Responding to a Security Breach: Insurance?

By Barbara Reeves
December 11, 2015

It is an otherwise normal day until you, the General Counsel, receive a call from the CIO: "We have a cyber-security breach. We've identified some unusual activity and it appears that data has been sent out through unknown IPO addresses. We don't know all the details yet. At last month's tabletop session on security you reminded us to bring you into the loop as soon as we suspected a problem." She fills you in about the data that seems to have been hacked: 40,000 customer files and the entire IT system is sluggish and not responding in many locations.

Stage 1

You review the incident response plan that you put in place last month: (1) who to notify within the company, with their emergency contact information (CEO, CFO, CIO, all the other executives who will no doubt want to be part of the excitement); (2) who to notify outside the company, with their contact information – outside counsel, vendors, regulators, law enforcement, the press; (3) the state-by-state analysis of requirements for notifying persons whose data has been hacked, in the various jurisdictions in which you operate (or is it better just to notify everyone, following the most demanding state's requirements?); (4) your recently negotiated contract with a forensic investigation firm; (5) your recently negotiated contract with an outside call center and mail house to handle the calls and breach letters.

You exhale and call the CEO and CFO. You are prepared. Until the CFO asks: "What is our coverage for this?"

Coverage? As in insurance? Well of course, let me check.

You call Risk Management. Do we have cyber insurance? No, what our broker offered was very expensive and far from comprehensive, full of exclusions. We decided to rely on our existing policies

Stage 2

Moving on, you have someone review the company's insurance policies, using keywords like "cyber breach," "data breach" and "cyber attack" or "cyberattack" and "cyber security." The bad news is that those words don't produce a hit: no express coverage. The good news is that those words don't produce a hit: no express exclusion. Could there be coverage under your existing policies?

Does your errors and omissions policy provide coverage? Do you have technology errors and omissions coverage?

Turning to your commercial general liability (CGL) policy, do you have a named peril policy that lists "covered causes of loss" (and probably does not list cyber-attacks) or an "all risks" policy? Is this cyber breach likely to give rise to "bodily injury," "property damage," or "personal and advertising injury?"

Is your electronic data "tangible property" subject to damage? A standard form definition of "property damage" includes "physical injury to tangible property, including all resulting loss of use of that property" and "loss of use of tangible property that is not physically injured." Were your

This article originally published in ***InsideCounsel.com*** *and is reprinted with their permission.*

company's servers or hard drives damaged? What about loss of use of tangible property, loss of use of computers, servers, hard drives. Did the attack cause malfunctions of other equipment?

Is "electronic data" expressly exempt from the definition of "property damage" in your policies? Or is your policy covered under the ISO "Electronic Data Liability" Endorsement that adds "electronic data" back to the definition of "property damage"?

Do you have indemnity agreements that may be covered by your CGL policies? Examine your crime and fidelity policies, and contingent business interruption coverage. Does the theft of your data amount to a "publication" that violates a "right of privacy?" Does your directors and officers liability policy cover investigation costs for something like this?

Stage 3

Now that you have all the policies lined up, and a lot of unanswered questions, what is it for which you are going to need coverage? What are your likely losses, expenses and damages? Here is a list:

Information security forensics: Hire an independent information security forensics firm. Someone has to dive into what happened and your IT department is already overworked trying to respond to the breach, and may not recognize the hole in the system that allowed the attack, especially if your IT people designed or modified the system.

Public relations: When and how do you go public? Unless you have a large and skilled PR department, you'll need an expert to maneuver through the coming days. If you go public before you know the full extent of the breach, your statements may be inaccurate. If you wait too long, you will be criticized for delay.

Call centers: Yes, you have a call center, but it will be overwhelmed, and you do not need the additional bad customer relations that will come when calls are unanswered and people are left on hold for extended periods of time.

Notification of affected parties: A mail house will need to be retained to send out notification letters, and to process the returns. What do you do when the people you need to notify have outdated addresses?

Legal advice: Figuring out when to notify regulators, law enforcement and customers requires expertise, knowing the laws of many jurisdictions, and coordination.

Additional costs could include defense costs as there will be lawsuits; expert costs as they will be needed to rebuild your system and to defend lawsuits; as well as media liability and crisis management services. Can you coordinate all of these issues, or do you need help?

There will also be costs to re-create and re-secure your systems and data. Additionally, there will be a significant business interruption. Unless you have a backup dark website and computer system, your business will be down for a while.

Your company will also need to assess the misappropriation of the intellectual property, trade secrets and confidential business information. Also be sure to anticipate fines and penalties, as there may be state and federal privacy statutes to be considered.

Finally, it's become customary to offer complimentary credit monitoring services for your customers.

Conclusion

Cyber-attacks are becoming more frequent. Cyber insurance is a rapidly growing and evolving area of insurance today. Coverage for cyber-attacks under traditional insurance policies is likely to be curtailed as time passes, insurance companies insert exclusions when policies are renewed, and cyber insurance becomes more standard. This checklist of questions and issues is offered as a starting point. ●

Barbara Reeves, Esq.is an accomplished neutral in the area of health care disputes. She is widely respected for her impartiality, ability to identify critical issues quickly and focus efforts to resolve disputes. She can be reached at ***breeves@jamsadr.com****.*

This article originally published in ***InsideCounsel.com*** *and is reprinted with their permission.*

1.800.352.JAMS | www.jamsadr.com