Frequently Asked Questions

1. **I outsource my all my data storage to a third-party; do I still need cyber insurance?** Yes, you can outsource your data storage to the cloud or some sort of third-party hosting facility, but this does not outsource your liability. Your customers and employees have the expectation that you will keep their sensitive information private. They are not concerned (typically) with what you do on the backend to ensure that sensitive data's protection. What they are concerned with is it remaining private. Third-party cyber liability coverage can extend to cover not just your fault, but also the fault of your providers.

2. **I outsource my payment processing and don't store any of the card information of my clients; do I still need PCI (Payment Card Industry) coverage?** Yes, even if you outsource your payment processing to a third-party (as nearly all companies do), this does not outsource your exposure to PCI-DSS. PCI-DSS (Payment Card Industry Data Security Standards) is a proprietary information security standard for organizations that handle credit cards from the major card brands including Visa, MasterCard, American Express, Discover, and JCB. PCI-DSS exists to ensure the continued protection of credit card information, and levies fines and penalties when there is a failure to do so. There is a common misconception that because a point of sale device comes out of the box PCI compliant, that it means that a merchant is forever PCI compliant. This is a myth - PCI compliance is an ongoing process that must be continuously addressed, just as computer software needs to be periodically updated/patched. PCI compliance requirements vary by number of transactions and the value of those transactions. If you are taking credit cards for payment, you need PCI coverage.

3. **Can I purchase a higher limit?** Yes. The total cost of a breach is not defined until a breach takes place. Cyber is not like property insurance where you can insure to your maximum foreseeable loss. A cyber incident can be a small $5,000 extortion incident that comes with forensics costs. A cyber incident can also be a multi-million dollar breach that comes with public relations, forensics, notification, business interruption costs, and data restoration costs, as well as costs arising from a third-party lawsuit. You will not know until the time of a breach what the total cost is. For this reason, we recommend that you consider what is financially viable for your organization. We also have data breach calculator tools and benchmarking tools that can help you make a more educated limit purchasing decision.

4. **What do I do if I have a claim?** Always report a claim to the carrier as listed on your policy and also to your insurance broker. You should also have an incident response plan in place prior to an event. If you would like our Incident Response Plan Guide, please contact us.

5. **I have cyber in my business owners policy, so why should I consider a mono-line cyber policy?** Mono-line cyber insurance policies have much broader terms and conditions and are also more equipped to handle a data breach. Remediation is the most important part after an incident takes place. BOPs do not cover all the costs that can be incurred as the result of a cyber event. Furthermore, mono-line carriers deal with cyber coverage daily and it is their primary skill set.

6. **Does this policy offer worldwide coverage?** Yes, all our policies offer worldwide coverage. Some even offer "anywhere in the universe" coverage.

7. **If a rogue employee was the case of breach, is that coverable?** Nearly 50% of the incidents that we see are the result of an internal bad actor. A state of the art cyber insurance policy is designed to cover acts of rogue employees. The exception to this would be if the employee is within the C-Suite, as cyber insurance policies are not designed to cover intentional acts of senior executive officers.

8. **I don't have any sensitive information in electronic format, so do I still need this coverage?** Yes, you do. You have sensitive information in electronic format because you use email. Email compromise can be the source of ransomware, phishing scams, password resets, social engineering instances and many other types of attack. Even if you do not email and you have no sensitive information available online, you should still be aware that cyber insurance can cover paper files, as well as copyright and trademark disputes both on and offline. It can cover ransomware and bitcoin expenses in the event your critical infrastructure is locked up via a DDoS or crypto locker attack. Cyber insurance can also cover human error that leads to system outages. Cyber insurance extends way beyond just electronic content or protection of payment card information.

9. **What is the difference between first-party and third-party coverage?** First-party coverage deals with costs that come out of your pocket to minimize and mitigate the chances that you ever face some sort of third-party suit. First-party costs are what every business who has an incident will incur, and include things like business interruption expenses, extortion expenses, notification costs, call center costs, identity restoration, forensics costs and several others. Third-party coverage provides legal defense costs against those pursuing damages from the insured.

10. **Can social engineering scams be covered by cyber?** Yes, they can. Traditionally, social engineering coverage was covered only by a crime policy. In 2015, crime carriers slowly began to realize that they were covering a risk that they never intended to. Rather than expressively excluding social engineering incidents, crime carriers came out with their own social engineering endorsements so that coverage was either absolutely provided or absolutely not provided. Because of this, we have a slew of markets in the cyber marketplace who are willing to cover social engineering. There are still some cyber markets, though, which believe it is better fit remaining in the crime market. Coverage that's provided varies by underwriting company.

insuretrust

Making cyber simple. Really.