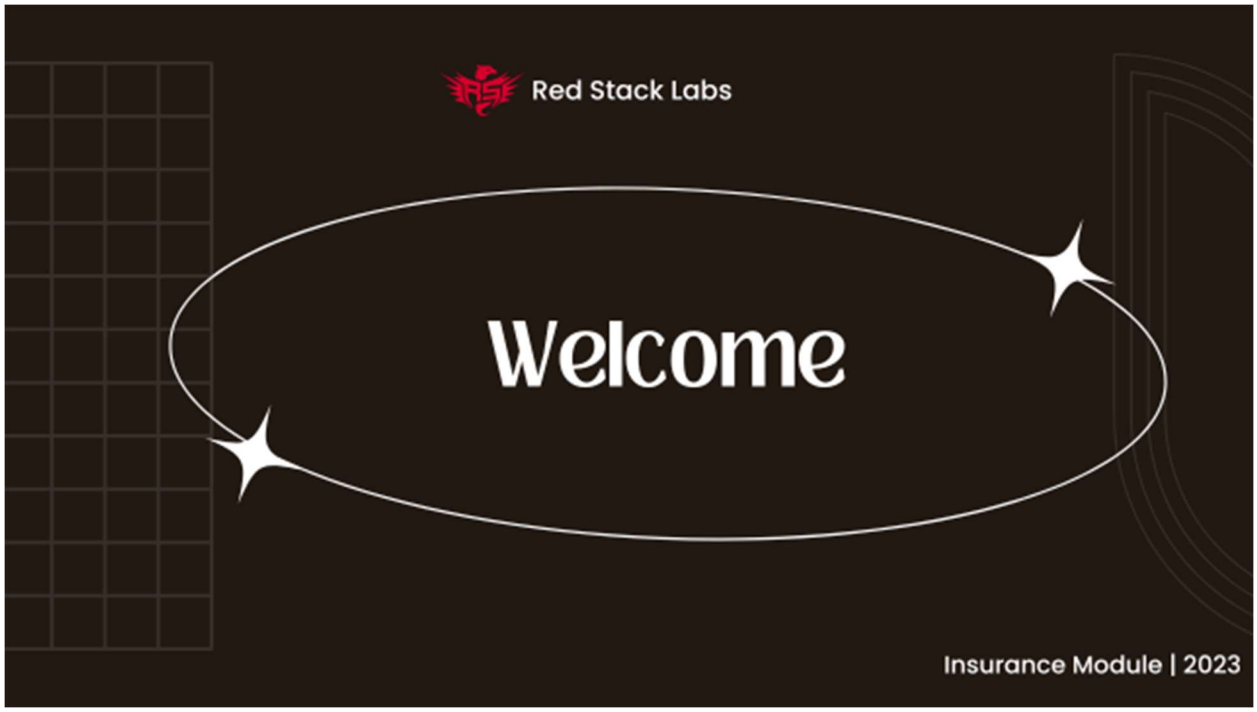
Insurance – Book 1

Corporate Liability Reduction

Ermis Catevatis
RED STACK LABS CORP

Version	Date	Author
0.1	July 28, 2022	Ermis Catevatis
0.2	Sept 18, 2022	Ermis Catevatis
0.3	Oct 04, 2022	Ermis Catevatis
0.4	Dec 08, 2022	Ermis Catevatis
0.5	Dec 22, 2022	Ermis Catevatis
0.6	Jan 06, 2023	Ermis Catevatis
1.0	Jan 15, 2023	Ermis Catevatis
1.1	Oct 09, 2023	Ermis Catevatis

Contents

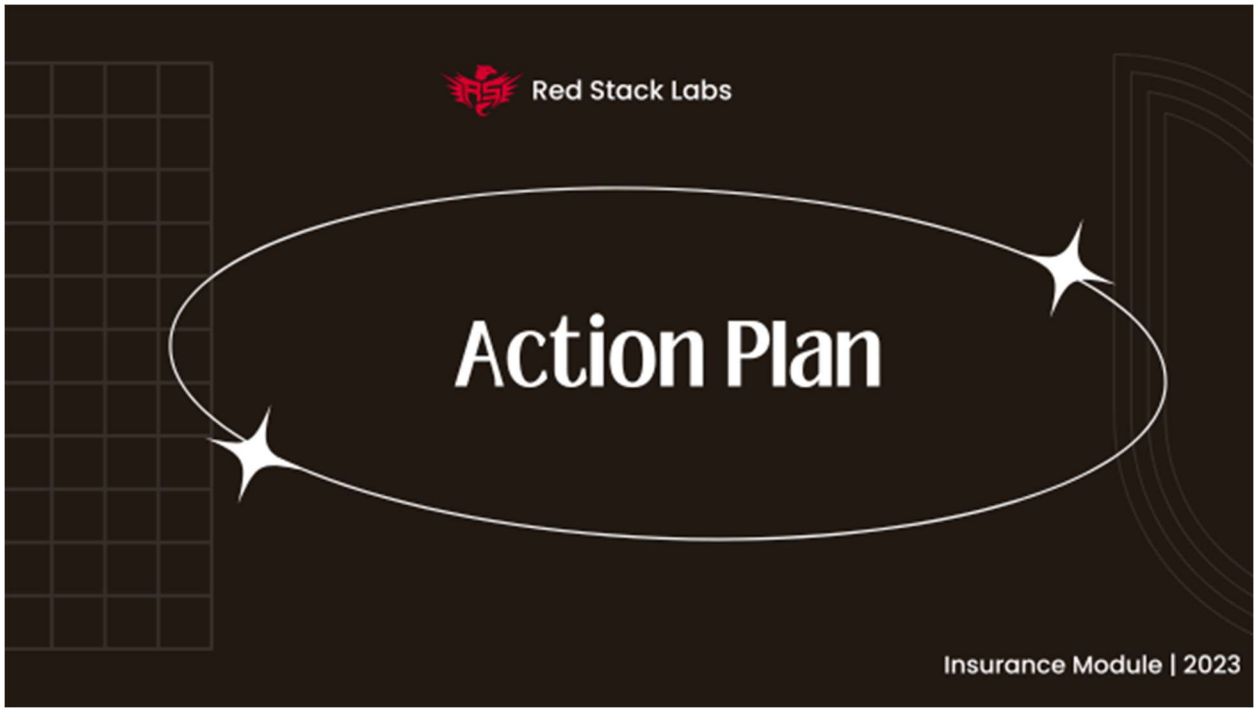


Welcome

We're thrilled to have you onboard for the "Navigating Cyber Insurance: A Comprehensive Guide for Corporate Cyber Insurance" course. This course has been meticulously designed to help you gain a deep understanding of the cyber insurance landscape. As you begin your journey with us, remember that each module in this course aims to empower you with the knowledge to safeguard your organization from cyber threats while optimizing your insurance investments.

In an age where digital security is paramount, having the right knowledge and tools can make all the difference. Throughout this course, we will navigate the nuances of cyber insurance policies, explore common exclusions, and provide insight into choosing the most suitable policies for your organization. We've curated expert content, case studies, and interactive assessments to ensure that you're not only learning but also applying this knowledge in a practical context.

Get ready to dive in! We believe that the insights and skills you gain from this course will significantly contribute to strengthening your organization's cyber preparedness posture. Remember, we are here to assist you throughout your learning journey. So, should you have any questions or require any help, do not hesitate to reach out. Here's to a successful and enlightening journey ahead!



Action Plan

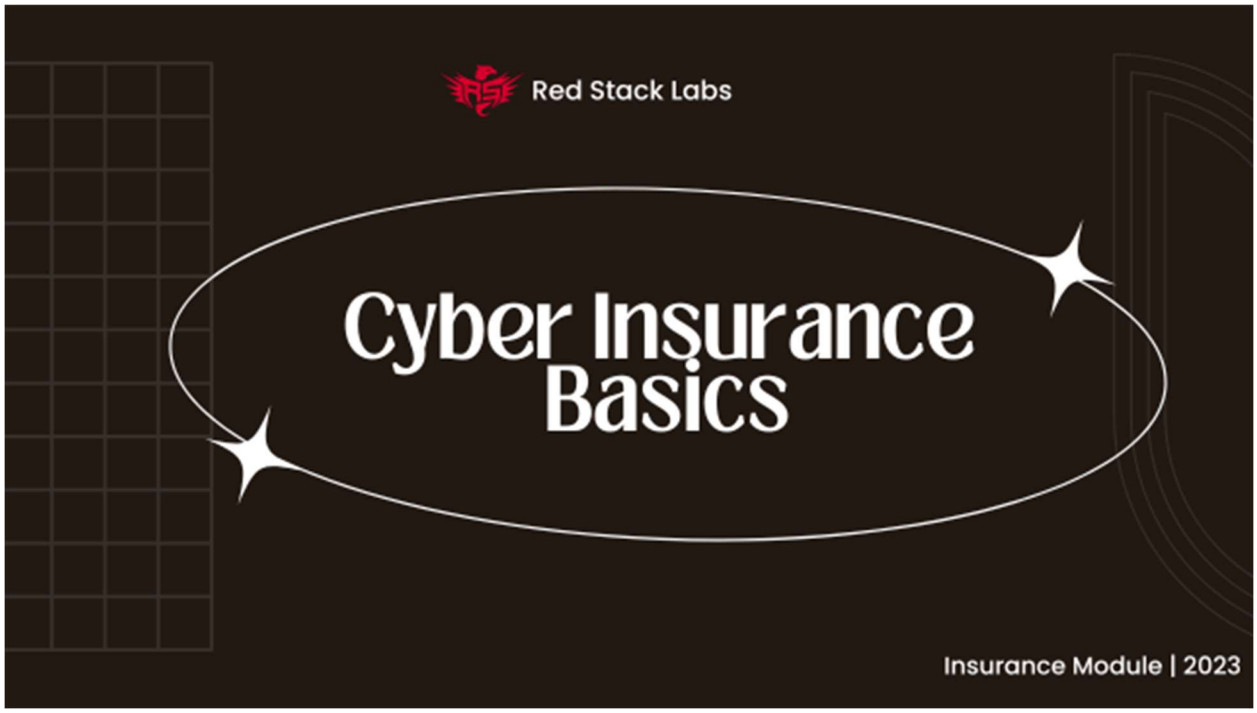
Welcome to the next stage of your learning journey. After completing this course's study materials, there are several tasks you are expected to undertake to fully benefit from this course:

1. **Comprehend Course Material**: Ensure you've thoroughly read and understood the course content. This foundational knowledge is critical to making informed decisions about cyber insurance.
2. **Review Current Cyber Insurance**: If your organization already has cyber insurance, the next step is to review your policy with the help of a lawyer, if possible, to understand its details and potential gaps.
3. **Procure Cyber Insurance**: If you don't currently have cyber insurance, your goal should be to seek coverage. Use the provided questionnaire to help assess potential insurers and identify a policy that aligns with your organization's needs. It is advisable to evaluate multiple insurers to ensure a suitable fit.
4. **Apply Your Knowledge**: Let's put your understanding into practice. Determine how your policy (or prospective policy) aids your business through its coverage and limits. Identify the policy's exclusions and any potential drawbacks. Understand the criteria that must be met to file a claim in the event of a cyber incident. If there are uncertainties, use the questionnaire as a guide to seek clarification from your insurer.

The main objectives of this course are as follows:

1. **Identify Suitable Coverage**: Assist your business in finding the right coverage to provide financial protection against cyber incidents, including damages, lawsuits, fines, etc.
2. **Awareness of Claim Factors**: Raise awareness about certain factors that could affect your ability to make a claim.
3. **Understand Cyber Security Requirements**: Educate you about potential cybersecurity requirements that an insurer may have, which could impact your ability to make a claim.
4. **Awareness of Policy Shifts**: Highlight that cyber insurance policies are increasingly shifting in favour of the insurer due to the surge in ransomware claims.

Remember, having cyber insurance won't prevent a cyber attack, business downtime, loss of revenue or clients, lawsuits, fines, or penalties. The goal of cyber insurance is to provide financial assistance to help your business recover and avoid excessive debt.



Cyber Insurance Basics

In this module we cover policy terms, coverage, requirements, and exclusions. It includes what to look for in your insurance policy, and how to work with the insurer during an incident.

Cyber insurance policies are different from other policies that are frequently templated. Policies such as Errors & Omissions and Commercial General Liability are often similar

across insurers. Cyber liability policies are rapidly changing as the landscape on incidents are growing. In fact, they can provide very different offerings, limits, restrictions, and exclusions from one provider to another, so some due diligence should be completed prior to purchasing a cyber insurance policy. Don't fret if you've already purchased one, our cyber insurance module and questionnaire will help you understand your policy and see if it's time for a change of providers or put you on track to purchase the right cyber insurance policy for your company.

Benefits of cyber policies during an incident

A good cyber insurance policy will set you up for success prior to and throughout an incident.

While cyber security requirements from insurers can help most businesses improve their security posture proactively, it doesn't provide entire protection. It's important to know which expenses will be covered by your insurer but also how your financial risk exposure changes with a good cyber insurance policy.

Cyber policies gaps in an incident

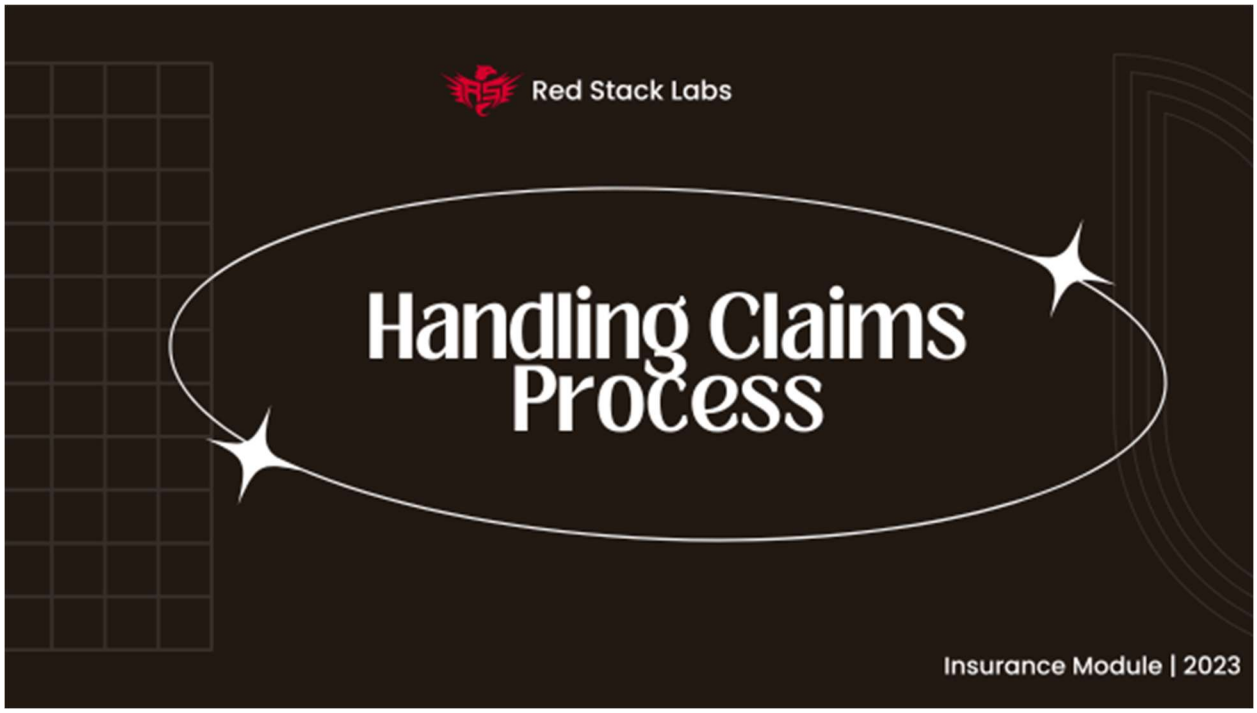
While it is in your benefit to be insured there are specific scenarios where an insurer can be contractually excused from supporting your business financially. These come in the form of exclusions, restrictions, limits, requirements and what is not listed inside the policy coverage. It is a good idea to comprehend each one of these sections fully before committing to a cyber insurance policy but also understand if it is not listed inside of the policy coverage it is not being covered.

Understanding your cyber insurance policy

Your business may not be insured for specific scenarios. Not asking the right questions about their exclusions or restrictions, could place your business in a tough spot after an incident occurs. To be prepared it is in your benefit to check everything now and make changes, if necessary, if that means making policy changes with your current insurer, or switching insurers to obtain the coverage you need, get it done before an incident occurs.

Disclaimer: This is by no means a complete list of all possible scenarios; the purpose is to educate you on the core concepts of cyber insurance policies and caveats to watch out for. It is possible that this program may not fully prepare a company for all potential scenarios, and as part of the course we advise to fully review all cyber insurance policy documents

with legal counsel and the insurer to obtain a complete understanding of your policy, coverage, requirements and obligations, exclusions, limitations, and restrictions.



Handling Claims Process

Don’t speculate with the insurer about the cause, the threats or the threat actors

1. If attribution is not confirmed by experts, do not make assumptions. If you aren’t sure of the current damages, don’t start guessing.
2. Anything you say to an insurer can be used against you for grounds to deny coverage. It helps to have legal counsel to guide you through this communication process. Within the incident checklist the first step is to call your independent lawyer.

Independent experts

1. Counsel provided by an insurer are their lawyers, without proper privilege established in a tripartite or dual client privileged confidentiality, everything you say to their lawyers could go back to them. It is a wise decision to have your own independent counsel for guidance when dealing with 6 or 7 figure claims.

Be truthful with your insurer

1. This can be not just for loss of claim or policy coverage, but it could result in a potential lawsuit with the insurer. You may want to recover premiums and the insurer may not want to reimburse, or the insurer may want claims they previously paid out to be reimbursed by your company.

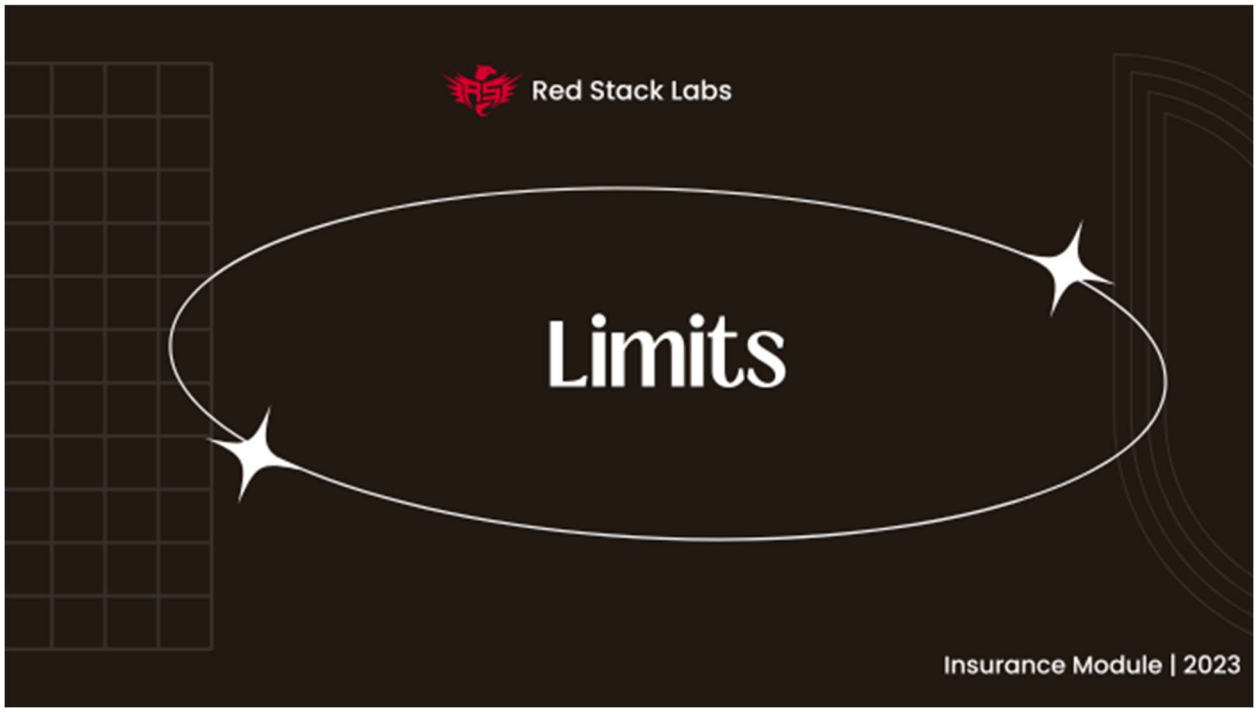
Be prepared

1. Knowing what is covered in your policy prior to making a claim and understanding the wording is useful while making a claim.
2. Context matters and words matter when making a report.
3. When discussing the situation or making a claim be prepared with all the facts. It is ok to not know something at the time of claim, there is no penalty for not having certain information on hand (see item #1 Don't speculate). You can say you are waiting on that information, or the team is still working to obtain that information and you can update them as soon as you know.
4. We recommend all communications between your company and the insurer are vetted by your independent legal counsel prior to contacting them at each step throughout the entire process.

Next Steps

Download the incident checklist and review the steps. Fill in the support system information and keep a physical copy available to you & your team.

Policy Terms



Limits

Policy Limits (includes sub-limits, rider, & maximum retention cap)

The maximum amount of money that could be paid if the claim is covered is governed by the policy limit. The limit can be *per term* or *per claim*, it is also *important* to know which if you have multiple incidents in the same term. The limit will include legal defence costs, settlements, and everything else covered in your policy.

Considerations

If your total expenses throughout the incident exceed that of your policy limit, they will have to be paid out of pocket. Please see Appendix A for loss mitigation strategies if your business may have difficulty paying without loans or loan deferrals.

Choosing the right policy limit is crucial - too high means you could be overpaying for your premiums resulting in over-coverage, too low & your business may not be fully protected.

You should complete a quantitative risk assessment of your business to understand your actual financial exposure when dealing with a cyber incident. Additionally, review business interruption for varying lengths of time and the implications to operations.

The quantitative risk assessment should include not just business interruption, legal fees, emergency services fees, overtime, but also the following should be taken into consideration:

- Contract requirements - professional liability or cyber insurance and policy limit requirements for certain contracts
- Clients - the number and size of your clients. You should be asking what's the chance of a lawsuit occurring? The higher your risk, the larger your policy limit needs to be.
- Industry - is it common for your industry to withstand cyber incidents and lawsuits following cyber incidents? Look at industry trends and apply to policy limits accordingly. If you're unsure, ask during your coaching sessions.
- Cost - what are the average number of claims within a term (if the policy limit is per term)? What is the median average of the lawsuit claims and settlements?

Policy sub-limit

You did your homework on your policy limits, now don't get caught off guard by the policy sub limits. Can narrow a specific category of coverage, placing a maximum payable amount to a specific type of loss instead of providing the maximum policy limit for any type of loss. Because of this it is important to be read up on the sub-limits.

For instance, a policy with a maximum limit of $2,000,000 could place a sub-limit on lawyer fees of $10,000. This means out of the $2,000,000 only $10,000 will cover lawyer fees, leaving the remainder out of pocket. Sub-limits could apply to any category of coverage, including emergency services, settlements, ransomware extortions, reputation damages or any category the insurer feels like setting a ceiling on.

Rider

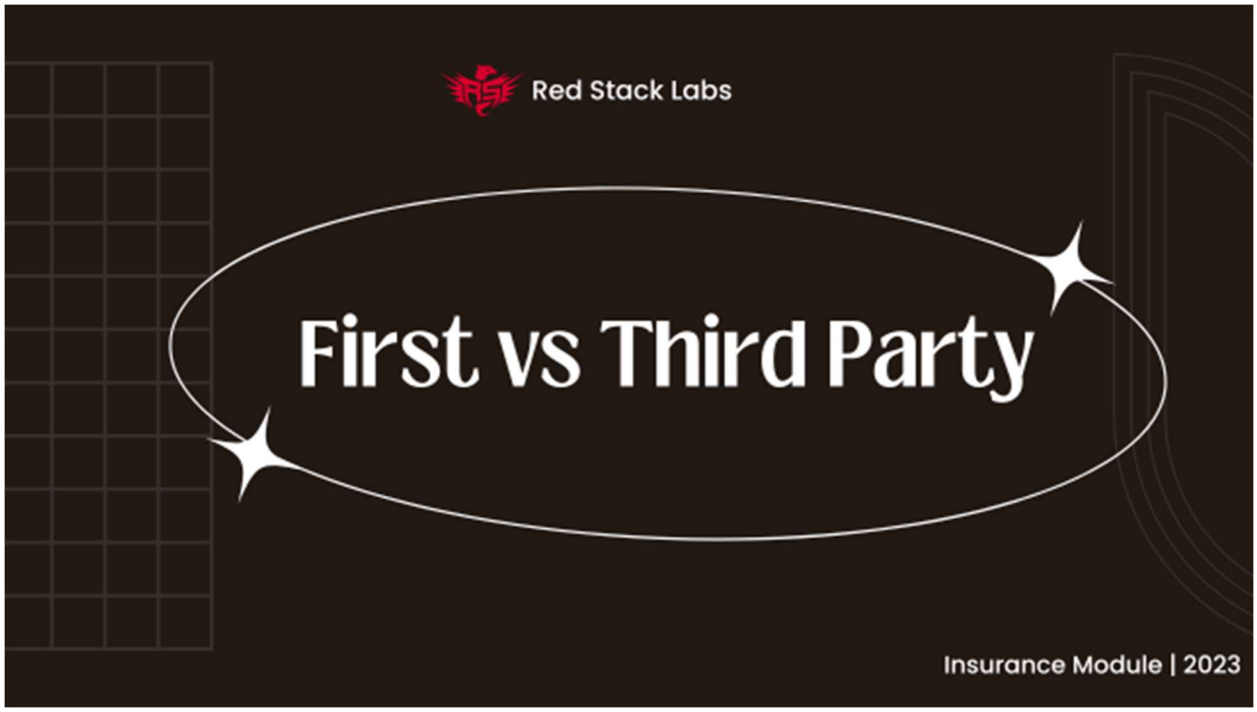
This is additional coverage that can be added to your policy. Because each business will be different, and each insurers riders could be different, the need for optional coverage becomes dependant on the business needs. Throughout this program, and filling out the **Cyber Insurance Questionnaire**, you should have a stronger opinion of what optional cyber insurance coverage is needed for your business.

Considerations

When reviewing riders or amendments to your policy, ensure you are fully aware of exclusions as they could potentially void coverage in specific scenarios. For example, if the initial foothold of a cyber incident was done prior to purchasing cyber insurance with riders, would your policy or it's riders still cover your business?

Deductibles

Most cyber insurance policies have a deductible. This is an amount defined in your policy your company will need to pay prior to receiving coverage from the insurer. The higher the deductible the lower the premiums, this is like a weight scale, when one side goes up, the other goes down and vice versa.



First vs Third Party

If your business holds sensitive data, has access to client systems, networks, data, works on client projects and could be held liable, you should consider both first-party and third-party cyber insurance coverage.

Look at your businesses risk exposure and potential liability – if a partner, client, or other business can claim damages or losses, even if it is related to fraudulent wire transfers or business email compromise resulting in a request for a fraudulent wire transfer, could another business hold your company accountable.

First party

First party will cover items such as cyber attacks or data breaches and the losses the business faces as a direct result, it should cover scenarios such as

- Business interruption and cost of business recovery including digital assets lost in the attack (intellectual property, client data, accounting), and physical assets (servers, networking equipment that was burned in the cyber attack, etc.)
- Revenue loss while handling the incident.
- Emergency service fees (cyber security investigators, legal counsel)
- Communications and credit monitoring
- Reputation damages and management

- Ransomware extortion payment

Third party

Third party will cover the financial liability of clients or partners that suffer because of a breach or cyber attack to your business. This should cover things such as legal fees from lawsuit and settlements.

Both

The grey area between the two types of coverage is when a hacker manages to compromise both your business and client's computer systems – a scenario where the insurer would identify the party responsible.

Next Steps

Download the First party vs Third party worksheet.

1. Review your risk exposure levels, list which ones are first vs third party.
2. Review which scenarios need to be discussed with insurer for clarity.

Claims Made vs Occurrence

Claims Made

"*Claims Made*" is the norm in cyber insurance policies and will only cover incidents that occur, and the claim is reported during an active policy or during an extended reporting period or tail coverage time frame.

Occurrence

Occurrence policies tend to be somewhat rarer in cyber insurance; they provide a lifetime coverage for incidents that occur during the endorsement period of the policy. This would mean an incident between the retroactive date or endorsement date up until the end of the policy period or policy termination would be covered regardless of when your company makes the claim. Insurers could limit or set a cap on an Occurrence policy, or the premiums could be higher.

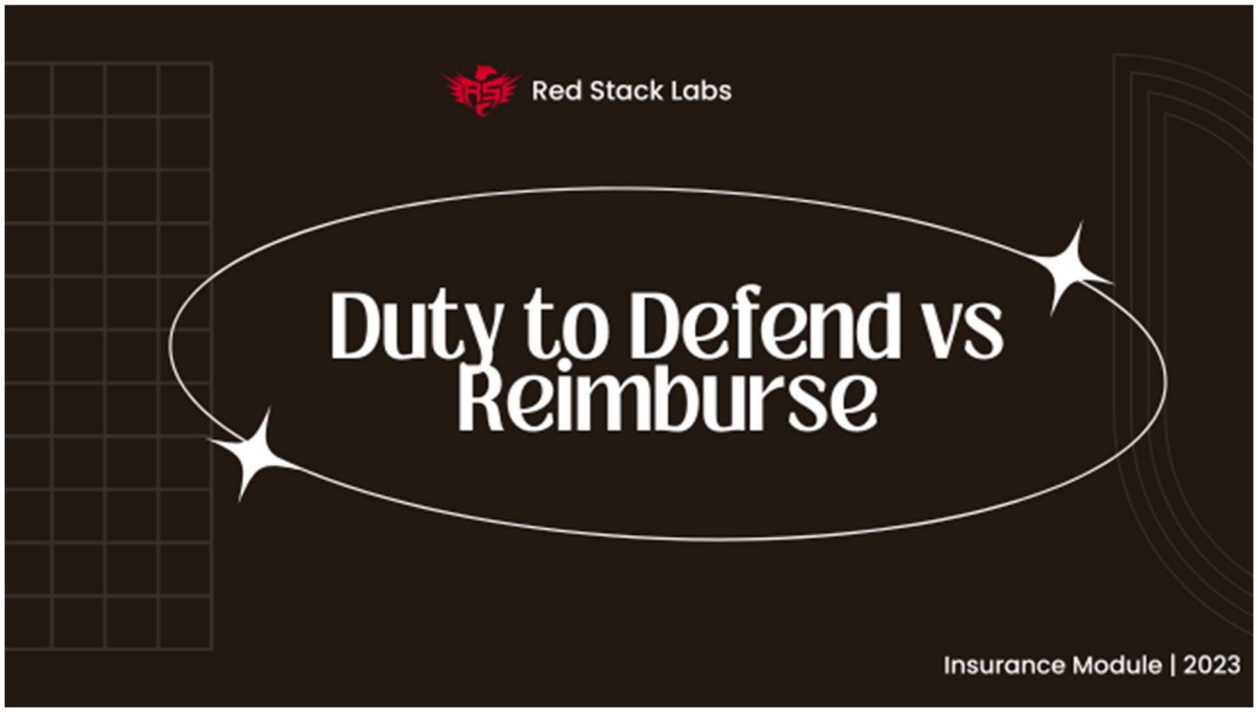
Considerations

Determine which is appropriate in your scenario, otherwise you might end up without enough coverage or overpaying. Ask yourself, is the risk reasonable enough for the business to accept?

Policy Termination

Typically, only applies to "*Claims Made*" policies unless an "*Occurrence*" policy states otherwise.

Once a policy is terminated, no claims can be made against the terminated policy even if the incident was during the endorsement period. There might be specific wording by certain insurers to allow coverage post-termination but for most of the cyber insurance policies they don't accept claims after termination.



Duty to Defend vs Duty to Reimburse

In most cases, if your company does not have legal counsel or reserved cash flow to retain a defense, duty to defend simplifies the entire process. This could be dependant on your company's staffing, expectations, and size. Smaller companies might opt for duty to defend because of the simplicity and ease of coverage whereas larger companies might wish to retain their own counsel throughout proceedings.

There are scenarios where privilege will want to be retained between your company and the chosen legal counsel vs the insurer so it is important to ensure that will be properly covered in your jurisdiction. Additionally, conflict of interest may rise between your company and the insurer, in those cases seek to obtain independent counsel could be the best path forward if the policy supports the clause.

Duty to Defend

Let's review several scenarios for your benefit.

The insurer has control and retains counsel for the policyholder with a law firm of the insurer's choice.

Defense obligations

(when the legal costs are triggered, and their restrictions)

When the defense is triggered. Ideally in your favour it will be triggered with little to no restrictions, in cases where legal counsel needs to handle the investigation or some type of government action – regulatory authority, fines, or even conversations with opposing counsels or authorities leading up to a lawsuit.

If the defense obligation is restricted by lawsuit or written demand, your insurers defense would only be triggered once either of those occur.

The insurer covers the entire claim.

In most cases even if it's only partially claimed under the policy.

If the duty to defend is triggered even partially, the coverage remains as long as the allegations that are covered remain open– and are not resolved, settled, or judged on or dismissed. Also, if the covered parties of an allegation remain defendants, the insurer should continue with their duty to defend. If the covered parties are dismissed their duty to defend could end.

True up on defense costs - A contract may include a true up if the policy provision does not state that 100% of the defense cost will be covered. The wording of true up depends on the policy wording and should be reviewed by legal counsel but the concept is the insurer may retain the right to "true up" on defense costs and allocate between covered and uncovered matters.

Coverage may be subject to reasonable and necessary defense costs, but if the insurer chooses their own legal counsel, it can simplify the billing practices and auditing.

Client attorney privilege with duty to defend can be guided dependent on local jurisdiction, because of this it is advised to speak with legal counsel about your jurisdiction and tripartite or dual client status to retain privilege through the insurers counsel choice. Coverage could be based on a case-by-case basis and jurisdiction.

You would want to consider the following:

- Direct conflict of interest between the insurer and insured could result in the right to obtain independent counsel.
- Insurer pushes to settle a claim that the insured might not want to settle. This is dependant on the consent defined in the policy or it may include a clause that any settlement must be consented on by the company or vice versa.

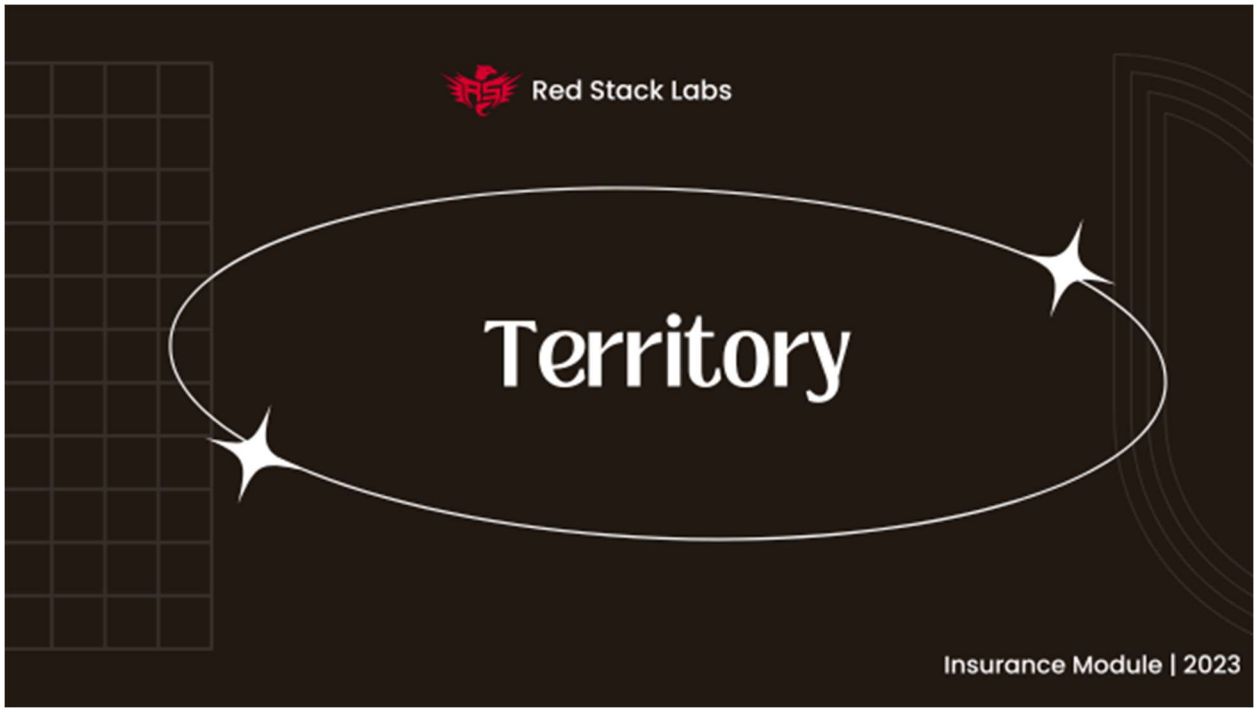
Duty to Reimburse

The duty to reimburse is an obligation that the insurer will cover the legal fees with the company's choice of legal defense. Considerations include:

- Law firm must follow insurance companies billing practices.
- This could be a lengthier process to receive reimbursement. They may choose to conduct an audit or adjust invoicing according to their guidelines.
- If your policy states duty to reimburse ensure your choice of legal counsel has validated all the requirements with your insurer properly to ensure a seamless process of reimbursement.
- There are scenarios where the law firm may be requested to reduce their invoicing to "reasonable and necessary" or they may ask the company to cover the excess – beyond the insurers recognized billing practices.
- This can become complicated in cases with covered and uncovered parties. The defense cost may be allocated from the beginning of the claim by the insurer.
- The upside in some cases is the pliancy is worth the additional billing challenges, this could be especially important in conflict-of-interest cases with the insurer.

<u>Next Steps</u>

1. Review the type of coverage provided by your insurance.



Territory

Worldwide coverage without restrictions would be beneficial against losses or damages occurring anywhere, ideally if your policy covers lost or stolen property like laptops, iPhone, USB devices for employees abroad (conferences, meetings).

Local coverage could be limited to events occurring in specific locations like offices or branches of the company. The territory coverage could also restrict lost or stolen property to specific locations. The main thing to consider is: if the policy covers an event but it is done outside of the approved territory it could void the claim.

It is important to note that stolen property could lead to a full cyber incident of a business, it is not just the potential cost of replacing stolen hardware or devices, but the potential access that could be gained from those devices.

Questions on incidents

- Is coverage of theft limited just to the premise (branch, offices)?
- What about laptops, cellphones, tablets, USB drives, etc.?
- Theft of electronic data by non-electronic means? For instance, what if a password is stolen from a notebook on a desk “credential theft” by non electronic means?

Cancellable Policy

Non-cancellable

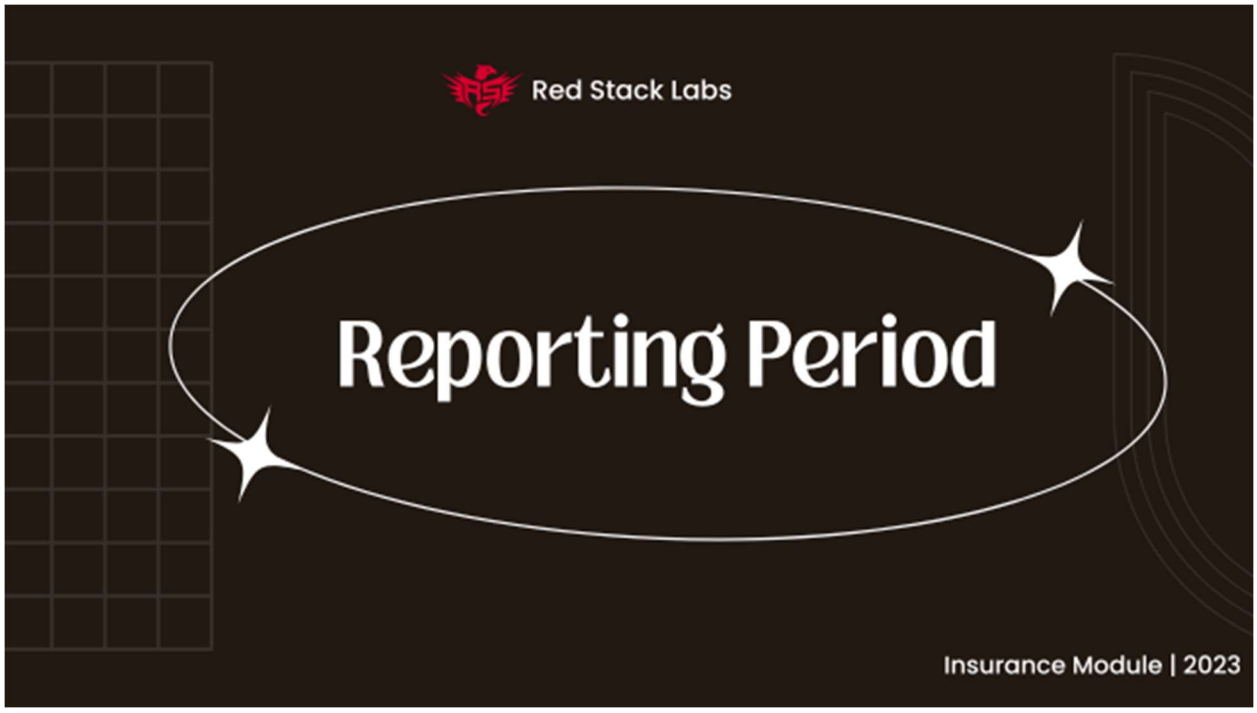
A non-cancellable policy cannot be cancelled by the insurer without consent of the company. This protects you from an insurer attempting to cancel your insurance policy for any reason, including during a claim or dispute. If you and the insurer are dealing with a claim and have a conflict of interest, they would be bound to the terms of the agreement. There might be a premium charge from the insurer for obtaining a non-cancellable insurance policy, and if that is the case it becomes subject to the requirements of your business and advice of your legal counsel. Ideally you won't want to be left high and dry without a cyber insurance policy.

Guaranteed renewable

A feature that guarantees the insurer will renew coverage if the premiums are paid on time. Under this class of underwriting the premiums can increase as long as the change effects all cyber insurance policy holders, not just your company. This option is different than the non-cancellable and normally you would choose one or the other if they are available from the insurer.

Rescindable

If a policy states it is rescindable, and the insurer exercises the right to rescission (the policy would define their obligations and exclusions of rescission) it would be as if the policy did not exist. In the case of this happening the insurer would be obliged to refund the premiums to the company, but the company would remain without coverage. It is recommended to ensure your policy is non-rescindable.



Reporting Period

The reporting period is when the coverage begins and ends allowing a claim to be submitted, it will be listed in the policy. This is the time frame when your company can make a claim.

Extended reporting period

If the policy is not cancelled for non-payment or fraud (or other reasons specified in the policy) a policy might provide an extended reporting period after the termination of coverage. The policy could also specific additional underwriting to provide a premiums quote and/or written notice if they decide to provide additional coverage or to explain the extended reporting period termination date. This section might also include specific text

around you obtaining a new insurer and excess coverage, and the aggregate limit during the extended reporting period.

Aggregate limits reinstatement

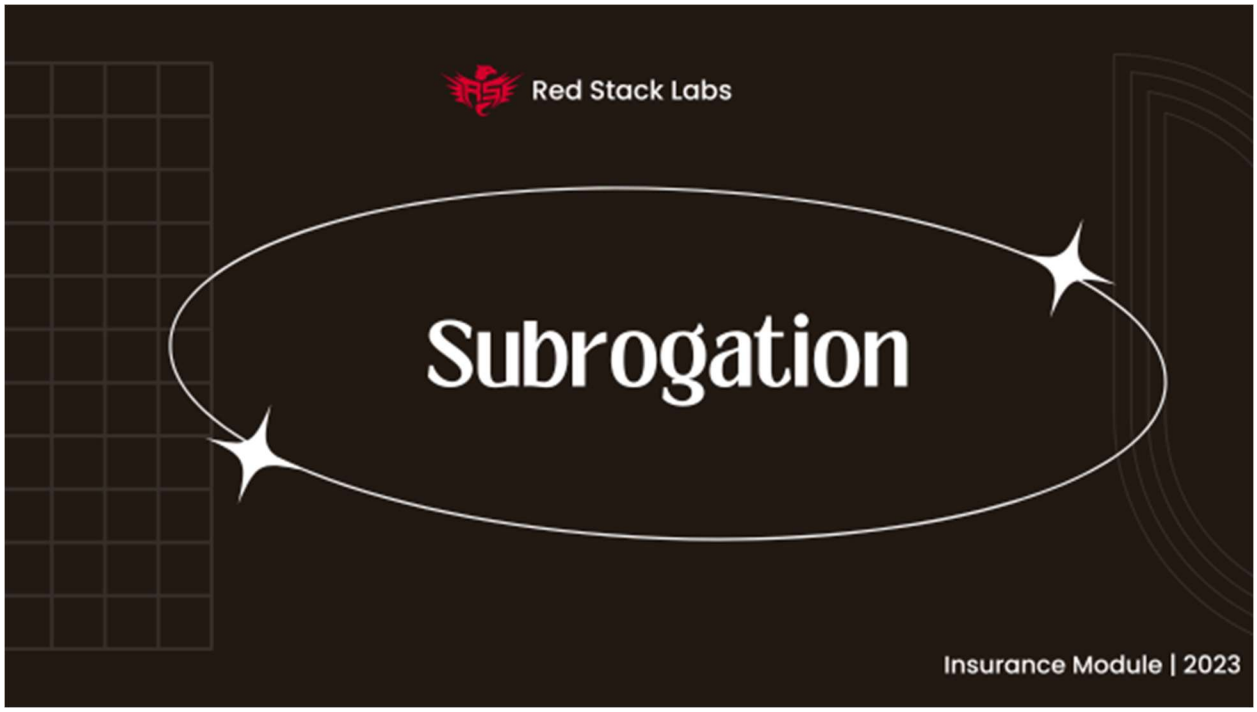
This clause can reinstate the maximum policy limit throughout an extended reporting period.

Retroactive date

The retroactive date is the first date the coverage begins, this could be negotiated to predate the policy effective date to obtain coverage from potential prior acts.

Prior Acts

It is possible certain insurers provide prior acts coverage (it may affect the premium) to obtain coverage for acts taken place prior to the policy being purchased. With prior acts coverage the insurer would allow claims to be covered under the new policy. This is usually tied retroactive date of the policy and defines the reason for needing one. This could be a rider (endorsement) for your policy.



Subrogation

Subrogation is when your insurance provider pays out a claim and seeks reimbursement from the third party who caused the incident. How this helps you is that if your insurance provider gets reimbursed on the claim, your premiums should not increase and you won't have a claim listed against your insurance policy, instead the at fault party will be liable and pay the reimbursement cost.

Waiver of Subrogation

This is an endorsement you would enter a contract with a third party to waive the right to subrogation, usually on their request you would provide this. What this means is if the third party is at fault for a breach in your network that causes damages, your insurer pays your claim, and does not have the right to go after the third party to be reimbursed for the losses. Essentially making it your claim and increasing your premiums when the third-party's insurance should be covering the claim and reimbursing your insurer.

Additional Insured

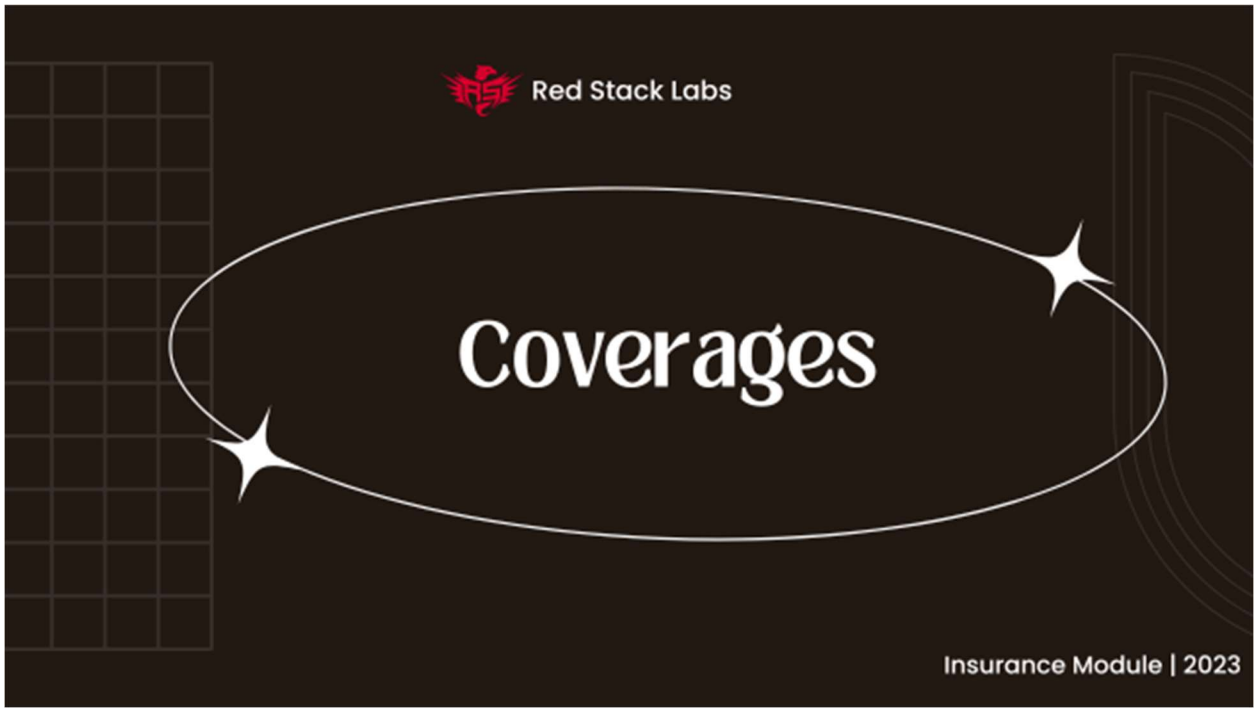
This endorsement is adding a third-party business to your policy directly under your coverage, doing this in most cases will provide protection from subrogation from the insurer if the cause of loss is within the scope of the policy contract. There have been cases

where the insurer recovers losses from a third party even when an Additional Insured in a policy because the cause of damage or loss is outside the scope of the policy.

Sample scenario

Alpha Tech Team (ATT) is a cyber security firm hired by your company to assess the security of your infrastructure. Your IT team provides them user credentials to login, one of the ATT staff members computers gets hacked or stolen, the credentials end up in the hands of an adversary, and that adversary uses the credentials to enter your network and deploy ransomware, encrypting all your data and locking up your machines. The ATT firm did not report this to you in time, you did not change their credentials, and ultimately, they would be at fault (In our quick scenario claim). You go through your incident response checklist, one of the key points is to contact your insurer and make a claim. After the incident is over, the cyber investigation firm you had on retainer provided evidence it was the user credential of the ATT staff member that caused the initial foothold into your network. Your lawyer checks the contract with ATT and discovers a waiver of subrogation endorsement. You and your insurer are stuck with the claim, and ATT gets to walk away from it paying low premiums to their insurer.

Policy Coverage



Coverages

Your company needs to decide what type of coverage is best suited for your industry and based on your risk profile. Ultimately if your insurer's policy is not properly covering your company it might be time to look for a new one that does. This section highlights what each of these items are and how they could affect your company.

Because there are so many items in this section, we want to convey that you may or may not need or want all these things covered, because of this we used the policy coverage section to explain what each one of these, but the financial exposure of each one and how they could affect your company are completely dependent on your business.

Note: if it's not listed in the coverage section of the policy it's not covered, there are no assumptions. Additionally, just because something is listed in the coverage section does not mean it is completely covered; there may be cases where an exclusion clause could carve a piece of the coverage back out of the policy. Knowing which of the following items are covered is important.

Bring Your Own Device (BYOD)

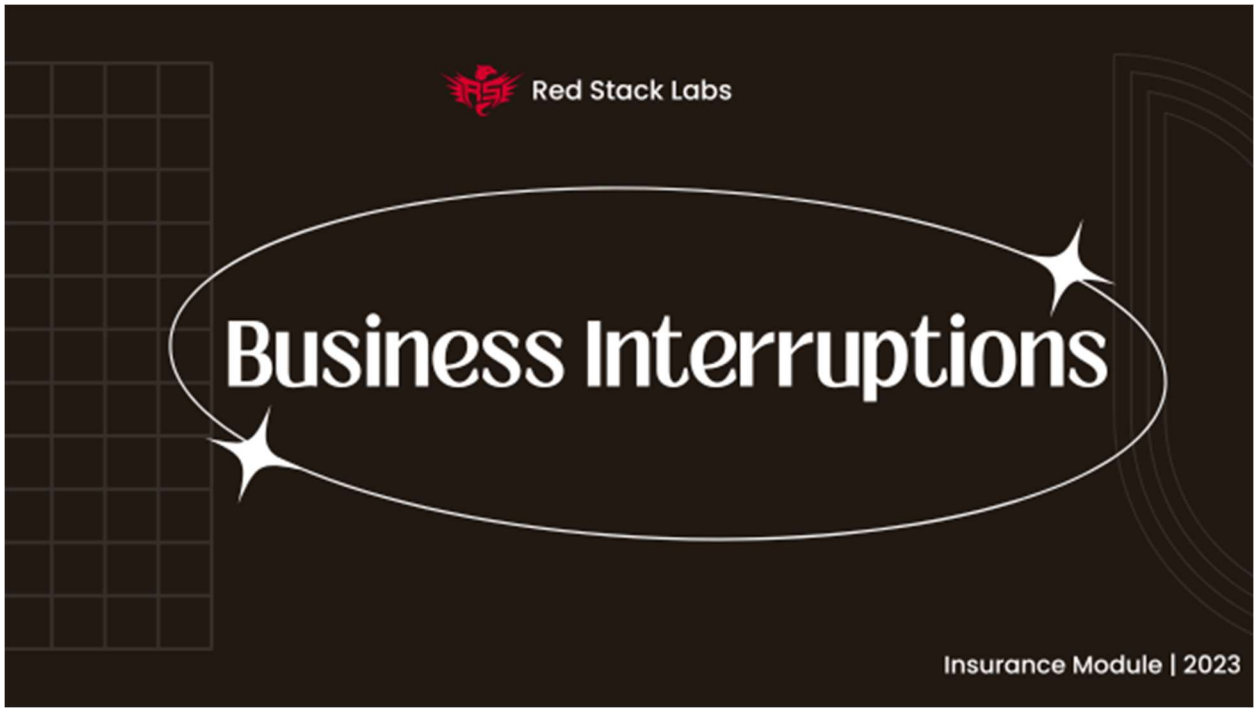
Personal devices used at the company may not be covered by the cyber insurance policy. Certain insurers do not cover personal devices even if they are damaged during a cyber incident that covers the organization and its hardware replacement costs. Company issued devices used by remote workers may have certain restrictions to their coverage or exclusions, ensure you are aware of the remote worker coverage when purchasing your cyber insurance policy.

Personal devices can also become infected through personal use, in most cases personal devices have less than acceptable security measures. If a personal device is infected and connects to your corporate network and spreads malware to corporate owned systems, is this type of cyber incident covered under your cyber insurance policy?

Note: These are two very important questions to discuss with your insurer if your employees bring in personal devices to work.

Next Steps

Review the Cyber Insurance Questionnaire at the end of this section to determine what could be in your policy coverage or what might be left out.



Business Interruptions

Business interruption (BI) claims can be large, statistically on average they are the biggest loss for most businesses going through a cyber incident.

Imagine what your financial exposure would be if your business stopped operating completely for two to four weeks, after the initial 7 to 12 days only segregated pieces of business functionality came back online, taking nearly a month for a full recovery.

The reality is Business Interruption is one of the biggest concerns for any company facing a cyber incident and imminent shutdown, loss of data, regulatory authorities, even adjusting expectations with partnerships or clients can all be explained and dealt with, but not being able to function as a business makes doing that incredibly difficult to manage.

While a loss mitigation strategy is important, equally important is the coverage of a cyber insurance policy during a cyber incident. Knowing how your policy will cover your business is key to working through an incident.

Interruptions that may affect your business

The following are parts of your business that may be impacted. This isn't an exhaustive list, rather shows what should be considered.

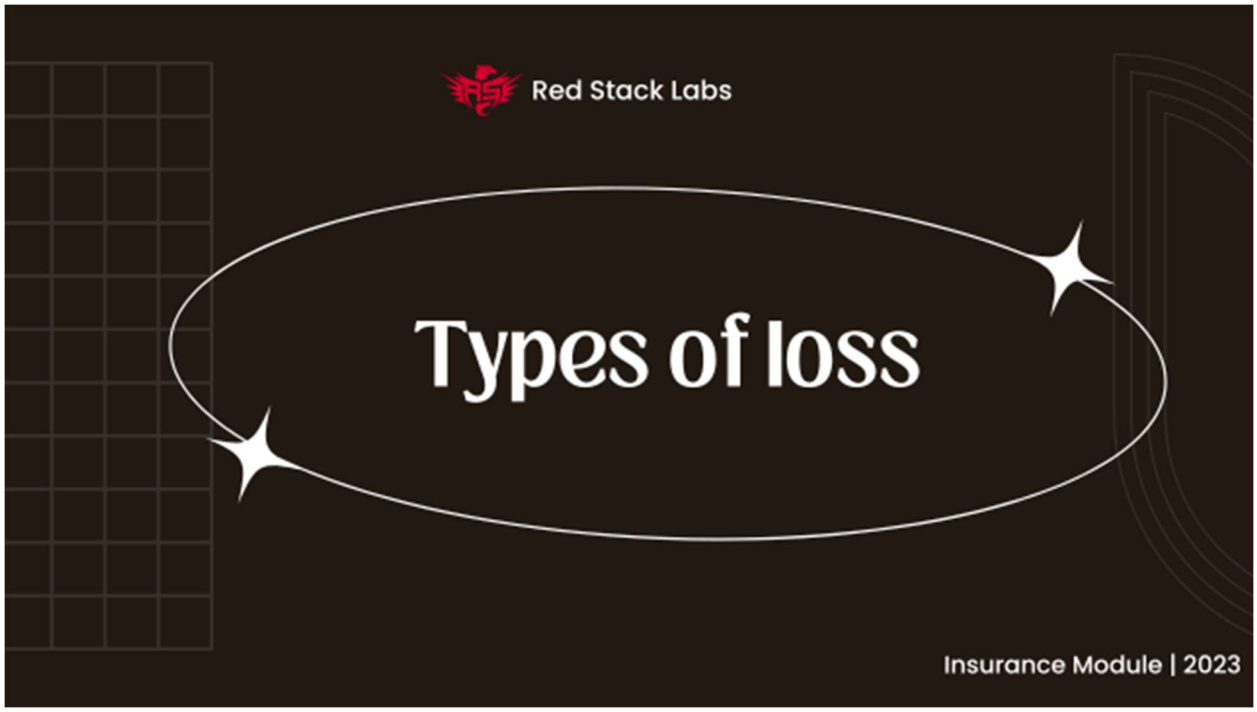
- Business operation at multiple locations, branches, or departments regardless of physical distance
- Procurement, logistics, & supply chains
- Sales disruptions
- Resource utilization when building a reactive strategy (like building an earthquake plan after the event occurred)
- Internal & external communication including email servers and office phones.
- Losing research & development IP
- Stock management
- Manufacturing / Development
    - Sufficient stock to withstand manufacturing setbacks.
    - Systems that manage stock or sales are they segregated to continue operations?

Market share & reputation damages

- Damaging relationships with strategic partners, clients, vendors
- Loss of potential investors
- Bearish stock prices, or negative news release for publicly traded companies

Next Steps

In the worksheet attached, highlight the exact areas of your business that would be impacted & potential financial impacts.



Types of Loss

Loss of Business

Loss of business could be potential income or revenue your business would otherwise have made, this may include future business that your sales team was working on, and in some cases when in talks to sell your company a cyber incident could either halt or end talks completely.

Dependent business interruption

When your income is dependant on a third-party business and a loss of income occurs because of an interruption to their service.

Cyber extortion and ransomware payments

This is an area that is changing based on frequency of incidents, regulations, and insurers trying to minimize cost. Some insurers cover extortion loss, however, others are beginning to exclude it because of that dramatic increase in cost, and the potential incoming government legislation change which could make paying ransomware illegal in the future.

Note: Depending on your primary region, this may be different. It's best to review with a lawyer the changing landscape.

If the policy only covers cyber extortion but does not cover business interruption and recovery efforts, be aware that paying extortion fees may not completely recover your data. On multiple occasions a company has paid the ransomware only to find out the malware malfunctioned or was never programmed properly by the criminal group in the first place – losing their data forever.

If this is having a risk of to your business, plan to have proper backups.

Digital asset loss/replacement

This is when company data or software is destroyed or lost because of an incident. The coverage wording is important because this could either or both cyber incidents and network failures– scenarios where a failure occurs and could be covered that would not be deemed a criminal act.

System failure and dependent system failures

System failure could mean a Denial-of-Service attack (DoS or DDoS), an adversary compromising your systems or networks, but it could potentially cover an unintentional or unplanned outage on your network.

Fund Transfer Fraud (FTF)

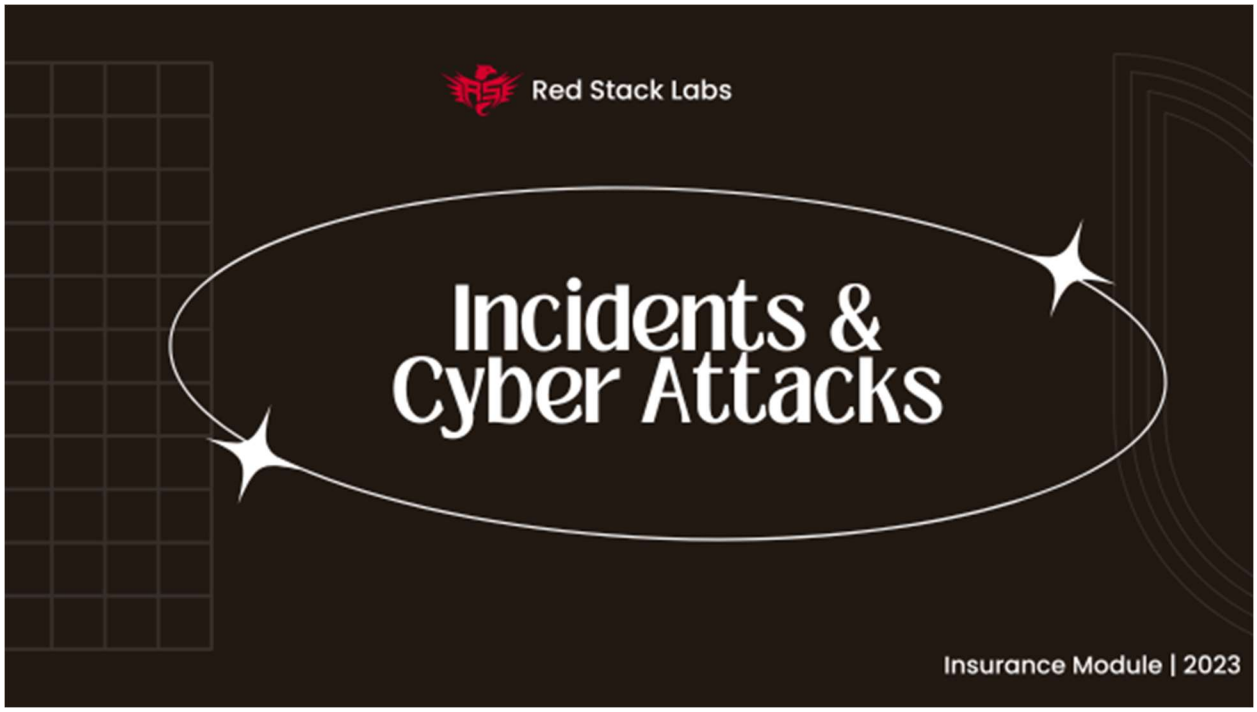
This could cover fraudulent funds transactions from your company to a criminal or adversary. The method of which could be specified in the policy, possibly covering only certain scenarios like through a cyber attack.

Social engineering FTF has seen to be carved out from some insurers policies, not covering scenarios where your employees are tricked into sending the funds to an adversary, an example of a social engineering attack would be Business Email Compromise (BEC) where an adversary uses a spoofed email or a vendor email account to send an invoice to be paid to their own mailing address or a “new account”.

These attacks are common and some training to your staff that handles funds transactions could help limit the possibility of losing funds to a social engineering attack.

There are multiple ways this could be covered by your policy, legal fees, reimbursement, settlements, etc. It would depend on the wording of your policy:

1. When the funds are fraudulently transferred out of your account, your company is the target.
2. When your company is compromised and used to obtain funds from a third party – sending an email requesting a specific invoice is paid to the adversary directly. This could result in a legal battle between your company and the third-party business.



Incidents & Cyber Attacks

Cyber attacks have many categories that you need to become aware of when interpreting an insurance policy and what it covers. Some insurers cover business email compromise (BEC) but not social engineering attacks, or they cover malware and ransomware but not phishing. Some insurers provide some of these types of cyber attacks as additional coverage or optional, while others provide a blanket across almost all these cyber attacks. When choosing an insurer, it is best to find one with broad definitions of cyber attacks, like "unauthorized access to private information", "unauthorized access to a computer system operated by the organization or third-party service provider". If the insurer delves into specifics about cyber attacks, it is important to understand what is being carved out of your coverage.

Below are some popular examples of cyber attacks a business could face.

Phishing

Phishing abuses trust through communication disguised as legitimate or originating from a reputable source. These attacks can impersonate a business or a person to obtain something from one of your employees, like user credentials, sensitive information, initiating fund transfer fraud, or even to convince the employee to download and run a file which could be a backdoor remote access tool (RAT), a command and control (C2) agent or malware to infect their system. Because phishing has so many applications and it is primarily based on human-to-human interaction and trust and not so much based on computer science for defence, this category of attack prevention falls under staff training. In our experience anybody can fall for a good phishing attack, coverage for phishing is highly recommended if it is available from your insurer.

Phishing attacks can be done through the following communication channels:

- Email
- Social media sites such as Facebook messenger, LinkedIn messenger, & Twitter chats
- SMS/Text
- Messaging apps and services including WhatsApp, Signal, Telegram

Business email compromise

Business email compromise (BEC) abuses the fact that people trust their email to conduct legitimate business. The scam involves an adversary sending an email that appears to be from a trusted source and asking for legitimate business transaction(s). For instance, asking to pay an invoice from a trusted vendor to a new bank account or mailing address.

BEC doesn't always come from the legitimate domain, they can also be sent from a spoofed email, or an email address that looks like the real domain.

Can you easily tell the difference between **doaboarid.com** and **daoboarid.com**? Notice the 'doa and dao' is different, and during a busy work week it can be easily missed – and is because this is one of the most effective cyber crimes to date.

Ransomware

The loss of business interruption and recovery costs would still fall onto the business without proper policy coverage. The following scenarios should be considered when reviewing coverage for ransomware.

1. **Files are encrypted**- Requires an extortion payment to the ransomware group in to receive a decryption key to decrypt the data and gain access.
2. **Double Encrypting**- Data is double encrypted, paying the ransomware decrypts once, files still encrypted and require a second payment.
3. **Double Dipping**- Data is exfiltrated as well as encrypted, the payment is a promise not to leak the files.
4. **Triple Extortion**- Double dipping the client then reaching out to their clients who could be affected by data dumps and extorting them directly as well.

System Failures

Systems can fail either because of interruptions to service or outages, not just cyber attacks. When reviewing the system failure coverage look for the definition of first party or third-party system failure coverage. If it is first party it will only cover systems your organizations run, owns and manages. It may not cover a third-party service like a managed service provider or cloud hosting like Azure, AWS, or GCP.

For first party system failure coverage, ensure whatever devices your business owns are covered in your policy, for example:

- Servers, desktops, laptops, workstations, mobile devices, tablets
- Networking and security network devices (Routers, Switches, Firewalls, IPS, UTM), storage equipment (SAN, NAS)
- Software

Data loss & data theft

It is possible to find partial data loss and data theft coverage in a cyber insurance policy, but your business may require data breach insurance specifically for the types of data your company holds, we recommend legal counsel if you are unsure which you need to properly cover your business type.

What your cyber insurance policy may cover is data recovery and data recreation costs, for example when ransomware encrypts the data on all your systems, your cyber insurance

policy may cover the costs to recover or recreate all that data to make your business operational again.

Because sensitive data loss or exfiltration and leaking can result in lawsuits or settlements between parties, we recommend reviewing the data breach coverage with your legal counsel and ensuring you are properly covered for the type of business your company conducts.

Penetration Testing

There could be mishaps during a penetration test with an engaged cyber security firm. If your insurer does not provide adequate coverage for these types of engagements, you will want to ensure your contracts with these cyber security firms will cover you in case their penetration testers accidentally allow an adversary into your network.

During a penetration test, the tester (ethical hacker from a cyber security firm you hire) can use backdoor agents (RAT, C2) that simulates malware and allows the tester to gain access to your systems. This is quite common in penetration testing engagements, but not all frameworks and tools are built with the same security that the testers use. If an adversary is snooping around on your network at the same time and finds an insecure agent with open access, they could be used to access your network through the backdoor the penetration tester setup to test the security of your infrastructure or devices.

Does your insurer provide coverage for these scenarios? If you are not at the phase of hiring penetration testers for your business, disregard this section for the time being.

Telecommunications Theft

Telecommunications theft is when an adversary compromises a phone system and uses it to make unauthorized phone calls that leave your company with the bill. Instances of this include.

Provider Fraud

This is when the adversary infiltrates the telephone provider itself, abusing the providers systems to either compromise your phone systems or use your company's phone service in some way resulting in billing ending up with your company.

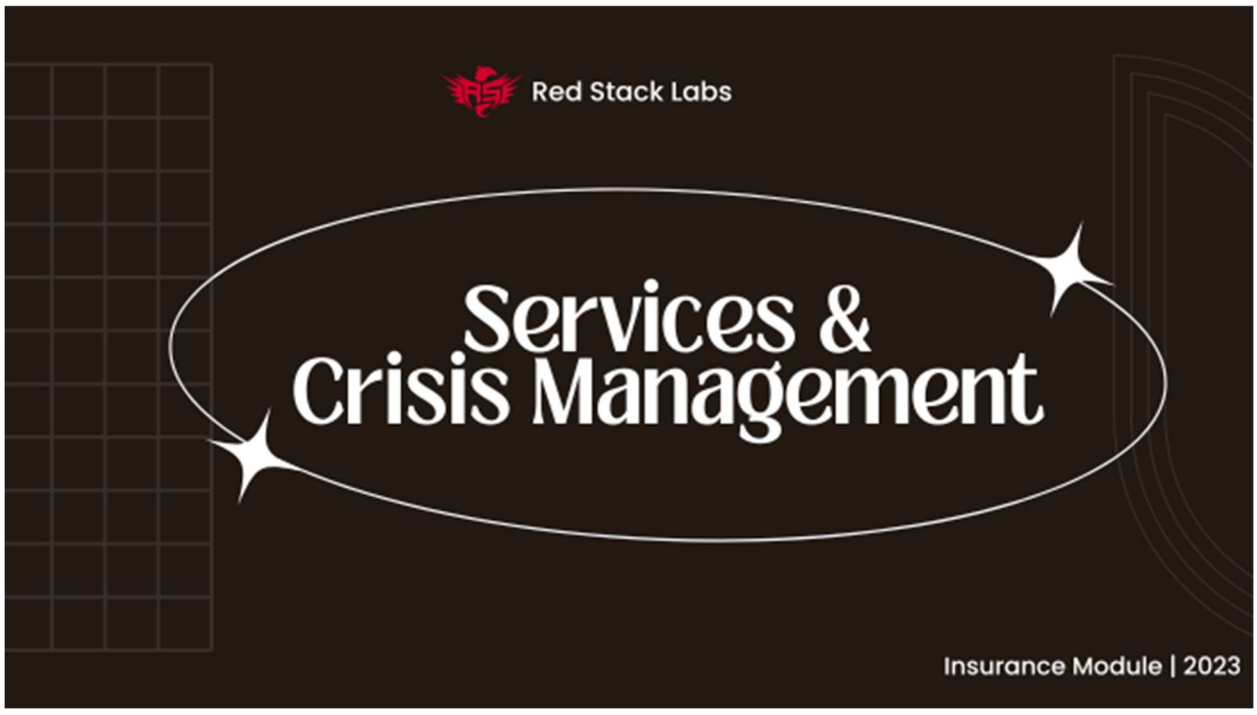
Customer Frauds

This is when the adversary compromises your phone systems directly, a few examples are.

- Using social engineering to obtain SIM cards for your corporate phone numbers (to abuse things like multi-factor authentication)
- Hacking voicemails
- Making unauthorized calls from your VOIP systems

Next Steps

Review the types of attacks above and what's your plan of mitigation today. For instance, you may have cloud services in multiple regions with redundancy as such System Failure maybe a lower priority.



Services & Crisis Management

There are considerations to make when choosing trusted service providers during an incident. Statistically the panel providers chosen by an insurer tend to do a better job and at a better price compared to service providers chosen by the company.

Disclaimer: The only caveat we will add there is we recommend you always have your own independent legal counsel throughout the entire program and during an incident.

Cyber Insurance will cover certain service providers dependant on the policy coverage, the following are a few examples of what you will need throughout an incident.

Legal counsel

Legal counsel is recommended to help reduce your liability and financial exposure when facing an incident, part of that legal work falls into fines, penalties, settlements, damages, disputes, but also reviewing the cyber insurance policy. Ensuring your cyber policy covers the specific needs of your business will ensure the cost won't fall to your business. Legal counsel will help guide you through the policy contract, while Cover Your Back program helps inform you of the realities of cyber insurance and caveats when interacting with insurers.

While independent legal counsel might seem like an additional cost, especially if the insurer providers legal counsel as one of their panel vendors, the client privilege and advisory before making a claim could be very valuable. We always recommend the first vendor you call when facing an incident is your legal counsel, to discuss the situation.

Areas of discussion should include, but not limited to:

- How to make the claim with the insurer
- How to deal with police
- How to deal with the criminal groups
- How to limit liability (financial exposure, brand reputation) with regulatory authorities and customers data

A good legal counsel would be on retainer to ensure they can provide you the service when you need it during an emergency.

Cyber security forensic investigators

A good cyber security forensic investigator can be hard to find, the big firms are expensive, and the smaller ones may not be a trusted service provider. We recommend going with one of your insurers forensic investigators because they are a proven and trusted entity, as they are usually kept on retainer with the insurer for you. If your insurer does not provide their own cyber security forensics investigator you will want to have one available to you either through previous working relations or on a retainer, because cyber incidents are emergency scenarios, and in our experience hitting on a late Thursday or Friday right before the weekend, making it difficult to source vendors.

It helps to know the acceptable conduct of dealing with a forensic investigator and the insurers policy, because the insurer will want to know the initial foothold, and cyber attribution, this is vital information for policy coverage especially with war or cyber terrorism exclusions and detailed cyber attack scenarios that may or may not be covered.

Considerations

It is possible the investigation could delay recovery efforts; it is important to ask the insurer questions like:

- If they are unavailable to start immediately, can we use a different provider?
- If they take a long time to provide results, when can we begin recovery efforts?
- If they are unable to identify the initial foothold or cyber attribution what happens (will the claim be covered with insufficient evidence or attribution)?

Crisis management and public relations

A cyber incident can be damaging to your company, not just financially but to the reputation itself through mishandling the incident and the communication to the necessary parties. Crisis management coverage can be a standalone policy providing coverage to a broader range of reputation damage, but some cyber insurance policies will include a subset of reputational and brand correction coverages. Some insurers under a cyber insurance policy will cover the cost of a public relations firm to help correct the reputation or brand of your company, how to properly handle notifications and documents such as privacy notifications to your clients, the policy might cover specific scenarios like a cyber attack that leads to a data breach.

If your company requires complete reputation coverage, we recommend looking into crisis management coverage policies beyond the scope of the cyber insurance coverage.

Credit and identity monitoring costs

Credit monitoring and identity monitor may be covered under your policy. Check your insurance policy but the coverage might be triggered after an incident and claim, and it could have a specific range of time for that coverage.

Business identity monitoring & identity restoration

If your company is concerned about business identity theft, you may require a separate policy focused on business identity theft. A few examples of business identity theft are:

- Obtaining fraudulent lines of credit

- Filing fraudulent tax returns for the refunds
- Hijacking your company trademark and hold it for ransom.

Call centre costs

The insurer could cover the cost of a call centre to handle phone communications for your business during an incident, they can relay messages and information to your customers or clients while your company focuses on dealing with the incident. This ensures that the communication channels are kept open, providing feedback to your customers and continual updates and frees up your staff's time, and mind of the stresses of dealing with clients directly during these incidents.

When you deal with a cyber incident that turns into a severity 1 (SEV-1) event, the last thing you want to do is spend 8 hours a day on the phone with clients yourself, you have a business to recover for those clients and a call centre can be a big help. Check if your policy covers call centre costs.

IT Administration Restoration services

Your company might need additional IT support to recover your business back to full operations. If your full-time staff is not as familiar with recovery procedures and the technical requirements, you may want to include this in your cyber insurance policy.

Next Steps

Review your policy for the following:

1. Does your insurance include forensic investigators? If not, do you have adequate support in case of an incident?
2. Review your risk profile and understand your need for crisis management, call centre support, and/or monitoring services.
3. Run recovery drills with your team and determine maturity, should you need additional support review your coverage.

Financial Coverage

A cyber incident can place unexpected stress on your business finances, your loans, payments, and accounting. Statistically it takes most businesses 23 days to recover from a ransomware attack, we recommend you crunch the numbers of what that would look like to your company from a financial perspective, and try to include any additional costs that may be incurred from the incident, this document and the list of coverages is a good place to start to realize how much it will cost, and what is needed to get a business operational again.

Then there are additional costs, like regulatory authority fines and penalties, but also legal costs like litigation, settlements, damages, and proceedings. From a financial exposure perspective, we recommend you obtain the right coverage from a cyber insurance policy that is in your favour because it can help shield your company from a lot of these additional costs and reimburse you for certain things. That is why getting the right cyber insurance is crucial because they are not all built the same. From there, it is up to your company to meet the requirements to retain that coverage and to pay the premiums on time.

Fines & Penalties

Regulatory Authorities

A cyber insurance policy should cover fines and penalties for problems arising from regulatory authorities and post incident or after an audit. The regulatory authorities your company deals with would depend on the location of your clients and they type of sensitive data your company retains about them. Your company can work to avoid these fines by properly handling breach notifications and communications with the regulatory authority within their incident time frames and also to the companies' clients. A regulatory authority investigation could also add additional costs which could be covered by a good cyber insurance policy, consider the time and cost of your staff to deal with an audit.

Examples of regulatory authorities your company may need to be compliant with and abide by:

- General Data Protection Regulation (GDPR – The Official European data privacy law and regulation)
- Personal Information Protection and Electronic Documents Act - (PIPEDA – Canadas data privacy law and regulation)
- California Consumer Privacy Act - (CCPA – The state of California rights and consumer protection for their residents)

Compliances

Your company may be liable for compliances fines if an audit happens, or an incident occurs that triggers an investigation into your compliancy. A good example is PCI compliance for a company that handles credit cards, depending on the level of PCI compliance, if a company is discovered to not be properly compliant after an audit or investigation there could be a fine. If your company is PCI compliant you should consider compliance fines and penalties coverages for PCI.

Payments

Customers, vendors, or strategic partners could enter a dispute or legal discussions, and this could result in settlement or damages reimbursement. There have been cases where class action lawsuits have been won over a cyber incident from the affected third parties.

Accounting

During a cyber incident and recovery your company is still expected to pay its expenses, and without income your business needs to be prepared to continue paying its expenses until it fully recovers. Some of these items might be covered under business interruption coverage, we are including this example list to give you an idea of things your company continues to pay, you should draft a full list of business expenses that are expected during an incident, downtime, or business interruption.

These can include:

- Rent
- Employee wages and benefits
- Suppliers and vendors
- Insurance
- Marketing and Advertising
- Manufacturing
- Shipping Fees

Next Steps

Questions to review:

- Consider the regions your business operates in; do you have enough coverage from regulatory perspective via insurance?
- Which compliance standards apply to your business? Review the coverage in your policy.

Legal Coverage

Your company will want a cyber insurance policy that covers all legal costs throughout an incident or service interruption that results in a legal situation with a third party.

Lawsuit

Before your cyber incident occurs, the focus should be to reduce your liability and financial exposure, this can happen through a combination of proper wording in your contracts with third parties, ensuring your business handles sensitive data properly and deals with the privacy regulations properly. During an incident your business can reduce liability by dealing with the insurer's procedures, but also when dealing with regulatory authorities, strategic partners, and clients. There is a right approach to communicating a cyber incident and there are many wrong ways to dealing with it, but even if you do everything right, you could still end up in a lawsuit, the idea is to stack all of the chips on your side to prove accountability, responsibility and proper handling of an incident, and all regulatory, compliance, and legal requirements, and this is where legal counsel shines on your behalf.

Fighting the legal battle is great, but when the dust settles if there are damages or settlements, we recommend your insurer covers these costs for you, the caveat being your policy would have to cover what your company is sued for, it is important to ensure you have the broadest coverage available with the least exclusions.

Examples of legal coverage costs you may want in your cyber insurance policy:

- Litigation, settlements, damage, and disputes
- Invasion of privacy, libel, slander, defamation, product disparagement
- PII data theft
- IP, trademark, copyright infringement

Regulatory proceedings

If you mishandle privacy data as a business and are audited or investigated by a regulatory authority you may be fined or penalized, you will want to ensure your policy covers defence costs in addition to regulatory fines and penalties.

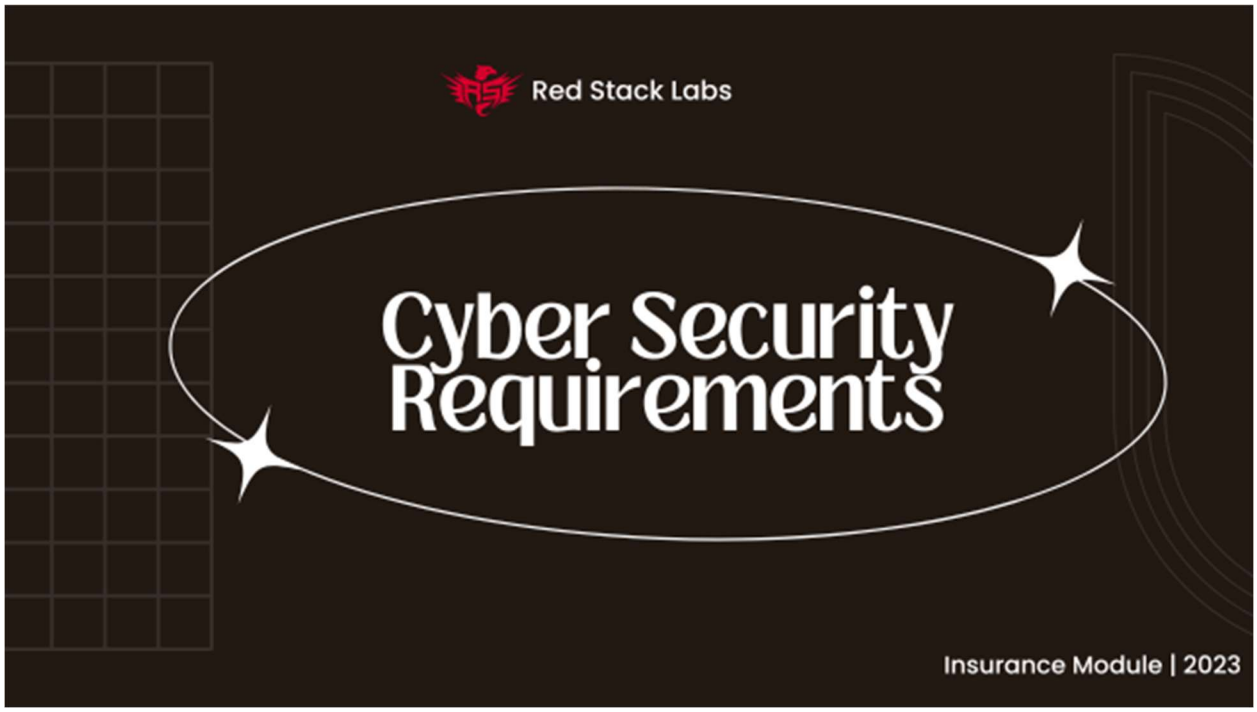
Electronic Media Liability Coverage

This would be optional and might be its own policy independent from your cyber insurance policy, but we add it in here in case your company would want this type of coverage. The legal defence costs and settlement costs for posting information electronically that could result in infringement, defamation, or a violation of rights to privacy.

Next Steps

Review the legal coverage in your policy noted above.

Policy Requirements



Cyber Security Requirements

You will want to read through the policy to understand the requirements, you could also ask the insurer to list them out if you do not have a copy of a policy (while shopping). You should have a strong grasp of the policy's contractual requirements to retain coverage during a claim.

Cyber Security

What cyber security requirements does your company need to implement and within what recommended time frame by the insurer do theses requirements need to be met? Do they need to be implemented prior to coverage being provided by the insurer, or will they provide coverage for claims during a security upgrade period?

IAM & MFA

Common asks of insurers is to implement certain Identity and Access Management (IAM) security controls, like Multi Factor Authentication (MFA), or least privileges, and they may even request periodic audits and tracking of all IAM users and controls.

AV & EDR

The insurer may ask to install an Anti Virus (AV) and/or an endpoint detection & response (EDR) solution like Carbon Black (CB) on all desktops, laptops and servers to record all security events which are logged to a cloud environment for you, where your IT, security personal or consultants can review events, fine tune and tighten controls, and manage the security events in the case of an incident investigation to identify the attribution.

Patch or Vulnerability Management

A patch or vulnerability management process may be requested, and specific vulnerability classes or scores might have to be patched to retain coverage. This process requires time from your IT staff or systems administrators to implement and follow through on a weekly basis.

Most ransomware attack vectors or initial entry into a network where over a public facing remote service or application. These internet facing servers were exploited by the threat actors using what are called 1-day exploits.

These are common exploits that have been patched by the operating system or software vendor and the patch is then reverse engineered by a threat actor to re-write the exploit based on the content of the patch that was released. Even though these exploits are called 1-day, most initial footholds using these exploits happen between 1-2 months later servers that remain unpatched.

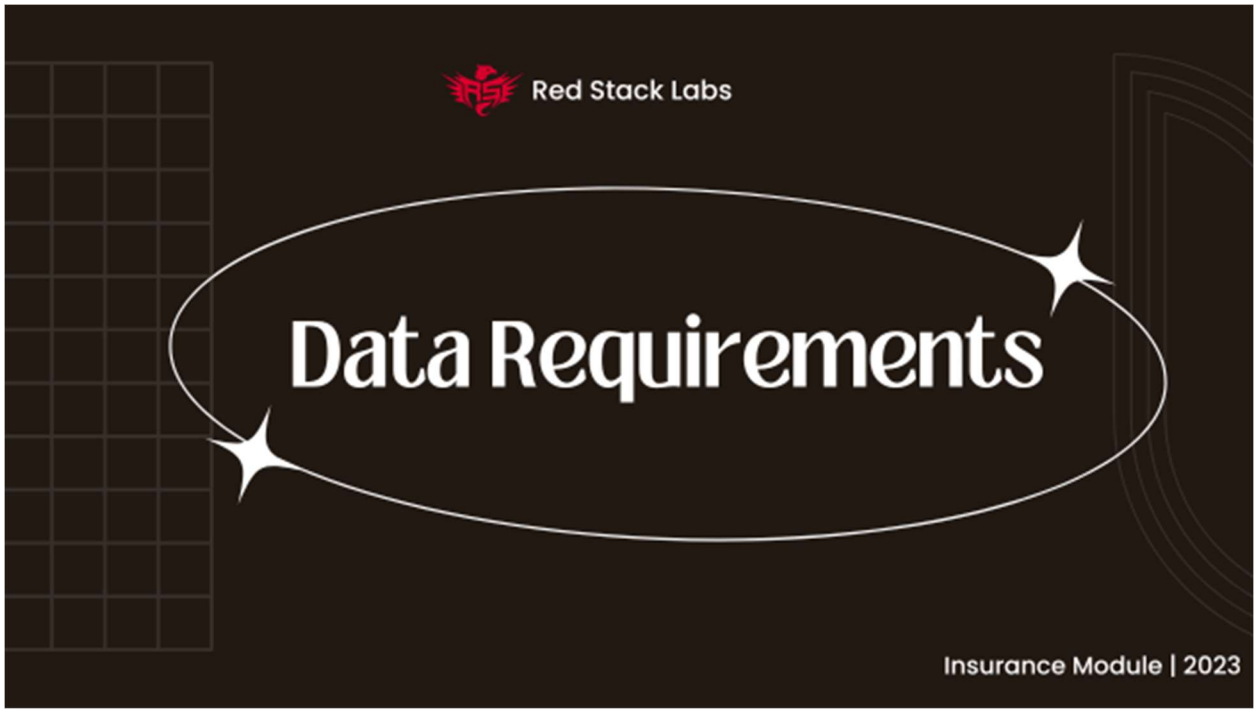
For some counter intel, phishing attack as an entry point for a ransomware attack were only 29% in 2020 and 26% in 2021.

Periodic Risk Assessment

An insurer may ask for a periodic risk assessment to be completed by a professional cyber security firm or a pre-approved internal security team. The insurer may ask for copies of the reports, or they may reserve the right to request a copy of a report throughout a specific time frame after a claim is made. This means the reports would have to be completed periodically and stored for future use, in a place that won't be affected by a ransomware encryption.

Staff Security Training

If an insurer asks your staff to obtain security training in a policy, we will argue it be defined well, as some courses are upwards of $10,000 per person. The policy definition should also very clearly state which providers are approved for training, the expected budget or cost, who covers the cost, and what information or courses they are expected to learn and do they require certification. Get all of this in writing if it is requested, do not make assumptions with security training requests.



Data Backups

For insurance this is important if you hold sensitive data or client's sensitive data. The insurer may request you retain complete backups of specific sensitive data or all company data. This is equally important for business continuity and recovery post-incident to minimize your business interruption and to recover quicker. Data recreation can take a long time, it is faster and cheaper to recover data from backup.

Data Breach

If your cyber insurance policy includes data privacy coverage, there could be requirements on data privacy standards that need to be followed. Your insurer may provide a separate insurance policy to cover data breaches, or it may cover a portion of data breach and data privacy under the cyber insurance policy. Ask your insurer for details on what is covered regarding a data breach with your cyber insurance policy.

Next Steps

1. Determine which privacy protections are applicable.
2. Determine security measures need to be followed to remain covered including best practices, international standards like ISO, NIST

Incident Requirements

Below is a list of questions to be asking when reviewing your insurance policy.

Acceptable Reporting Time

What is the acceptable time to contact insurer, lawyer, cyber security firm, regulatory authorities when an incident is discovered?

What if this is portion of the policy contract is broken, or late to contact regulatory authority and fined? What are the implications - does it effect the entire coverage of the claim? Does it effect just the fine from the regulatory authority? Does it have no effect at all – for instance is their leniency for working through the incident with a small team?

Evidence Preservation

What evidence is required to be preserved or obtained to make a valid claim with the insurer? Is it necessary to identify the initial foothold or entry point of compromise? And if the computer or event logs are lost during a cyber attack does it affect the claim?

Attribution

Who was responsible and what happened? Is it necessary to identify the cyber attribution for a claim?

Having the expectations of the insurer around attribution for a claim will validate what needs to be discovered during an incident investigation with the cyber investigation firm, this could help sign a proper contract with the investigation firm setting the expectations of their professional services up front and in writing.

How are threat actors categorized as working with a government or sponsored by? Is the definition based on the government, does that need to be defined by the government at the time of policy underwriting and endorsement date, during the incident itself or at the time the claim is made?

If the government does not define a threat actor as government sponsored can the insurer claim it is on their own? Does the insurer provide a list of government affiliated hacking groups that would fall under their exclusion list?

Premium Reductions

There are certain ways to reduce premiums like increasing deductible or lowering the aggregate limit but those are not always desirable to the company. Insurers sometimes offer a path to decreased premiums by implementing specific Cyber Security requirements and improving the company security model. Be sure to ask your insurer what your company can do to receive lower premiums.

Paying Extortion Demands

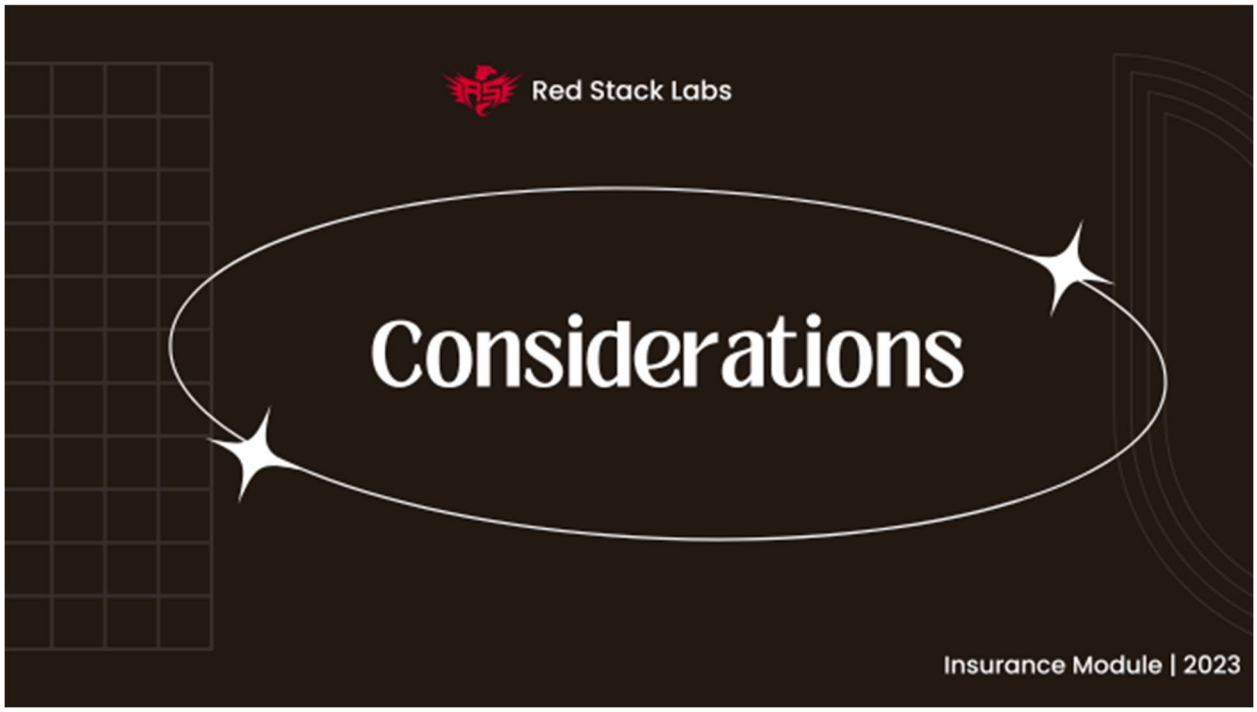
Extortion demand is in three sections, coverage, requirements, and exclusions because different policies can word their inclusion or exclusion differently dependant on the insurer.

If paying the ransomware is a requirement in your policy, what else is left out or excluded in its place such as business loss, damages and/or recovery costs? Does the insurer demand you pay or is it optional, and what if your company refuses to pay the extortion fee, could it trigger a loss of coverage event?

Next Steps

Download the provided checklist, review your insurance policy, and speak with insurer if necessary for clarifications.

Exclusion



Considerations

Non-panel vendors

Panel vendors are trusted vendors of the insurer, these are chosen because of the skill, efficiency, and alignment with the insurers billing practice. Your policy may include exclusions for non-panel vendors (legal, credit monitoring, public relations, and cyber security investigators) stating you must use trusted panel vendors. Some insurers allow pre-approved non-panel vendors to be added to your policy after undergoing an application process and receiving approval by the insurer. The non-panel vendors must be added and approved by the insurer prior to a claim or incident, in certain scenarios they may go through some form of screening or questioning by the insurer, and they would have to agree with the insurers billing practices and rates prior to approval.

War Exclusion or Hostile Act Exclusion

This section includes Cyber terrorism, act of war, or foreign state sponsored adversaries. This includes:

- Origin of cyber attack from Countries at war or Countries with sanctions

- Do sanctions need to be from the country of origin of the company, or any country the insurer operates in?
- Have the insurer clearly define the wording of these exclusions? Go over them with legal counsel to receive a clear picture of the exclusion holes in your coverage.

Prior acts that predate the retroactive date

This is the same as the prior acts listed in the policy term section, that policy term is an endorsement stating if prior acts would be covered. The prior acts wording could cover all prior acts before inception of the policy, it can be limited to a retroactive date, or it can be worded as an exclusion. For example an exclusion prior acts clause would look something like the following:

"THERE IS NO COVERAGE UNDER THIS ENDORSEMENT FOR CLAIMS ARISING OUT OF INCIDENTS, OCCURRENCES, OR ALLEGED WRONGFUL ACTS WHICH TAKE PLACE OR FIRST COMMENCE PRIOR TO THE RETROACTIVE DATE STATED IN THIS ENDORSEMENT. THIS ENDORSEMENT COVERS ONLY CLAIMS ACTUALLY MADE AGAINST THE INSURED WHILE THE COVERAGE REMAINS IN EFFECT. COVERAGE UNDER THIS ENDORSEMENT CEASES UPON TERMINATION OF COVERAGE, EXCEPT FOR THE AUTOMATIC EXTENDED REPORTING PERIOD, UNLESS YOU PURCHASE ADDITIONAL EXTENDED REPORTING PERIOD COVERAGE."

It is important to note that the words "prior act" is not mentioned in this specific exclusion clause, but the wording defines the contract all the same.

Future profits and future losses

Does the policy have a clause to cover future profits or future loss extending from this incident? If a future profit or future loss exclusion exists the wording needs to be very clear, ensuring it does not carve out the business interruption or recovery coverage.

Intellectual property

This might require a different insurance policy for coverage, cyber insurance may not cover theft of intellectual property properly or at all depending on the insurer and your policy. If your company has CGL insurance, between the two it may provide the coverage you need, in this case read through both policies and have your counsel review them on your behalf.

Improve or upgrade devices or software

During or after a cyber incident, it may be necessary to replace certain devices that could have been burned. Is there an exclusion that carves out the company's ability to purchase upgraded models of these devices? Devices including but not limited to servers, desktops, laptops, tablets, phones, software, operating systems.

Social engineering attacks

Social engineering is one of the attack vectors used to enter a company network, a popular attack being phishing. But other social attacks are impersonation to convince your staff to send money – this is more commonly referred to as Business Email Compromise (BEC). Another term you may affiliate to this is Fund Transfer Fraud (FTF) when funds are fraudulently transferred to the wrong party.

It needs to be very clear in the wording of the policy what is covered and what isn't (either by omission or exclusion) because Fund Transfer Fraud can both be categorized as a criminal attack activity or social engineering attack depending on the process. The cyber crime version of FTF is when a threat actor gains access to a company device and uses their access to this device to transfer themselves funds. The social engineering version of this attack is when a threat actor contacts your staff, either email or phone call.

Understand the policy coverage, omissions, and exclusion definition of social engineering because it is a vast topic with potential overlap with cyber attacks that may be covered. Some insurers provide social engineering coverage by default (at the time of writing this course - Chubb), other insurers carve certain parts of social engineering by adding it to exclusions.

Insider threats

Employees could be the threat to your business, without your company having proper security, policies, and audits in place you may never realize it. An employee could abuse privileged access or rights to launch an attack from within the organization. They can exfiltrate data and sell it or give it away, or even sell their credentials to a threat actor.

Failure to maintain

Minimum security requirements must be maintained, or an exclusion could carve out your coverage when dealing with a claim. This could be defined as a recommendation or

exclusion endorsement in your policy and not maintaining specific standards could affect coverage.

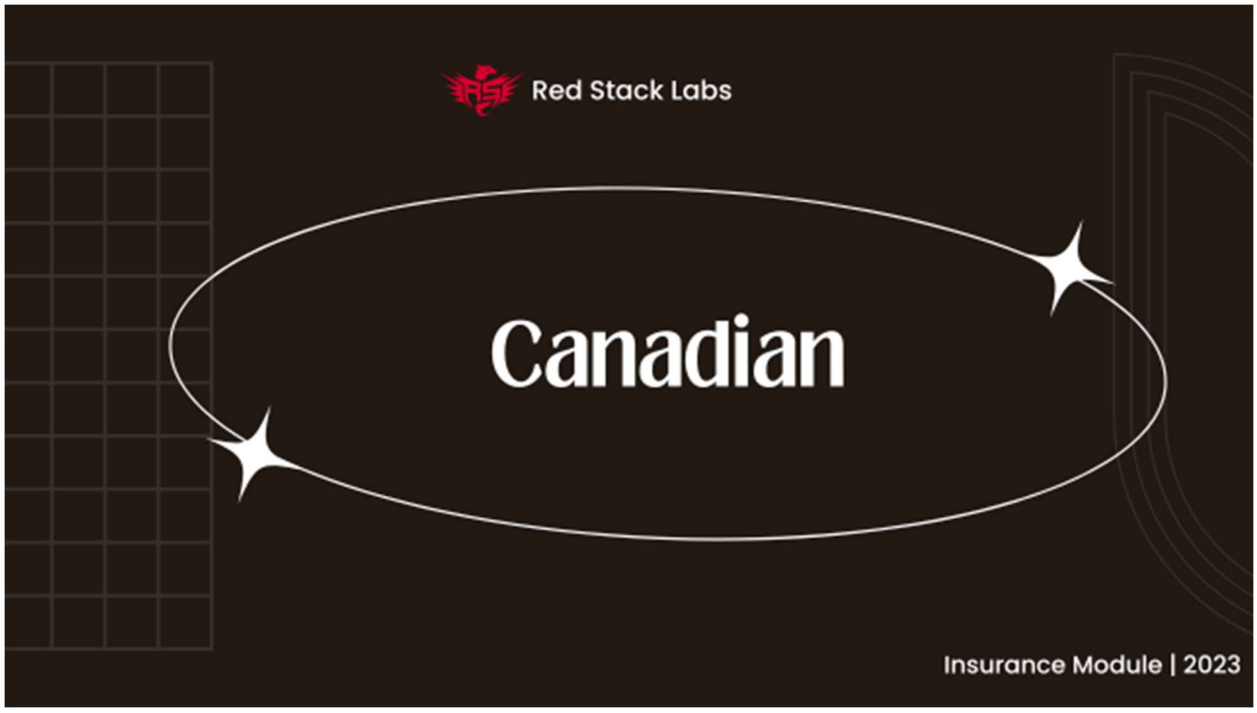
Standards

If your company is required to uphold specific standards or certifications beyond basic cyber security requirements from the insurer. For example: CIS, ISO, or NIST and it fails to do so, a “maintaining standards” exclusion could affect your policy coverage. These exclusions could also cover data privacy regulations like PIPEDA, GDPR, and CCPA which if not properly handled might void policy coverage. If there are no exclusions for maintaining standards it is possible the insurer has carved out support for fines to these regulatory authorities. Some of the larger insurers are still providing coverage for fines to data privacy regulation authorities, governments, etc. – if you expect you require the reimbursement or financial support for sensitive data make sure your policy covers it.

Examples of standards - PCI, ISO, NIST, HIPPA

Cyber Extortion

Some insurers cover extortion loss, and some are now beginning to exclude it because of that dramatic increase in cost, and the potential incoming government legislation change which could make paying ransomware illegal in the future.



Canadian

High Risk Suppliers

Recently Canada introduced Bill C-26, An Act Respecting Cyber Security (ARCS) which effects certain critical sector companies with mandates and fines. How this can affect your company if you are not in the critical sector is, Bill C-26 restricts Canadian companies from using products and services from high-risk suppliers, and this Bill introduced on June 14, 2022 could effect your policy or future policies.

We are not listing out the high risk suppliers list here because this list can change at any time, it can be obtained from https://canada.ca, and while this list is dynamic if it is mentioned in your cyber insurance policy, you need to make sure a list of high risk suppliers is also stated right on the policy along with the exclusion.

Course Completion!

Now that you've embarked on this voyage of understanding cyber insurance policy reviews, how will you leverage this fundamental knowledge to bolster your corporation's insurance?

Locate the "Cyber Insurance Questionnaire" included in the first chapter for your convenience. Feel free to download and utilize it, as it will help you delve deeper into your organization's current cyber insurance policy or support you in scrutinizing potential new ones.

Kudos on successfully completing the course, "Navigating Cyber Insurance: A Comprehensive Guide for Corporate Cyber Insurance." This marks a significant step in your journey to master the complex landscape of cyber insurance, and we trust it will serve as a valuable resource in managing your organization's cyber risks.