BARNES & THORNBURG LLP

Increasing Data Breach Costs Should Lead To A Review Of Insurance Policies And Vendor Contracts

May 8, 2014 | | Cyber Insurance, Data Breach, Privacy, Policyholder Protection

Scott N. Godes
Partner
Data Security and
Privacy Co-Chair

cybersecurity - motherboard and lockThe Ponemon Institute has released its 2014 Cost of Data Breach Study: Global Analysis. The Ponemon 2014 study, (additional registration is required), offers fascinating insights into the changing world of data breaches, data security, data privacy and cybersecurity incidents. The report is dated as of the year of publication (May 2014), with the majority of incidents that were evaluated having taken place in 2013.[1] One fact in the report that likely will make the most headlines, is that "the average total cost of a data breach for the companies participating in this research increased 15 percent to $3.5 million."[2] The report explains further that "[t]he average cost paid for each lost or stolen record containing sensitive and confidential information increased . . . to $145 . . . ."[3] US companies reportedly experience an average cost per record in a breach based on malicious or criminal attacks that is significantly higher, at $246 per compromised record.[4] Enterprises in the industry classification of "healthcare" had a per record cost of $359, the most expensive classification in the list.[5] What exactly does the cost per compromised record entail? The report explains:

> **How do you calculate the cost of data breach?** To calculate the average cost of data breach, we collect both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

Post data breach costs and lost business costs also are reported to be the highest in the US, with an average post data breach cost of $1,599,996, and average lost business costs of $3,324,959.[6] Could this average actually be significantly higher? Note that the study's average costs excludes large breaches:

> The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience. In order to be representative of the population of global organizations and draw conclusions from the research that can

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

RELATED TOPICS

cyber insurance
data breach
Data Privacy

> be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than approximately 100,000 compromised records in our analysis.[7]

What does all of this mean? One significant takeaway is that enterprises should continue to elevate cybersecurity and data privacy as risks that should be considered at the highest levels. That includes analyzing insurance, vendor contracts and being aware of other risk management techniques. Before starting with insurance, an introductory note should be made. Perhaps the most heartwarming point in the entire report relates to insurance, and with one paragraph, it eliminates the "sky is falling" proclamations made around the internet that people who buy insurance are less interested in security measures and reducing their overall risk of a cyber incident, thinking that insurance will cover it all. The Ponemon Report explains, with emphasis added:

> An interesting finding is the important role cyber insurance can play in not only managing the risk of a data breach but in improving the security posture of the company. **While it has been suggested that having insurance encourages companies to slack off on security, our research suggests the opposite.** Those companies with good security practices are more likely to purchase insurance.[8]

Continuing that good security practice, consider strongly a cyberinsurance policy (and tower above the primary policy). A well-written cyberinsurance policy should provide coverage against the costs of investigating and remediating a data breach, among other things. A good insurance broker who is familiar with the products offered by various insurance carriers, including endorsements that may be available, can be invaluable. If you are looking for 5 quick tips for buying cyberinsurance, read Scott Godes' article, "5 Tips For Reviewing And Buying Cyberinsurance." Beyond cyberinsurance, if facing a loss or a claim, think broadly about whether potential coverage for data breaches under other insurance policies, such as CGL and crime insurance policies. Keep in mind, however, that insurance carriers have been known to fight against providing coverage for cybersecurity-based claims under non-cyberinsurance policies. Finally, it is worth reviewing vendor contracts to determine whether there are clauses addressing risks relating to privacy, cybersecurity, data breaches, or other cyber risks. Review limitations on liability, indemnifications, and other clauses regarding responsibility closely, as those provisions could be crucial in the event of a data privacy incident. [1] Ponemon Institute 2014 Research Report at 1 n.1.↩ [2] Ponemon Institute 2014 Research Report at 1.↩ [3] Ponemon Institute 2014 Research Report at 1.↩ [4] Ponemon Institute 2014 Research Report at 2.↩ [5] Ponemon Institute 2014 Research Report at 7.↩ [6] Ponemon Institute 2014 Research Report at 16.↩ [7] Ponemon Institute 2014 Research Report at 3.↩ [8] Ponemon Institute 2014 Research Report at 22.↩