THE NATIONAL CYBERSECURITY SOCIETY

# Cyber Insurance FAQs

## DID YOU KNOW?

- ✓ What's a throw-in policy? That's where another insurance policy just adds in a provision for another coverage type – such as cyber, yet you're not fully covered.
- ✓ Policies don't cover employees who are negligent and click on links through phishing.
- ✓ Each policy is different – read the fine print.
- ✓ Cyber insurance is an important part of your cyber risk strategy, it should be considered as a backstop, not your first line of defense
- ✓ The twelve PCI-DSS standards are best practices for all businesses, not just merchants.

### 1. *If I have cybersecurity controls in place, can I receive a discount?*

- Most cyber insurance carriers take cybersecurity controls such as firewalls, antivirus, encryption, backups, etc. into account when determining the policy premium. However, there is not currently a discount model that is universally accepted across the cyber insurance industry.
- Cybersecurity controls play a bigger role in the cyber insurance process if your organization has experienced a cyber incident or data breach. If so, the cyber insurance carrier will need some information about improvements implemented post cyber event to minimize the likelihood of reoccurrence.
- Each cyber insurance carrier uses different methods for rating cyber insurance policies. Some cyber insurance carriers make certain coverage elements contingent upon specific cybersecurity controls or policies. For example, if you are interested in adding coverage for losses from Wire Funds Transfer fraud, some carriers will want to see evidence that you have a Wire Funds Transfer or Social Engineering policy in place.

### 2. *I heard cyber insurance has a lot of exclusions, is that true?*

Some cyber insurance policies will include exclusions that limit or restrict coverage to reduce the exposure to the cyber insurance carrier offering the policy. Some exclusions are common across the cyber insurance marketplace and others are unique to each cyber insurance carrier.

Some common exclusions to consider:

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.



## JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

# Cyber Insurance FAQs continued...

a. Contractually assumed liability. In most cases this is not terribly concerning, however if this exclusion is in a policy, Payment Card Industry Data Security Standard (PCI DSS) fines and penalties passed down to your organization by a 3rd party such as a payment processor will not be covered.
b. Defects in software and computer technology that gave rise to a cyber incident.
c. Data on mobile devices and laptops not in your care, custody or control.
d. Cyber incidents/breaches caused by 3rd party technology service providers and vendors.
e. Acts committed by unwitting employees. This type of language in an exclusion could limit the coverage of the policy if a loss is triggered whereby an employee is tricked into providing unauthorized access or information to a cybercriminal.
f. Acts committed by rogue employees.
g. Some policies will limit coverage to data on "Your Network." This will not typically show up as an exclusion, so pay close attention to the definition of "Your Network" in your cyber insurance policy. If coverage is limited to data on your network it may restrict coverage by excluding breaches involving data you entrust to 3rd parties, such as a cloud service provider.

### *3. I don't have any sensitive data; do I need cyber insurance?*

Even if your business is not responsible for large amounts of sensitive, confidential or personal information, a small data breach can still be costly. Data breach response expenses and defense costs for law suits, cyber incidents can cause a variety of other business impacts. Other costs that cyber insurance can help address include:

a. Reimbursement for lost income due to business interruption following a cyber incident.
b. Reimbursement for lost due to damage to your reputation following a cyber incident (i.e. lost customers).
c. Costs to contain, eradicate and restore your network following a cyber incident.
d. Expenses you incur to restore, recover or replace data following a cyber incident.
e. Losses from theft of money by a cybercriminal via unauthorized access to your systems or through the use of social engineering.
f. Ransomware and network extortion payments.
g. Losses resulting from data breaches or cyber incidents impacting your 3rd party service providers and cloud service providers.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

# Cyber Insurance FAQs continued...

## 4. What information is needed to get coverage?

While every cyber insurance carrier will require different information in order to provide a quote, most will ask for the following:

a. Your industry
b. Annual Revenue
c. Whether you process credit cards and if so, whether you are compliant with the Payment Card Industry Data Security Standard applicable for your merchant level.
d. What type of sensitive data your organization handles (Personally Identifiable Information (PII), Protected Health Information (PHI), non-public sensitive data as defined by a state, federal or international data privacy law, corporate confidential data).
e. Whether you process, store or manage PHI and whether you are required to be HIPAA compliant. If so, are you HIPAA compliant?
f. Estimated count of sensitive data records your organization is responsible for.
g. Whether you backup critical data and whether you have an incident response plan to help recover from cyber incidents.
h. Most cyber insurance applications will include questions about your network and information security controls (firewalls, antivirus, intrusion detection, patch management, encryption, corporate cybersecurity policies, etc.).
i. Affirmation whether you have any prior knowledge of any incidents that are ongoing or could happen that could cause a loss.

## 5. Is it expensive?

For the scope and amount of coverage being provided, cyber insurance is relatively inexpensive. See the company profiles under our cyber Insurance page for additional information about the estimated costs of a cyber insurance policy.

## 6. What does it cover?

Most cyber insurance policies offer coverage in the following areas:

a. Your liability to others
b. Your expenses to respond to a breach or incident

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

# Cyber Insurance FAQs continued...

c. Expenses incurred due to a business Interruption and extra expenses
d. Cybercrime

### *7. I have another policy that mentions some coverage for cyber loss/data breach, do I really need a stand-alone policy?*

While every business's exposures are different, most businesses that use data and technology to operate are not fully covered by "throw in" cyber insurance coverage included in a General Liability or Business Owners Policy. Cyber coverage included with one of these policies is significantly limited compared to a standalone cyber insurance policy. The other issue you may discover is the limits on coverages are typically very low and may not sufficiently cover the costs of a cyber related loss.

### *8. If I buy cyber insurance, does this mean I don't need to spend money on other cyber risk products and services?*

No, cyber insurance does not replace proactive cyber risk management and defenses. Cyber insurance helps protect your organization against the unforeseen, unexpected or catastrophic losses from a cybersecurity failure. Cyber insurance is an important part of your cyber risk management strategy, but it should be considered as a backstop, not your first line of defense.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.