

Cyber-Crime and Your Business. Are You Adequately Protected? Review this Checklist and Find Out.



By Richard Mather, Vice President, North American Claims Group

There is no real substitute for working with your insurance broker to understand the variety of coverages available under cyber liability policies and which ones fit your business's needs. However, reviewing the insuring agreements to confirm that both cyber security breaches and breachless exposures are included is a good place to start. While most of us are familiar with breaches involving the exfiltration of data from a business's computer system (think Target), many of us are not aware of breachless claims and the necessary coverage to help protect our businesses. These exposures occur frequently and can lead to significant lost time and expense if the company does not have coverage in place to deal with them.

Here is a short checklist of breachless coverages for consideration when buying a cyber-insurance policy:

- Coverage for violations of privacy statutes or regulations;
- Coverage for media liability;
- Coverage for social engineering and ransomware attacks; and
- Business interruption, both direct and contingent coverage.

What are "breachless" cyber claims?

Breachless claims are when a situation that does not involve the theft or exposure of data triggers coverage under a cyber-insurance policy. Cyber policies typically include a variety of coverages that may apply to breachless claims. Whether there is coverage will ultimately depend upon policy language and the particular circumstances.



Ransomware and Data Restoration Exposures

Ransomware attacks typically fit within the "breachless claim" scenario. While they do involve a "breach" of the company's computer system, they do not typically involve the exfiltration of data. The data is typically encrypted, not copied or downloaded.

Ransomware attacks can also trigger coverage under "data restoration" provisions, where the policy pays for trying to recover and restore data damaged in an attack.

Privacy Statutory and Regulatory Violations

Allied World's Cyber policies provide coverage for, inter alia, a "violation of... law or regulations associated with the control and use of Protected Information" (as defined in the policies). Note that the policy language is designed to automatically include any statute or regulation dealing with Protected Information, including new ones that may not even be contemplated today. Such statutes and regulations can impose a variety of requirements on a business that do not arise from data breaches.

For example, for companies connected with the medical industry, HIPAA imposes a variety of obligations that include record keeping and record retention requirements, disclosure requirements and reporting obligations, etc. In addition, the Health and Human Services website contains a prominent link for filing complaints. We have seen complaints filed against our insureds by a variety of people, including disgruntled ex-employees who complain about

the company's information security practices. When the Office of Civil Rights, the HIPAA enforcement arm, investigates a covered entity, it looks into whether the entity complies with all HIPAA requirements. Even if no fines or penalties are ultimately imposed, the insured typically will incur significant legal fees defending itself in the investigation. Cyber policies, such as those offered by Allied World, will pay for the defense, and the fines and penalties.

Wrongful Collection of Data

Merely collecting certain types of data can lead to liability. For example, some states have statutes regulating the collection of biometric data, such as fingerprints, which are sometimes used for identification purposes by employers.

Social Engineering Fraud

Other common breachless claims involve "social engineering" fraud. This is when the business is tricked by seemingly legitimate emails into wiring funds or transferring protected information.

Pre-breach Theories of Liability

Plaintiffs' firms are increasingly focusing on "pre-breach" theories of liability, which greatly expand the universe of targets of litigation. For example, there are law firms that examine devices that connect to "the Internet of Things" for perceived "security flaws" that can be the subject of a lawsuit.

Media Exposures

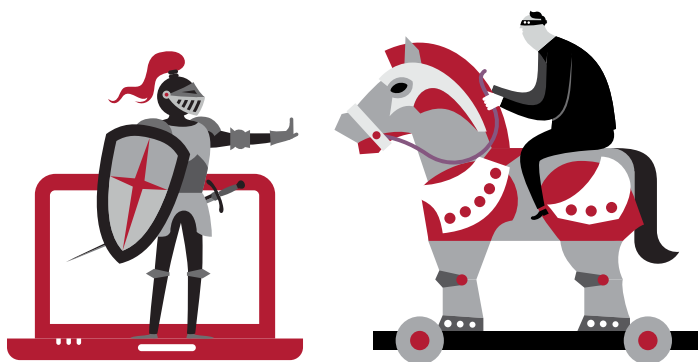
Another type of breachless claim can arise under the "media liability" coverage in the policy. Every company with a website is a "publisher" and may have exposure to libel, slander, and copyright or trademark infringement. Coverage can be purchased not only for content hosted on a company website, or contained in emails, but also for "off-line" material. This is very significant coverage. We have seen many claims come in over the years that triggered coverage under the media liability provisions in the policy.

Business Interruption

Cyber policies can contain various provisions relating to business interruption coverage. This could be triggered by, inter alia, a denial of service attack on the company or, in the case of contingent business interruption coverage, an attack on a third party, such as an important supplier.

Conclusion

Now is as good as time as any to review your Cyber Security Liability insurance policy to ensure your business is adequately protected. Remember to review the short checklist of breachless coverages for consideration. Finally, talk with your broker and/or reach out to us directly for more information on how to protect your company from breaches and breachless cyber risks in this ever-changing world.



ABOUT THE AUTHOR

Richard W. Mather, Esq.

Vice President, North American Claims Group,
Allied World

Rich is responsible for claims under Allied World's technology errors and omissions ("E&O"), privacy and network security E&O, lawyers E&O, insurance agents and brokers E&O, insurance company E&O, media, and miscellaneous professional E&O lines.

Prior to joining Allied World, Rich spent sixteen years litigating cases in the state and federal courts in Connecticut.

He received his B.A. from the University of Connecticut, his M.A. from Trinity College, and his J.D. from the University of Connecticut School of Law.

For more information contact rich.mather@awac.com about Allied World's Claims Services.