JacksonLewis

Vendor Data Security and Breaches

September 6, 2023

H. Bernard Tisdale III
864.346.3737
Bernard.Tisdale@jacksonlewis.com

Duty to safeguard systems and information:

- International, federal, state, and local laws
- Contractual and/or common law obligations
- Organizational policies, procedures and practices
- Industry guidelines
- Rules of professional responsibility

It’s a CLE, so . . .

Obligations for Attorneys

- An attorney's duty to protect client and personal information generally arises from one or more of the following sources:
  - Federal, state, and local laws applicable to
    - Law firms as businesses
    - Law firms as law firms (service providers, business associates, etc)
    - Law firms' group health plans
  - Contractual obligations
  - Organizational policies, procedures and practices for in-house counsel
    - Selecting and managing outside counsel
  - Rules of professional responsibility

Ethical Obligations, Some Examples

- Rule 1.1 of the Model Rules of Professional Conduct states, in Comment 8:
  - 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 . . .
- **Rule 1.6(c):**
  - 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.
- Rules 5.1 (responsibilities of partners, managers, supervisory lawyers), 5.3 (responsibilities regarding nonlawyer assistants), and 5.7 (responsibilities regarding law related services):
  - Requires policies and procedures in place to ensure compliance with Model Rules – most significantly, for our purposes, Rule 1.6(c).

Ethical Obligations, Some Examples

- ABA Commission on Ethics 20/20 provides that analysis of the reasonableness of an attorney's efforts should consider:
  - Sensitivity of the information
  - Likelihood of disclosure if additional safeguards not employed
  - Cost of employing additional safeguards
  - Difficulty of implementing the safeguards
  - 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)

Remember the 6 P’s

- Prior
- Planning
- Prevents
- P&%
- Poor
- Performance

Federal and State Laws

- Interagency Guidelines for Safeguarding Member Information – financial institutions
  - Requirements for selection of service providers, protection of information, and periodic audits of service providers
- HIPAA
  - Business Associate Agreements
- California Consumer Privacy Act
- Colorado Privacy Act
- Massachusetts regulations
- Virginia Consumer Data Protection Act
- Is there international law exposure?

Examples of Cyber Supply Chain Risks and Effects

- Risks
  - Ransomware
  - Software Vulnerabilities
  - Physical and Virtual IT Access
  - Stolen Credentials
  - Compliance Violations
- Effects
  - Inability to function/operate
  - Can’t get key parts
  - Can’t treat patients
  - Can’t service customers

Vendors and Data Breaches

- Vet vendors' privacy and security standards
- Include contract terms to address outages, data privacy and costs associated with both
- Develop and train on contingency plans
- Actively seek out network vulnerabilities, in addition to the defensive antivirus and firewall solutions.
- Develop and continually update incident response plans

Internal Procedures

- Determine internal individual or team responsible for compliance
- Identify and train individuals/titles with responsibility for responding to individual rights requests
- Develop written policies and procedures for responding to and documenting individual rights requests
- Develop form/template responses to requests concerning information
- Assessing changes to personal information collection, use, disclosure, and retention practices, and make updates as needed
- Monitor legislative and regulatory developments for changes

Strategic Imperatives – Incident Response Plan

- Data security, incident response is not and **should not be** just the job of IT
- Line up external resources in advance (insurance, MSP, forensics, outside counsel, recovery, ransom negotiations, letters/credit monitoring)
- Understand your regulatory environment, contractual obligations, ethical requirements, client relationships
- Rank and file employees must be vigilant
- Assess risk across the business, competency, availability
- Understand data, clients, nature of products and services
- Live/virtual exercises annually
- Training/awareness are required

What is a Vendor Risk Assessment?

- An assessment to evaluate the risks a company may encounter when working with a third party, such as a vendor, supplier, contractor, or other business partner. Assessments can/should be conducted at various stages in the vendor relationship, including:
  - During sourcing and selection to identify and shortlist low-risk vendors
  - During onboarding as due diligence to gauge inherent risk before granting access to critical systems and data
  - On a periodic basis, to check SLAs, evaluate contract adherence, or satisfy audit requirements
  - During offboarding, to ensure that system access is terminated, and that data has been protected or destroyed according to regulations
  - Or during incident response, to determine the potential scope and impact of security breaches

Assessment Frameworks

- There are many assessment standards or frameworks to choose from. Common assessment standards include:
  - ISO 27001 & ISO 27701 - data security
  - NIST SP 800-53 - data security
  - SIG Lite and SIG Core - risk assessments
  - CSA CAIQ - Cloud security
- There are also standards for specific industries, including:
  - HITRUST - healthcare
  - HECVAT - higher education

Cyber Supply Chain Risk Management (C-SCRM) Best Practices

- Build Security Requirements into Supplier Contracts
- Understand Vendors' Risks
- Use Vendor Risk Questionnaires and Repositories
- Practice Continuous Monitoring Throughout Cyber Supply Chain
- Nth Party Risk
- Identify and Map Vendors in your Cyber Supply Chain
- Reassess
- Create a supplier incident response plan
- Maintain Due Diligence During Offboarding

Vendor/DPA Agreements

- Process in the case of a breach
- Identity specific business services and purposes for processing information
- Prohibit retaining, using, or disclosing information for any purpose other than the specified business purpose
- Prohibit retaining, using, or disclosing information outside the direct relationship
- Require applicable law compliance
- Grant audit rights
- Notice to business if no longer able to comply with applicable laws
- Grant right to stop service provider's unauthorized use of information
- Require service provider to push down similar provisions to subcontractors in writing

Vendor/DPA Agreements

- Return or destroy the processed data to the Company when their duties are no longer required.
- Inform potential data breaches to the Company as soon as possible.
- Prohibit from selling or sharing personal information
- Indemnity / limitation of liability provisions.
- Maintain the rights of the clients along with the vendor.
- Prohibition from using sub-processors/vendors without the authorization and approval of the Company.
- The processor-sub processor contract shall have an equivalent degree of data protection offered by the DPA between the Company and the vendor.

Vendor/DPA Agreements

- The vendor shall only perform processing of the data and other essential operations related to it upon the consent of the company.
- All the personnel tasked to handle the data should commit and uphold confidentiality.
- The vendor shall assist the Company in upholding their statutory obligations, such as securing the data rights.
- At the end of the contract, the vendor is compelled to delete or return, depending on the Company's choice, all the processed data.

Vendor/DPA Agreements

- Encryption and pseudonymization of the personal information obtained shall be employed.
- Confidentiality, integrity, availability, and resilience shall be maintained during the processing of data.
- In the case of physical or technical issues, the personal data shall be quickly restored.
- There shall be a procedure for testing, measuring, and evaluating the efficacy of the current technical and organizational measures regularly to guarantee the security of the processing of data.

HHS C-SCRM Guidance

- The U.S. Department of Health and Human Services published a presentation with a high-level overview of C-SCRM best practices based on NIST and covers specific controls and control families that should be implemented as part of a C-SCRM program.
- See, https://www.hhs.gov/sites/default/files/hph-cyber-supply-chain-risk-management.pdf

YOU LEARN OF A DATA BREACH

NOW WHAT?

General Incident Response Checklist (IRP)

- **Consult Legal Counsel**
  - Federal and state privacy laws – e.g. HIPAA, state breach laws.
- Notify Cyber Liability Insurer
- Investigate
  - When, How, Which systems, What data, Who, Which states
  - Access/exfiltration - Completed or ongoing?
- Eradicate/Recover/Monitor – *Secure Systems*
- Coordinate with Law Enforcement
- Pay the ransom? FBI advises against, business decision, OFAC, effective?
- ***Notification*** – individuals (children), owners, state agencies, substitute?
  - *Without unreasonable delay (30/45)*
  - Content requirements + Credit monitoring (CA, CT, DE, MA)
- Lessons Learned - Incident Response Report & Review

Preserving Attorney/Client Privilege

- Consider having outside counsel should retain outside expert firms
- Consider running two investigations – internal and external
- Be sure to integrate business and technical issues with opinions about legal exposure
- Consider FRE 502 when producing information/documentation to governmental agency
- Be careful with public relations consultants
- Consider international attorney/client and work product rules

You have been informed of a data breach . . .

- What categories of Company data does the vendor have? How sensitive is it?
- What is the volume of data that the vendor has?
- Is the Company providing the vendor with data on an ongoing basis?
- Does the vendor have direct access to the Company's network?
- Should we stop any data flows and disable the vendor's access to Company systems until we learn more?
- What are the business continuity risks if we cut off our relationship with this vendor?
- Do we have cyber insurance? Does it cover damage from vendor breaches? What is the deductible? Do we need to notify our insurer?

You have been informed of a data breach . . .

- If any of our data was involved, do we have regulatory, statutory or contractual notification obligations? If so, do we want to make those notifications or do we want the vendor to make them?
- Depending on what data was involved, are there steps the Company should be taking to reduce risk, such as alerting customers whose data may have been impacted?
- What do the relevant contracts with the vendor say about its cybersecurity obligations, breach notification requirements, indemnity, cooperation, limitations of liability, termination rights, etc.?
- What cyber diligence was done on the vendor?

You have been informed of a data breach . . .

- What is the impact of the incident on the vendor's operations?
- Is there any reason to believe that the Company's systems are at risk? If so, what indicators of compromise should we be looking for?
- If the vendor has direct access to the Company's systems, what assurances can be provided as to why it is safe to allow that access to continue?
- Is any Company data held by the vendor at risk?
- Have you confirmed that any Company data was accessed or exfiltrated? If so, can we obtain a copy of the data?
- Do you know who the attackers are or the purpose of the attack?
- Do you have any reason to believe that Company data was targeted?

You have been informed of a data breach . . .

- Has the data that was involved been misused?
- Have you retained an outside law firm and cyber firm to assist?
- Are you conducting Dark Web monitoring? What are the results?
- When did the compromise of our Company data first occur?
- When did you discover the compromise?
- What steps have been taken to contain the breach?
- Do you know how the attacker got into the system, and if so, has that vulnerability been closed?
- Does the attacker still have access to your system? If not, when was the last time the attacker was observed in the system?
- Who else have you notified (law enforcement, regulators, customers, etc.)?

Strategic Imperatives – Response

Communications/Legal Viewpoints

- Demonstrate empathy, accountability, action…*avoid admissions*
- Be transparent…*preserve attorney client privilege*
- Stay out of the weeds…*satisfy disclosure requirements*
- Tier and tightly sequence communications…*notify timely without unreasonable delay*
- Message consistently across audiences…*observe contract obligations*
- Prioritize partner and stakeholder comms…*avoid disadvantaging others*
- Track sentiment and emerging themes…*be ready to mitigate*

General Takeaways - Key Action Items

1. Get management awareness and support
2. Assign responsibility
3. Conduct risk assessment
4. Develop written policies and procedures
5. Harden security, including remote access and software development procedures
6. Develop disaster recovery and business continuity plan
7. Develop and practice incident response plan
8. Training and awareness
9. Regular review – logs, threats, performance, etc.
10. Implement vendor management program

JacksonLewis

Questions?

JacksonLewis

Thank you.