imagine IT

The Q4 2024 State of Cybersecurity

imagineiti.com

Businesses are Signing Contracts with Unfavorable Security & Privacy Content

Many of us have large, enterprise customers that require their vendors (you) to uphold a high standard for security & privacy. After a cyber incident, your business could be held accountable to contractual language that stipulates granular requirements for a robust security & privacy program and processes.

What types of content might be unfavorable?

- *Being required to shift most (if not all) the risk to your business.*
- *Being required to maintain enterprise level security, well beyond a reasonable budget for a small to medium-sized business.*

Here are some examples (mostly obtained from Microsoft Copilot) of unfavorable contract language for security & privacy requirements that businesses should watch out for:

Vague Security Standards

"The vendor will implement commercially reasonable security measures."

Why it's unfavorable: This phrase is too vague and lacks specificity. It doesn't define what "commercially reasonable" means, leaving it open to interpretation and potentially inadequate security measures.

No Indemnification

"The vendor is responsible for any data breaches or security incidents."

Why it's unfavorable: This clause absolves the customer of any responsibility for security incidents, placing the entire burden on the vendor. In a fairly worded contract, customers also have an obligation to maintain a strong security posture and to educate their staff.

Weak Incident Response

"The vendor will notify the customer of a data breach within 7 days."

Why it's unfavorable: Your business needs reasonable time to investigate if any customer data was exposed. This could take many days or weeks. Once it is determined data was exposed, and after discussing with your legal counsel, promptly notify impacted customers to avoid further liability. Many vendor fines are levied due to slow notifications after data exposure.

Lack of Compliance Requirements

"The vendor will comply with applicable laws."

Why it's unfavorable: This clause is too general and doesn't specify which laws or standards the vendor must adhere to, potentially leading to non-compliance with critical regulations.

To protect your business, it's essential to negotiate for clear, specific, and robust security and privacy terms in your contracts. Consulting legal and cybersecurity experts can help ensure that your contracts adequately protect your interests.

How to Reduce Contract Exposure Risk

1. Make a strategic decision to significantly improve your org's security & privacy posture and processes. The best way to avoid contractual liability is to avoid breaches in the first place.

    - The worst thing you can do is to be untruthful when completing customer security assessments (and cyber insurance applications), as this lays all the blame on you during a breach.

    - Engage with an IT Managed Service Provider (MSP) that specializes in cybersecurity (like Imagine IT) to help build and execute the strategy.

2. Negotiate better security terms in contracts as this is crucial for protecting your business. Here are some strategies to help you secure more favorable terms:

    - Understand Your Needs: Identify your specific security requirements and risks. This includes understanding the types of data you handle, regulatory requirements, and potential threats.

    - Negotiate Liability and Indemnity: Clearly define liability in case of a security breach. Ensure the customer is largely responsible for any breaches resulting from their negligence and that they have adequate cyber insurance coverage.

    - Seek Expert Advice: Consult with legal and cybersecurity experts to review and negotiate the contract terms. They can provide valuable insights and help identify potential issues.

    - Plan for Termination: Include terms for data return or destruction upon contract termination. This ensures that your customer's data is securely handled even after the contract ends.

Conclusion

Vendors need to scrutinize customer-required security and privacy contracts to protect themselves from significant legal and financial risks. Unfavorable terms can lead to non-compliance with data protection regulations, resulting in hefty fines and legal penalties. Additionally, vague or inadequate security clauses can shift liability for data breaches to the vendor, exposing them to costly legal disputes and damages.

By carefully reviewing and negotiating these contracts, vendors can ensure they have clear, specific, and robust security and privacy protections in place, safeguarding their operations, reputation, and financial stability.

Also, if you are pursuing a potential new client, and their requirements are going to cost your business tens of thousands of dollars (and time) to be compliant, make a business decision to determine if it is worth it.