2018 Government Practice Seminar

CYBERSECURITY FOR STATE AND LOCAL GOVERNMENT ATTORNEYS

11:00 a.m. - 12:00 p.m.

Presented by

Luke Dawson
Assistant Attorney General
Office of the Attorney General of Iowa
1305 E. Walnut St.
Des Moines, IA 50319
Phone: 515-414-6187

Beth Manley
Iowa State Association of Counties
5500 Westown Parkway, Suite 190
West Des Moines, IA 50266
Phone: 515-244-7181

John Lande
Dickinson Mackaman Tyler & Hagen PC
699 Walnut St, Suite 1600
Des Moines, IA 50309

FRIDAY, MAY 4, 2018

Cybersecurity for State and Local Government Attorneys—Outline

Why is cyber security important?

- **Good Target.**
  - Public sector entities solicit, store, process, and transmit large amounts of sensitive information. Examples include:
    - Personal Information.[1]
    - Protected Health Information.[2]
    - Federal Tax Information.[3]
    - Criminal Justice Information.[4]
    - Other state sensitive information.[5]
    - Trade secrets.[6]
    - State secrets/classified information.
  - Public sector entities are responsible for managing and maintaining critical infrastructure that supports a variety of citizen services and government programs, including communications infrastructure, election systems, energy infrastructure, transportation infrastructure, and water systems. Much of this infrastructure is accessed/operated by or through electronic systems.
- **Actually Targeted.**[7]
  - Public sector entities are persistently targeted by a variety of actors, through a variety of methods and means.
    - General (all sectors):
      - In 2017, there were 53,000 incidents,[8] 2,216 with confirmed breaches[9]
      - Of the 2,216 confirmed breaches: 73% were perpetrated by outsiders; 28% involved internal actors; and 2% involved partners.
      - Of the 2,216 confirmed breaches: 48% featured hacking; 30% included malware; 17% were the result of errors; 17% were social attacks; 12% involved privilege misuse; and 11% involved physical actions.
    - Public Sector:
      - In 2017, in the public sector, there were 22,788 incidents, 304 with confirmed breaches.
      - Of the 304 confirmed breaches: 67% were perpetrated by outsiders; 34% involved internal actors; and 2% involved partners.

- Of the 304 confirmed breaches: 44% featured cyber espionage, many of which were state affiliated; 50% were the result of errors; 24% involved phishing; and 17% involved privilege misuse.

■ In Iowa:

- In Iowa, in 2017, the Office of the Chief Information Officer's (**"OCIO"**) Security Operations Center (**"SOC"**)—a centralized Cyber Threat monitoring center—identified 2,019 incidents involving the cities, counties, school districts, and state agencies to which the SOC provides services.

■ Case studies:

- IPERS/Account Takeover: Criminals obtained Social Security numbers and birth dates from other sources and used that information to register for online accounts for retirees who had not yet set up an online account.They then changed the bank account where the IPERS-member's monthly payment was electronically deposited.[10]
- Johnston Schools/Hacking: Hackers obtained and posted student information online, which was subsequently used to send anonymous text messages to parents threatening violence in schools.[11]
- *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F.Supp.3d 471 (S.D.N.Y. 2017): Fraudsters sent ghosted emails to corporate accounting departments that convinced accounting employees to initiate $4.7 million wire transfers.
- *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*, --- Fed.Appx. ----, 2018 WL 1804338 (9th Cir. April 17, 2018): Seafood importer did not have insurance coverage for wire transfer initiated by employee when the employee was duped into initiating funds transfer based on spoofed email from fraudsters. Insurance policy excluded coverage for data that was entered into electronic system by authorized by employees.
- *See* the Iowa Attorney General's Office's Consumer Protection Division's Website for Data Breach Notices issued in Iowa: https://www.iowaattorneygeneral.gov/for-consumers/security-breach-notifications/.

○ **Costly/Time Consuming.**[12] In 2017, the average **per-record** cost of data breach was **$225** in the United States. Public sector entities are on the lower end of the scale, at **$71** per record, in large part because citizens cannot opt out of their government, like they can their health care provider or bank.

■ Forensics to determine cause and scope.

■ Organizing breach response team.

■ Contacting/working with law enforcement.

■ Notifying those affected. *See, e.g.*, Iowa Code § 715C.

- Providing credit-monitoring services to victims.
- Reporting to regulators.
- Subsequent audit/remedial measures.
- Regulatory penalties, including fines and loss of access to information necessary to carry out core mission.
- Loss of reputation/public trust.
- Legal fees/Litigation.

What are some of the ethical components of Cybersecurity that attorneys need to consider?

- **2012 "Technology Amendments" (Effective in Iowa as of October 15, 2015):**
  - Iowa R. Prof. Resp. 32:1.1 (Competence): "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation."
    - **Comment 8:** *Maintaining Competence*. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology** . . . .
      - "[This rule] requires a lawyer to provide competent representation, and [the corresponding comment] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice. . . . [I]n order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology . . . . For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."[13]
  - Iowa R. Prof. Resp. 32:1.6(d) (Confidentiality of Information): "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."
    - **Comment 18:** "Paragraph [(d)] requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. . . . The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph [(d)] if the lawyer has made **reasonable efforts** to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to[:]

      (1) the sensitivity of the information,

      (2) the likelihood of disclosure if additional safeguards are not employed,

      (3) the cost of employing additional safeguards,

      (4) the difficulty of implementing the safeguards, and

      (5) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

      A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forgo security measures that would otherwise be required by this rule. Whether a lawyer may be required to take additional steps to

safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these rules. . . .

- **Comment 19:** Applies the same general principles as outlined in comment 18 to transmitting communications.

- Iowa R. Prof'l Resp. 32:1.15 cmt. 1 (safekeeping of property): "A lawyer should hold property of others with the care required of a professional fiduciary."

- **ABA FORMAL OPINION 477, MAY 11, 2017: SECURING COMMUNICATION OF PROTECTED CLIENT INFORMATION.**

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. . . .
>
> [I]n an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the **reasonable efforts** standard: . . . "rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a **'process'** to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."[14]

- **Takeaways:**
  - Engage in an ongoing risk assessment process. Fact specific, no one size fits all.
    - Understand the sensitivity of the information under your control, who wants to get it, and how they are most likely to go about that.
    - Understand where information enters, is stored or processed, and exits. *E.g.*, networks, servers, devices.
    - Identify reasonable, cost-effective security measures you can institute to safeguard that information over the course of its lifecycle. *E.g.*, firewalls; Anti-Malware, Anti-Spyware, Antivirus; remote wipe, encryption, multi-factor authentication.
    - Take into consideration where/how recipients of communications may receive confidential information transmitted by you. For example, sending attorney-client

privileged communications to clients who may access such communications on work devices that are subject to employer-monitoring policies can waive the privilege.[15] You may need to warn the client or implement an encryption solution.

- Label communications as privileged/confidential where appropriate.
- Train non-lawyer assistants.
- Conduct due diligence on Vendors providing services.
- Engage experts to assist in developing and implementing best practices.
- Discuss security practices with clients and obtain informed consent in cases of deficient security measures.

What statutes and regulations apply to the Information I have? In the United States, security/privacy laws are sector specific, such as HIPAA, FERPA, or Gramm-Leach Bliley. However, all jurisdictions have breach notification laws, which generally apply to Personal Information or Personally Identifiable Information.

- **Iowa Code section 715C:** Breach notification statute that applies to **"Personal Information"** of **"Consumers**."
  - **Key Definitions:**
    - **"Personal Information"** means: "an individual's [(a)] first name or first initial and last name [(b)] in combination with any one or more of the following data elements that relate to the individual [(c)] if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable *or* are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security:

      (1) Social security number.

      (2) Driver's license number or other unique identification number created or collected by a government body.

      (3) Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account.

      (4) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

      (5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.

    - **"Consumer"** means: "an individual who is a resident of *this state*."

    - **"Breach of security"** means the "unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. **'Breach of security'** also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.

- **Requires:**
    - Notice to consumers impacted by breach of security.
- **Dictates:**
    - Timing: In "the most expeditious manner possible and without unreasonable delay," subject to coordination with law enforcement and time to identify those affected, scope, and remediation.
    - Manner of notice: written notice to last available address; electronic notice if customary method of communication is by electronic means; substitute notice, *i.e.*, email, posting online, and major statewide media, where cost of notice would exceed $250,000.
    - Content of notice: description of the breach; date of occurence; type of information obtained; information for consumer reporting agencies; advice to consumer to report suspected incidents of identity theft to local law enforcement or attorney general.
- **Does not apply:**
    - To data of entities (*e.g.*, FEIN #s): "an individual's."
    - To non-residents: "this state."[16]
    - When data is merely accessed by an unauthorized individual, as opposed to "acquired."
        - Is the information in the physical possession and control of an unauthorized person? Lost or stolen laptop?
        - Has the information been downloaded or copied?
        - Has the information been used by an unauthorized person? Fraudulent accounts opened or instances of identity theft reported?
    - When after appropriate investigation or consultation with law enforcement, no "reasonable likelihood of financial harm."
    - "Encryption Exception" (or redacted or otherwise altered).[17]
    - "A person who complies with notification requirements or breach of security procedures that provide greater protection to personal information and at least as thorough disclosure requirements than that provided by this section pursuant to the rules, regulations, procedures, guidance, or guidelines established by the person's primary or functional federal regulator."
    - "A person who complies with a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breach of security or personal information than that provided by this section."
    - "A person who is subject to and complies with regulations promulgated pursuant to Tit. V of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801-6809.

- "A person who is subject to and complies with regulations promulgated pursuant to TI. II, subtit. F of the federal Health Insurance Portability Accountability Act of 1996, 42 U.S.C. § 1320d–1320d-9, and Tit. XIII, subtit. D of the federal Health Information Technology for Economic and Clinical."[18]

- **Health Insurance Portability and Accountability Act ("HIPAA"), 45 C.F.R. Parts 160, 162, and 164:** Privacy and security rules that apply to "**Protected Health Information**" held by a "**Covered Entity**" or a "**Business Associate**."
  - **Key Definitions:**
    - **"Protected Health Information"** means individually identifiable health information...that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. [19]
    - **"Individually Identifiable Health Information"** is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[20]
    - **"Covered Entity"** means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.[21]
    - **"Business Associate"** means: with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement...in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter[.][22]
    - **"Breach"** means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.[23]
    - **"Unsecured Protected Health Information"** means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5.[24]
  - **Requires:** Covered Entities and Business Associates must comply with security standards and report Breaches of Unsecured Protected Health Information to the individuals impacted, the media, and the U.S. Department of Health and Human Services ("HHS").
  - **Dictates:**

- **Individuals:** shall be notified of a Breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[25]
- **Media:** shall be notified of a Breach "involving more than 500 residents of a State or jurisdiction...without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[26]
- **HHS:**
  - For Breaches involving 500 or more individuals: Shall be notified of a Breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[27]
  - For Breaches involving less than 500 individuals: The "covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification" electronically to HHS.[28]

- **Does not apply to:**
  - Data held by anyone that is not a Covered Entity or Business Associate.
  - The definition of Protected Health Information excludes Individually Identifiable Health Information:
    - In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
    - In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
    - In employment records held by a covered entity in its role as employer; and
    - Regarding a person who has been deceased for more than 50 years.[29]

- **Iowa Code 554.12101, et. seq. (Uniform Commercial Code).**
  - Governs liability for unauthorized electronic fund transfers (wire transfers or ACH). Payroll is generally processed via ACH transactions, and large payments are made via wire transfers.
  - Under UCC, a bank is liable for unauthorized payment orders (requests for ACH/wire transfers) unless the bank and depositor have agreed to verify the authenticity of payment orders via a commercially reasonable security procedure and the institution accepts the payment order in good faith.
  - UCC governs all payment orders not subject to federal Electronic Funds Transfer Act (EFTA), which only applies to consumer accounts. 15 U.S.C. 1693a(6). EFTA protects consumers from fraudulent transactions (i.e. credit card fraud), but does not apply to non-consumer accounts like schools, local governments, and businesses.

- **Children's Online Privacy Protection Act ("COPPA").**
    - "It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b)." 15 U.S.C. § 6502.
    - 15 U.S.C. § 6502(b) requires:
        - **(A)** websites to provide notice that they are collecting information and obtain verifiable parental consent
        - **(B)** require the operator to provide, upon request of a parent under this subparagraph whose child has provided personal information to that website or online service, a description of the information gathered and an opportunity to refuse further gathering information.
        - **(C)** prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and
        - **(D)** require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

- **CUI (Controlled Unclassified Information) Rule:** Requires Federal Agencies sharing information with Non-Executive Branch entities (including State and Local Governments) to enter into agreements requiring compliance with the CUI Rule, which in turn requires compliance with National Institute of Standards and Technology (**"NIST"**) Special Publication (**"SP"**) 800-171, Revision (**"r."**) 1 for Non-Federal Information Systems (**"CUI Basic"**); unless, specific law, regulation, or policy imposes additional or more specific safeguarding requirements (**"CUI Specified"**).[30]
    - **"Controlled Unclassified Information"** or **"CUI"** is "information the [Federal] Government creates or possesses, or that an entity creates or possesses for or on behalf of the [Federal] Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information . . . or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency."[31]
    - **NIST SP 800-171, r. 1:** "[P]rovides federal agencies with a set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for

protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry."[32]

- **Takeaways:**
  - The CUI Rule is **NOT** self-executing; thus, be sure to review agreements (*e.g.*, data sharing, grant documentation) to see if they impose NIST 800-171, or require compliance with CUI Rule and thereby NIST 800-171, r. 1.
  - Non-Federal Entities (includes State and Local Governments) receiving CUI will increasingly be required to sign data-sharing or other like agreements imposing NIST 800-171, r. 1 as a condition of receipt of federal data/information.
  - Become familiar with NIST 800-171, r.1, implement a security program to ensure compliance, and flow-down requirements to Vendors/other entities that store or process information on your organization's behalf.
  - Remember that NIST 800-171, r. 1, is a *BASELINE* standard, meaning applicable laws, regulations, or Government-wide policies may impose additional/more specific safeguarding requirements. Check out the CUI Registry,[33] for a catalogue of CUI types and corresponding laws, regulations, and policies that may apply to the information your organization receives.
  - Consider requiring NIST 800-171, r. 1 of entities with which your organization shares information.

If I want to start an evaluation of what my organization's cybersecurity risks, where can I start?

- **Risk Assessment:**
  - Establish a committee of diverse participants who each bring different perspectives/knowledge of risks, both organizational and technical.
  - Inventory and Map Data--where information enters, is stored or processed.
  - Assess what legal obligations apply based on the type/origin of data and where it is processed/stored.
  - Consider potential threats based on sensitivity of information, where/how information is stored/processed/transmitted, and threat/vulnerability analysis. Consider leveraging centralized active-threat monitoring services, such as US CyberCom, Multi-State Information Sharing and Analysis Center ("MS-ISAC"), or OCIO's SOC.
    - The SOC is the State's centralized Information Security and Analysis Center. It provides Information Security services, cities, counties, and school districts (71 total participating) and state agencies in Iowa at no charge (except to state agencies) through a federal grant.[34] The SOC combines information from state and federal monitoring systems, cyber intelligence sources, and other sources to facilitate real-time, data-driven decision making.
  - **Conduct a Gap Analysis:**
    - Determine the physical, technical, and administrative safeguards/controls that ***should*** be in place in light of legal/compliance obligations, sensitivity of the information, where information is stored/processed/transmitted, and threat/vulnerability analysis.
    - Assess the physical, technical, and administrative safeguards/controls currently in place.
    - Close gaps by implementing cost-effective safeguards/controls; prioritize safeguards that will produce the greatest results at the lowest cost.
    - Document reasons for selecting (or not selecting) certain safeguards/controls.
    - Repeat this process on an ongoing basis and continually refine your approach to security.
  - After identifying gaps and attempting to close them, identify key risk areas that need enhanced coverage from insurance:
    - First party loss including loss of funds.
    - Third party loss including loss of information.
    - **Compare:**
      - **Iowa Code § 670.7(2) (Municipal Tort Claims Act):** "The procurement of this insurance constitutes a waiver of the defense of governmental immunity as to those

exceptions listed in section 670.4 to the extent stated in the policy but shall have no further effect on the liability of the municipality beyond the scope of this chapter, but if a municipality adopts a self-insurance program or joins and pays funds into a local government risk pool the action does not constitute a waiver of the defense of governmental immunity as to the exceptions listed in section 670.4." **With,**

- **Iowa Code § 669.20 (State Tort Claims Act):** "If a claim or suit against the state is covered by liability insurance, the provisions of the liability insurance policy on defense and settlement shall be applicable notwithstanding any inconsistent provisions of this chapter. The attorney general shall cooperate with the insurance company" *Swanger v. State*, 445 N.W.2d 344, 349 (Iowa 1989) ("We conclude that section 25A.20 does not allow the terms of the State's insurance policy to supersede the administrative process or increase the district court's limited jurisdiction over tort claims against the State.").

- **Risk Assessment Resources:**
  - HIPAA Risk Assessment Tool:
    - Covered Entities and Business Associates are required by HIPAA to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."[35]
    - The Office of the National Coordinator for Health Information Technology and HHS created a tool to assist Covered Entities and Business Associates conduct a risk analysis. The Security Risk Assessment Tool can be found here: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment.
  - Federal Financial Institutions Examination Council ("FFIEC") Risk Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm.
    - Evaluates organization's level of inherent risk and compares it to the level of cybersecurity maturity.
    - Primarily designed for financial institutions, but it provides a useful starting point for organizations of all kinds to determine the level of risk and whether an organization needs to enhance its security controls and processes.

- **Important Steps/Controls to Consider:**
  - Limit collection/retention of data in accordance with applicable records-retention schedules/obligations. The less information you have, the less exposure you face.
  - Limit access to only those who need it (and protect with NDA/Confidentiality Agreements). This can be done through a variety of means:

        - Physical/technical restrictions to areas or systems housing sensitive information. For example, if Information Technology staff is helping you design a new system, push changes from a test environment that does not contain sensitive information to a production environment that is only accessible to individuals with permission to access that information.
        - Policies and procedures applicable to employees, contractors, and agents who may have access to sensitive information.
    - Segregate sensitive information and systems.
    - If employees/contractors are using personal devices to access sensitive information, at a minimum, have a "Bring Your Own Device" (**"BYOD"**) policy establishing minimum security requirements.
    - Ensure strong passwords.
        - Don't write down.
        - Don't share.
        - Use different passwords for different accounts.
        - If suspected compromise, change immediately.
            - **Note:** New NIST Guidelines encourage long, personalized passphrases, rather than complex passwords/strings of characters. Easier to remember, less need to write down, longer and therefore harder to crack.[36]
    - Implement Multi-Factor Authentication.
    - Explore encryption solutions. Encryption can be costly so, to the extent feasible, focus on encrypting information that would trigger a breach under applicable law, *e.g*, data elements that comprise "Personal Information." This is especially important, as many data breach notification statutes do not require notification when data is encrypted.[37]
    - Install remote wipe software on devices that will store sensitive information. If a device is lost or stolen, quickly wiping them can help you establish data was not inappropriately accessed by unauthorized individuals.
    - Intrusion detection/active monitoring. Actively monitoring your network and all connected devices can help you identify and address incidents before they turn into breaches.
    - System Maintenance: follow manufacturer instructions, patch and error-correct immediately. Equifax!
    - Train employees on security best practices. Create a culture of awareness where reporting incidents is valued, not punished.
        - Consider creative training opportunities. For example, there are a number of phishing test tools, such as KnowBe4, that you can use to simulate a phishing attack, then track

which employees interact with the email, and use the information for training opportunities.

- Perform background checks.
- **Don't forget about third parties!**
  - Source selection matters. Choose trusted partners with proven track records of success.
  - Assess third-party information security-practices.
  - Review/update contracts/data-sharing agreements to include robust data security/privacy protections; ensure compliance with applicable law, rules, and regulations; and shift risk to providers to ensure they have skin in the game.
    - Require a third party certificate-of-audit demonstrating compliance with industry standards (e.g., NIST 800-171, NIST 800-53, ISO 27001). If a third party states on their website, or in other marketing literature, that they comply with certain standards, make it a contractual obligation.
    - Permit access to information only for purposes of providing services under the agreement, or as otherwise required by law, and restrict access only to those who need it for such purposes.
    - Ensure your organization retains all rights to your information.
    - Ensure your organization has a way to get the information back at the end of any engagement, *e.g.*, export/transition assistance, and ensure providers are required to permanently delete all of your data such that is not recoverable and in accordance with industry standards.
    - Require that your organization be immediately notified and kept up to date about major cyber incidents or data breaches adversely affecting your information.
    - Shift risk of data-security breach through indemnification provisions. Be specific about the types of costs/expenses you intend to recoup, *e.g.*, root cause assessment, forensic audit, consumer notification, reporting to regulators, staff time, remediation, and legal fees.
    - Be on the lookout for provisions that purport to limit the liability of third parties or provide for sole and exclusive remedies. These provisions often attempt limit liability by a multiplier of contract value and/or for consequential, incidental, indirect, special, or punitive damages. Seek to raise the monetary cap to a higher multiplier (2x, 3x, 4x), refuse to limit Vendor's liability as it relates to consequential, incidental, indirect, special, or punitive damages, and/or include additional "carve outs" to remove certain damages categories as it relates to anticipated or unacceptable risks, such as security breach and breaches of confidentiality or privacy.[38]

- Require third parties to maintain Technology Errors and Omissions and Cyber Liability insurance policies and that you be named as an additional insured.
- Consider whether there are any ancillary agreements required by applicable law. For example, HIPAA: Business Associate Agreements
    - Covered entities are required to obtain satisfactory assurances, in the form of a Business Associate Agreement, that a Business Associate will appropriately safeguard the information before the Business Associate "create[s], receive[s], maintain[s], or transmit[s] electronic protected health information on the covered entity's behalf[.]"[39] Business Associates are also required to obtain the same satisfactory assurances from subcontractors."[40]
    - Examples of Business Associates[41] include cloud storage companies that store Protected Health Information, accounting firms that audit data that might include Protected Health Information, and lawyers that require access to Protected Health Information in order to provide legal counsel.
    - Business associate agreements must contain specific elements specified in 45 C.F.R. § 164.504(e).

■ Enforce!

With all of the security incidents from the Office of Personnel Management, Target, Home Depot, the election, Equifax, and Facebook, odds are that you may be involved in or impacted by a security breach at some point. If that happens, what are the next steps?

- **Don't wait until it happens. Develop a written Incident Response Plan:**
  - Identify and document who is on your incident response team and what their duties and responsibilities are, to include doing everything possible to prevent further exposure, preserve evidence, gather facts, and, if required, notify/report to required persons, and entities, and the media.
  - Establish communication protocols with legal counsel to protect confidentiality under the attorney-client privilege and work product doctrine.
  - Develop procedures to secure/preserve physical and digital evidence, including sending preservation letters to cloud providers.
  - Develop procedures to interview individuals with knowledge of the incident.
  - HIPAA Specific Guidance for Breaches:
    - A Breach is presumed and must be reported unless the Covered Entity or Business Associate can demonstrate "there is a low probability that the protected health information has been compromised based on a risk assessment."[42] The risk assessment must contain at least the following four factors:
      - (i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
      - (ii) The unauthorized person who used the protected health information or to whom the disclosure was made;
      - (iii) Whether the protected health information was actually acquired or viewed; and
      - (iv) The extent to which the risk to the protected health information has been mitigated.[43]
  - Document the incident. Develop tools to help quickly identify key facts:
    - Data type(s) (*e.g.*, personal information) and origin (*e.g.*, federal government)?
    - Who accessed or acquired?
    - How and to what extent was information accessed or acquired?
    - Where do those affected reside?
    - Steps taken to identify scope and cause?
    - Evidence of acquisition or access?
      - System access logs?

- Is the information in the physical possession and control of an unauthorized person? Lost or stolen laptop?
- Has the information been downloaded or copied?
- Has the information been used by an unauthorized person? Fraudulent accounts opened or instances of identity theft reported?

■ Was data encrypted, redacted, or otherwise altered so as to render it unreadable?

■ Magnitude of/evidence of harm?

■ **Helpful Resources:**

- *See* Sample Information Security Data Breach Incident Report for HIPAA Incident (Iowa DHS): https://drive.google.com/open?id=1o70TKfFqjEAHLkpuNTy587BT09FjIqBD.
- *See* Sample Breach Notification Risk Assessment Tool for HIPAA Breach (Iowa DHS): https://drive.google.com/open?id=1o70TKfFqjEAHLkpuNTy587BT09FjIqBD.

○ Define when and under what circumstances to report to law enforcement and credit and identify which specific law enforcement agencies and under what circumstances.

■ If money is involved, immediately report to the FBI's IC3 website: https://complaint.ic3.gov/default.aspx.

- The FBI may be able to stop a wire transaction that is in process if information is promptly reported.
- FBI will collect information and may open an investigation.

■ Consider contacting FBI in the event of a debilitating attack, such as ransomware, because they may have resources to help respond.

■ Law enforcement may direct you to delay sending out the notice if it is conducting an investigation.

○ Define when and under what circumstances to contact credit reporting agencies.

○ Identify and document when an incident becomes a breach, *i.e.*, information/thresholds trigger notification/reporting requirements—may vary based on type of organization, type of information, where it resides, how it's protected, and whether it was acquired or merely accessed. Specifically identify when to:

■ Report to federal and state agencies.

■ Notify consumers pursuant to various federal and state laws, rules, and regulations.

■ Notify the media.

- Develop template breach notices drafted to be customized depending on the facts.

- **When it happens:**
    - **Do:** Follow your plan.
    - **Don't:**
        - Delay in providing notices when they are required or advisable.
        - Communicate with the public about the breach until you know the fundamental facts.

Endnotes:

[1]*See* Iowa Code § 715C.1(11) (defining personal information).

[2]*See* Health & Human Services, *HIPAA for Professionals*, HHS.GOV (last updated June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[3]*See* Internal Revenue Service, PUBLICATION 1075: TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES, I.R.S. PUB NO. 1075 (September 30, 2016), https://www.irs.gov/pub/irs-pdf/p1075.pdf.

[4]*See* Criminal Justice Information Services Division, U.S. Dep't of Justice, CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) SECURITY POLICY (June 5, 2017), https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center.

[5]*See, e.g.*, Iowa Code § 272C.6(4)(*a*) (classifying complaint files, investigation files, other investigation reports and other investigative information in the possession of a licensing board or [its agents] which relates to licensee discipline [as] privileged and confidential).

[6]*See* Iowa Code § 22.7(3).

[7]Statistics in this section were taken from the Verizon, 2018 DATA BREACH INVESTIGATION REPORT (11th ed.), https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf.

[8]An "Incident" means a "security event that compromises the integrity, confidentiality or availability of an information asset."

[9]A "Breach" means an "incident that results in the confirmed disclosure— not just potential exposure—of data to an unauthorized party."

[10]William Petroski, *IPERS: Pension thefts may be linked to Iowa state employees' salary database*, Des Moines Register (Mar. 5, 2018), https://www.desmoinesregister.com/story/news/politics/2018/03/05/ipers-pension-thefts-linked-iowa-state-employees-salary-database/394636002/.

[11]Jason Clayworth, *Iowa governments vulnerable to Johnston-like cyber attacks*, Des Moines Register (Oct. 6, 2017), https://www.desmoinesregister.com/story/news/2017/10/06/iowa-governments-vulnerable-johnston-like-cyber-attacks/741025001/.

[12]Statistics/information in this section were taken from the Ponemon Institute, 2017 COST of DATA BREACH STUDY(June 2017), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

[13]ABA COMMISSION ON ETHICS 20/20 REPORT 105 A (Aug. 2012).

[14]ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 477 (2017) (quoting JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 48-49 (2013). *See also* IOWA STATE BAR ASS'N COMM. ON ETHICS AND PRACTICE GUIDELINES, IA Ethics Op, 14-01 Computer Security (Mar. 10, 2014), http://c.ymcdn.com/sites/iowabar.site-ym.com/resource/resmgr/IA_Lawyer_Weekly/IA_Ethics_Op_14-01.pdf ("Some may elect to modify their existing operating systems, others may determine that their existing systems can be patched or otherwise modified, yet others may determine that no modifications are necessary. Rule 32:1.6 and IA Ethics Opinion 11-01 require only a due diligence process, not a specific result."); IOWA STATE BAR ASS'N COMM. ON ETHICS AND PRACTICE GUIDELINES, Ethics Opinion 11-01 Use of Software as a Service – Cloud Computing (Mar. 10, 2014), http://205.209.45.153/iabar/IowaEthicsOpinions.nsf/b6868944e3311dd0872581100042934f/a092fcd35bb508e0872581100042b927/$FILE/Ethics%20Opinion%2011-01%20--%20Software%20as%20a%20Service%20-%20Cloud%20Computing.pdf ("We believe the Rule establishes a reasonable and flexible approach to guide a lawyer's use of ever-changing technology.").

[15]*Miller v. Zara USA, Inc.*, 56 N.Y.S.3d 302, 303 (N.Y. App. Div. 1st Dept. 2017).

[16]Do not forget to check data breach laws in other states, especially if a breach impacts non-residents. *See* Foley & Lardner LLP, STATE DATA BREACH NOTIFICATION LAWS (last updated Jan. 1, 2018), *available at* https://www.foley.com/files/Publication/c31703ac-ee93-40a5-b295-7e1d9fe45814/Presentation/PublicationAttachment/d6373e89-f460-44fa-afec-a2cbe9fa23fd/17.MC5826%20Data%20Breach%20Chart%200817%20R1.pdf (chart summarizing data breach notification laws in other jurisdictions).

[17]Amended in 2018 to incorporate "accepted industry standards" into definition of **"Encryption."** S.F. 2177, 87th G.A., 2d. Sess. § 8 (Iowa 2018).

[18]Amended in 2018 to expressly exclude HIPAA. S.F. 2177, 87th G.A., 2d. Sess. § 9 (Iowa 2018).

[19]45 C.F.R. § 160.103.

[20]*Id.*

[21]*Id.*

[22]*Id.*

[23]45 C.F.R. § 164.402.

[24]*Id.*

[25]45 C.F.R. § 164.404.

[26]45 C.F.R. § 164.406.

[27]45 C.F.R. § 164.408(b).

[28]45 C.F.R. § 164.408(c).

[29]45 C.F.R. § 160.103.

[30]32 C.F.R. § 2002.14(*h*)(2).

[31]32 C.F.R. § 2002.4(*h*).

[32]*See* Nat'l Inst. of Standards and Tech., U.S. Dep't of Commerce, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS, NIST SPECIAL PUBLICATION 800-171, r. 1 (December 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[33]See U.S. Nat'l Archives & Records Administration, *Cui Categories*, ARCHIVES.GOV (last updated April 2, 2018), https://www.archives.gov/cui/registry/category-list.

[34]For more information about the SOC and the services it provides, *see* https://www.iowacounties.org/wp-content/uploads/2016/05/ISAC-Smart-Connections-Conference-State-of-Iowa-Initiatives-Jeff-Franklin-4.28.16.pptx.

[35]45 C.F.R. § 164.308(a)(1)(ii)(A).

[36]*See* Nat'l Inst. of Standards and Tech., U.S. Dep't of Commerce, DIGITAL IDENTITY GUIDELINES: AUTHENTICATION AND LIFECYCLE MANAGEMENT, NIST SPECIAL PUBLICATION 800-63B (June 2017), https://pages.nist.gov/800-63-3/sp800-63b.html.

[37]*See* Foley & Lardner LLP, STATE DATA BREACH NOTIFICATION LAWS (last updated Jan. 1, 2018), *available at* https://www.foley.com/files/Publication/c31703ac-ee93-40a5-b295-7e1d9fe45814/Presentation/PublicationAttachment/d6373e89-f460-44fa-afec-a2cbe9fa23fd/17.MC5826%20Data%20Breach%20Chart%200817%20R1.pdf (chart summarizing data breach notification laws in other jurisdictions).

[38]*See* Iowa Administrative Code rule 11—120.5 for list of damages categories Iowa Executive Branch Agencies are required to carve out of limitation-of-liability provisions as it relates to information-technology contracts.

[39]45 C.F.R. § 164.308(b)(1).

[40]45 C.F.R. § 164.308(b)(2).

[41]*See* 45 C.F.R. § 160.103.

[42]45 C.F.R. § 164.402(2).

[43]*Id.*