Insurance: Your Safety Net for the Internet

By James R. Murray and Kristin C. Davis

Over the past decade, social media websites such as Facebook, Twitter and YouTube have gone from big news to many people’s only source of news. These days you are just as likely to come across an Internet posting from your child as you are from a Fortune 500 company.

Everyone seems to be taking advantage of the connectivity and information the Internet and, specifically, social media offer. Of course, with the increasing use and reliance on social media, there come increasing costs and risks.

Cyber liability risks come in many shapes and sizes. The proliferation of state, federal and international privacy laws means increased obligations and risk for companies and individuals in cyberspace.

For companies that store personal or financial information, a data breach can mean liability to thousands of people. Sometimes a data breach is a result of a resentful or careless employee, other times an anonymous hacker, or just a side-effect of a software malfunction. For companies and individuals alike, the release of private or incorrect information on Facebook or Twitter, whether intentional or not, could lead to expensive lawsuits. Even relying on storing information online can result in significant business delays if a network outage or software malfunction occurs.

Thus, for all policyholders, it is important to remember that where there is risk, there is often insurance.

The availability of insurance coverage for social media or cyber liability risk has yet to be challenged in Washington courts, but several jurisdictions across the country have found coverage for data breaches and other cyber liability risks. Several companies have successfully procured coverage in court rulings and through settlement under a variety of different policies. In many instances, coverage is available for both defense and indemnity costs.

When purchasing insurance for cyber risks or considering current coverage for a cyber liability, it is essential to consider all policies, as coverages may be written and offered in different modules and on varying policy forms. Some insurers sell specific media, technology or cyber liability policies, which offer varying degrees of coverage, depending on the form and the risk to be insured.

As social media evolve though, insurers may change forms and create different policies. Therefore, when purchasing or renewing a cyber liability policy, carefully review new exclusions and endorsements to ensure you are purchasing the coverage you intend.

Before you run out and buy a media or technology policy though, you should thoroughly review your existing policies. Standard Commercial General Liability (CGL) and Business Owners Liability policies are a good place to start. Indeed, a policyholder may already have coverage for a cyber liability risk and not know it.

Typically, CGL policies provide coverage for “personal and advertising injury” claims and liability for the “publication” of private or personal information. A standard data breach or inappropriate use of social media may be covered under the personal and advertising injury portion of a CGL policy.

Likewise, a CGL policy may cover the investigation, mitigation and remediation costs associated with resolving a data breach, especially if a lawsuit results. Indeed, even if the claims against a company are groundless, false or fraudulent, an insurance company has a duty to defend the claim if even a portion of the complaint could be covered. At a minimum, a CGL insurance policy with personal and advertising injury coverage should provide a defense for the claims, even if just one allegation in a lawsuit is covered.

Other policies also may provide coverage. For example, a first-party policy may cover damage caused by an outage or data loss. This may include physical damage to software or the loss of use of data; corrupted, lost, stolen or ransomed data resulting from data theft, virus or breach; or the inability to conduct business because of loss of data, software or network failure.

In other instances, courts have found coverage for data breaches under a commercial crime policy. Coverage could also be available under an errors and omissions policy or even a kidnap and ransom policy. Coverage may also be added to a policy by endorsement or within the basic insuring agreement of the policies.

The easiest way to control risk is to put in place internal protocols and policies that limit your risk. Ensure that employees know the risks associated with losing or inadvertently releasing personal information. For official use of social media, create a protocol that ensures that published information is vetted and accurate. If storing personal and financial information, install proper security measures and test your systems.

Unfortunately, even with proper precautions, a data breach may occur. In the event of an incident, alert potential customers immediately so they can mitigate their own risks. Depending on the information released, you also may be obligated to report the data breach to a regulator or other entity. Keep your technology managers involved in the process; often, they may be able to provide valuable information to customers and regulators alike on what went wrong and how the problem will be prevented in the future.

Most importantly, do not forget about your insurance policies or assume that you are not covered. While some insurers started to add media and cyber liability exclusions to policies, the truly evolving nature of cyber liability risks means that insurance companies are more often in a reactionary position than on the cutting edge.

Therefore, even if you are unsure about the harm that may have been caused by a data breach or inaccurate posting, it is imperative to notify your insurer immediately in the event of a cyber incident and conduct a full review of your policies.

Jim Murray is deputy leader of Dickstein Shapiro LLP’s Attorney Insurance Coverage Group (policyholders only). Kristin Davis is an associate in the firm’s Washington, D.C. office and practices in the Insurance Coverage Group. Murray and Davis are members of the firm’s Cyber Security Insurance Initiative. They can be reached at murray@dicksteinshapiro.com and davisk@dicksteinshapiro.com.

Reprinted with permission of the King County Bar Association.