Reassessing Your Cyberinsurance Coverage

by Joshua Gold

Just when you thought it was safe to assume that cybersecurity breaches took a serious, but at least predictable path, along comes the Sony Pictures breach. This type of breach would seem to underscore virtually every concern a risk manager could have about the perils of data security. It is also safe to say that most are hoping that this sort of breach is not the new normal. Any breach that imperils or implicates (almost simultaneously) proprietary and intellectual property, employee personal information, sensitive management communications, reputation/goodwill, extortion, threats of bodily injury, and business income is "bad news." If hackers are now going to open up the playing field of targeted data beyond just the usual targets of customer credit card numbers, addresses and health-related data, then risk managers are going to need to re-prioritize certain protections (including insurance protection) that used to be a lot lower down on the to-do list.

While cyberinsurance coverage has been available for business income losses and reputational damage from a slew of different insurance companies over the past few years, that coverage, for the most part, was not nearly as coveted as class action privacy litigation coverage, breach notification costs or regulatory proceedings coverage. Now, the reality that a breach can imperil the very core of the policyholder's ability to continue business operations takes on much greater import for risk management objectives. Couple this new reality with a recent statement from an FBI agent that 90% of successful breaches aimed at the private sector were possibly preventable, and it is clear that risk managers have a lot of work on their plate.

Insurance coverage for technology-related insurance claims has been murky for a long time. This is certainly true under standard commercial insurance and even true under cyber stand-alone insurance policies. There is not a lot of uniformity of product and many of the insurance policies are confusing and densely written, making it hard to determine the scope of actual protection provided.

Accordingly, a regular review and tune-up, as necessary, of insurance coverage is always a good idea. A few things to be on the look-out for when working with your insurance broker:

1. Get the clearest and broadest coverage you can—some policy forms are noticeably worse than others in these respects.
2. Continuously monitor trends in computer hacks and data breaches. Remember that data breaches can still occur the old fashioned way with sensitive hard-copy documents being accessed, or they can occur in cutting-edge ways not currently imagined.
3. Business income coverage and reputational damage cybercoverage take on added importance in the wake of recent hacking events.
4. If you can afford better and more coverage, strongly consider purchasing it—it is a relatively good problem to have added coverage that the company never needs to invoke.
5. Resist efforts to include breach of contract exclusions in your coverage—these provisions should be obsolete in an era when so many policyholders do business these days pursuant to a contract (whether with customers, credit card companies, financial institutions, etc.). These exclusions are used all the time by certain insurance companies to challenge insurance claims. While some recent court decisions have curtailed this use, it is best not to have the fight in the first place.
6. Resist efforts to include exclusions, warranties, representations or "conditions" in insurance policies over the soundness or reasonableness of the policyholder's data security efforts/protocol. These types of insurance policy clauses are a recipe for disputes on potentially every security incident.
7. Keep your directors and officers (D&O) insurance program (primary, excess, Side A, etc.) clean from any cyber-related exclusions or sub limits. Management will be highly concerned with any argued "gap" in coverage should a cyberevent ensue and D&O coverage be contested on the basis of an exclusion or limitation for suits

where cyber may be the underlying cause or context of the claim.

8. Complete insurance applications carefully and gather information from other business units where necessary in answering questions.
9. Make sure your cyber-specific coverage protects losses involving mobile devices, home offices, data that is off-line at the time security is breached and devices that may not be owned by the policyholder.
10. Make sure that your cyber-specific coverage protects against losses where others manage, transmit or host data for your company.

With the rapid pace of electronic innovation, we have not seen all the twists and turns that a data breach can take and likely will not for the foreseeable future. A static assessment on data security risk management will not work in most instances. Be vigilant and adaptable with managing the security risk. Work with your colleagues in other departments to reduce risk where you can and secure the best insurance your company can afford to protect against losses in the event that your company gets hit despite its best efforts and intentions. ■

***Joshua Gold**, a shareholder in Anderson Kill's New York office and chair of Anderson Kill's Cyber Insurance Recovery Group. He regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property/casualty insurance coverage issues.*

RISK MANAGEMENT

Reprinted with permission from *Risk Management*.

www.rmmagazine.com