Robinson+Cole

What to do if your vendor has a security incident

Linn Foster Freedman, Esq.

December 1-3, 2021

Overview

- Recent Vendor Risks
- Minimizing Third Party Vendor Risks:
- MAP
- Third Party Vendors – Who are they and What are the Risks of the Vendor to your Organization?
- ASSESS
- • What happens if there is a Security Incident caused by a Third Party Vendor?
- How can you properly assess the vendor?
- MITIGATE RISK
- What can you do to Protect Your Organization?
- How to Manage Third Party Vendors and Minimize Risk?
- Cyber Liability Insurance Coverage for Third Party Vendors

Recent Risks--What are the Third Party Vendor Risks to your Organization?

- Data Breach
- Ransomware Attack
- Zero Day Vulnerabilities

DATA BREACH

- Vendors that experience a security incident that involves personal information (PI) or protected health information (PHI) may cause a data breach
  - A data breach is a legal term that is determined by the unauthorized access, use and disclosure of PI
- All 50 states have different definitions of a reportable data breach
- If your vendor causes an incident that is a reportable data breach with your data, it is your problem

Ransomware

- Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid (usually in bitcoin).
- Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.

Zero Day Vulnerabilities

- What is a **zero-day vulnerability** **and how could it harm your organization?**

- **A zero-day vulnerability** is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw.

Case Example: The Blackbaud Breach

- Blackbaud is a software vendor for non-profit organizations (health care, education, etc.).
- Victim of ransomware between February 2020-May 2020
- Notified hundreds of customers of the attack that affected personal information stored in Blackbaud's database
- Relying on hackers' Certificate of Destruction

"Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly."

Case Example: Blackbaud

- Blackbaud notified its customers of data exfiltration and payment of ransomware
- As business associate, Blackbaud was responsible to notify covered entities—its customers
- Covered entity responsible under HIPAA to determine whether it is a reportable data breach that requires notification to individual and OCR
- If PHI accessed, used or destroyed in an unauthorized manner, then it is reportable
- But it wasn't covered entities' fault

ASSESS: Your Organization Has a Vendor Security Incident – What Do You Do?

- **Be Prepared!**

- **Activate Your Incident Response Plan**

Response to Vendor Incident

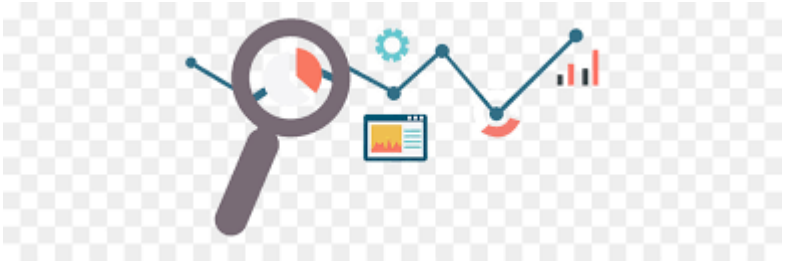
- Tricky Nuances
- Cooperate or lawyer up?
- Need information, but have to assess legal obligations
- Steps to take
  - Find and have legal review existing contract
  - Review notification obligations, responsibilities, cooperation, payment of expenses, limitation of liability
  - Contract language is crucial

Response to Vendor Incident

- Monitor forensic response of vendor
- Obtain information regarding specific data that has been involved
- Assess facts of incident and whether data was actually accessed or exfiltrated
- Obtain written assurances or confirmation of forensic analysis
- Daily, weekly update calls
- Obtain specific details on involvement of your data

Be Prepared:
MAP: Who are your High Risk Vendors?

- Map all vendors who have access to PI
  - Follow the data



Who are your High Risk Vendors? (cont'd)

- Utility or other online payment vendors
- Retirement system administrators
- HR/payroll administrators
- Health insurance/dental system administrators
- Business Associates
- IT/Cloud Service Providers
- Web Hosting Services
- Legal/Accounting Services
- Any vendor who has access to your data, either with direct access to your system or if you disclose to vendor

MITIGATE: How to Protect Your Organization

- Manage the Risk
- Mitigate the Damages from Third Party Vendors

MITIGATE: How to Protect Your Organization (cont'd)

- **Implement a Vendor Due Diligence Plan**

MITIGATE: How to Protect Your Organization (cont'd)

- Utilize Security Questionnaires to Assess Cyber Security Practices and Compliance with Data Security Laws
- Utilize and implement right to audit your Vendors
- Utilize written contracts with vendors that put security risks and expenses on the vendors, not the municipality
- Vendors must also have sufficient cyber liability coverage for security incidents
- Consider creating a vendor database for your agreements, questionnaires, and related documents
- If there's PHI, HIPAA requires it!

How do you Manage the Risk and Mitigate the Damages from Third Party Vendors?

- What is a Security Questionnaire and Why do you need it?
  - It is a document you provide to your vendor that should identify their controls and practices for:
    - Handling Risks
    - Security controls, including technology
    - Process controls
    - Training

- It will tell you about the vendor's security practices and it will document your due diligence in hiring the vendor

How do you Manage the Risk and Mitigate the Damages from Third Party Vendors? (cont'd)

- What are Audit Rights and Why do you need them?
  - Your right to audit a vendor's security practices and protocols will allow you to better understand the vendor's security practices
  - It will assist you in analyzing security incidents should they occur and obtaining access to information needed to evaluate security posture of vendor and improvements

How do you Manage the Risk and Mitigate the Damages from Third Party Vendors? (cont'd)

- Look Closely at Your Written Contracts with
  - Vendors (Vendor Agreements/Business Associate Agreements)
    - Which entity is bearing the risk?
    - Is the vendor attempting to shift its risk to you?
    - What are the vendor's data security protections?
    - What are the requirements for notification of a security incident involving your data?
    - Do your vendor confidentiality agreements contain data security provisions?
    - Who is bearing the cost of the incident and resulting costs?
    - Are they trying to limit their liability?

How do you Manage the Risk and Mitigate the Damages from Third Party Vendors? (cont'd)

- **Create Better Vendor Agreements/Business Associate Agreements:**
  - Don't automatically settle for the vendor's boilerplate agreement – Read it carefully -
    - Vendors will try to limit their risk and/or limit their exposure if there is a security incident to the amount of the contract--insufficient
    - How do you protect yourself?
    - Consider use of SLAs
  - Negotiate for appropriate cyber security protections and provisions
    - Your organization should not have to take on the vendor's risk

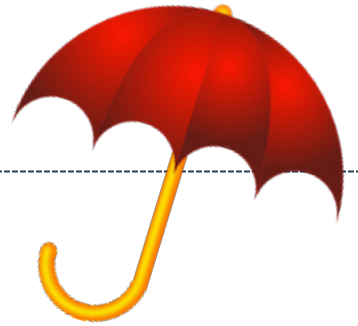
Tips for Vendor Agreements

- Require compliance with applicable data, privacy & security laws (HIPAA);
- Require prompt patching of vulnerabilities;
- Require prompt reporting of potential cyber incidents;
- Require cooperation in investigating an incident and preserving relevant evidence;
- Utilize sufficient liability limits;
- Require incident response and mitigation expenses;
- Require appropriate cyber liability insurance coverage;
- Require use of strong passwords & multifactor authentication.

Tips for Vendor Agreements (cont'd)

- **Address Indemnification + limitation of liability issues**
  - **Liability for causing a data breach or security incident**
  - **Reimbursement for all costs**
  - **First v. Third Party Claims**
  - **Limiting liability to the amount of the contract has no relevance to actual costs and damages**
  - **Supercap for data breach**
- **Consider cyberliability insurance for actions of 3rd parties like cloud providers**

Cyberliability Insurance



- Cyberliability Insurance
  - Need to cover information you have in your possession AND the data held by your service providers
  - Most comprehensive general insurance liability policies DO NOT cover a data breach
    - Those general policies were not designed for when information gets into the wrong hands

Cyberliabilty Insurance (cont'd)

- **Cyberliability insurance in general will cover: liability for failure to protect personal information held on computer systems or mobile devices, costs to notify individuals, investigative costs, public relations, legal fees, media coverage, mitigation, etc.**
- **Talk to broker who has experience with cyberliability policies**
- **Work with insurer to have existing relationships approved**

Cyberliabilty Insurance (cont'd)

- Questions to Ask Your Broker about Ransomware
  - Is there coverage for costs to access/restore data and for the actual payment of a ransom amount in the event of a ransomware attack?
  - Is there coverage if there is a cyber extortion event that blocks access to the business' telephone or computer system or its data, including potential lost business and/or business interruption?
  - Is data that is stored or backed up using cloud services covered in the event of a cyber incident, regardless of the type of attack; i.e., hacker, virus, malware, etc.?

Cyberliability Insurance (cont'd)

- Is there coverage for damages, costs, fines, etc. resulting from social engineering fraud; e.g., an employee clicks on a link in an email that installs malware causing a virus or ransomware?
- If there is a data breach, is there also coverage for loss of net profits / income if the business is shut down or can't operate because of a data breach, virus, ransomware attack or other incident?

Additional Tips & Considerations

- Robust Back-ups
- Robust Contingent Operations and Disaster Recovery Plans
- Address any configuration issues
- Consider keeping high-risk data in-house
  - May consider adding high-risk data to cloud-based service provider's systems after a 'test period' has passed
    - Use Encryption at Rest
    - Limit access

Conclusion

Know the questions to ask and the risks to your data

Linn Foster Freedman
lfreedman@rc.com

Robinson + Cole
One Financial Plaza
Suite 1430
Providence, RI 02903
401-709-3353

Thank you

QUESTIONS?

www.dataprivacyandsecurityinsider.com