DHG | views

June 2019

Protect Your Business from a Cybersecurity Breach

RJ Sudlow, CEH, Pentest+, Manager | DHG IT Advisory

Julian Sylvestro, RPLU, Risk Advisor | Hylant

By the end of 2018, there were more than 2,000 confirmed breaches, with more than half of those breaches targeting small to middle-market sized businesses. In each of these cases, almost 30 percent were due to internal threat actors, with 76 percent of the attacks being financially motivated[1]. Within the first two weeks of 2019, Collection #1 revealed approximately 775 million records from various sources were made available for the public to download. A week later, 24 million more financial documents, including mortgage loans and bank statements, were hosted on a web server that did not require a password. It is now safe to say it is no longer a matter of if, but when, companies will experience a cybersecurity incident.

In 2018, the total cost associated with a breach in the U.S., of less than 100,000 records, increased from $7.35 million to $7.91 million. Additionally, the average size of U.S. breaches increased by 10.4 percent. Of studied countries, the U.S. has the highest average cost per record of $233[2].

Companies should examine their risk management practices and tolerance to allocate resources in order to reduce the potential costs and exposure to a data breach.

There are several areas that feed into calculating the total cost of a breach:

- Detection and Escalation Costs
- Notification Costs
- Post Breach Costs
- Lost Business Costs
- Regulatory Fines and Penalties
- Fraudulent Transactions

Similar to any insurance product, it is important for a company to have a firm understanding of loss-related costs covered by their insurance policy by reading the language of their individual policy. A cyber insurance policy should provide coverage for both first and third-party liability. First-party liability should include a breach coach (legal services), forensic investigations, public relations expenses incurred in response to the breach,

cost of notifications, cost to maintain a call center to respond to questions by affected individuals, credit monitoring, data recovery, cyber extortion demands and business interruption due to a system outage from the breach. Third-party liability should respond for suits from affected parties, as well as state, local, federal and foreign regulatory authorities.

One significant cost area where the cyber liability insurance industry has not fully matured is coverage of lost business costs. According to the Ponemon Institute, lost business costs is the single largest impact to cost factor associated with data breaches[3], in some cases reaching up to 50 percent. Some insurance carriers offer coverage in this area through a reputational damage endorsement, but it is critical that an organization understand the complexity involved in providing proof of loss.

Not all costs associated with a breach are fully insurable. Data protection regulations such as GDPR, CCPA and other government regulations could overshadow lost business cost as the largest cost factor. All regulatory fines and penalties have a varying degree of insurability, so it is paramount for companies to understand the privacy regulatory environment.

It is vital that an organization implement risk management processes and procedures to reduce its overall exposure. Significant cost-reducing actions to prevent a breach include the following: 1) create and test an incident response plan, 2) extensive use of encryption, and 3) engage a third-party vendor to perform network security assessments, IT risk assessments and system and organization controls (SOC) reports.

Understanding the risk factors that organizations face within the cybersecurity ecosystem is crucial to protect business and customer data. As costs associated with breaches continue to rise, measures taken to transfer risk and additional proactive approaches to cybersecurity will positively impact future returns on investments.

Authors

RJ Sudlow, CEH, Pentest+
Manager, DHG IT Advisory
itadvisory@dhg.com

DHG IT Advisory works with companies to manage technology risk while maintaining data integrity, protecting privacy and complying with regulations. From project management and regulatory compliance assistance to digital forensics and incident response, Dixon Hughes Goodman is equipped to meet your IT advisory needs that drive your business. To learn more about DHG IT Advisory, visit **dhg.com/itadvisory**.

Julian Sylvestro
Risk Advisor, Cyber Risk
julian.sylvestro@hylant.com

Hylant is one of the country's largest privately held insurance brokerages in the United States. Founded in 1935 and headquartered in Toledo, Ohio, we offer complete risk management services, employee benefits brokerage and consultation, loss control, healthcare management and insurance solutions for businesses and individuals locally, nationally and internationally. Learn more at **hylant.com**.

SOURCES

(1) Verizon DBIR

(2) Ponemon 2017 Cost of a Data Breach

(3) Ponemon 2018 Cost of a Data Breach (Part 4, Page 13)