**The History of Cyber Coverage**

Since 1997, when we wrote of the first cyber insurance policies in the industry, we have consistently been here to help our partners place this coverage

The roots of cyber coverage go back about 20 years. Back then, technology companies bought errors and omissions (E&O) insurance, which over time, was extended to include things like a software product bringing down another company’s network, unauthorized access to a client system, destruction of data, or a virus impacting a customer. (For a while there, spreading a computer virus was the big concern – remember [the Love Bug](http://en.wikipedia.org/wiki/Love_bug_virus%20) Virus that swept the globe in 2000?)

The companies that bought this early cyber insurance were generally in the technology space and already buying E&O insurance. The technology coverage, often called “network security” or “Internet liability” was an add-on.

Five to 10 years ago, we saw these “network security” policies expand into the privacy space by providing clear coverage for breaches of confidential information. That got the attention of retailers and other companies holding considerable consumer data, but who weren’t providing the type of technology services that would warrant buying E&O insurance.

Those companies wanted standalone cyber products that covered network security and privacy liability. That evolution has been important to where we are now because those exposures are so dominant today.

Now more than ever companies of all sizes require “cyber” insurance. Technology has transformed the business world and with it the corporate risk landscape. Each new advancement from more powerful computers to mobile devices, corporate networks and the public internet has brought new exposures.

Policies are divided by first party coverage and third party coverage. Although each insurance company’s policy wording is unique. The basic skeleton is:

 **Errors and Omissions:** E&O covers claims arising from errors in the performance of your services. This can include technology services, like software and consulting, or more traditional professional services like lawyers, doctors, architects and engineers.

**Media Liability:** These are advertising injury claims such as infringement of intellectual property, copyright/trademark infringement and libel and slander. Due to the Internet presence of businesses today, technology companies have seen this coverage migrate from their general liability policy to being bundled into a media component in a cyber policy (or a separate media liability policy). Coverage here can extend to offline content as well.

**Network Security:** A failure of network security can lead to many different exposures, including a consumer data breach, destruction of data, virus transmission and cyber extortion. The culprits might be looking to shut your network down so you can’t conduct business, either for financial or political gain. Network security coverage can also apply if you’re holding trade secrets or patent applications for a client, and that information is accessed due to a failure of your security.

**Privacy:** Privacy doesn’t have to involve a network security failure. It can be a breach of physical records, such as files tossed in a dumpster, or human errors such as a lost laptop, or sending a file full of customer account information to the wrong email address. Companies have also faced liability from returning a photocopier with a hard drive that contained unwiped customer tax records. A privacy breach can also include an action like wrongful collection of information.

All insurers use different terminology for cyber coverage; some subdivide the four components above even further, which means that cyber policies can be very difficult to read and compare.

**Network Security and Privacy Liability Coverage**

What’s unique about the privacy and network security coverages is that both first-party costs and third-party liabilities are covered: First-party coverage applies to direct costs for responding to a privacy breach or security failure, and third-party coverage applies when people sue or make claims against you, or regulators demand information from you.



In addition to the advances in data storage, increasingly stringent laws and regulations enacted over the past decade at both state and federal levels have heightened the standards for the duty of care companies must take to protect personal information, including formal notification to individuals should their data be compromised.

 Insert Map

Besides the risk of theft or loss of sensitive information, companies face escalating regulatory risks should they fail to adequately protect consumer or patient information. In addition to industry specific privacy legislation enacted during the last decade, including The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Gramm-Leach-Bliley Act of 1999 (GLBA), Sarbanes Oxley Act of 2002 (SOX) and The Payment Card Industry Data Security Standard 2006 (PCI DSS) but the most significant impact has come from legislation at the state level. Roughly three dozen states have enacted laws that require companies to notify consumers when their personal information has been exposed to POTENTIAL fraud. Companies face possible class action litigation as the plaintiff’s bar get more aggressive.

CONCLUSION

Privacy exposure exists for every company that deals in personal information, including law firms, accounting firms, healthcare, retail, real estate, service industry, educational, and financial institutions.