Vendor Supply Chain Attacks: Practical Guidance to Manage Risk

William R. Denny, Esquire
Secure Delaware Workshop

October 28, 2021
Agenda

The Threat Landscape

Regulatory Focus on Vendor Management

Key Components of Managing Vendor Risk

Special Issues

Data Breach and Incident Response

Resources
Attacks Targeting Third-Party Vendors

- Kaseya provided software to managed service providers
- Most widespread ransomware attack to date
- Devastating damage to thousands of businesses
- Many chose to pay ransom
Microsoft Exchange – Hafnium Hack

- Nation-state attack on software infrastructure.
- Hacker gained control of over 30,000 email servers.
- FBI got warrant to access private email servers and inject command to erase web shell
  - No notice or consent of owner
  - How did FBI gain access?
SolarWinds Wake-up Call

- Hacker embeds trojan in software security update to 18,000 customers.
- Infects upstream to M365 cloud environment
- Monitored email of private and government servers for months
- Highlights risk of supply chain security
Regulatory Focus on Vendor Management

- Federal Trade Commission (FTC)
- Gramm-Leach Bliley Act (GLBA)
- OCC Bulletin 2013-29 Third Party Relationships
- FFIEC Information Security Examination Handbook
- Health Care Institutions
- Payment Card Industry Data Security Standard
- New York Department of Financial Services
- California Consumer Privacy Act
- Executive Order on Cybersecurity
Key Components of Managing Vendor Risk

- Due Diligence
- Contract Terms
- Monitoring
- Insurance
Due Diligence Issues – Data Access

- Does the vendor have the right to use your data?
- Is your data stored in the cloud?
- Are you uploading data to a third-party site that will then be manipulated or placed in some type of report and returned?
- Is the vendor required to notify you in the event that the vendor has a security breach which might involve your data?
- Does the vendor subcontract or allow others access to your data?
- Is the vendor using the data for its own business and not just to provide the services to you?
- Do your practices in collecting, using and transferring data match your vendor’s?
Due Diligence Issues – Cloud Providers

- Cloud providers are increasingly under cyber attack.
  - Cloud systems often maintain their own access controls
  - Hackers steal login credentials through phishing and malware attacks
  - Malicious penetration using stolen credentials is difficult to detect

- Common-sense precautions include:
  - Two-factor authentication
  - Enforcing strong password policy
  - Training employees to spot fishy emails
Questions to Ask Cloud Providers

- Where will the data be collected, processed or stored?
- What laws apply to the cloud provider?
- What additional burdens will those laws impose?
  - Data transfer regulations
  - Consent requirements
- What is the culture of compliance in the other jurisdiction?
  - Confidentiality
  - Security
  - Privacy
Due Diligence Issues – 4th Party Providers

- Threshold Assumptions:
  - You have a multitude of vendors.
  - Each vendor may have multiple contracts.
  - Each vendor may interact with multiple parts of your business.

- Bank must consider the entire vendor ecosystem
  - Only 1 in 10 global companies identify and regularly monitor their vendors’ subcontractors.
  - You can’t outsource your accountability.
  - Who are the business partners and service providers of the bank’s vendor?
  - Who will have access to the bank’s data?
Due Diligence Issue – Open Source Code

- Vendors are often:
  - Unaware of the open source components of their software
  - Out of compliance with open source licensing obligations
  - Unsecure in failing to upgrade to new versions with security fixes
  - Using stranded code not supported by an active community

- Patches for open source code are difficult to track

- Recommendations:
  - Independent verification of all open source code used
  - Confirmation of up-to-date patching of all open source components
  - Include open source compliance obligations in contract
Vendor Contracts Offer Thin Protection

- You may be held liable for a vendor breach.
- Hold harmless and indemnification provisions
  - Often can include limiting and exclusionary language:
    - Caps on indemnification amounts
    - Exclusions for certain types of data breaches
  - No protection if the vendor becomes insolvent or goes into bankruptcy
  - No protection if the vendor decides not to honor the agreement
Make a Plan – The Vendor Contract

- Prepare standard data privacy and security terms
  - Ensures that vendors protect the company’s data and adheres to company policies and applicable regulations
  - Helps to assess and manage the risk of using vendor-supplied terms
- Consider entire vendor relationship lifecycle
- Customize to address unique risks
Contract Issues – Vendor Security Standards

Written Information Security Program
Annual Risk Assessments/Program Review
Security Manager
Consent for Third Party Disclosure
Third Party Due Diligence
Access Controls
Password and Authentication Controls
Physical Access Controls
Training
Hardware and Software Encryption
Remote Access
List of Systems
Co-Mingling of Data

Written Approval for Relocation
Patch Management
Data Loss Prevention
Portable Media, Prohibition
Incident Response Plan and Notification
Incident Response Investigation
Enforcement
Penetration Testing
Mitigation of Vulnerabilities
Intrusion Prevention System
Change Control
Business Continuity and Disaster Recovery
Audit
Assistance
Contract Issues – Vendor Privacy Standards

Data ownership and Limitation of Use
Description of Processing
Confidentiality
Cardholder Information
Compliance with Law
Subcontracting
Cross-Border Transfers
Data Integrity
Return or Disposal
Data Subject Access, Correction and Portability
Requests
Production Requests
Regulatory Investigations

Third Party Beneficiaries
Other Requirements
Failure to Comply
Indemnity
Survival

Annex 1: Description of Processing Activity:
Nature and purpose, duration, retention, types of data, location
Annex 2: Technical and Organizational Measures
Business Associate Agreement (if PHI)
Standard Contractual Clauses completed by vendor if EU resident personal data and not certified under Privacy Shield
Sample Provisions – Notice Clause

. . . Vendor agrees to notify Company within twenty-four (24) hours of the discovery of a breach or potential breach of security . . .

“Breach of Security” is any actual or probable unauthorized acquisition of or access to Confidential Information that compromises the security, confidentiality, integrity or availability of such information] . . .
Periodic Review and Assessment

- Dedicate sufficient staff with the necessary expertise, authority, and accountability to monitor the relationship
- Regularly scheduled checkups
- Vendor self-assessments
- Third party audits and reviews
- Training and awareness
Managing a Vendor’s Data Breach

- Legal and contractual obligations (e.g., notice)
- Cooperation
- Maintaining attorney-client privilege
- Involving law enforcement
- Interacting with vendor’s other customers
- Indemnity
- Insurance
- Managing PR / communication
- Continue or terminate relationship
CISA Resources for Supply Chain Risk Management

Other Resources

- Vendor Contracting Project: Cybersecurity Checklist
  https://www.americanbar.org/products/ecd/ebk/411859099/

- NIST Cybersecurity Framework -
  http://www.nist.gov/cyberframework/

- FINRA Regulatory Notice 29-21, Aug. 2021,

- FFIEC Handbooks - http://ithandbook.ffiec.gov/

- NCUA Guidance -

- FDIC Guidance -
Contact Us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
Wilmington, DE 19801