IECC Legal and Insurance Working Group

Cyber & Technology Insurance Guide Version 1

August 2018

CYBER & TECHNOLOGY INSURANCE COVERAGE

Today, consumers, businesses, and government agencies use internet-capable devices every day. These high tech devices – from laptops to security systems to medical devices – increase efficiency in the collection and exchange of data, and revolutionize industries. Cyber technology also brings new risks. Large companies subject to data breaches have made headlines, but small and mid-size companies that collect data and private information may also be vulnerable. Businesses may be obligated to protect private information by governing laws and regulations – such as Personally Identifiable Information, Personal Health Information and Confidential Corporate Information. Smaller businesses may not be able to survive the costs associated with a data breach. One of the largest growing financial risks a business must face is a cyber breach. Insurance is a necessary component of a business's risk management and disaster recovery plan. Inadequately insured businesses are unlikely to survive major incidents.

Until recently, most businesses have insured only computer equipment and mobile devices against physical risks such as damage, theft, or fire loss. Electronic equipment was insured on the same basis as furniture and automobiles, with no coverage for lost, stolen or disrupted data. Some organizations may have had wider, more extensive policies that also include coverage for equipment breakdown and limited expenses for reinstatement of data, but most cyber risks are now excluded under traditional commercial general liability policies.

Insurers and businesses have recognized that traditional insurance is inadequate, and there is a need for tailored cyber liability insurance to cover a wide variety of exposures that can result from technology-related activities -- from misplaced company cell phones to cyberattacks. Cyber liability insurance is intended to address an insured's obligation to protect private information from inappropriate access undergoing significant changes and likely will continue to do so as it is linked to the ever-changing world of technology. Therefore, it is important to know the terminology, to review your risks, and to determine your coverage needs. Cyber liability insurance is increasingly becoming an important consideration for conducting business in a high-tech marketplace.

FREQUENTLY ASKED QUESTIONS

Q What is cyber liability?

A Cyber liability is the risk of a data breach as a result of online activities and the use of electronic storage technology.

Q What is cyber liability insurance?

A While policies vary, cyber liability insurance is designed to protect a business or organization from:

- Liability claims involving the unauthorized release of information for which the organization has a legal obligation to keep private or confidential, such as employee, patient or customer records.

- Liability claims alleging invasion of privacy.
- Liability claims alleging failure of computer security that results in alterations of data and defense costs.

- Data Response Services, including legal, computer forensics, notification services, credit and identity monitoring products and crisis management expertise, and the reimbursement to the insured for certain out-of-pocket expenses.

Q What is a data breach?

A A data breach occurs when secured information is released to or accessed by unauthorized individuals. The lost data may be employee personnel records, customer financial accounts, or business trade secrets. The incidents pose serious risks for organizations as well as the individuals whose data has been lost or disseminated.

Q How do data breaches happen?

A Data breaches can occur by accident, such as an employee sends out an unsecured email, or by crime, such as a malicious hacker.

Q What data or information do businesses need to secure?

A Most businesses generate vast amounts of data which is available and stored on their electronic storage network systems, which may be subject to certain privacy laws:

- Personal information:
  - Personally identifiable information (PII): name, address, date of birth, telephone number, email address, Social Security number, zip code, biometric data.
  - Protected health information (PHI): healthcare-based treatment information, medical history, health insurance information, including member identification numbers.

- Corporate information: intellectual property, business, contracts, attorney-client privileged information:
  - Payment cardholder information (PCI): credit/debit card data, including account numbers, security codes, insurance account information, etc.

- Cyber-based data: web browser history, cookie information, metadata, and IP addresses.

Q Why consider cyber liability insurance?

A

There are various reasons why a company may want to consider cyber liability insurance as a way to protect confidential data and insure the risk against financial exposure:

- Frequency of privacy breaches are on the rise;
- Threats are getting dramatically worse;
- Almost all 50 states have enacted privacy laws in response to privacy breaches;
- Consumers expect that their confidential information will be protected.
- Class action litigation is becoming more active as a result of privacy breaches.
- Many business contracts now require cyber insurance.
- Cyber liability insurance products are becoming more widely available.

GLOSSARY OF CYBER INSURANCE TERMS

Breach Response – Investigation. Costs incurred to investigate data breach; investigate potential indemnity.

Breach Response – Notification. Costs incurred to notify individuals of breach.

Breach Response – Public Relations. Costs incurred to hire public relations firm.

Breach Response – Remediation. Costs incurred to remediate data breach (e.g., credit monitoring, call center, etc.).

Business Income (or Business Interruption Income Loss) is defined as net profit or loss before income taxes, as well as the continuing normal operating and payroll expenses.

Claim Expenses include reasonable and necessary legal fees, costs, and expenses incurred in the investigation, adjustment, defense, or appeal of a claim. They also typically include the cost of any bond or appeal bond required in any defended suit.

Computer System means computer hardware and software, and the electronic data stored thereon, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the internet, intranets, extranets, or virtual private networks.

Cyber Attack (Denial of Service Attack) is action preventing an information system from functioning in accordance with its intended purpose; the inability of an authorized third party to access the company's Computer System; and the inability of an authorized third party to access his or her Computer System, where such inability is directly cause by the company's Computer System.

Cyber Extortion. Losses and expenses arising out of a criminal threat to release sensitive information or bring down a system/network.

Damages/Loss includes the amounts the business is legally obligated to pay as a result of a covered judgment, award, or settlement; costs charged against the business in any suit; or pre-

judgment and post-judgment interest and defense costs. It also includes punitive or exemplary damages where insurable by law.

Data Restoration – Security Failure. Costs to restore lost data caused by security failure.

Data Restoration – System Failure. Costs to restore lost data caused by system failure.

Denial of Service Attack is action preventing an information system from functioning in accordance with its intended purpose (see Cyber Attack).

Extra Expense means any reasonable and necessary expenses in excess of the business's normal operating expenses that the business incurs during the Period of Restoration associated with restoring and resuming operations, including securing temporary third-party Internet Service Provider services, temporary website and/or email hosting services, rental of temporary networks, or other temporary equipment or service contracts.

First Party Claim. A first party claim is brought by an insured under the insured's cyber policy for a loss that occurs because of loss or damage to the insured's business.

Funds Transfer and Computer Fraud – Social Engineering. Loss of money or property arising from *bona fide* wire instructions induced through social engineering.

Funds Transfer and Computer Fraud – Traditional Coverage. Loss of money or property arising from fraudulent wire instructions or fraudulent entries into a computer system.

Identity Restoration Services typically means consultation and assistance to an individual receiving notification services to determine whether identity theft has occurred, and, if so, to restore the individual's identity to pre-theft status.

Media or Electronic Publishing Incident means the actual or alleged unintentional libel, slander, trade libel, or disparagement resulting from the insured electronic publishing. It also includes plagiarism, violation of privacy, infringement of a copyright or trademark, or unauthorized use of titles formats, plots, or other protected material resulting from the insured's electronic or media publishing.

Media Liability. Claim by third party in connection with the insured's media content, which may include claim for trademark infringement, defamation, libel, product disparagement, copyright violation, or invasion of privacy.

Network/Computer System typically includes the computer hardware, software, and electronic data, as well as associated input and output devices, terminal devices, data storage devices, networking equipment, components, software, and electronic backup facilities, including systems accessible through the Internet, intranets, extranets, or virtual private networks.

Network Interruption – Contingent BI. Loss of income arising from business interruption caused by third-party service failure (including mitigation expenses).

Network Interruption – Security Failure. Loss of income arising from business interruption caused by security failure (including mitigation expenses).

Network Interruption – System Failure. Loss of income arising from business interruption caused by system failure (including mitigation expenses).

Network Security Liability. Claim by third party arising from the insured's failure of network security.

Network Security/Cyber Incident typically means any Unauthorized Access/Use of, or introduction of malicious code into, or Denial of Service Attack upon, the company's Computer System, that directly results in an interruption in services; or the corruption of deletion of digital assets.

Notification Services typically mean the preparation and distribution of notice letters from the insured advising individuals of the network security event and the availability of related resources if such notices are required by applicable law, as well as call center support services.

Period of Restoration is the period from which the business first suffered an interruption in service to the date and time it was restored (or could have been restored) with reasonable speed to substantially return to the level of operation that existed prior to the interruption. There is typically a limit on the policy that the period of restoration cannot exceed thirty days.

Personal Identifiable Information (PII) is information not available to the general public from which a person can be identified. This definition should be broad enough to include a person's name, telephone number, Social Security number, medical or healthcare data, driver's license number or state identification number, account number, credit and debit card number, or password.

Privacy Incident is the unintentional and unauthorized disclosure of Personal Identifiable Information or confidential information in the care, custody, or control of the business or service provider; a violation of a Privacy Regulation; or failure to comply with the term's own privacy policies.

Privacy Liability – Business Records Claim. Claim by third party arising from the insured's failure to protect trade secrets or other confidential business information.

Privacy Liability – Privacy Claim. Claim by third party arising from the insured's failure to protect personal information (including PII, PHI and FAI).

Privacy Liability – Regulatory Claims. Third party liability coverage that generally is designed to protect an insured business in connection with certain requests for information, investigative demands and/or civil proceedings often brought by or on behalf of a governmental agency arising from the insured's failure to protect personal information. The coverage often includes civil fines and penalties imposed on the insured, to the extent such fines and penalties are insurable by law.

Privacy Notification Costs are reasonable and necessary costs to hire a security expert to determine the existence and cause of a breach; costs to notify consumers under a breach notification law; or fees incurred to determine the actions necessary to comply with a breach notification law.

Privacy Regulation means statutes associate with the control and use of personally identifiable financial, medical, or other sensitive information.

Public Relations Expense typically means the hiring of a public relations firm or crisis management firm for communication services to explain the nature of the network security/cyber event and any corrective actions taken.

Regulatory Fines includes civil money penalties imposed by a federal, state, local, or foreign government entity pursuant to a regulatory proceeding.

Regulatory Proceeding is an investigation of an insured by an administrative, regulatory, or government agency concerning a Privacy Incident; or an administrative adjudicative proceeding for a privacy Wrongful Act or network security Wrongful Act.

Regulatory Injury means injury sustained by a person due to actual or alleged disparagement of an organization's products or services; libel or slander of natural person; or violation of such person's rights of privacy or publicity result from cyber activities.

Retroactive Date means the date in the declarations section of the policy. If no date is set forth in the declarations page, then the retroactive date is the date of the inception of the policy.

Reward Payment/Expenses/Cyber Extortion Costs means the reasonable amount paid by the business, with prior approval of the insurer, to an informant for information not otherwise available, which leads to the arrest and conviction of persons responsible for a cyber attack or threat covered under the policy.

Service Provider means a business the business does not own, operate or control, but that the insured hires and contracts to perform services related to the business' computer systems, including maintaining the computer system; hosting the business' internet website; handling, storing or destroying information and confidential materials; or providing other IT-related services.

Technology Errors & Omissions. Claim by third party for financial loss arising from errors or omissions in the technology-facing component of the insured's business (tech services or products).

Third Party Claim. A third party claim is a demand against the business for monetary damages or non-monetary relief; a written demand for arbitration; or a civil proceeding brought by the service of a complaint or similar pleading.

Unauthorized Access/Use is the use of, or access to, a computer system by a person unauthorized by the insured to do so, or the authorized use of, or access to, a Computer System in a manner not authorized by the insured.

Wrongful Act typically means the actual or alleged act, unintentional error, omission, neglect, or breach of duty by an insured business or Service Provider that directly results in a breach of the insured's network.