EXECUTIVE PROTECTION

INSURING

Privacy Liability / Network Security & Related Risks

In recent years, numerous insurance policies have been designed to address the "cyber risks" of companies operating in today's interconnected business environment. While many products can roughly be described as "internet liability" policies, these policies vary considerably in scope.

There are four distinct categories of "internet liability" that can be insured. Of the four, we believe the most important is Privacy Liability/Network Security.

1 PRIVACY BREACH & NETWORK SECURITY LIABILITY

By simply collecting, storing and transmitting data, a company is potentially exposed to a data breach. If a data breach occurs, an organization faces the threat of expensive litigation brought by the affected parties (including regulatory fines and penalties), substantial response and remediation costs not to mention fundamental harm to their reputation that can result in a loss of customers.

Network Security covers liability arising from a cyber attack or unauthorized access to digital records. Privacy Liability covers negligence or failure to protect or safeguard confidential data— even for acts of rogue employees or vendor employees. Some policies will also pick up instances of employee negligence, such as lost or stolen laptops.

In addition to liability coverage, policies can include fines and penalties coverage and expense reimbursement (typically sub-limited) for: regulatory defense costs; ID Theft notification expense which can include credit monitoring programs; and, Crisis Management such as public relations and, sometimes, legal expense.

The best example of exposures related to a **privacy breach / network security** is the TJX credit card security breach and subsequent litigation: *The retailer experienced "unauthorized intrusion" by hackers resulting in the breach of up to 96 million unencrypted credit and debit card numbers. TJX was sued by their affected customers as well as the credit card issuers. In addition, the FTC and 37 states launched investigations. The company incurred heavy investigation, notification, credit monitoring, defense and settlement costs and announced a $107 million reserve in connection with the breach.*

2 CYBER EXTORTION

Think of this coverage as Kidnap & Ransom for computer systems— it covers extortion ransom payments and related expenses. A common tactic in cyber extortion scenarios is to threaten to incapacitate a victim's transactional website or other components of their information system; this is known as a denial-of-service (or DOS) attack. Cyber criminals know that the threat of disclosure of a security breach— or the threat of damage to a system / network— is valuable.

An example of a **cyber extortion scenario**: *After refusing to pay a $10,000 extortion threat received by email, a service provider's website went down for several days. The e-mail had threatened to cripple the site if the ransom was not paid.*

3 INTERNET MEDIA LIABILITY

Any company with a website can face claims related to their dissemination of content over the Internet. Basically this coverage responds to claims of libel, slander, copyright infringement or other "electronic advertising" or personal injury arising out of content posted or published on the internet site. The CGL and its Personal/Advertising Injury Coverage is problematic for "electronic" exposures. Specific limitations and exclusions apply to electronic data, chat rooms, bulletin boards, etc.

An example of a covered **internet media claim**: *A business used a competitor's trademarked name as a "metatag" (a piece of code used to increase the number of "hits" from internet searches) and was sued by the competitor for trademark infringement and unfair competition.*

4 "FIRST PARTY" INTERNET LIABILITY

In the event of accidental or malicious loss or damage to data or a network, first party internet loss can take the form of e-business interruption as well as reimbursement coverage for the cost to replace or reconstruct digital assets.

An example of a covered **e-business interruption claim**: *A virus is launched on a retailer's online system. The attack causes the company's system to be brought down for 36 hours. The company struggles to identify the attacker and to bring their services back online so that customers can log on and transact business. The e-business interruption caused by the cyber attack results in a quantifiable loss of profits and extra expenses.*

An example of a covered **digital property claim**: *A disgruntled employee sabotaged a computer network at a major national investment firm and deleted files on over 1,000 of the company's computers. It cost the company millions to assess and repair the damage.*

CONTACT US

Conner Strong & Buckelew
connerstrong.com | 1-877-861-3220

NEW JERSEY PENNSYLVANIA DELAWARE FLORIDA