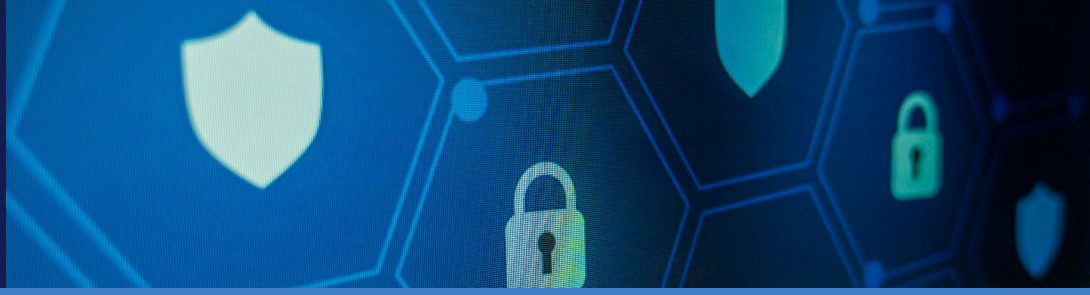
RISK strategies



CYBER RISK MITIGATION

Improve Your Security Posture With Robust Vendor Management

Who reviews your vendor contracts? Is that person looking at the contracts through cybersecurity, insurance, and risk management lenses? You can avoid taking on unnecessary liability by carefully examining the fine print. Are vendors "washing their hands" of responsibility in the contract language? Do you have the protections you need? Here's a checklist of topics to consider.

Data security obligations

Your organization is responsible for data protection, even if you are utilizing third parties to collect, process, and store your data. Requiring vendors to follow recognized standards and compliance measures helps you avoid breaches that could lead to financial loss and reputational damage. Ask vendors to:

- ☐ Adhere to specified standards (i.e., NIST, CIS, ISO 27001, SOC 2) to shield your data from unauthorized access.
- ☐ Comply with data protection laws (state, federal, GDPR) to prevent legal ramifications.
- ☐ Adhere to HIPAA for healthcare data to ensure patient privacy.

Security policies

Just as you have a structured security policy and continuous employee training for your organization, your vendors need to commit to the same precautions. Ask them to agree to:

- ☐ Maintain and enforce an information security program with clear policies and procedures to uphold data integrity. (Ask for a copy of their policies and procedures, so you can identify and resolve areas of concern.)
- ☐ Conduct ongoing cyber awareness training for all employees to mitigate human error. (Request details on the employee training. A once-a-year video is inadequate. Ideally, your vendors provide employee education at least once a month and conduct phishing simulations to check employee knowledge.)

Encryption

A hacker can intercept information when it's in transit to or from a third-party vendor. To protect against unauthorized data access, tokenize and encrypt your data and ask your vendors to do the same. At minimum, contractually require third parties to:

- ☐ Encrypt all data in transit and at rest with AES-256 or higher standards to safeguard sensitive information.

Patch Management

To reduce risk of security incidents, ensure vendors are safeguarding their software against the latest threats. Contractually require them to:

- ☐ Implement a schedule for regular patch updates to address known vulnerabilities promptly.
- ☐ Deploy emergency patches within a defined timeframe (e.g., 24 to 48 hours) after discovering a critical vulnerability to minimize the window of exposure to potential exploits.
- ☐ Test and validate all patches in a controlled environment before deployment to ensure they do not disrupt existing systems or introduce new vulnerabilities.
- ☐ Provide regular reports on patch management activities (define "regular"), including details of patches applied, pending updates, and any issues encountered during deployment. This keeps you informed and establishes accountability.

Incident response and notification

Cybercrime is so rampant that you need to plan for it. Swift and coordinated responses are crucial for minimizing damage during a cybersecurity incident. Effective communication and collaboration can significantly reduce downtime and financial impact. If a breach happens, what steps will you take, and what actions do you expect from your vendor? Your contracts need to spell out these requirements. Ask your vendors to:

- ☐ Provide a written incident response plan, documenting how they will manage breaches involving your data.
- ☐ Report incidents to you within 24 hours and supply continuous updates to maintain transparency (specify the frequency).
- ☐ Submit a detailed incident report within 72 hours to evaluate impact and response.
- ☐ Work with your company's incident response team for effective management.

Cyber insurance

The right insurance can help cover costs associated with responding to and recovering from a cyber incident. When you engage a vendor:

- ☐ Require the vendor to carry cyber insurance (at the same limits you carry or more).
- ☐ Ask to be named as an "additional insured pursuant to contract" on the vendor's cyber policy. (If the vendor experiences a breach and you are an additional insured on the vendor's policy, their insurer will need to provide your business with response and recovery resources.)
- ☐ Request annual certificates of insurance and prompt notification of any coverage changes (define "prompt" in the contract).

Indemnification

Indemnity clauses in contracts can protect you from financial liabilities arising from a vendor's failure to secure data. Even when you have these clauses, you remain responsible for the security of your customer data. But these clauses can help ensure you are not bearing the full cost of the breach. Make sure vendor contracts:

- ☐ Indemnify your company against breaches due to vendor negligence.
- ☐ Spell out that vendors are liable for third-party claims arising from vendor non-compliance with data protection laws.

Exceptions to liability carve-outs

Clearly defining exceptions to liability ensures vendors cannot evade responsibility for failing to meet security expectations. Make sure your vendor contracts:

- ☐ Exclude liability limitations for inadequate security measures or confidentiality breaches.

Right to audit and security assessments

Perform yearly audits to confirm the vendor is adhering to all contractual agreements and security benchmarks. In your contracts, require vendors to:

- ☐ Permit annual audits of vendor cybersecurity practices to verify compliance.
- ☐ Provide security certifications and regularly test for vulnerabilities.

Data handling and protection

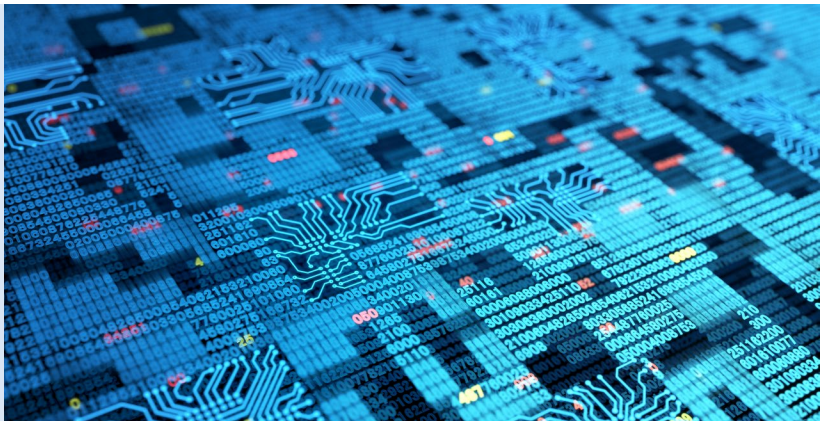
For vendors who will handle sensitive data (PII, PHI, intellectual property, etc.), you need additional protections for that data. In your contracts:

- ☐ Limit data access to only what's needed for performing the vendor's service.
- ☐ Spell out the purposes for the access (make sure the contract specifies that you retain ownership of your data).
- ☐ Require data segregation to prevent breaches, and a list of personnel with access.
- ☐ Mandate background checks on all personnel accessing data.
- ☐ Oblige the vendor to return or destroy company data upon contract termination, with certification.

Termination rights

You want to be able to sever ties quickly with a non-compliant vendor. To safeguard your data and facilitate a smooth transition, include contract provisions to:

- ☐ Allow contract termination for inadequate security or significant breaches.
- ☐ Ensure vendor cooperation for data transition post-termination.



Force majeure exclusions

Prevent vendors from citing "unforeseen events" as an excuse for lax security. In your contract language:

- ☐ Exclude cyberattacks from force majeure to hold vendors accountable.

Confidentiality

Robust confidentiality measures protect proprietary information and foster trust in business relationships, crucial for maintaining competitive advantage. Contractually require your vendors to:

- ☐ Maintain confidentiality of company data and prevent unauthorized disclosures.

Subcontractors

Sometimes, a third-party will utilize subcontractors, so you need to manage their access and compliance, too. To ensure a consistent security posture across all parties involved, require vendors to:

- ☐ Disclose all subcontractors with data access for approval.
- ☐ Ensure subcontractors comply with the same terms as the vendor.

Any time you engage a third-party to provide software or services, there's risk involved. What level of risk is acceptable? And how do you manage and mitigate the risk? This checklist provides a starting point but is not exhaustive. Get input from your organization's legal counsel and executive team before finalizing vendor contracts. With effective vendor management contracting, organizations can fortify themselves against potential breaches, ensuring continuity and resilience in the face of cyber threats. Stay vigilant. Stay secure.

If you want a second opinion about the insurance elements in a vendor contract, contact:

Allen Blount
National Cyber & Technology Product Leader
ablount@risk-strategies.com
212-338-4321