Rendigs
ATTORNEYS AT LAW

Business Briefs
Legal Update

Donald C. Adams
Partner

Email: DCA@Rendigs.com
Direct: 513 381 9361
Fax: 513 381 9206

The Legal Repercussions of a Cyber Security Breach Part 3/3

This article is the third installment of a 3-part series on cyber security.
Read Part 1 here.
Read Part 2 here.

In addition to being unaware of the growing menace, many companies do not have the appropriate insurance coverages in place to deal with a cyber breach. It is estimated that only less than half have any coverage at all (*Insurance Journal Nov. 6, 2015*). In fact, insurance experts have characterized the cyberinsurance marketplace as the "Wild Wild West". Policies differ, policies from the same carrier differ, and the policies differ year to year. Trusted counsel and insurance experts should scrutinize if cyber attacks are covered and what services are paid for by the policy. Just because it happens online and it's connected with a computer does not mean that it's covered by what an insurer would consider a cyber –policy. It depends on the terms of the policy and not the mere buzz words of cyber or privacy liability insurance. There also may be exclusions dealing with the failure by the insured to implement requisite risk controls and procedures on a continual basis.

Adding to the confusion, is a coverage ruling by the federal court of appeals in Virginia that a commercial general liability policy(CGL) may cover a data breach. In a case involving the publication of private medical records on the internet, the court found that coverage included in a CGL for personal or advertising injury applied. The policy provided coverage for injuries arising from the "electronic publication of material that ... gives unreasonable publicity to a person's private life" ....or "electronic publication of material that... discloses

Rendigs, Fry, Kiely & Dennis, LLP
600 Vine Street, Suite 2650
Cincinnati, Ohio 45202

information about a person's private life." The U.S. Court ruling is at odds with at least two state court rulings in Connecticut and New York.

While the opinions in support of CGL policy coverage for data breach are encouraging, it is doubtful that the decision of fourth circuit will be the final say. Further, the damages in connection with a data breach are potentially so significant that chancing coverage in connection with an event could be devastating to almost any company from the standpoint of attorneys fees and expense alone, not to mention the potential damages to third parties, business interruption and notification costs. From this author's perspective, obtaining coverage that is certain is the appropriate way to go until there has been additional activity in the courts.

In looking at various policies there are some very strong coverages that leave no room for doubt. These policies provide coverage for liability to a third party for privacy and data breach. The policy should cover all defense costs and damages arising out of the same. The policy should cover regulatory costs and fines as well. In addition there should be coverage for business interruption and hacker theft. There should be coverage for cyber extortion, public relations expenses and expert fees to calculate the type and monetary range of the loss.

Exclusions of coverage should be limited. Recognized exclusions relate to intentional criminal or dishonest conduct of the insured. Bodily injury is a reasonable exclusion as well as pollution. Coverage will also be excluded if the insured fails to take reasonable precautions to protect its system. A common exclusion relates to terrorism, war and governmental acts. This exclusion causes some consternation because not all cyber threats are profit driven but relate to political gain in a terroristic fashion. These events are too close to call from a coverage perspective.

Where companies go from here involve multiple resources. Management needs to formulate and implement strategy. Information technology departments need to think about not only the scientific aspects of the dilemma but how to communicate those aspects to others within the company without an IT background. It has to be a team approach involving not only legal counsel but insurance coverage experts with an understanding of the cyber threat and the security and coverages needed to combat it.
Companies should remember that it's not a scenario of if you are going to get hacked, but when. It is imperative that policies, practices and coverages are intact to mitigate cyber risk.

Don Adams'*s practice focuses on civil litigation in the area of medical defense litigation, transportation, maritime and wrongful death and injury. He defends hospitals, corporations, nursing homes, and physicians. He counsels clients on risk management and quality assurance matters.*