



Understanding Cyber Liability Insurance

More and more insurance firms are separating cybersecurity coverage from general liability insurance policies. Therefore, it's important to ensure you have coverage for a potential incident such as a ransomware attack, compromise of sensitive information, or funds transfer fraud.



Table of Contents

1 Executive Summary	3
2 Elements of Cyber Coverage	3
3 Surprising Benefits of Cyber Insurance	4
4 Responding to Cyber Insurance Questionnaires	4
5 Understanding Exclusions	5
6 Choosing a Carrier	6
7 Include Lawyers Proactively in Your Cyber Risk Management Strategy	6
8 If You Have an Incident	7
9 Ensuring Claims Don't Exceed Your Coverage	7

1 Executive Summary

More and more, insurance firms are separating cyber liability coverage from general liability insurance policies. Therefore, it's important to ensure you have coverage for a potential incident such as a ransomware attack, compromise of sensitive information, or funds transfer fraud. Even if you outsource your IT to a third party, which maintains coverage, it's important for you to have your own policy. Your outsourced IT provider's policy will only reimburse you if you can prove that an incident was the result of negligence on the part of the provider, while your own policy will protect you regardless of who was at fault.

2 Elements of Cyber Coverage

Any cyber insurance policy should include these seven key coverage elements:

- **Forensic Expenses:**

If you have determined that data has been compromised, this covers the expense of hiring an outside forensic team to investigate what happened, how it happened, and what information was accessed.

- **Legal Expenses:**

In the event of a breach, this covers the cost of legal assistance to determine whether any state or federal statute requires you to report the incident and to whom, and the cost of hiring legal counsel to defend you if someone files a lawsuit against you as a result of the breach.

- **Notification Expenses:**

If you are required to let individuals know that their data was compromised, this reimburses the cost of the related postage, paper, printing, call centers, etc.

- **Regulatory Fines and Penalties:**

This covers the potentially substantial fines and penalties a breach might incur from relevant state, federal, and foreign regulations, such as the General Data Protection Regulation (GDPR).

- **Credit Monitoring and ID Theft Repair:**

This covers the cost of offering consumers remedies to a compromise of their confidential information.

- **Public Relations Expenses:**

This covers the expenses of reporting the breach to the media and public so that you can restore your reputation and maintain your relationships with clients, vendors, business associates, partners, and patients.

- **Liability and Defense Costs:**

It's not uncommon for data breaches to lead to class action lawsuits. This coverage provides and pays for a legal team that is experienced in defending such cases.



There are 7 key coverage elements your cyber insurance policy should include: forensic, legal, notification and public relations expenses, regulatory fines and penalties, credit monitoring and ID theft repair and liability and defense costs.

3 Surprising Benefits of Cyber Insurance


These are some underpublicized benefits to carrying cyber coverage:

- **Insurance places a dollar value on your organization's cyber risk.**
This metric is useful when discussing security budgets with senior management. A nontechnical CFO may not be fully versed in how Denial of Service (DoS) mitigation services work, but they will understand the cost of your inability to serve customers due to a DoS attack.
- **The underwriting process can help you identify cybersecurity gaps and opportunities for improvement.**
In the same way property insurance has helped make buildings safer, cyber insurance can help improve cybersecurity practices and policies. During the underwriting process, your organization must be able to adequately describe and maintain its administrative, technical, and physical controls (i.e., its cyber hygiene profile). The insurer provides a third-party assessment of that profile and can then assist in identifying areas of improvement or adjustment that can help lower insurance costs.
- **Policies generally include risk mitigation tools and post-incident response assistance.**
This help can make all the difference in limiting damage and reducing the burden of regulatory noncompliance, especially for smaller organizations that lack the experience and staffing to respond to cybersecurity incidents. In both the EU and the U.S., regulatory scrutiny is high, and the penalties for noncompliance, such as the GDPR's fine of 4% of global turnover, could be too much for many small and midsize businesses to survive. That adds significantly to the value of carrying cyber insurance.

4 Responding to Cyber Insurance Questionnaires

When you request coverage, insurance carriers must ask you certain questions to assess your risk and price the policy accordingly. You will be asked about your industry, the number and type of records you maintain that might place you at risk (personal financial records, health records etc.), and the size of your business. Answer these as best you can.

You may also be asked to detail your cybersecurity practices. We advise our clients to answer these questions truthfully but conservatively. In general, if you're asked whether you have a certain type of protection, and you aren't sure whether you've implemented it or don't know the extent of it, you should indicate that protection is not in place. Insurance companies have been known to deny coverage if their investigation of an incident shows that claimed protections were not in place.



When completing cyber insurance questionnaires, answer as best you can. Insurance companies have been known to deny coverage if their investigation of an incident shows that claimed protections were not in place.

5 Understanding Exclusions

As you evaluate a cyber insurance policy, be mindful of these key exclusions:

- **Portable electronic device exclusion**

If the device leading to a cyber breach is portable, many policies could exclude coverage completely for any resulting loss. You can request the insurer to remove the exclusion from the policy. If the insurer refuses, you can request an exception to the exclusion to cover losses involving portable devices if the data is encrypted. However, given the proliferation of portable devices, it makes more sense to find a policy that does cover them.

- **Intentional acts exclusion**

A crime or fidelity policy generally covers first-party loss to the insured party, even when they cause that loss. A liability policy generally covers damages or losses the insured party causes to a third party. Most cyber insurance policies do not adequately provide for both first-party and third-party loss. For example, liability policies typically exclude coverage for damages or losses intentionally caused by an insured party. So, if one of your employees created a cyber breach accidentally, the resulting loss would be covered (either under a general liability or umbrella policy that does not exclude cyber perils or under a stand-alone cyber policy). However, if one of your employees created the exact same cyber breach intentionally, the presence of this inclusion would mean the resulting loss would not be covered.

Since IT experts agree that your own employees are among your biggest cyber risks, you need to be sure you're covered for intentional as well as accidental breaches. Request that exclusion for intentional acts applies only to your highest-ranking directors or officers. In addition, make sure that exclusion only applies after a finding of intentionality has been fully adjudicated on the merits in a court of law. If the claim is settled outside of court, insurers may deny coverage for the claimed intentional act.

- **Nation/state, terrorism, and cyber terrorism exclusions, and “Acts of God”**

You should be able to expect your cyber insurance to cover your losses for any breach, regardless of who caused it or why. If your policy excludes coverage for nation/state actions, terrorism, or “Acts of God,” it may fall short just when you need it most – for example, a state-sponsored attack that causes a power cut, or a tornado that damages your facility.

Limit Nation/State exclusions to those recognized by the U.S. Government or the United Nations. Limit exclusions for acts of terrorism or cyber terrorism to those recognized by the U.S. Government as such. Review “Acts of God” exclusions carefully and negotiate to limit exclusions as much as possible. Discuss and clarify with brokers/insurers whether certain elements of loss (i.e., actual damaged property, loss of use of network, extra costs associated with restoring network connectivity, etc.) would be better covered under a property policy instead of a cyber policy, and explicitly state where coverage applies.



A liability policy generally covers damages or losses the insured party causes to a third party. Most cyber insurance policies do not adequately provide for both first-party and third-party loss.

- **Negligent computer security exclusion**

Some policies exclude coverage if data is unencrypted or if the insured party has failed to appropriately install software updates or security patches.

Review policy terms to see if/when data is to be encrypted and what your responsibility is to install updates, apply security patches, or take other security measures to protect confidential information.

- **Third party breach**

Many standard cyber policies exclude coverage for data an organization has entrusted to a third-party vendor that is breached.

Institute and maintain thorough vendor network review requirements when you employ third parties to handle confidential, sensitive, or personally identifiable information.

Ensure all the third-party vendors with which you do business maintain cyber insurance policies of their own.

Review policy terms to see if/when data is to be encrypted and what your responsibility is to install updates, apply security patches, or take other security measures to protect confidential information.

6 Choosing a Carrier

Assuming you are working with a broker with the scale to have experience in all areas of insurance coverage, you should buy your cyber insurance policy along with your other coverage. This ensures that your policies do not have unexpected gaps between them. Do not buy your policy from a firm that only wants to sell a cyber-insurance policy or claims to specialize in this coverage. Recommendations on coverage limits vary wildly, so consult with your broker to determine what best meets your needs.

7 Include Lawyers Proactively in Your Cyber Risk Management Strategy

As mentioned above, nearly all policies provide legal coverage. Make a point of conferring with this legal team *before* you have an incident, because they know better than anyone else what they will need to defend you from liability if an incident occurs. Ask them what they recommend that you do and not do now to make it easier for them to defend you in the future, and incorporate their answers into your cyber risk management strategy.

8 If You Have an Incident

If you suspect an incident has occurred, notify your insurance carrier immediately of the potential liability. In protecting their own interests, they will work to protect yours as well: providing experts to investigate and help contain the breach and a legal team to help determine your potential reporting requirements and prepare a defense against any potential lawsuits. Your policy may require you to work with their cyber incident response specialists, but even if it doesn't, you should avail yourself of their expertise.

9 Ensuring Claims Don't Exceed Your Coverage

Contracts are often written to limit any claim of damages in the event that the client suffers some harm arising from the contracted services, but these contractual limitations do not apply if the person(s) harmed can prove that the provider was grossly negligent or engaged in willful misconduct in carrying out their obligations. To defend yourself against an attempt to claim damages beyond the limits allowed for in your contract, you must promise to take only the measures to protect yourself against a cyber-attack that you can actually carry out, and then you must do those things diligently. For example, if you claim that you encrypt all data on portable devices, you have effectively announced that you consider that important, so if it's subsequently discovered that you don't actually do so, it will be difficult for you to defend yourself.



Ready to learn more?
Get the latest news and IT tips from Xantrion.

Subscribe

XANTRION
CYBERSECURITY • IT SUPPORT

Xantrion
651 20th Street
Oakland, CA 94612
xantrion.com