DATA BREACH + NO INSURANCE + NO LEGAL COUNSEL = #LOSS

Hodgson Russ Publication
June 18, 2014

INTRODUCTION

Welcome to the new age! Data breaches are embedded in our lives – there is no escape. The costs to any company to operate a business without cyber liability insurance and legal counsel are astronomical. Is your company equipped with adequate reserves to fund a data breach? This article outlines the 2014 average costs of a data breach, the 2013 data breach reported claims to insurers, what a cyber liability policy covers, the types of claims being reported to insurance carriers, and why you need legal counsel.

Are you ready for the truth?

WHAT ARE THE COSTS OF A DATA BREACH?

Without any exaggeration, the costs of a data breach places a significant dent in the operating budget of a company. The risk of a negative figure on the balance sheet is inevitable unless a company has cyber liability insurance or a substantial cash reserve. The out-of-pocket cost to handle a data breach could jeopardize the solvency of a company. Proceed at your own peril.

These are the hard facts. In 2014, the costs of a data breach in the United States, as reported by the Ponemon Institute,[1] are:

- The average organization cost of a data breach is $5,850,000.
- The average detection and escalation costs are $417,700.
- The average notification costs are $509,237.
- The average post data breach costs are $1,599,996.
- The average lost business costs are $3,324,959.

These figures demonstrate that liability for a data breach will subject a company to unexpected costs and adversely affect operating costs, resulting in a loss of revenue. This does not include the tangential losses of market share loss and diminution of a brand, reputation, and client loyalty, which may exceed the actual damages from the data breach.

WHAT DOES CYBER INSURANCE COVER?

What does a cyber liability policy offer? Generally speaking, the term "data breach" means:

. . .the unauthorized taking, use of, or disclosure of personally identifiable information, in paper or electronic form, or information stores on a computer system, including but not limited to, charge, debit, and credit card information, banking, financial, and investment services account information, proprietary information, and personal, private, and confidential information.[2]

A cyber policy offers two types of coverage. The first type is third-party coverage usually for technology services and miscellaneous professional liability, technology products liability, privacy liability, network security liability, and media communications services liability.[3] The second type is first-party coverage for crisis management expense, regulatory fines and defense, business interruption, privacy notification costs, and extortion.[4] There are also coverage enhancements for early claim resolution incentive, soft hammer, contingent bodily injury and property damage, and punitive damages. The limits of liability vary and may be subject to deductibles or a self-insured retention, or even sub-limits.

Additional resources available to policyholders under a cyber policy may include:

- Breach coaching: law firm notification and remedy support in the event of a cyber breach
- Incident roadmap: post-incident response steps, breach consultation and team response
- Risk management tools: self-assessment and cyber risk management
- Learning center: articles, webinars, and white papers from today's top technology and legal experts
- News center: cyber risk and security resources from across the Internet
- eRisk resources: directory of external experts in prevention and response fields

Understanding the nuances and coverage afforded under a cyber liability policy can be daunting. Insurance coverage counsel can explain policy terms, limitations, and conditions, including but not limited to, exclusions, carve-outs, and the coverage defenses insurers rely on to disclaim coverage or reserve their rights under the policy.

WHAT TYPES OF CLAIMS ARE BEING REPORTED TO INSURANCE CARRIERS?

NetDiligence's "2013 Cyber Liability & Data Breach Insurance Claims, a Study of Actual Claims Payouts," provides some insight into the actual costs of claims. The key findings are:

- PII—personal identifiable information—was the most frequently exposed data (28.7 percent breaches), followed by PHI —personal health information—(27.2 percent of breaches).
- Lost/stolen laptop/devices were the most frequent cause of loss (20.7 percent), followed by hackers (18.6 percent).
- Health care was the sector most frequently breached (29.3 percent), followed by financial services (15.0 percent).
- Small-cap ($300M-$2B) and nano-cap ($100B) companies lost the most records (45.6 percent).
- The average number of records lost was 2.3 million.
- Claims submitted for this study ranged from $2,500 to $20 million. Typical claims, however, ranged from $25,000 to $400,000.
- The average claim payout was $954,253. Many claims in the dataset have not yet been paid. If *we assume that, at a minimum, the self-insured retention will be met, the average claim payout would be $3.5 million.*
- The average per-record costs was $6,790. *However, if NetDiligence excludes outliers (incidents with a low number of records exposed but extremely high payouts), the average per-record cost was $307.*

- The average cost for crisis services was $737,473.
- The average cost for legal defense was $574,984.
- The average cost for legal settlement was $258,099.

What should a company do with this information? Contact a broker and shop around for a quote on premiums. If any company believes it is immune from a data breach, think again!

WHY DOES A COMPANY NEED LEGAL COUNSEL?

As part of any risk-management program, a company should retain legal counsel in conjunction with purchasing a cyber liability policy. The benefit of legal counsel is to mitigate damages, ensure the proper preventative measures are in place in case of a data breach; ensure compliance with federal, state, and local law governing retention, accuracy, and access; and, overall, to minimize the risks if the company faces a data breach. Legal counsel also acts as a data breach coach to ensure the proper third-party vendors are contacted in the event of a breach. Legal counsel is also effective in interpreting a policy and negotiating the terms and conditions with the broker and the insurance company to limit the risk of a disclaimer or carve-outs in the policies. The most important reason to retain outside counsel is to ensure that the protection of the attorney-client privilege extends to communications about the breach.

CONCLUSION

The costs of a data breach are real. Do not fall under the false impression that your company is not susceptible to a data breach because you are a small or mid-cap company. If you are in possession of any type of personal identifiable information or your computers are hacked, your company is at risk. Rest assured that the costs of cyber insurance and legal counsel are far less expensive than the costs of a data breach. Preventative measures are the best defense against a data breach. Be ready!

Footnotes:

1 Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis," Benchmark research sponsored by IBM, Independently Conducted by Ponemon Institute LLC, May 2014.

2 See, XL Eclipse ProTM 2.0 Policy.

3 Id.

4 Id.