By Jacqueline M. Brettner and Andrew J. Brien

Most businesses will experience a cyber-attack or data breach. If your business does not currently carry cyber insurance, it is time to ask: "why not?" Data breaches can level even the largest and most sophisticated of companies, and response costs for these incidents are only increasing. However, demands for streamlined services and more efficient processes in a competitive market economy put increasing pressure on small and mid-size businesses to adapt to survive. This evolution includes increased use of electronic databases, digital client management software, and other cloud-based or electronic storage, which, in turn, escalate the risk of cyber liability. While you cannot turn back the hands of time, you can control how technology is integrated into your business and how you insure yourself against unavoidable risks.

Approximately 80 percent of small businesses do not have a cyber-attack response plan. Even more startling is the fact that more than 90 percent of small business owners carry no cyber insurance at all. This, even though nearly half of all cyberattacks target small businesses. Given the escalating costs of dealing with a cyber breach, business owners cannot afford to ignore these threats any longer.

As the name suggests, cyber insurance policies provide coverage for liability from cyber security breaches and for violations of privacy and data breach notification laws. Typically, cyber policies are broken into first-party and third-party coverages.

First-party coverages are meant to protect the policyholder against its own losses resulting from the cyber breach. These losses include the expense of paying a forensic investigator to determine the cause of the breach and legal advice to determine notification and regulatory obligations if third-party information was compromised because of the breach. Other covered costs may include notifying third-parties whose information may have been disclosed, public relations expenses, and lost profits and extra expenses incurred because of computer network downtime.

Conversely, third-party cyber liability policies indemnify the policyholder for its liability to others. These costs include legal defense costs, settlements, damages, and judgments related to the breach, liability to banks for re-issuing credit cards if credit card information was compromised, and costs incurred responding to regulatory inquiries and regulatory fines and penalties.

No matter how many measures an organization takes to protect its electronic data, a cyber breach is still possible. The question then is not if, but when. While cyber insurance is a relatively new product, it is a worthwhile investment for companies of all sizes. The massive data breaches that brought commercial giants Target and Sony[i] to their knees, and crippled the U.S. State Department,[ii] prove it.

As of 2014, the National Small Business Association assessed the average cost of a data breach for small business at $20,752, up from $8,699 in 2012.[iii] For larger businesses the costs are even higher. For example, Target's 2013 data breach cost approximately $252 million before insurance compensation and tax deductions![iv] Liability is, of course, driven by many factors – including the size and type of business you are in; however, all businesses with electronic data are vulnerable. And the costs of cyber breaches escalate every day.

Because data breaches can make or break your company, the way that you handle electronic data and how you insure against the risks of doing business online should be top priorities. Simply purchasing cyber coverage is not enough; you need to know your business and reassess how you process and store electronic data in the face of e-commerce hazards. Among the many things to consider in such an assessment are proper procedures for timely applying security fixes as they become available; evaluating contracts with software vendors; auditing computer systems for unauthorized access; and an assessing insurance coverage needs for data security breaches.

Start by making sure the individuals responsible for placing your business' cyber liability coverage understand the nuances of your industry including, for example, the types of data you receive, transmit, and store as well as how you handle these processes. It is also crucial that they be familiar with the varying cyber liability policy forms, the types of coverage provided, and the most commonly invoked exclusions to coverage. Cyber insurance policies are finally being tested in the courts. It is, therefore, important to ask the individuals placing your coverage about their experience in placing cyber liability policies and their involvement in claims handling. Be wary of professionals who do not thoroughly vet your electronic data management and storage procedures before recommending a specific policy form. Do you store electronic data on your own servers or third-party servers? What about customer information? What types of information are you storing? The answers to these questions, and others,[v] may determine whether your claim is paid or rejected. This is not something you want to find out on the back end of a breach.

Finally, make sure you read your policy. In most jurisdictions the policyholder is charged with knowledge of the policy regardless of their reliance on the representations of an insurance agent.[vi]

Ultimately, in cyber liability, as in life, an ounce of prevention is worth a pound of cure.

[i]The cost associated with restoring Sony's financial and IT systems as a result of its 2014 cyber-attack was $35 million for the fiscal year through March 31, 2015. *See* Sony,

Consolidated Financial Results Forecast for the Third Quarter, February 4, 2015, *available at* http://www.sony.net/SonyInfo/IR/library/fr/150204_sony.pdf.

[ii] *See* Dany Yadron, Three Months Later, State Department Hasn't Rooted Out Hackers, The Wall Street Journal, February 19, 2015, http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453

[iii] National Small Business Association 2014 Year-End Economic Report, *available at*http://www.nsba.biz/wp-content/uploads/2015/02/Year-End-Economic-Report-2014.pdf.

[iv] Target Corp., Target Reports Fourth Quarter and Full-Year 2014 Earnings, Feb. 25, 2015, *available at* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=2019880

[v] Other considerations impacting coverage including "cloud based computing" issues.

[vi] The time period and burden of proof associated with pursuing a claim against an insurance agent for improper coverage placement are often shorter and more onerous. Even in the case of successful claims, agent contracts usually have a limitation of liability clause that restricts possible recovery to a sum lower than the policy limits contemplated by the original coverage request.