CYBER COVERAGES EXPLAINED

AHT INSURANCE
A BALDWIN RISK PARTNER

Cyber policies have continued to progress over the last couple of decades to keep up as the Internet and Internet of Things (IoT) evolved - adding more first-party coverages and more.

THIRD-PARTY COVERAGES

Third Party "Liability" coverages in a Cyber policy protect the insured from third-party suits alleging financial damages. The insurer pays the damages and defense expenses that the insured becomes legally obligated to pay; up to the policy limits based on terms and conditions.

Technology Errors & Omissions

Liability coverage for a suit from a third party alleging financial damages due to technology products or services. When choosing a limit, consider current contractual agreements, peer benchmarking and table-top exercises to understand each cyber stakeholder's perception of the risk.

Contingent Bodily Injury and Property Damage

Liability coverage for bodily injury & property damage arising out of a cyber event. As a rule, Technology Errors & Omissions/Cyber policies exclude Bodily Injury and Property Damage (as this is typically found in the General Liability policy). To broaden a Cyber policy to include coverage for Bodily Injury and Property Damage, it must be endorsed to grant coverage for a cyber breach that results in property damage or bodily injury to a third party.

Network Security & Privacy Liability

Liability coverage for financial damages alleging data breach or security failure that result in dissemination of Protected Data and/or Third-Party Corporate Confidential Information. Types of information breaches include:

- PCI (Payment Card Information)
- PHI (Protected Health Information)
- PII (Personally Identifiable Information)

A robust cyber risk management framework should be based on understanding and protecting core assets and optimizing recourses. This will continue to shift over time based on changes in exposures, third-party relationships, contractual agreements, and threat vectors.

Media Liability / Intellectual Property

Liability Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander or invasion of privacy. Typically, these policies are limited to "content" in electronic form; we suggest re-defining the coverage to include "off-line" content to broaden the coverage to apply "in any format". This maybe a lower risk than Network Security or Privacy Injury, however every company has a risk for libel, slander or infringement; specifically, content that is published by the Marketing Department.

Patent Liability

Liability coverage for legal expenses and damages that can include coverage for Patent Infringement and Trade Secrets. It is a common misnomer that Patent Liability is included in the Intellectual Property coverage available in a Cyber policy. Patent Liability is separate and distinct from Media Liability/Intellectual Property; a stand-alone policy must be purchased to protect Patents.

Regulatory Proceeding and Fines

A Regulatory Proceeding grant provides coverage for a request for information, investigation or civil, administrative or regulatory proceeding brought by federal, state, local or foreign authority. Regulatory Fines coverage is for the resulting civil fines or penalties that are payable to the Governmental entity resulting from said breach. For example, these can include PCI-DSS that are legally obligated to pay under a merchant services agreement post breach. This is the area of coverage that is becoming more difficult to track due to multiple regulations from 50 states within the US and a multitude of countries. Examples are Global Data Privacy Regulations (GDPR), New York Financial Services (NYDFS), and Health Information Portability and Accountability Act (HIPAA).

FIRST-PARTY COVERAGES

First Party coverages are non-liability coverage grants that a company sets aside for their own usage in the event of a breach or claim. Most of the policies pay claims "reimbursement" form, which meant the client procures the services, pays for them and is reimbursed by the carrier. Many policies are moving to the "pay on behalf of" approach, but then may require the insured to utilize the carrier's pre-selected Third-Party Vendor.

Privacy Breach Response Costs & Notification Expenses

Coverage applies to notify affected individuals in the event of the dissemination and can include hiring legal assistance to research and determine legal obligations for notification expenses, notifying individuals in compliance with a Data Privacy Law, establishing call center services and credit monitoring. This was one of the original first party coverage grants when cyber coverage evolved from Technology Errors & Omissions many years ago.

Claims Example

After a suspected breach, company X must hire third-party firms to assist in the investigation to understand where consumers reside post breach (to understand statutory or country requirements). Also necessary is to hire lawyers to research and address the reporting requirements of each state and country and notify each individual in the specific way their regulatory requirement is written.

Computer Forensics

Provides coverage for third-party computer forensic analysis to investigate a breach. This is quickly becoming one of the most expense first-party coverage grants due to the increased cost of investigations. Note that most policies afford this coverage to investigate the cause and scope of an actual or suspected breach, not to fix or amend the issue that caused the breach or claim. In the event of a breach, a company must procure third-party assistance to investigate and analyze their computer systems, servers, backups and BYOD (bring your own devices). Depending on the location of which geographic location the forensic company is engaged, the hourly rate of computer forensics is very high; sometimes up to $1,000/hr.

Cyber Extortion

Coverage for a credible threat from a third party to corrupt data, penetrate the insured's computer system, including interrupting or suspending activity, preventing access, introducing malicious code and to steal or publicly disclose Protected Data. Note that this coverage can be given as a small limit coverage grant on a Kidnap, Ransom & Extortion Policy; both policies would need to be reviewed thoroughly to create a thoughtful coverage approach. Many times these policies define "payment" as regulated money, which would have to be reviewed, as this would negate the use of bitcoin for extortion payment.

Cyber Crime

Cyber Crime coverage can be placed on both a standard Crime policy, as well as a Cyber policy. Both should be reviewed closely to appropriate coverage in conjunction with each other. Many times, a well written Crime policy are more appropriate for theft of money or securities as these policies have been time tested for years and is likely broader on a traditional crime policy.

Social Engineering Fraud / Deceptive Transfer Fraud

Provides coverage when a third party intentionally misleads an employee (duping them) to release Protected Data, such as money or securities. Note that the term Social Engineering is also utilized for accidental dissemination of data; this would fall under the basic Cyber coverage grant. The difference between the two is money (crime/fraud) vs. data (cyber).

Funds Transfer Fraud

Provides coverage for fraudulent instruction directing transfer, payment or money delivery to a vendor by an impersonator without your consent or knowledge.

Telecommunications Fraud

Coverage for intentional, unauthorized and fraudulent access to a telephone service, in which services are manipulated and the insured charged for calls not made by the insured.

Business Interruption

Coverage for loss of income and extra expense from a business interruption due to a Security Breach or System Failure; for example a virus or unauthorized computer access. This coverage is specifically for a system that you own or control. Keeping close track of lost time and expenses are key, as these claims can be very difficult for quantify and require a forensic accountant and investigator.

Contingent or Dependent Business Interruption

Coverage for loss of income and extra expense for a business interruption due to a security breach or system failure on a third-party computer system or when a third-party administrator has control of data. This protects the insured for income loss, interruption expenses and special expenses, incurred because of an interruption, degradation in service, or failure of a computer system operated by an independent contractor or outsourced IT service provider. More companies are utilizing outsourced cloud providers, creating a significant risk for clients that may not understand that the contractual risk transfer is not as they expect.

Data Restoration Expenses / Digital Asset Expenses

Coverage for restoration of digital data due to a result of corruption, damage, impairment, destruction of deletion of data caused by an incident or claim.

Reputational Harm

Coverage for continuing profit a company suffers due to brand reputation damage. This is a relatively new coverage grant and typically only found with a small sublimit to reimburse another client's aversion to a brand or company following a publicized breach.

Bricking

Coverage for the replacement of tangible equipment that is rendered useless by a malware attack. This Is also a relatively new coverage grant within the past few years and is not found on all policies.

Terrorism

Coverage for an act or the threat thereof against an Insured to access or damage a computer system based on social, ideological, religious or political purposes.

Punitive Damages (Wrap-Around)

Many liability policies exclude punitive damages, and only cover Compensatory damages to compensate the aggrieved. Indemnity coverage is available for punitive damages through a few select carriers, where applicable (statutorily unavailable in three states and capped in 27 others). Currently there are two options to procure punitive damages:

1. Language applying to "most favored jurisdiction or venue"
2. A stand-alone punitive damage wrap policy (Puni-Wrap) is available through a Bermuda policy that is not subject to regulatory and public policy 27 restrictions and is triggered when the domestic policy prevents punitive damages to be paid because of the jurisdiction.

AHT Insurance is an insurance brokerage and consulting firm offering property and casualty, employee benefits, retirement, private client and international services for clients throughout the United States and 42 other countries. Supporting numerous industries and boasting national recognition in the technology, manufacturing, government contracting and nonprofit practice areas, AHT offers clients highly customized solutions to identify and help mitigate risks they may face. AHT's professionals put clients' needs first and focus on what they do best –providing best-in-class service and solutions. Learn more about AHT at ahtins.com.