DATA IN DANGER

A CYBERSECURITY INSURANCE PRIMER FOR BUSINESSES OF ALL SIZES

BY BETH BURGIN WALLER AND R. PATRICK BOLLING

A key component of today's 24-7 news barrage is the data breach *du jour*. The front page usually covers big names like Yahoo, Uber, Target, Ticketmaster. But businesses of all sizes should pay attention to the risks posed by data breaches. Just like the big names, local and regional companies handle sensitive personal data like employee Social Security numbers, customer credit card information, and addresses. They pay vendors and accept customer payments via wire transfer. They may sell via an online shop. Though necessary, these practices are not without risk. And, unlike the Ticketmasters of the world, these companies may not have the resources to deal with a data breach, which could be devastating to operations, reputation and, ultimately, the bottom line.

Cybersecurity insurance should be a significant piece of any cybersecurity protection plan. You should discuss cybersecurity insurance during your regular "check-up" with your insurer, and know that not all policies are created equal. Cybersecurity insurance policies vary just like other insurance policies. Here are just a few topics to consider:

1. Be conscious of the coverage exclusions. Consider a cautionary tale. In 2014, restaurant chain P.F. Chang's ("***Chang's***") found itself on the losing end of a costly dispute with MasterCard, Bank of America and Chubb, its cybersecurity insurer. Hackers had stolen 60,000 credit card numbers from Chang's, which, at the time, had paid more than $100,000 in cyber insurance premiums to Chubb. Chang's was caught between two contracts. Chang's had, on one hand, a master service agreement ("***MSA***") with Bank of America to process credit card transactions at Chang's restaurants. On the other hand, Bank of America had an agreement with MasterCard that allowed MasterCard to assess fees against Bank of America in the event of a data breach like the one suffered by Chang's.

MasterCard assessed Bank of America approximately $1.7 million for costs arising from the breach. Bank of America then pushed that assessment cost back onto Chang's pursuant to the MSA. Chang's gave notice to Chubb for Bank of America's $1.7 million claim, which the insurer denied. The dispute between Chang's and Chubb went to court, where it was held that coverage under Chang's cybersecurity policy by Chubb did not exist for the Bank of America claim because the policy did not cover third party contractual fees. As a consequence, Chang's had to pay the $1.7 million fees out of pocket (plus the $100,000 premium already paid).

2. Cybersecurity policies can be hyper technical and difficult to understand. Many cybersecurity insurance policies contain lots of technical cyber terms in their endorsements. So, while your business may purchase a $1 million cyber policy, look closely at the exclusions within the policy. Many policies have lower levels of coverage for "social engineering" or "phishing" crimes. Phishing means, broadly, impersonation. For example, imagine your business owes payment to a vendor for supplies or services. Your manager for this account communicates regularly with a point of contact at this vendor at johndoe@vendorname.com. Your employee receives an email with new payment information (bank account and routing number) from johndoe@vendername.com. Spot the difference? A busy account manager could miss it too and unknowingly wire funds to the wrong account. There may be limited coverage in your policy—i.e., you may not be covered for the full loss, even with a $1 million policy.

3. Shop around and get coverage that can cover the worst. With phishing events on the rise, it is important to know what your insurance would cover in the event the worst happens. It is easy to imagine, in our safe community, that "it won't happen here." But, although the Targets of the world have a broader footprint, your business has no less of a bull's eye on its back for hackers. It is said that there are two types of companies: those that have been hacked and those that will be hacked. Just as you insure the brick and mortar components of your business, make sure you have a policy that is sufficient to cover business interruption or large- scale incidents. Imagine a property insurance policy that covered fire damage—but only if the fire were started by a strike of lightning, and not by intentional arson with a match. Cybersecurity insurance policies can have similar nuances. Always ask for more than one policy to consider when shopping for cybersecurity insurance.

As with any legal issue, an ounce of prevention is worth a pound of cure. Help your employees understand the cybersecurity issues facing your business and you may prevent major problems. But have a good insurance policy in place because odds are you'll need a cure. Make sure you have a lawyer or technical expert help you decode the terminology and what events may be covered.

Want to learn more about cybersecurity and training points for your employees? Attend Woods Rogers Labor & Employment Seminar in Lynchburg on Tuesday, October 2, 2018. For more information visit www.woodsrogers.com and click on News + Seminars. LB

Beth Burgin Waller is chair of the Cybersecurity Practice Group at Woods Rogers' Roanoke office. She advises clients on an array of technology-related issues including data breaches, privacy regulations, and intellectual property concerns.

R. Patrick Bolling is an associate at Woods Rogers Edmunds & Williams in Lynchburg and advises clients on corporate matters including cybersecurity and data privacy.