Legal – Book 2

Corporate Liability Reduction

Ermis Catevatis
RED STACK LABS CORP

Version	Date	Author
0.1	August 05, 2022	Ermis Catevatis
0.2	Sept 14, 2022	Ermis Catevatis
0.3	Sept 28, 2022	Ermis Catevatis
1.0	Dec 10, 2022	Lawyer Review
1.1	Jan 15, 2023	Ermis Catevatis
1.2	Oct 04, 2023	Ermis Catevatis

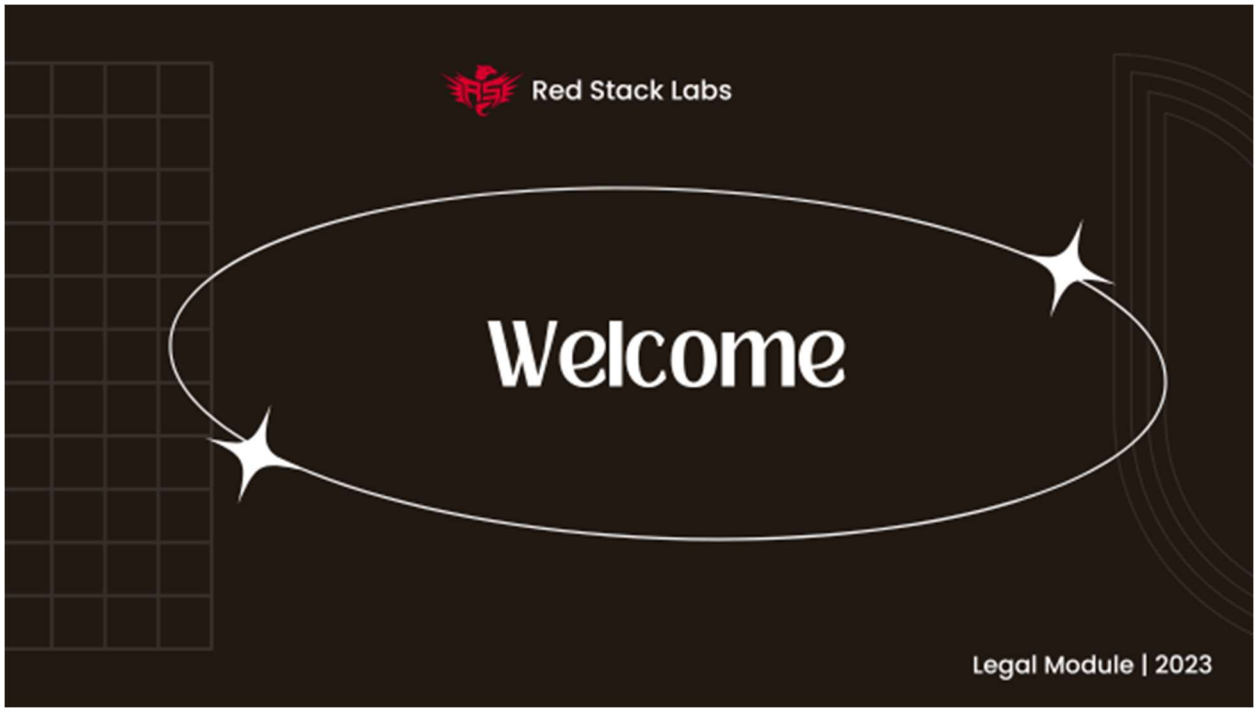
This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Contents

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

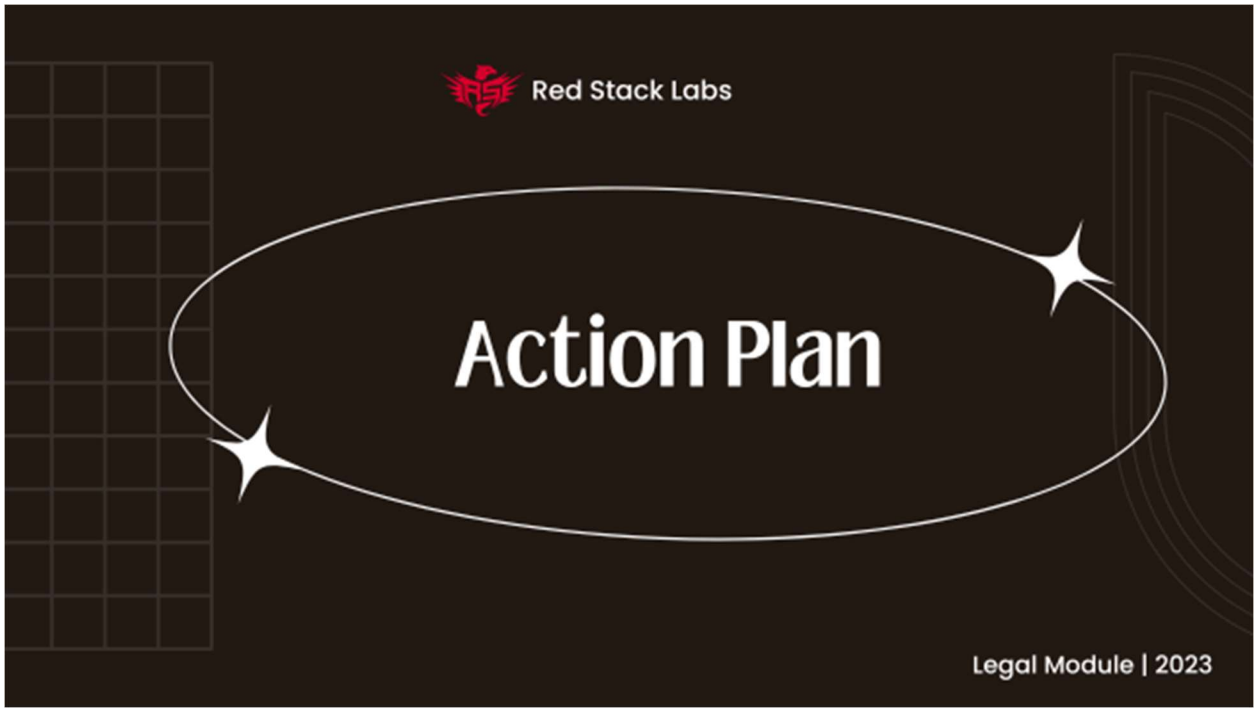


We're delighted to welcome you to "The Legal Module " course. This expertly crafted course is designed to provide you with an in-depth understanding of the intricacies of business contracts and liabilities. As you commence this educational journey, remember that each module is intended to equip you with the knowledge required to protect your organization from contractual risks and optimize your legal strategies.

In the modern business landscape, having the right knowledge and tools is essential for successful contract management. Through this course, we will delve into the details of contractual obligations, dissect common liabilities, and offer guidance on liaising effectively with legal counsel to select the most beneficial agreements for your organization. We've brought together expert input, real-life case studies, and interactive assessments to create a holistic learning experience with tangible applications.

Ready to get started? We are confident that the insights and skills you will gain from this course will significantly enhance your ability to manage contractual risks in your organization. Remember, we're here to support you every step of the way. So, if you have any questions or require assistance, don't hesitate to reach out. Here's to a rewarding and enlightening journey ahead!

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.



Welcome to the next phase of your educational journey. After going through this course's study materials, there are several tasks you should perform to fully leverage this course:

1. **Understand Course Material**: Make sure you have meticulously read and understood the course content. This foundational knowledge is vital for making informed decisions about your business contracts.
2. **Review Existing Business Contracts**: If your organization has ongoing contracts with vendors, partners, or contractors, the next step is to review these agreements with the assistance of your legal counsel, if possible, to understand their details and potential liabilities.
3. **Establish New Business Contracts**: If you're in the process of initiating new contracts, your goal should be to optimize these agreements. Use the provided templates and guidelines to assess potential partners and formulate contracts that align with your organization's needs. Evaluate multiple options to ensure the best fit.
4. **Apply Your Knowledge**: It's time to put your understanding into practice. Determine how your contracts (existing or prospective) can impact your business, identifying potential liabilities, regulatory risks, and benefits. Understand the criteria that must be met to maintain compliance with these contracts. If there are uncertainties, use the course materials as a guide to seek clarification from your legal counsel.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

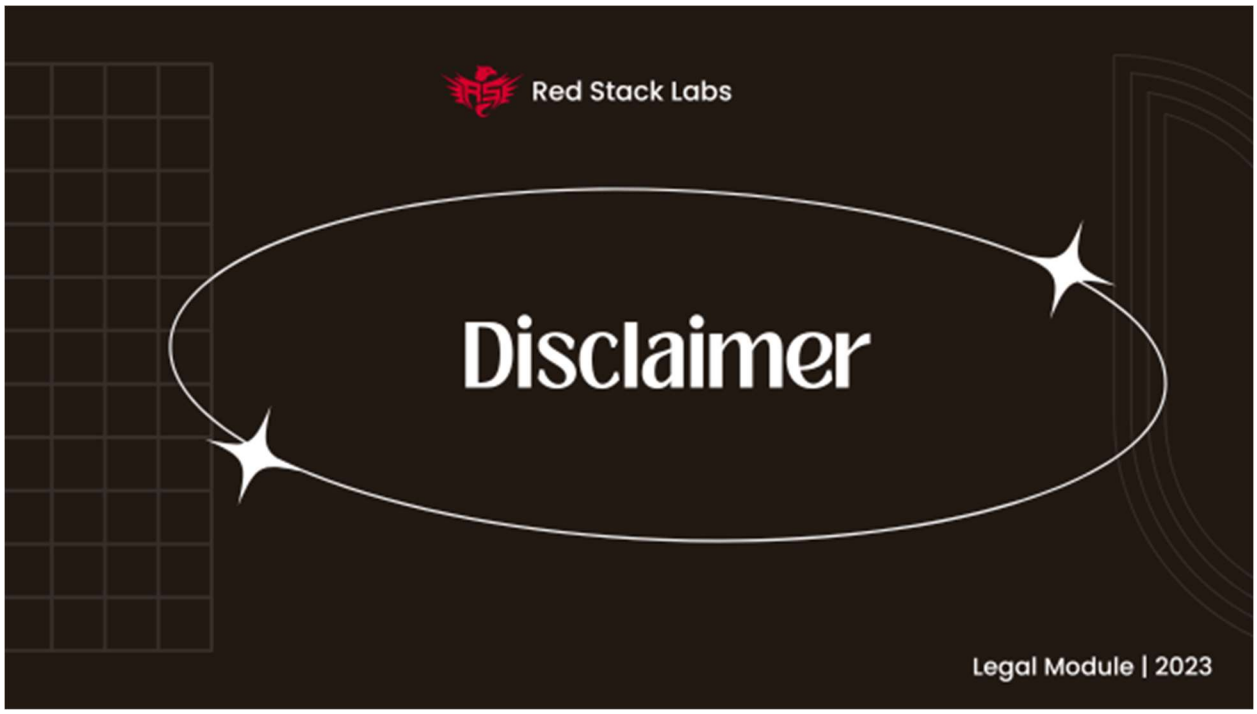
The main objectives of this course are as follows:

1. **Identify Suitable Agreements**: Assist your business in formulating agreements that offer optimal benefits while minimizing potential liabilities and regulatory risks.
2. **Understand Contract Compliance**: Raise awareness about certain factors that could affect your ability to maintain compliance with your contracts.
3. **Learn about Regulatory Requirements**: Educate you about potential regulatory requirements related to your contracts, which could impact your legal and financial standing.
4. **Awareness of Contract Changes**: Highlight that business contracts are constantly evolving, and staying abreast of these changes is crucial to avoid unwanted liabilities.

Remember, having well-structured business contracts won't prevent all liabilities, lawsuits, or financial losses. The goal of effective contract management is to provide a legal framework that helps your business operate efficiently and mitigate potential risks."

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Legal Basics



Disclaimer

This program is educational, and we provide information from a cyber incident perspective that should be discussed with your independent legal counsel. This is not a replacement for legal counsel. Each cyber incident differs on a case-by-case basis and counsel will have a different line of sight during the cyber incident compared to our suggestions or advice through this program or workshop. Because of this we always recommend you prioritize your independent legal counsel's advice.

Note: For the purposes of this module when we refer to counsel it means legal counsel.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Legal Counsel

Legal Privilege

During a cyber incident your staff will be communicating with multiple external companies, from cyber security, insurer, public relations, IT, a legal counsel will provide protection to certain documentation and communications from discovery during legal processes. Without legal counsel, any reports produced by these firms could be turned over to prosecution during a lawsuit. With counsel they are under attorney-client privilege and protected.

This privilege could extend to protect sensitive information that could be exposed during the cyber incident conversations with third parties.

Lawsuits

Legal counsel, during a cyber incident will work to understand if companies you are dealing with are negligent or with malintent and if they could be held liable.

Contractual Obligations

Contracts need to be reviewed by legal counsel to understand contractual obligations, requirements, and liabilities. These can include:

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

1. Time frame or period of notification
2. Liability exposure because of data breach or cyber incident
3. Indemnification of third parties following a data breach or cyber incident
4. Cyber forensic obligations to identify cyber attribution, footholds, etc.

Data Privacy Regulations

Your company may be subject to data privacy regulations if you host personal data, and a breach occurs. Legal counsel would have to review your data classifications, local and international regulatory requirements dependant on who's sensitive data your company stores or processes, and then advise you on the best course of action.

If your company works in or with a specific industry it may have additional reporting obligations:

1. Financial institution
2. Telecom provider
3. Payment service provider / Banking
4. Digital service provider
5. Professional Secrecy laws (medical, legal)

In addition, there could be organization policies or employment laws that could affect your company when processing certain employee data.

Note: We often see a misconception with many companies of which regulations apply to them. You need to understand your data flow and the regions the data is coming from; this includes using 3rd party solutions that may increase your data regulation footprint.

Next Steps

Download the Data Residency worksheet, and work with your IT team to fill out the appropriate information. Make sure to update this regularly prior to any conversation with your counsel.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Cyber Extortion

There could be risks to paying ransom, in some cases it could be illegal if it is viewed as funding a criminal organization or terrorism group.

Most law enforcement agencies including CISA, FBI and NCSC recommend not to pay ransoms as it continues to fund and motivate these groups. But ultimately the decision to pay should be your boards decision while calculating the risks and the possible outcome scenarios of paying.

You Should Know

Prior to paying any ransom, it's worth reviewing the stats:

1. The median average for recovered data is 65% with only 8% of organizations recovering all data.
2. Decryption can take time depending on how much data there is and there is no guarantee. The paid decryption tool can fail and leave your files permanently encrypted and useless.
3. Some ransomware groups exfiltrate all data prior to encryption and threaten to leak the data if you do not pay. They hold this downloaded data as ransom and promise to delete it if you pay the ransom – do you trust the criminal group to delete your data if you pay?

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

4. There are scenarios that could result in multiple extortions, these include double, triple, and data leak extortion. Ensure you understand what you are paying for before agreeing or sending payment.
5. If you are one of the companies that pays the ransom, you might get a target on your back by criminal organizations that you are a paying victim and good for repeat business.

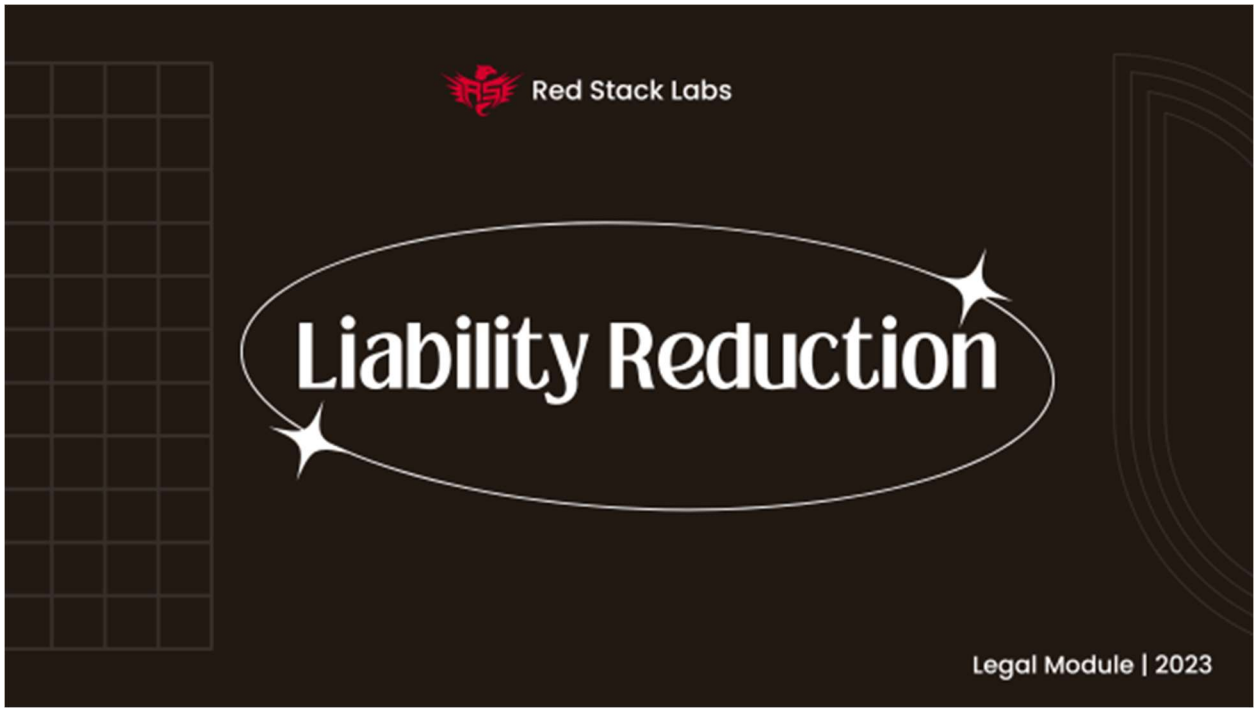
If you decide to pay ransom

Involve your legal counsel, law enforcement and security professionals into the conversation prior to communicating with these criminal groups, they could have insight about them that could be helpful

Be aware it can take a few days to deal with ransom payments, and during those days you won't be able to work on restoration. Plan your recovery efforts in parallel to ransomware decryption efforts so that time is not lost just in case the decryption fails.

Most payments will be via crypto. You will likely need the support of a firm to supply the crypto coins on short notice, most people don’t have the buying power necessary to convert capital into crypto over a weekend.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs’s Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.



Liability Reduction

During a cyber incident your company could face multiple financial exposures due to different liabilities. It is imperative to work through liability reduction to reduce the financial risk.

Personal data and privacy regulations can affect your company through fines, penalties, or civil suits. Data your company stores for clients, partners or third parties that could result in damages or losses to their business such as intellectual property or stolen credentials you used to login to their networks or computers.

Contract obligations and breach of contract could result in lawsuits for something as simple as a delay in your delivery because of a cyber incident, or not notifying them of a cyber breach, and more complex scenarios which result in damages and losses to their business they would want to reclaim.

Contract obligations could also be in breach in the event one of your vendors suffers a cyber incident that consequentially affects your ability to perform work for your client. Throughout this module we touch on contract and business law to give some insight into these areas of liability.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

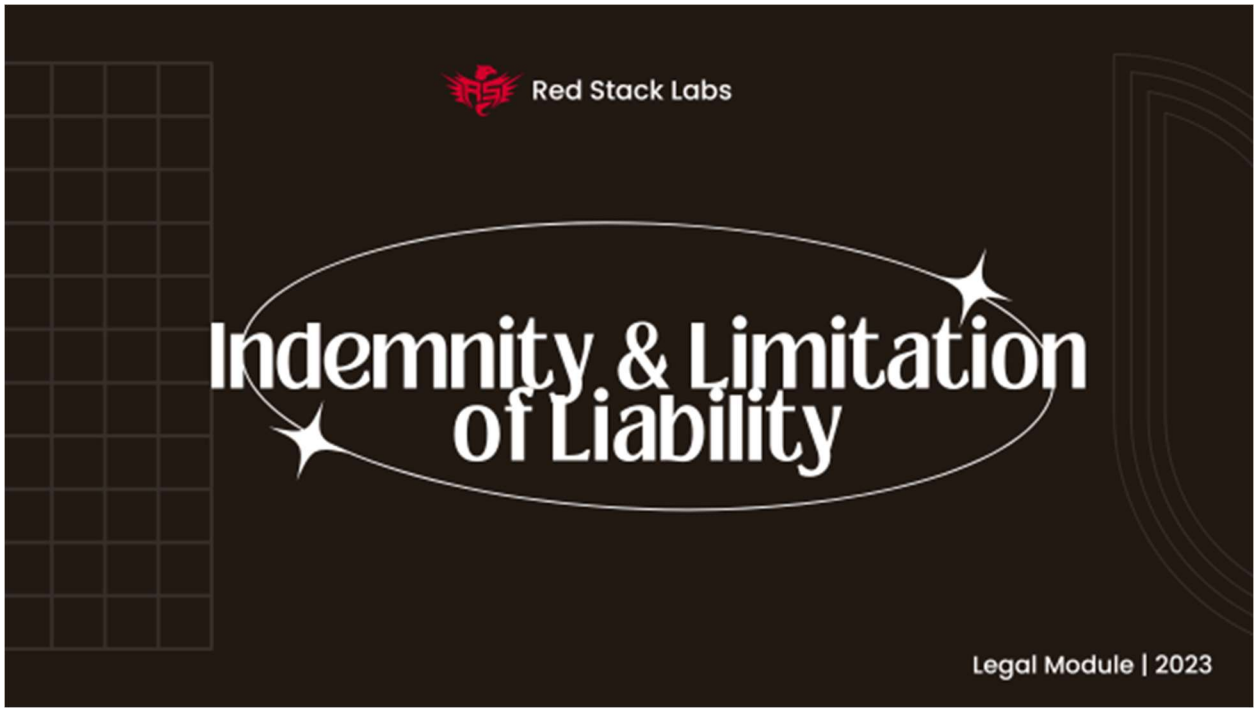
The cost of a cyber incident is not just to your business; it can affect many additional parties. This could be unplanned or unforeseen interruptions, damages, costs going beyond business interruption, recovery costs, staff costs, loss of revenue, etc.

Disclaimer: Contract terms are important to understand. Always consult with your lawyer and have them review any important contract you are presented with, before signing.

Next Steps

While learning about additional financial exposures and cost vectors reflection on your current contract obligations. Are you exposed in a way you didn't previously consider? Download the worksheet, identify your risks & associated legal obligations.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.



Indemnity & Limitation of Liability

Indemnity

An indemnity within a contract is important to pay attention to because it is essentially a promise to pay the other party in the event of some specified occurrence that causes that other party loss. For example, an indemnity clause might say that you must pay the other party if the other party is sued by a third party for reasons related to your work.

Indemnification can be for a certain claim, period, certain product, include interest, attorney fees, all costs, damages, losses. Indemnification can also stipulate that if there is a loss that attorney fees can be covered by the other party.

Indemnity vs Limitation of Liability Considerations

These should be read in tandem, even if written in different areas of a contract, because they both apply in the event of a loss incurred by your client.

Indemnity seeks to increase your liability, whereas limited liability clauses are meant to reduce your exposure.
In general, you want the limitation of liability clause to be as wide as possible for you. It is important to read the limitation of liability clause closely to see if it protects you from all losses that are not subject to your duty to indemnify.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Questions to ask include - in a contract are the indemnities limited and to what extent? There could be a balance between the two of these, in the end your company needs to ensure you are covered, and your vendor or partner is liable for the responsibility they take. Think bout how they would breach a contract and how it would affect your company. Does the contract obligate them to cover losses and damages for your business and your customers if they have a cyber incident?

Contractual Indemnity vs Third-Party claim indemnity

Contractual Indemnity

- Contractual can cover losses and damages for matters of indemnity such as breach of contract but does not provide indemnification for third-party claims

Third Party Claim Indemnity

Third-party claim indemnity only covers third-party claims

Exclusion of Liability

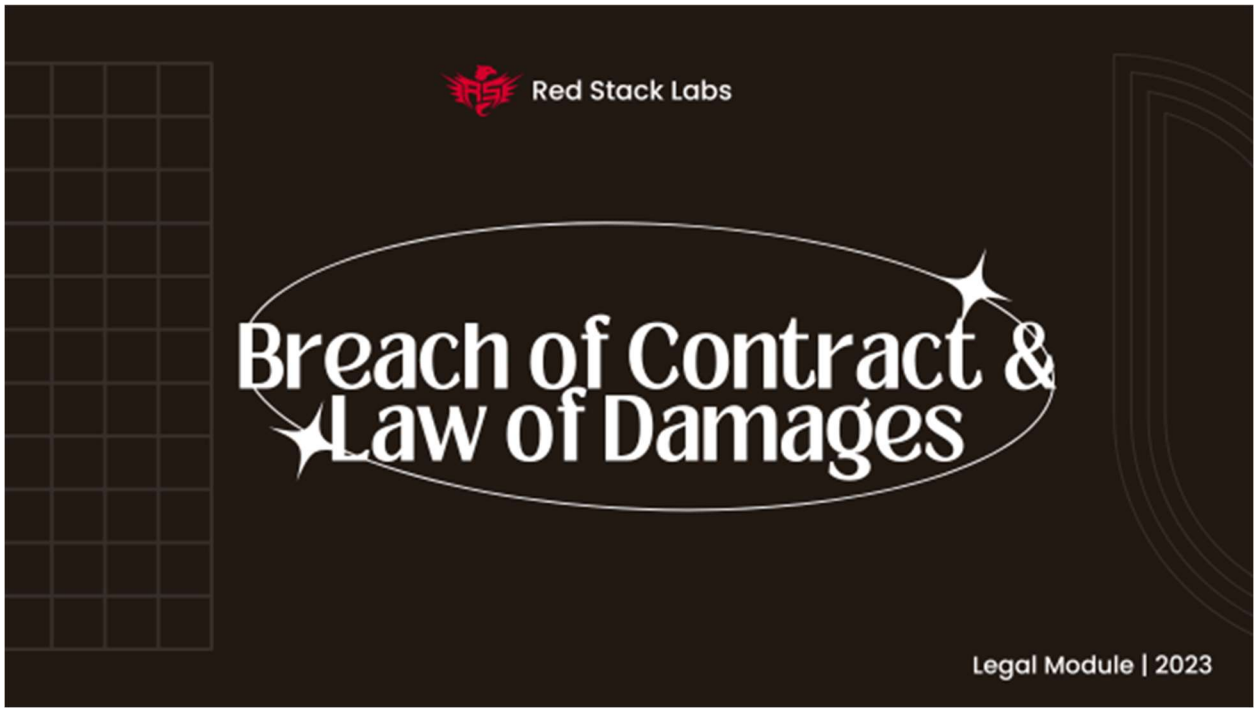
- Damages can arise in tort or contract law. As well, the law of equity provides remedies for wrongdoing in the context of a contract such as injunctions, specific performance, and restitution. All of these are different ways that you can be exposed to liability.
- Exclusions can aim to reduce your liability, it may try to limit liability to only direct damages and exclude indirect, consequential, incidental, exemplary, special, or punitive damages.
- Exclusions could also seek to reduce liability for loss of profits and lost business.
- Ensure your legal counsel can confirm how clear the exclusions in your contracts are, and how they would affect your business if a third-party where compromised which led to some form of loss to your business would otherwise not have faced.
- Your lawyers can include specific wording to reduce the scope of the exclusions for contracts your company signs and expand the liability for contracts your company provides to others to sign.

Carve out

Carve outs can be used during negotiations to find amicable solutions to exclusions and limitations of liability

Disclaimer: Again, having a lawyer review your contract beforehand is strongly recommended, so that you can get a more precise sense of what exposure you have in the proposed contract.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.



Breach of Contract & Law of Damages

If a vendor or partner breaches the contract, the innocent party may sue for damages as compensation. Types of damages to consider:

- **Compensatory Damages**: The basic goal of the law of damages is to put the innocent party in the same economic position it could have been in if the contract had been performed. The innocent party may also be entitled to compensation for losses that would not have occurred but for the breach of contract.
- **Punitive Damages**: These kinds of damages are rarer because the standard to be met for them is much higher. The defendants' conduct must be malicious, oppressive, high-handed, and/or in a cyber incident they are usually based on bad faith conduct such as dishonesty, intention to cause harm and other more severe factors.

The extent of compensation must be reasonable to the parties at the time of contract, this means the losses caused by a breach that your vendor or party suffers must be reasonably foreseeable at the time of contracting.

Disclaimer: It is strongly recommended that you consult with a lawyer if you believe the other party has breached the contract and want to know what damages you might be able to recover.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Direct Damages vs Consequential Damages

Each case is circumstantial depending on the views of the court to define direct or consequential damages.

Direct

- Naturally and immediately from a breach.
- These should be recoverable by your company.

Consequential

- Indirect damage and incidental damage, one step removed from the breach but still caused by and not too remote from the breach.
- They can be recovered depending on the court if they are proven to be derived from a breach during a contract- if the damages are reasonably.
    - This might require special knowledge.
    - Example: if the party in breach knows that its performance is essential to the innocent party's compliance with a very serious regulatory requirement or a contractual requirement, they can foresee that their breach would cause severe losses.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Contracts and Liability

Small and medium sized companies are not immune from contract liability, in fact the risk of financial exposure comes down to the contract and which party is responsible for the damages that incur from a cyber incident, in addition to how the incident is handled. The businesses you deal with and become contractually obligated to, their cost of business is not your cost of business, in comparison their cost of business could far outweigh your entire company valuation and if a cyber incident to your company opens a hole into their networks, computer systems or sensitive data that results in large damages to their business and you are contractually obligated to cover those costs, that could put your company in a precarious situation.

The goal is to reduce your liability and risk of loss in contract negotiations, because ultimately every business is at risk of loss during a cyber incident, so you want to minimize the potential outcomes to your company. Some things that your contractual partners or clients may hold you liable for are data privacy violations or data breaches that occur either because your company was breached and had the data exfiltrated, or because one of your third parties (vendor, contractor) unreasonable security practices led to a breach and exfiltration or loss of their data and you are on the hook for their negligence to your client. This is important to understand in contracts with clients and partners, that you might be responsible for your vendors security practices and cyber incidents regarding your client or partners sensitive data.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Beyond the financial obligations there could be other contractual obligations that could result in a breach of contract, like specific security requirements for your company and third-parties, breach notification periods and reporting. Which means you would have to properly vet and assess your third-parties security.

Minimize Cyber Risks with Contract Language

Employing vigilant cybersecurity practices and protecting yourself with insurance are the two best data breach risk management strategies. You can also include clauses in contracts to help minimize your liability. Legal counsel can help you draft contracts for your projects.

Examples of ways you might protect yourself include:

1. Limiting product or service warranty times.
2. Limiting the types of damages for which you are liable.
3. Limiting the amount of money for which you are liable.
4. Holding the original software or hardware manufacturer liable for product defects.

Contracts Reporting Requirement

A contract with certain partnerships or customers might have a requirement or obligation to notify them of a security incident within a certain time frame. Failing to report could have consequences and put your company at breach of contract. This could open your company to a potential lawsuit, or contractual obligation to cover losses or damages because of the breach depending on the wording in the contract.

It is important to have your legal counsel explain the legal and contractual obligations of your partnerships and customers contracts and to plan out how to deal with them in case of a breach. If your company deals with lots of different customers, and you use different contracts for each one (perhaps because of negotiations or some larger clients use their own contracts instead of yours) you might have quite a few different contractual obligations that you need to be aware of during a cyber incident, to manage the requirements and expectations with your customers.

Notes on Contract Liability

Contracted Indemnities can cover all losses, liabilities, and damages. This can be worded to include direct, indirect, and consequential and incidental damages, making it so there is no line drawn between direct and other types of damages.

Indemnities can be written by a lawyer to expand liability to include losses for those who

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

are not parties to the contract. Have your counsel look for a limitation of liability or loss monetary amount. Is it capped to a specific amount or a type of contractual work?

Contract negotiations, including discussing indemnities, exclusions and limitations can cause frustration between both parties. It helps when both parties have proper legal counsel to translate the legal contract language. Negotiations can result in take it or leave it position from one or both of the parties, it is important to understand realistic risk and financial exposure in these negotiations, are you better off taking the risk of an unfair contract, or - if there is an incident would you better off with specific provisions to protect your company liability and reduced financial exposure.

In a negotiation parties can agree to a knock for knock arrangement. That is, each party indemnifies the other party for their staff, responsibilities, etc., this way if damages arise each party is responsible for their own side. When dealing with cyber breaches you may not want to provide specific indemnities to a third-party vendor or contractor.

Contracts could have a set period - this can be dependant on your location or the location of the other party.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Vendors & Suppliers

Regulations and contracts can impose security requirements on the vendors and suppliers your company works with. Your company is expected to know your third-party suppliers and in what ways they interact with consumer data, the activities they perform and their security posture. The company to supplier relationship usually focuses on the commercial goals but not the secondary risks or security requirements.

For instance, in British Columbia the regulatory requirement is:
"As organizations engage vendors/contractors to undergo pieces of work, vendors should understand and maintain the same (or higher) security posture as the organization. Security requirements for vendors should be clearly stated in contracts, and contracts should be reviewed regularly, ensuring vendors are keeping to the requirement before it is renewed."

Disclaimer: Review with your counsel to understand requirements based on your locations where the business operates.

Similar requirements and responsibility can be found in contracts with third-parties or other regulatory bodies, because of this we highlight some basic principles and objectives based on the BC PIPA regulatory requirements that could help reduce risk:

1. The vendor requirements are documented, reviewed, and updated regularly.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

    a. Maintain a scorecard or spreadsheet on your vendors and suppliers.
2. The vendors security posture should meet or exceed your organizations security policies.
    a. Complete a vendor security assessment or obtain a copy of their third-party security audit report and have the vendor sign off on the legitimacy of the statements made about their security. If they are later found to be false or negligent it could be a breach of contract holding them liable.
3. Supply chain security risks are identified, mitigated, and reviewed regularly.
    a. Through a supply chain assessment process your company should have a good understanding of what privacy or sensitive data your vendors or suppliers have access to and how it is processed, as well as their security programs and compliances with security frameworks and regulatory authorities.

Legal Impact against a supplier

It would be based on the contract that is signed between the parties and this can come down to the sophistication of the two parties and how they negotiate the contractual requirements during a cyber incident, and what type of legal recourse. Who pays the bills for forensics? Who pays for damages and losses?

Regulatory and Legal

Regulatory authorities might ask what type of security practices your vendors and suppliers use? Have you checked and done a security assessment with your vendors and suppliers?

Vendor Security Assessment

It is important to assess your vendors security, for both contractual and regulatory obligations. There are a few suggestions on completing this requirement. A security assessment or a third-party report on their assessment would provide an overview of their current security posture and could provide evidence if the vendor is later breached and proven to have been misleading or purposefully negligent in their security assessment or report.

1. Request a report of the vendors most recent cyber security assessment or security audit. This should contain their current security posture and possibly the future of security evolution.
    a. Do this over email and have it in writing, both the request and the response and report document.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

2. Request a vendor hire to a third-party auditor or hire a third-party auditor yourself to conduct a risk assessment of your vendor.
    a. This could be done if they have not had a third-party security assessment done before. Any vendor whose business revolves around storing client or sensitive data should already have a security assessment done and the report readily available.
3. Run your own security assessment of your vendors either by sending a questionnaire or in a workshop setting over a zoom call.
    a. If you deal with a smaller or newer vendor and neither of your companies can budget a proper security assessment, you can run your own security assessment workshop with the vendor to ensure they follow a proper security program that would keep your client data safe.
4. This security assessment should be signed off by both parties to validate the understanding of their security posture.

The result of the security assessment is you should have written responses from your vendors on what their security posture and practices are. Providing you a security baseline to compare against your own organization, is your vendors security better than your own, because it should be.

Liability for Vendors data breach

Your company could be held liable for your vendors cyber incidents and breaches. For example, you store your customers data with a vendor, and they have a cyber breach, and all of the data is exfiltrated and leaked online because your vendor did not pay the ransomware.

(This section is compiled against the FTC requirements and laws, but a lot of if not all these also apply to Canadas privacy regulations and laws as well.)

Vendor should have the same or better data standards than you do. You should have good visibility into your vendors data standards, how they handle and store data information. This could be gathered from a recent audit report from a third-party.

Vendor Contracts

1. Include indemnification clause in the contract to obligate the vendor through contractual liability to reimburse the losses if they have a data breach and your customer data is lost or stolen.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

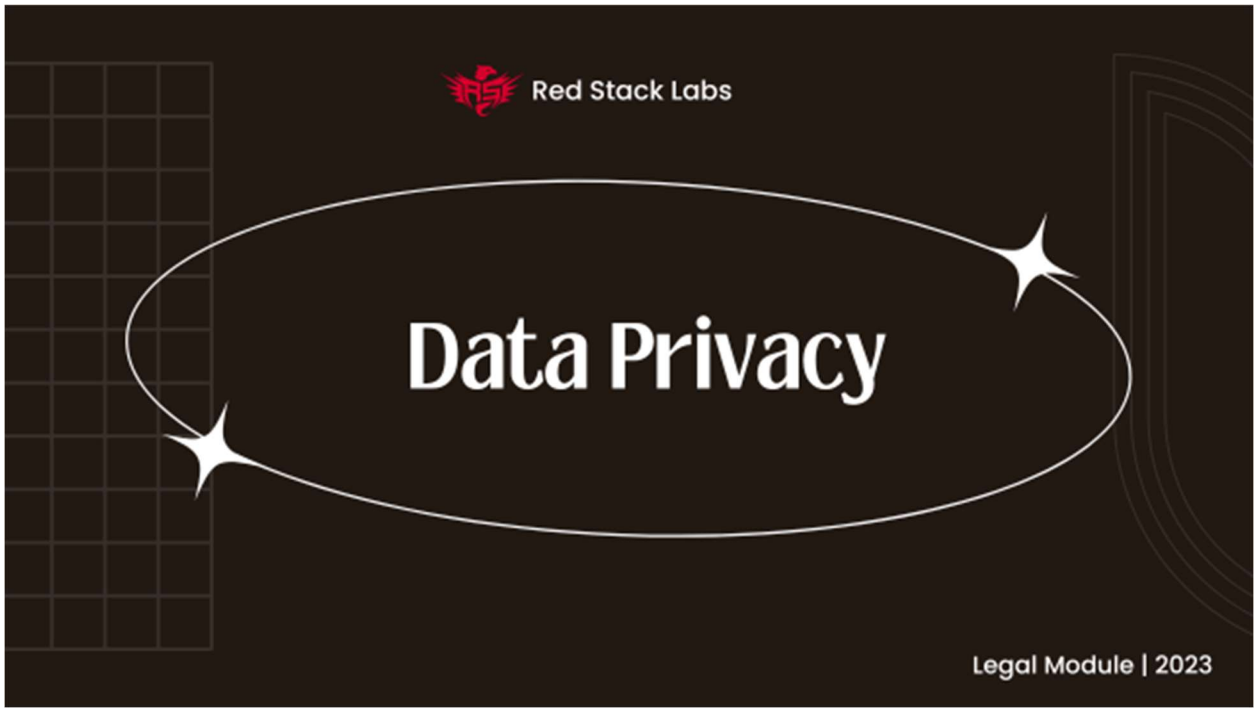
2. If your vendor has a cyber incident and your customers data is lost or stolen your company could be held liable for the data loss, damages, or for any regulatory action, fines, or penalties.
3. Require your vendor and suppliers have a set of security standards, compliance, frameworks + safeguards to sensitive information and privacy protection of your customers information.
    a. The vendors security standards should match or exceed your own companies' requirements.
4. Do not waive subrogation rights in contracts with a vendor.
    a. Your insurer should have the contractual freedom to sue a vendor who mishandles your customer data, either through negligence or cyber incident.
5. Vendor shows proof of cyber insurance coverage.
    a. This will provide additional coverage for protection under your vendors breaches.
    b. If a vendor is responsible for a large-scale breach, they may end up in financial duress and have difficulty reimbursing damages or losses to your company or your clients. But their insurance could still cover the costs.
    c. You can ask to be added as an additional insured on their insurance policy.
6. Vendor expectations and security practices
    a. Review if a vendor does not claim proper security practices on their website, or sales deck.

Next Steps

Download the Vendor Contracts Checklist to review current & potentially new vendors.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Regulations



Data Privacy

Personal data regulations and laws, if not handled properly, can place your company at financial risk. The regulations you must comply with are dependant mostly on your customers and the type of sensitive or personal data you process or store. If you have European customers (GDPR), Canadian customers (PIPEDA, PIPA), or America (Californian CCPA) customers and process or store personal identifiable information (PII), you will have to comply with all those countries data privacy regulations. Each data regulation differs in requirements, reporting and enforcement and you are expected to comply with every data privacy regulation that affects your business.

Your goal with privacy regulation

The goal with data privacy regulation is to enforce a tight enough security and follow a proper data handling process to meet their requirements, in the result of an audit or investigation your company will be compliant, leaving the reporting during a cyber incident and contractual obligations with vendors and suppliers as your liability vectors, both of which can be tightened up and complied with easy enough.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Multiple Regulations

If you are required to comply with multiple data privacy regulations and there is a cyber incident, you will have to report to each commissioner individually, we recommend following your legal counsel's advice on this.

United States

America does not have a single data protection legislation; it is comprised of hundreds of federal and state laws to make up the data protections of U.S. citizens. At the federal level, the Federal Trade Commission (FTC) is empowered to protect consumers against unfair or deceptive practice regarding privacy and data protection regulations. Regarding the FTC enforcing against deceptive practice, this includes failure to comply and failure to provide adequate security to personal data and information. There are multiple federal laws that provide protection to data privacy rights in the U.S. a few examples are the Drivers Privacy Protection Act, Children's Online Privacy Protection Act, Video Privacy Protection Act, and Cable Communications Privacy Act.

State laws can also provide protection to consumers from businesses while imposing obligations and restriction on the use, retention, and disclosure of certain types of information. A few examples are Social Security Numbers, bio metric data, medical records, drivers license information, library records, email addresses, tax or insurance records, criminal justice information, phone records and education records.

Because certain states have independent data protection regulations, some states provide stronger protections than others. For example, California has the California Consumer Privacy Act (CCPA). Massachusetts has the 201 CMR 17. New York has the New York Shield Act. Illinois has complex state law such as the Illinois Biometric Information Privacy Act (BIPA). Virginia has the Consumer Data Protection Act (CDPA). Colorado has the Colorado Privacy Act (CPA). Utah has the Utah Consumer Privacy Act (UCPA). Connecticut has the Act Concerning Personal Data Privacy and Online Monitoring.

These federal and state laws and regulations as so specific and complex we recommend connecting with your legal counsel and a data privacy expert in the U.S. when dealing with consumers in these different states. It is beyond the scope of this program to dive in depth, but this is a legal issue that should be addressed as a business to reduce your liability.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Canada

Cross border transfers and outsourcing

PIPEDA

- Requires a vendor has comparable level of protection when dealing with your customers personal information or personal information is being processed by a third party, same as the FTC requirement in the USA.
    - The protection of the vendor must be reasonable.
- Does not have a regulation prohibiting the transfer of personal information outside of Canada, assuming there is consent to the transfer.

PIPA

- Imposes obligations when you use a service provider outside of Canada to collect, use or disclose or store personal information, including the duty to inform your customers.
- Organizations also have special duties when they use a service provider to store data outside Canada, including the duty to notify individuals that their data is being stored outside the country.

When storing Canadian personal data in the USA

Once the data is stored on a server inside of the USA it is subject to U.S. law, including the Patriot Act, and U.S. government entities will have the legal right to access all the personal and sensitive information. If your customer requires privacy protection from the USA government, you need to be aware of where their data is being stored and what legislation it falls under. Certain types of data from Canada cannot be stored on US servers, for example: health information (HIPPA), and legal documents.

Next Steps

Download the Regulations Chart and review which regulations apply to your business.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

Regulatory Authority Reporting

Regulatory authorities and all data privacy regulations require breaches to be reported if the sensitive or personal information has been compromised, and to be safe if there is even a chance it was compromised.

The reporting asks of personal or sensitive data breached is if there's real risk of significant harm and not just speculative or theoretical harm. One way to define a real risk of harm is through financial loss, identity theft, physical harm, humiliation, or damage to a personal or professional reputation. If the cyber breach and compromised data can lead to these significant situations, it's best to fair on the safe side often and report the breach.

Failure to report could put your company in violation of data privacy regulations and result in fines or penalties which would add additional costs to an already financial impacting situation. Failure to comply with data privacy regulation requirements would also put you in violation of data privacy regulations, if an audit or investigation is triggered because of a breach or a violation notice to the commissioner from a customer or third-party, this could also result in fines and penalties for failure to comply.

Enforcement

Data privacy regulatory authorities use the carrot and stick approach to entice companies to become compliant. In this case the stick is fines and penalties for non-compliance or

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

failure to adhere to requirements for a specific regulatory authority. Different data privacy regulations have their own requirements and penalties for non-compliance, these can be found in the regulation's comparison chart for a few of the major privacy regulations. Our recommendation is to adhere to the data privacy requirement standards that apply to your business and clients sensitive or personal data and follow the requirements during a cyber incident on reporting. This will help reduce your financial exposure and liability during a cyber incident by ensuring you do not suffer additional costs during the cyber incident.

Regulatory authorities are government mandated and have been making examples of both large and small companies during the last few years of their inception. They are not lenient in most cases and work hard to keep people's personal data safe.

Next Steps

1. Data Privacy Regulation Chart Download

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.

This material and all content within this document are copyrighted and based on proprietary concepts from Red Stack Labs's Corporate Liability Reduction program. Do not duplicate, distribute, publish, share, or train from without written permission. For inquiries, contact hello@redstack.io. ©2023 Red Stack Labs Corp. All rights reserved.