alerts and/or is blocked). Such logging can help determine the scope of an intrusion or a breach after it has been detected.

An organization should align the services it procures with the cyber threats that would cause it the greatest harm. Some services do not provide adequate protection against certain threats. For instance, off-site data back-up capabilities may provide only marginal protection against the unlawful exfiltration of data but can be critical when faced with a ransomware attack. Similarly, traffic filtering services can fend off a denial-of-service attack,[6] but they provide no defense against a business email compromise.[7] Technological solutions should be tested regularly by the organization or by contracted third parties to ensure they perform as expected.

Some organizations choose to retain the services of an incident response firm in preparation for a cyber incident. Incident response firms have technical knowledge, equipment, and experience that many organizations are unable to maintain in-house. Therefore, an incident response firm can increase the speed and effectiveness of an organization's response to a cyber incident. Many incident response professionals are also accustomed to working alongside law enforcement, which may expedite coordination when an organization contacts law enforcement following an incident. Government services associated with mitigating and recovering from a cyber incident may also be available. Organizations may check with the Department of Homeland Security (DHS) or their sector-specific agency regarding the availability of such services.[8]

Some organizations use cloud storage[9] services for the convenience and security such services can provide. There are numerous benefits to using cloud storage; however, it is not a remedy to all cyber threats. Organizations should still assess the sufficiency of the security services they receive in connection with their cloud storage services to ensure they provide adequate protection. Also, contracts and agreements with cloud service providers should anticipate the need to furnish third parties, such as law enforcement and incident response firms, with access to the organization's information and resources during a cyber incident. Organizations should consider including provisions in their contracts and agreements requiring cloud providers to assist third parties with access to an organization's data at the organization's request.

---

[6] A distributed denial-of-service (DDOS) attack uses multiple computers or devices to (1) transmit a torrent of communications traffic at another computer or network to block communications to and from the targeted system (a volumetric attack), (2) consume the processing capability of the target computer (a protocol attack), or (3) establish a connection with the target computer that exhausts its resources by monopolizing processes (an application attack). The attacking computers or devices are typically infected by malware that allows them to be centrally controlled by the perpetrator of the attack.

[7] A "business email compromise" is a sophisticated scam targeting businesses working with foreign suppliers and businesses that regularly perform wire transfer payments. The FBI has provided more information about such schemes at https://www.ic3.gov/media/2015/150122.aspx

[8] Organizations can contact DHS for such assistance at https://www.us-cert.gov or by calling (888) 282-0870.

[9] Cloud storage involves storing data on remote servers rather than locally. For instance, an organization may choose to store its data on a cloud storage provider's network rather than on its own system. Cost, accessibility, and security are often cited as advantages of using cloud storage.

H. Have Appropriate Authorization in Place to Permit Network Monitoring

The ability to monitor network traffic is critical to detecting and preventing cyber incidents. Monitoring can also be instrumental to analyzing an ongoing intrusion or other security breach. But monitoring network communications can implicate federal civil and criminal statutes. Accordingly, in addition to procuring the technical ability to monitor their systems and devices for cybersecurity threats, organizations should also establish the legal authority to conduct such monitoring before it begins.

In general, the monitoring of wire and electronic communications is regulated by federal electronic surveillance statutes. The Wiretap Act prohibits the interception of wire and electronic communications, except with a court order or consistent with one of the statute's exceptions.[10] Similarly, the Pen Register/Trap and Trace (PRTT) Act prohibits the use or installation of a device or process that captures, records, or decodes non-content information (i.e., dialing, routing, addressing, or signaling information), except with a court order or consistent with the statute's exceptions.[11] As discussed below, both statues include exceptions that may apply to cybersecurity monitoring, including an exception for providers of wire or electronic communication services who conduct monitoring to protect their "rights or property."[12] Many states have comparable laws with similar exceptions. Congress simplified matters in 2015 when it enacted the Cybersecurity Information Sharing Act of 2015 (CISA), which explicitly authorized organizations to conduct many cybersecurity activities.

CISA provides private entities with broad authority to conduct cybersecurity monitoring of their own networks, or a third party's networks with appropriate consent.[13] CISA expressly preempts contrary state law and authorizes cybersecurity monitoring "notwithstanding any other provision of law," meaning it overrides any conflicting laws, including the Wiretap Act and the PRTT Act.[14] CISA also provides private entities with liability protection against any legal action brought in any court—state or federal—for cybersecurity monitoring conducted in accordance with CISA.[15]

It is important, however, to recognize the limits of CISA's monitoring authority. CISA only authorizes private entities to monitor information or an information system for a "cybersecurity purpose." A "cybersecurity purpose" means for the "purpose of protecting an

[10] 18 U.S.C. § 2510 et seq.
[11] 18 U.S.C. § 3121 et seq.
[12] 18 U.S.C. § 2511(2)(a), 3121(b)
[13] Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, div. N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), N., 129 Stat. 2242, 2936 – 2956 (2015).
[14] 6 U.S.C. §§ 1503(a), 1507(k).
[15] 6 U.S.C. § 1505(a).

information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[16] Thus, CISA authorizes monitoring to prevent a cyber incident and to inform response efforts to avoid further damage. However, CISA does not authorize monitoring conducted for purposes unrelated to cybersecurity, such as in support of administrative investigations for employee misconduct having nothing to do with a cybersecurity threat.

Because CISA only allows monitoring for cybersecurity purposes, organizations that intend to monitor their networks for other reasons must have another legal basis for doing so that satisfies the Wiretap Act and PRTT statute. The most common means of complying with those statutes is by obtaining prior consent to monitor using network log-on warnings or "banners."[17] For example, an organization may use log-in banners with click-through buttons to obtain consent or to inform users that their use of the network constitutes consent to the organization's interception of their communications.

In the absence of a log-on banner, organizations may look to computer user agreements, workplace policies, and personnel training to establish that users of their network consented to monitoring. It is advisable, though, for organizations to obtain written acknowledgement from their personnel that they were notified that their communications were monitored and that use of the organization's network constituted consent to such monitoring. Doing so will provide an organization with ready proof that its monitoring was lawfully conducted with users' consent.

An organization might also lawfully intercept communications using other statutory exceptions. For instance, the Wiretap Act and PRTT Act each have an exception that allows a provider of an electronic communication service—such as e-mail—to intercept communications to protect its rights or property.[18] The Department's Computer Crime and Intellectual Property Section, which manages the Cybersecurity Unit, has published an online manual on monitoring electronic communications that includes guidance on the rights or property exception, as well as other exceptions to the Wiretap Act and PRTT Act.[19]

---

[16] 6 U.S.C. § 1501(4).

[17] 18 U.S.C. §§ 2511(2)(c)-(d), 3121(b)(3). More guidance on banners, including a model banner, can be found in our manual on searching and seizing electronic evidence and in a 2009 legal opinion prepared by the Department of Justice's Office of Legal Counsel. *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (3d ed. 2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf; Stephen G. Bradbury, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, 33 OP. O.L.C. 1 (2009), http://www.justice.gov/sites/default/files/olc/opinions/2009/01/31/e2-issues.pdf

[18] 18 U.S.C. §§ 2511(2)(a) (ii), 3121(b)(2).

[19] *See* COMPUTER CRIME AND INTELLECTUAL PROP. SECTION, *supra* note 16, at 172-177.

I. Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management

Preventing and responding to cyber incidents can raise a host of unique legal questions. Furthermore, decisions made during a cyber incident may later have legal consequences. During a cyber incident, many organizations have found it beneficial to obtain legal advice from attorneys who are conversant with technology and knowledgeable about relevant laws, including the Computer Fraud and Abuse Act[20] and laws governing electronic surveillance, communications, data privacy, and information-sharing. Legal questions may also arise concerning how to interact with investigators, whether the thresholds for mandatory breach reporting have been met, and how to weigh liability for taking specific remedial measures or failing to do so. Even before an incident, organizations may face questions regarding the workplace policies required to institute threat detection and data loss prevention programs and the suitability of different types of cyber insurance.

Many private sector organizations retain or consult outside counsel who specialize in legal questions associated with data breaches, while others manage cyber issues so frequently that they have their own cyber-savvy attorneys on staff. Regardless of how an organization chooses to structure its legal representation, having ready access to advice from lawyers who are well acquainted with cyber incident response can speed up an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing. Regardless of whether an organization uses outside or in-house counsel, its lawyers should be included in incident response planning and exercises to acquaint them with legal issues likely to arise during a cyber incident and to give them the opportunity to prepare to address them in advance.

J. Establish Relationships with Private and Public Cyber Information-Sharing and Analysis Organizations

Staying up-to-date on new and emerging cyber threats can be a daunting task, but having access to cyber threat intelligence and information about commonly exploited vulnerabilities can help an organization set its security priorities. Information Sharing and Analysis Centers (ISACs) exist for every sector of the "critical infrastructure" and provide actionable cyber threat information.[21] The "critical infrastructure" of the United States consists of 16 sectors,[22] and most

[20] 18 U.S.C. § 1030.

[21] Presidential Policy Directive – Critical Infrastructure Security and Resilience (PPD-21), 2013 WL 503845 (Feb. 12, 2013).

[22] As set forth in PPD-21, the critical infrastructure consists of the following sectors: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy;

sectors have a dedicated ISAC. ISACs share analysis of cyber threat information within their respective sectors, with other sectors, and with the government. Depending upon the sector, they may provide other cybersecurity services as well.

The federal government has also encouraged the creation of information-sharing entities called Information Sharing and Analysis Organizations (ISAOs) to accommodate organizations that do not fall within an established sector of the critical infrastructure or that have unique needs.[23] ISAOs are intended to provide such organizations with the same benefits of obtaining cyber threat information and other supporting services from ISACs.

As discussed above, CISA authorizes monitoring for a cybersecurity purpose; however, it was enacted principally to facilitate cyber threat information sharing. CISA authorizes non-federal entities to share cyber threat indicators with and to receive cyber threat indicators from the federal government and other non-federal entities, such as ISACs and ISAOs. When a non-federal entity engages in indicator sharing in accordance with CISA, it receives liability protection for the act of sharing that information and other statutory protections as well, including exemptions from federal and state disclosure laws and protection from having shared information used for certain state and federal regulatory purposes.[24]

The federal government is also a valuable source of cybersecurity information. As discussed further below, the FBI and Secret Service regularly share cyber threat information with the private sector through established programs. Furthermore, the DHS National Cybersecurity and Communications Integration Center (NCCIC), while not a law enforcement organization, routinely provides alerts, vulnerability information, and analysis reports that can help organizations detect, prevent, and mitigate incidents. It also provides automated feeds of indicators of compromise that organizations can access for free.[25]

Historically, some private sector organizations have expressed concern that the Federal

---

financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation; and water and wastewater systems. *Id.*

[23] *See* Exec. Order No. 13,691, 80 Fed. Reg. 9347 (Feb. 20, 2015), available at http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf.

[24] For instruction on how to share and receive information consistent with CISA, please review DEP'T OF JUSTICE & DEP'T OF HOMELAND SEC., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf, and DEP'T OF HOMELAND SEC., CYBERSECURITY INFORMATION SHARING ACT – FREQUENTLY ASKED QUESTIONS, https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf.

[25] See the US-CERT web site for additional information, available at https://www.us-cert.gov; https://www.us-cert.gov/ais.

Trade Commission (FTC) or Department of Justice might consider sharing cybersecurity threat information with other private sector organizations to be a violation of federal antitrust laws. Those concerns, however, have been addressed in policy and by statute. The FTC and the Department's Antitrust Division issued a joint statement in 2014 reaffirming their views that antitrust laws are not—and should not be—an impediment to legitimate cyber threat information sharing. Furthermore, CISA included a statutory exception to liability under antitrust laws for sharing cyber threat indicators and defensive measures in accordance with that statute.[26]

II. Responding to a Cyber Incident: Executing Your Incident Response Plan

An organization can fall victim to a cyber intrusion or attack even after taking reasonable precautions. Consequently, being prepared to execute a vetted, actionable cyber incident response plan is critical. A robust incident response plan does more than merely provide procedures for handling an incident; it also provides direction on how a victim organization can continue operating while managing an incident and explains how to work with law enforcement and/or incident response firms as an investigation is being conducted. An organization's incident response plan should give serious consideration to all of the steps outlined below.

Step 1: Make an Initial Assessment

a. Data Collection

During a cyber incident, a victim organization should immediately assess the nature and scope of the incident. It is important at the outset to ascertain whether the incident was caused by a malicious act, human error, or a technological glitch—or possibly a combination of those factors. The nature of the incident will determine the type of assistance an organization will need, the type of damage it will need to mitigate, and the remedial efforts that may be required.

Having appropriate logging capabilities enabled can be critical to identifying the origin of a cyber incident. A system administrator should use all available logs to attempt to identify:

- the affected computer systems;
- the apparent origin of the incident, intrusion, or attack;
- any malware used in connection with the incident;
- any remote servers to which data was sent (if information was exfiltrated); and
- the identity of any other victim organizations, if such data is apparent in logged data.

[26] See 6 U.S.C. § 1503(e)(1).

In addition, the initial assessment of the incident should document:

- which users are logged onto the network;
- which processes are running;
- current external connections to the computer systems; and
- all open ports and their associated services and applications.

Any communications received by the organization that might relate to the incident (in particular, threats, claims of credit, or extortionate demands) should be documented and preserved. Suspicious calls, emails, or other requests for information about the incident should also be treated as part of the incident.

Evidence that an intrusion or other criminal act has occurred will typically include network logs and file creation data indicating that someone improperly accessed, created, modified, deleted, or copied files, logs, or other data; changed system settings; or added or altered user accounts or permissions on the network. In addition, an intruder may have left behind indicators of compromise, such as "hacker tools" or data from another intrusion.

An intruder with "root level access" has the highest privileges given to a user working with an operating system or other program and has as much authority on the network as a system administrator, including the authority to access files, alter permissions and privileges, and add or remove accounts. In the case of a root-level intrusion, victims should be vigilant for signs that the intruder has gained access to multiple areas of the network.

The victim organization should ensure that its actions do not unintentionally or unnecessarily modify stored data. *Such modification could hinder incident response and internal or criminal investigations. In particular, potentially relevant files should not be deleted and, at the very least, any modifications should be recorded.*

b. Working with Incident Response Firms

Increasingly, victim organizations enlist private sector cybersecurity or incident response firms to assess and respond to cyber incidents on their behalf. Incident response firms are often on scene collecting evidence before federal investigators are even initially contacted. Therefore, in choosing such a firm, an organization should ensure it selects one that is well acquainted with forensically sound methods of evidence collection that do not taint or destroy evidence. An incident response firm should also be capable of preserving data in a manner that will allow it to

be used later as evidence.

A victim organization may direct its incident response firm to prepare a forensic report about the causes and consequences of a cyber incident. The organization may later seek to protect that report from disclosure in connection with any civil litigation or regulatory action that results from the incident. When a forensic report is prepared at the direction of an organization's attorneys, the organization may seek to withhold it from anyone outside the organization under a claim of attorney-client communications or attorney work product privileges. Setting aside the legal viability of such claims of privilege, withholding of such information from law enforcement—or even delaying the sharing—can make criminal investigation more difficult.

It is important to emphasize that law enforcement's need for a crime victim's information differs from that of parties interested in assessing whether the victim organization is liable for the incident. Law enforcement is responsible for investigating a criminal violation with the objective of identifying, apprehending, and prosecuting the perpetrator, as appropriate. Accordingly, law enforcement is focused on collecting information *about the perpetrator's criminal conduct* that can be used to identify and prosecute her or him. Therefore, the information that law enforcement needs is frequently limited to technical data that can be used to track activities and events on a victim company's network.

Such technical information is distinct from, but sometimes commingled with, an incident response firm's assessment of the strengths or weaknesses of an organization's cybersecurity practices prior to an incident or its performance during the incident. Law enforcement is flexible and willing to work with a victim organization to find a suitable means of obtaining technical information about a cyber incident consistent with the victim organization's concerns and the needs of law enforcement, which may sometimes mean obtaining something other than the full forensic report. Alternative means of producing sought after technical data may include producing a summary of an incident response firm's report, creating an excerpted version of a forensic report, or interviewing personnel who can provide the required technical data.

Federal investigators may need to coordinate with a victim organization's incident response firm to procure the technical data the firm has already collected. A victim company can assist law enforcement by facilitating such coordination. Good channels of communication between federal investigators and an incident response firm will avoid duplication of effort, minimize disruption of the victim organization's operations, and expedite the investigation.

Step 2: Implement Measures to Minimize Continuing Damage

Understandably, an organization that has suffered a cyber incident typically will

immediately institute measures to prevent any further damage. Such steps may include rerouting network traffic, filtering or blocking a distributed denial-of-service attack, or isolating all or parts of the compromised network. In the case of an intrusion, a system administrator may elect either to block further unauthorized access to the system or to allow it to continue to help identify the source of the attack and/or the scope of the compromise.

An organization that has prepared for a cyber incident by backing up its data may elect to abandon data stored on a compromised network and restore the network to a prior state using saved data. However, before doing so, it should confirm that the backed-up data is not also compromised. Failure to confirm the integrity of the backed-up data may result in re-infection.

If a victim organization obtains information regarding the location of exfiltrated data or the apparent origin of a cyber attack, it has several options. First and foremost, we strongly recommend that it share this information with law enforcement *immediately*. Federal investigators may be able to secure the stolen data using its legal authority. However, the organization may also choose to contact the system administrator of the network on which its stolen data resides or from which the attack originates. Doing so may stop the attack, assist in regaining control of stolen data, or help determine the true origin of the malicious activity. A victim organization may also choose to blunt the damage of an ongoing intrusion or attack by "null routing"[27] malicious traffic, closing the ports being used by the intruder to gain access to the network, or otherwise altering the configuration of a network to thwart the malicious activity. Wherever possible, the organization should coordinate its actions with law enforcement to avoid taking measures that unnecessarily taint evidence or limit investigative options.

The victim organization should keep detailed records of whatever steps it takes to mitigate the damage and keep track of any incurred costs. Such information may be used later to establish criminal violations, recover remediation costs from the perpetrator, or determine the perpetrator's sentence if he or she is later prosecuted and convicted.

Step 3: Record and Collect Information

1. *Keep Logs, Notes, Records, and Data*

A victim organization should take immediate steps to preserve existing log files. *If a victim organization has not enabled logging on an affected system, it should do so immediately*. It should also consider increasing the default size of log files on its servers to prevent vital information from

[27] A null route directs the system to drop network communications that are destined for a specified IP address on the network, so a system will no longer send any response to the originating IP address. This means the system will continue to receive data from the attackers but will no longer respond to them.

being overwritten. Computer file logs that may assist in analyzing or investigating an incident come in a variety of forms, including event logs, active directory logs, and browser history logs. Forensic examinations are based on artifacts found in various repositories (e.g., registry hives, prefetch data, and scheduled tasks). Preventing as much of that data as possible from being erased or overwritten can be crucial to performing a post-incident analysis or investigation.

A victim organization should document or record any ongoing suspicious network activity. A victim organization may use a "sniffer" or other network-monitoring tool to record communications between the intruder and any of its targeted servers during an attack. Such monitoring implicates federal surveillance statutes such as the Wiretap Act but is typically lawful when conducted in accordance with CISA's cybersecurity monitoring provision[28] or a statutory exception, such as consent[29] or the rights or property exception.[30] Many organizations consult with their legal counsel beforehand to make sure such monitoring is conducted lawfully and consistent with the organization's employment agreements and privacy policies.

In addition, a victim organization should direct its personnel and personnel from incident response firms to keep a contemporaneous written record of all steps undertaken. Documenting actions while responding to the incident or shortly thereafter will minimize the need to rely solely on the recollections of personnel to reconstruct the order of events. As the investigation progresses, information that was collected by the organization during incident response may have unanticipated significance.

The types of information that a victim organization should record and retain include:

- a description of all incident-related events, including dates and times;
- information about incident-related phone calls, emails, and other contacts;
- the identity of persons working on tasks related to the intrusion, including a description of their role or responsibilities, the amount of time spent, and the approximate hourly rate for those persons' work;
- the identity of the systems, accounts, services, data, and networks affected by the incident and a description of how these network components were affected;
- information relating to the amount and type of damage inflicted by the incident, which can be important in civil actions by the organization and in criminal prosecutions;

[28] 6 U.S.C. § 1503(a).
[29] 18 U.S.C. §§ 2511(2)(c)-(d).
[30] 18 U.S.C. § 2511(2)(a)(ii).

- information regarding network topology;
- the type and version of software being run on all affected systems; and
- any peculiarities in the organization's network architecture, such as proprietary hardware or software.

Ideally, as few employees as practicable should be assigned the responsibility of retaining custody of such information. This will help to ensure that records are properly preserved, can be produced later, and are available as evidence. Proper handling of this information can be useful in rebutting claims in subsequent legal proceedings (whether criminal or civil) that electronic evidence has been tampered with or altered.

2. *Image the Affected Computers and Check Backups*

A victim organization, or the incident response firm it hires, may make a "forensic image" of the affected computers to preserve a record of a server at the time of the incident for later analysis and potentially for use as evidence at trial. A "forensic image" is an exact, bit-for-bit copy of data on an electronic device. An image provides a perfect "snapshot" of the system at the time the image was created, including deleted files, slack (apparently empty) storage space, system files, and executable files. It is important to create an image using forensically sound procedures; otherwise, there is a risk of altering the system in a manner that compromises its analytic or evidentiary value.

Once a victim organization makes copies, it should write-protect the media to help ensure that it is not altered. A victim organization should also restrict access to the preserved media. Doing so and documenting who has maintained possession of the media (i.e., recording the "chain of custody") will help later establish the authenticity of the copy. It may also protect it from malicious insiders. Properly trained personnel will know the generally accepted methods of generating and preserving copies of data.

The victim organization should also locate any regularly generated backups, which may assist in identifying any changes an intruder made to the systems. Such backups should be isolated from the affected systems to prevent them from being overwritten or altered. If they are later used to restore the system, they should first be checked on isolated computers in case they also turn out to be compromised or infected.

Computer intrusions are commonly only discovered long after the initial intrusion occurred. Consequently, an organization should be prepared to retrieve backups that are quite old to find one that pre-dates the intrusion.

Step 4: Notify

1. *People Within the Organization*

The incident response plan should identify the appropriate points of contact (POCs) within the organization who must be notified of the cyber incident. POCs will typically include senior management, incident response firms, information technology and physical security coordinators, communications or public affairs personnel, and inside and outside legal counsel. POCs should be promptly alerted *in the manner described in the incident response plan*. Adhering to the agreed upon means of contacting POCs will help prevent social engineering attacks designed to extract sensitive information from unsuspecting personnel. Once contacted, POCs should be apprised of any information needed to inform immediate incident management decisions.

In addition to identifying POCs, the incident response plan should describe the circumstances under which POCs should be contacted. Minor cyber incidents may be handled without immediately notifying all POCs; if so, the plan should describe those incidents and the subset of POCs who should be contacted. An incident response plan that sets triggers or thresholds for notification can help avoid over-notification, which can undermine the effectiveness of the plan.

2. *Federal Responders*

A victim of a cyber incident can receive assistance from federal agencies that are poised to investigate the incident, help mitigate its consequences, and help prevent future incidents. Federal law enforcement has highly trained investigators who specialize in responding to cyber incidents to identify, apprehend, and disrupt the activities of criminals who cause cyber incidents and to prevent harm to other potential victims. In addition to law enforcement, other federal responders like DHS provide technical assistance to protect assets, mitigate vulnerabilities, and can offer on-scene response personnel to aid in incident recovery.[31]

a. Contacting Law Enforcement

If an organization suspects a cyber incident was the result of criminal activity, it should contact law enforcement as soon as practicable. Historically, some companies have been reluctant to contact law enforcement following a cyber incident fearing that a criminal investigation could disrupt their business or cause unwarranted reputational harm. Such fears are misplaced. Federal

[31] Annex D of the NATIONAL CYBER INCIDENT RESPONSE PLAN (2016), available at https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf, provides detailed instructions for reporting a cyber incident to the federal government.

investigators are committed to minimizing the harm and inconvenience that might result from reporting a cyber incident. Recognizing that a data breach or cyber attack can be a harrowing event, investigators take care not to further victimize an organization that has suffered a breach or attack.

The FBI and Secret Service strive to conduct cyber investigations that cause as little disruption as possible to a victim organization's normal operations. They also recognize the need to work cooperatively and discreetly with victims. Whenever possible, they will use investigative techniques that avoid computer downtime or displacement of an organization's employees. When it is necessary to use a disruptive investigative technique, the FBI and Secret Service will do so with the goal of minimizing the duration and scope of any disturbance and will work alongside the victim organization to ensure that any concerns are fully addressed.

The FBI and Secret Service also will work with victim companies to avoid unwarranted disclosure of information. They will generally coordinate public statements concerning the incident with victim companies to ensure that harmful or sensitive information is not needlessly disclosed. Victim companies should likewise consider sharing press releases regarding a cyber incident with investigators before issuing them to avoid releasing information that might impede the ongoing investigation.

i. The Benefits of Contacting Law Enforcement

Contacting law enforcement may also prove beneficial to a victim organization. Law enforcement can use tools and legal authorities that are unavailable to private entities to identify and apprehend whoever is responsible for a cyber incident. Federal investigators can obtain data to trace an intrusion or attack to its source using search warrants, court orders, and subpoenas. U.S. law enforcement also frequently enlists the assistance of international law enforcement partners to obtain evidence and conduct investigations in other countries. These tools and relationships can greatly increase the odds of successfully apprehending an intruder or attacker and securing exfiltrated data. An arrest can also prevent further damage to the victim organization and deter other would-be cyber criminals.

Law enforcement also has incident response services it can deploy in connection with major cyber incidents. The FBI's Cyber Task Forces located in each of its 56 field offices across the country deliver investigative response services through the FBI's Cyber Action Team (CAT), which consists of a cadre of highly trained and experienced FBI special agents and computer scientists capable of deploying globally in response to particularly sophisticated cyber incidents. The FBI is also equipped to collect and analyze malware and to provide programs and resources that allow companies to receive intelligence on cyber threats affecting their industries.

Reporting a data breach to law enforcement may also affect data breach notification requirements. As of August 2018, all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have passed data breach reporting laws requiring companies to notify customers whose data has been compromised or to report breaches to state agencies. However, many data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice will impede an investigation. Some state laws also allow a victim company to forego notification altogether if the victim company consults with law enforcement and thereafter determines that the breach will not likely result in harm to the individuals whose personal information has been taken or accessed.

Reporting a cyber incident to law enforcement may have additional benefits for organizations in regulated industries. Regulatory agencies will sometimes inquire about the cause of a data breach or other cyber incident. The FTC has affirmed that it views companies that report data breaches and cyber incidents to law enforcement and cooperate with the subsequent investigation more favorably than those that do not.[32] Upon request of the company, the Department of Justice is also willing to inform regulatory agencies of any cooperation that a company facing a regulatory inquiry has furnished to the government.

ii. Law Enforcement and Information Sharing During a Cyber Incident

The enactment of CISA has made cooperating with law enforcement simpler by addressing common concerns about legal impediments to sharing information with the government. While CISA was not enacted to address law enforcement's evidence-gathering needs, its information-sharing provision authorizes private entities to share specific types of cyber threat information with any federal agency, including law enforcement agencies. Specifically, CISA authorizes non-federal entities to voluntarily share "cyber threat indicators"[33] and "defensive measures"[34] with law enforcement for a cybersecurity purpose,[35] notwithstanding any other provision of law.[36] Such authorized sharing can be particularly helpful during a cyber incident.

CISA's authorization to share information with the federal government is bolstered by liability protection that covers cyber threat indicators and defensive measures that a private entity

---

[32] Mark Eichorn, *If the FTC Comes to Call*, FTC: BUS. BLOG (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call.
[33] A "cyber threat indicator" is defined by 6 U.S.C. § 1501(6).
[34] A "defensive measure" is defined by 6 U.S.C. § 1501(7).
[35] A "cybersecurity purpose" is defined by 6 U.S.C. § 1501 (4).
[36] *See* 6 U.S.C. § 1503(c).

shares with other private entities and with DHS, as provided for by CISA.[37] CISA's explicit liability protection also extends to communications between non-federal and federal entities—including law enforcement agencies—about cyber threat indicators and defensive measures that were previously shared with DHS pursuant to CISA and subsequently shared by a non-federal entity with another agency to describe a cybersecurity threat or develop a defensive measure.[38]

Organizations that report incidents or other information to law enforcement receive certain legal protections for doing so. Law enforcement treats information collected during a criminal investigation as sensitive information that is safeguarded from unwarranted or unnecessary disclosure. In addition, the Freedom of Information Act[39] (FOIA) exempts certain records or information gathered for law enforcement purposes from disclosure. CISA also affords protection from state and federal disclosure laws when cyber threat indicators are shared with the FBI, Secret Service, or another federal entity consistent with CISA.[40] It is also noteworthy that law enforcement does not routinely disclose evidence it gathers during its cyber investigations to regulators.

b. The Department of Homeland Security

DHS has components dedicated to cybersecurity that not only collect and report on cyber incidents, phishing, malware, and other vulnerabilities, but also provide certain non-law enforcement incident response services, including technical assistance. The NCCIC serves as an around-the-clock centralized location for cybersecurity information sharing and non-investigative asset response coordination.[41] By contacting the NCCIC, a victim organization can both share and receive information about an ongoing incident that may prove beneficial to both the victim organization and the government.

3. *Regulators*

Some private sector organizations are regulated by state and federal regulatory agencies and may be required to report a data breach or other cyber incident. While guidance to such organizations concerning how to notify regulators is beyond the scope of this document, a cyber

---

[37] *See* 6 U.S.C. §§ 1503(c), 1504(c)(1)(B), 1505(b)(2).
[38] *See* 6 U.S.C. § 1504(c)(1)(B)(i).
[39] 5 U.S.C. § 552, as amended by Pub. L. No. 104-231, 110 Stat. 3048.
[40] Relevant FOIA exemptions include Exemption 4 (which provides for non-disclosure of confidential commercial information) and Exemption 7 (which provides for non-disclosure of certain information compiled for law enforcement purposes). *See* DEP'T OF JUSTICE, GUIDE TO THE FREEDOM OF INFORMATION ACT (2009), https://www.justice.gov/oip/doj-guide-freedom-information-act-0. Further, cyber threat indicators and defensive measures shared in accordance with CISA with the federal government or with or by a State, tribal, or local government is exempt from FOIA and similar disclosure laws. *See* 6 U.S.C. §§ 1504(d)(3), 1503(d)(4)(B).
[41] *See* Presidential Policy Directive – United States Cyber Incident Coordination (PPD-41), 2016 WL 3996354 (Jul. 26, 2016).

incident response plan should take into account whether a victim organization may need to notify regulators and how best to do so. Organizations should consult with counsel to ascertain their obligations under state data breach notification laws and similar applicable regulations.

It is worth noting that the Department of Justice does not have a regulatory role in regard to data breaches or cyber incidents. Accordingly, reporting a cyber incident to the Department or to federal criminal investigators will not lead to regulatory enforcement action by the Department for the incident.

4. *Other Potential Victims*

If a victim organization or the incident response firm it hires uncovers evidence of additional victims while responding to a cyber incident, it should consider promptly notifying the other presumed victims. A notifying organization may choose to contact other victims directly; however, there are benefits to allowing law enforcement to contact other victims. Doing so may insulate the notifying victim from unwanted exposure and allow law enforcement to conduct further investigation.

Similarly, if a forensic examination reveals an unreported software or hardware vulnerability, the victim organization should notify law enforcement, the relevant vendor, or a public or private entity that receives and disseminates vulnerability disclosures, such as the NCCIC. Such notifications may prevent others from being victimized and afford potential victims the opportunity to protect themselves. The notifying organization may also benefit because other victims may be able to provide helpful information from their own experience managing the same cyber incident, including information regarding the perpetrator's methods, a timeline of events, or effective mitigation techniques that may thwart the intruder.

III. What Not to Do Following a Cyber Incident

A. Use a Compromised System to Communicate

The victim organization should avoid, to the extent reasonably possible, using a system suspected of being compromised to communicate about mitigation strategies or how it intends to respond to the incident. Otherwise, it risks informing the perpetrator of its plans, which may allow him or her to circumvent or disrupt mitigation efforts.

To avoid becoming the victim of a "social engineering" attack (i.e., use of a ruse or guile to lure a target into taking action that will compromise the security of the system or data), employees of the victim organization should not disclose incident-specific information to anyone

inquiring about an incident without first verifying their identity. A victim should keep track of any odd or suspicious inquiries concerning the incident and share them with law enforcement.

B. Hack into or Damage Another Network

A victim of an intrusion or data breach may conduct an investigation that uncovers information linking a computer that is not controlled by the victim to the incident. For instance, a victim organization's server logs may reveal the Internet Protocol (IP) address of a computer that suspiciously accessed the victim's network or downloaded data.[42] Such information may provide valuable information that government authorities can use to investigate the incident.

However, a victim organization should not unilaterally respond to a cyber incident by accessing, modifying, or damaging a computer it does not own or operate, even if the computer appears to have been involved in an attack or intrusion. Regardless of the victim's motive, doing so may violate federal law[43] and possibly also the laws of many states[44] and foreign countries, if the accessed computer is located abroad.[45] A violation of those laws could result in civil and criminal liability.

Taking retaliatory action may be ill-advised for other reasons too. For instance, it may cause unintended harm. Many intrusions and attacks are launched from systems a perpetrator has compromised and used as an intermediary to relay his or her communications. This tactic is commonly adopted by perpetrators to conceal their identities by interposing systems between them and their victims. But it also means that efforts to access or attack a computer linked to the incident—sometimes called "hacking back"—could wind up targeting an unwitting, innocent victim whose system is being exploited by the perpetrator. Accessing data on an intermediary system may also intrude upon the privacy of third parties whose data is stored there.

A private party who accesses another computer in response to an intrusion may also unknowingly interfering with a law enforcement investigation. A perpetrator targeted by a private party may change tactics or modify operations if he or she detects a hack back attempt; such a deviation in behavior can undermine an ongoing law enforcement investigation that is tracking the perpetrator. Furthermore, a perpetrator who detects a hack back attempt may choose to retaliate, causing further damage to the victim.

---

[42] An Internet Protocol address is a number assigned to every device connected to a network. It is used to route Internet communications between a sender and a recipient.

[43] *See* 18 U.S.C. § 1030.

[44] A summary of state computer crime statutes is available at http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[45] A summary of the computer crime statutes worldwide is available at http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

Instead of taking unilateral action, a victim should promptly contact and begin collaborating with law enforcement by providing any information that might help trace the perpetrator. Federal investigators possess legal authority that can help identify the perpetrators and secure stolen data, even if either (or both) is located abroad. Law enforcement is prepared to use such authority to assist victims and advance an investigation.

IV. What to do After a Cyber Incident Appears to be Resolved

Even after a cyber incident appears to be under control, a victim organization should remain vigilant. Many intruders attempt to regain access to previously compromised systems. It is possible that, despite its best efforts, a company that has addressed known security vulnerabilities and taken all reasonable steps to expel an intruder has not discovered all of the intruder's means of gaining entry to the network. A victim organization should continue to monitor its system for anomalous activity and be vigilant for new signs of re-infection and compromise.

Once the victim organization has recovered from the attack or intrusion, it should adopt measures to prevent similar attacks in the future, such as addressing shortcomings in its security practices, acquiring resources to better secure its systems, and fortifying relationships with law enforcement and other key response organizations. It should conduct a post-incident review of the organization's performance and assess the strengths and weaknesses of its execution of its incident response plan. Part of the assessment should include ascertaining whether the organization followed each of the steps outlined above and, if not, why not. The organization should note and discuss deficiencies and gaps in its response and take remedial steps as needed.

Cyber Incident Preparedness Checklist		
Before a Cyber Attack or Intrusion		
Educate the organization's senior management about cyber threats and risk management.		
Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.		
Identify mission critical data and assets (*i.e.*, your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.		
Create an actionable incident response plan.	Test the plan by conducting exercises.	
	Keep the plan up-to-date to reflect changes in personnel and structure.	
Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident.		
Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable).		
Institute basic cybersecurity procedures, such as a patch management program.		
Have procedures in place that will permit lawful network monitoring.		
Ensure legal counsel is familiar with legal issues associated with cyber incidents.		
Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan.		
During a Cyber Attack or Intrusion		
Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.		
Minimize continuing damage consistent with your cyber incident response plan.		
Collect and preserve data related to the incident by --	"Imaging" the network.	
	Keeping all logs, notes, and other records.	
	Keeping records of ongoing attacks.	
Consistent with your incident response plan, notify --	Appropriate management and personnel within the victim organization.	
	Law enforcement.	
	Department of Homeland Security.	
	Other possible victims.	
Do not --	Use compromised systems to communicate.	
	"Hack back" or intrude upon another network.	
After Recovering from a Cyber Attack or Intrusion		
Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.		
Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.		