THE NATIONAL CYBERSECURITY SOCIETY

CYBER INSURANCE

In 2016, Symantec reported almost half of cyber-attacks worldwide were against small businesses, and the FBI reported that more than 7000 U.S. companies of all sizes were victims of phishing email scams with losses of more than $740 million.[1]

Have you wondered if you were a victim, would you have the resources to cover the loss and whether cyber insurance will protect you?

One important fact to consider is that cyber insurance is not a replacement for cybersecurity. Cyber insurance is an element in your arsenal to protect against a breach, cyberattack, and/or ransomware. Cyber insurance often covers the cost to restore your business from an attack, pay legal fees, conduct breach notification, provide identity theft monitoring and cover regulatory fines and penalties. A good cyber insurance policy protects against these type of events, but each policy is unique and covers cyber risks differently. This tip sheet provides a list of provisions you should consider when selecting an insurance policy.

DID YOU KNOW?

- ✓ Nearly half of all cyber-attacks worldwide were against small businesses
- ✓ Cyber criminals are targeting small businesses because they are easy gain
- ✓ Not all cyber insurance is the same
- ✓ An insurance agent will meet with you, evaluate your business situation and suggest the best policy to meet your needs
- ✓ Use this “cheat sheet” to be prepared for your first meeting with your agent
- ✓ The NCSS has partnered with an insurance broker to ensure your organization is provided a policy to meet your specific needs
- ✓ Some policies are designed to “pay claims” others are set to “deny claims”

POLICY ELEMENTS THAT COVER YOUR LIABILITY TO OTHERS

1: CYBER INCIDENT

This element covers your organization’s legal fees to defend your organization in a civil lawsuit when your organization failed to prevent the spread of a cyber incident. Protects against your failure to protect the integrity of the data and services, as well as ensuring the data and services are available. For example, this element would cover when a malicious actor manipulates your data which ultimately causes harm to a client.

2: DATA BREACH

If your organization fails to protect disclosure of Personally Identifiable Information (PII), Protected Health Information (PHI), corporate confidential information, or other sensitive, non-public data, this element helps cover your legal fees to defend your organization in a civil lawsuit.

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 continued...

3: CONTENT & MEDIA

Protects your organization from online content which causes non-physical harm to another party. Specifically, covers content that is defamatory, contains misrepresentations, or misstatements, infringes on intellectual property or title of another party. As an example, cyber criminals compromise your website with defamatory content, redirect customers to their sites, or change content completely. It should be noted - “content” is defined differently from one policy to another.

4: REGULATORY PROCEEDING

Covers the cost of legal expenses and damages to defend your organization from an actual or alleged act, error or omission that results in a violation of any statute or regulation governing data security that leads to a civil, administrative or regulatory proceeding by a federal, state, local or foreign government entity.

POLICY ELEMENTS THAT COVER EXPENSES & REIMBURSEMENT

5: REGULATORY INVESTIGATION & REIMBURSEMENT

Covers reimbursement of necessary expenses to comply with the investigation for any actual or alleged act, error or omission that results in a violation of any statute or regulation governing data security.

6: REGULATORY/CONTRACTUAL FINES, PENALITIES & ASSESSMENTS

Covers reimbursement of fines and penalties for violating any statute, law, regulation or contractual obligations related to data security. This can include, but is not limited to, fines from violating one or more state data breach statutes, breach of merchant service agreements related to the Payment Card Industry Data Security Standard (PCI-DSS), or violation of the Health Insurance Portability and Accountability Act (HIPPA).

7: DATA BREACH EXPENSES

This element covers reimbursement for direct expenses to respond to a data breach or cyber incident. Covers forensic investigation expenses, legal fees, victim notifications, costs to implement a call cyber or identity theft hotline and provide credit monitoring/credit repair services for victims and others impacted by the incident. Some policies may include expenses to minimize reputational damage as well as provide coverage for crisis communications support from a professional.

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 continued...

8: CONSEQUENTAIL REPUTATION DAMAGE

This is a relatively new element to certain policies – and is considered an "Endorsement to the policy." Covers reimbursement for financial loss directly related to the loss of current or future clients, customers or other opportunities due to an actual or alleged data breach or cyber incident.

9: SYSTEM DAMAGE & DATA EXPENSES

Covers reimbursement for the costs to retrieve, restore or replace data, software, programs and equipment damaged by a data breach or cyber incident. This coverage may also include containing an active incident and/or re-securing data to the state it existed prior to the event. A small subset of cyber insurance policies may also cover equipment damaged directly by a cyber event or attack. If you have unique business equipment that is difficult to replace, this option might be something to seriously consider.

10: BUSINESS INTERRUPTION & EXTRA EXPENSE

There are three components of this clause to consider.

1. Business Interruption – Covers reimbursement for income that would have been earned during the period of network, system, service impairment and restoration.
2. Contingent Business Interruption – Covers reimbursement for income that would have been earned during the period of network, system, service impairment and restoration of a third-party vendor (such as an IT service provider), who is responsible for providing essential business systems or services to insured.
3. Extra Expense – Covers reasonable and necessary expenses over and above normal operating expenses incurred during periods of network impairment associated with restoring and resuming operations.

POLICY ELEMENTS THAT COVER CYBERCRIME

11: CYBERCRIME ELECTRONIC THEFT

Covers reimbursement for the theft of money or securities by electronic means. Some policies may also cover theft of finished goods or work in progress by electronic means.

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 continued...

12: IDENTITY THEFT

There are policies that cover some level of business identity theft, however at the current time, this coverage is only offered by a small subset of insurance carriers.

13: TELECOMMUNICATIONS THEFT

Covers reimbursement for unauthorized calls and use of bandwidth due to unauthorized use of telephone systems by a third party. May include crypto hijacking.

14: RANSOMWARE, COMPUTER & SYSTEM EXTORTION

Covers reimbursement for funds paid to a cyber-criminal threatening malicious actions related to data and computer networks, and/or demanding ransom for release of encrypted data.

15: DECEPTIVE FUNDS TRANSFER & SOCIAL ENGINEERING

Covers reimbursement of money and securities stolen through the intentional misleading of an employee by an external actor. This could include fraudulent transfer of funds, and/or theft of account information that leads to a theft of money.

The NCSS suggests you read and annotate this “cheat sheet” before your meet with your insurance agent. The majority of these elements should be included in your insurance policy. Don’t be another small business that fails after a cyber-attack, be prepared by being insured!

The NCSS would like to thank PSA Insurance and Financial Services for the content of this informational guide. Specific coverage and definitions in the insuring agreements will be different with each policy.

[i] https://www.foxbusiness.com/features/cyber-attacks-on-small-businesses-on-the-rise

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