Hiren Shah

Research Report #1 – Data Breach Incident Analysis & Report

Padgett-Beale Inc.

9/12/2021

Introduction

CyberOne Business and Casualty LTD, is Padgett Beale’s (PB) cyber insurance company. CyberOne has recently sent out an audit team to scan and analyze PB’s current security policies and procedures. “A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event.”(Tittel, 2016) CyberOne has concluded that Padgett Beale does not have specific plans in place to address the data breaches, hence, PB is not ready to effectively prevent a data breach. Due to PB’s existing security posture, CyberOne has decided not to renew PB’s cyber insurance coverage. In order for CyberOne to renew Padgett Beale’s cyber insurance policy, PB must meet certain requirements in terms of security posture. PB’s executive leadership team has established an internal task force to address these problems mitigate any potential security risks. Cyber insurances provide various coverages of insurance plans and it isn’t about whether the company will suffer from a data breach attack, but when. Insurance policyholders can access tools and resources, to help manage and mitigate cyber risk, for both pre and post data breaches (Travelers, 2019). This report will analyze the breach that occurred at the Marriot International and review the practices for PB data breach response policy.

Marriot International Hotel Data Breach

The Marriot International Hotel had one of the largest data breaches of all time, and this affected over 400 million customers. The breach began in 2014 and was discovered 4 years later (Nohe, para4). During this time of this specific network data breach, over 500 million guests used and made reservations using the breached system. These guests now potentially have stolen information. “For approximately 327 million of these guests, the information includes some combination of name, mailing addressess, phone number, email addresses, passport numbers, Starwood Preferred Guest (“SPG”) account information, date of birth, gender, arrival and departure information, reservation dates, and communication preferences.” (Nohe, 2019) The Marriott data breach has put people at risk from the following properties: W Hotels, Regis, Aloft Hotels, Design Hotels, Sheraton Hotels & Resorts, Westin Hotels, Element Hotels, Luxury Collection, Tribute Portfolio, Four Points by Sheraton, and Starwood Properties (Connor, 2020).

Court Findings Against Actions Marriot Should Have Taken

Marriot’s security posture before the data breach was terrible, in addition, their response to the data breach was even worse. Not only did it take over 4 years to identify the data breach, but it took them over 2 months to disclose this information to the public. According to the SEC, there are timeframes on which a company should disclose data breaches and it is possible that Marriott may have violated these protocols (Nohe, 2019). Although Marriot did have cybersecurity liability insurance during the time of the breach, Marriot did not know to what extent the insurance will cover losses related to all types of claims that are related to cyber-attacks. If Marriot had a better understanding of their existing cybersecurity insurance policy, they would be able to communicate professionally with customers. It is a good idea for all companies to have an Identify, Protect, Detect, Respond, and Recover plan to mitigate certain cyber threats that occur (Cybersecurity Basics).

Court Findings

As of March 2019, Marriot had incurred $28 million in expenses related to the breach. By May, the company had cut it’s losses to a mere $1 million because they had cybersecurity insurance. Fortunately, the insurance covered much of the initial costs associated with the crises (Fruhlinger, 2019). “The Media reports speculate that the hotel group has between $250 million and $350 million, of affirmative cyber insurance coverage” (Nohe, 2019). This maybe just the beginning, Fruhlinger expects the damages to be greater as more information is revealed. Marriott states they have $125 million of cyber insurance coverage, and was compensated $95 million for the recoveries (JLT, 2019).

Review of Best Practices and Recommendations

* **People**

PB should follow the General Data Protection Regulation (GDPR), which requires that all organizations disclose data breaches to the relevant authority within a 72 hour time frame of identifying the breach. If the data breach has stolen sensitive information then organizations should notify the authorities immediately (Strawbridge, 2020). A communication strategy should be implemented which would keep everyone informed of the current situation. Another solution would be to create a communications page in which users are allowed to keep up to date with data breach information and training for prevention. (Strawbridge, 2020).

* **Processes**

It is recommended that companies should have robust cybersecurity programs or defense that are structured according to FTC recommendations. “These recommendations include; assessment of current cybersecurity posture, proper training of personnel, and reducing data retention and collection” (Burke, 2019). Padgett Beale should adopt best data protection practices such as hiring competent service providers to manage their work and use in-depth defense. The company should employ a multilayered security approach coupled with “access control to prevent unauthorized access from the consumer end (Burke, 2019).”

* **Technologies**

The organization should evaluate all systems, to see how the breach occurred and what steps could have been taken to prevent future attacks. PB should implement a formidable defense by limiting the data retained and collected and minimizing publication of data collected and retained. The company should try and reduce any third-party applications installed by employees on workplace computers. The company should come up with a comprehensive data breach plan that involves technical specialists and legal counsel in case of a future data breach.

* **Policies**

Be able to identify the parties and leadership involved in case of a data breach is important. Next, document a proper response plan by securing all systems, data and network access. PB should implement a policy in which they need should disclose the any future data breaches immediately to the appropriate authority. A Policy should also be put in place where specialized cybersecurity teams, and lawyers can be identified to implement better cybersecurity practices within the organization (Strawbridge, 2020).

Conclusion

In conclusion, there is plenty Padgett Beale can learn from the Starwood hotel data breach. The need to have an effective cyber insurance and data breach policy set in place to mitigate risks and protect assets is critical to the company’s reputation. No matter how expensive and secured the cybersecurity posture is, it is important to note that you are not 100% secured from data breaches. PB’s number one concern is to protect the confidential information such as people, technologies, policies, and processes. So it is critical the PB follow the GDPR guidelines, communicate properly, adopt best practices for data protection, hire technological specialist and legal help, and evaluate all systems and networks involved.

Reference Page

Travelers. (2020). Cyber Liability Insurance: Travelers Insurance. Retrieved September 9th, 2020, from <https://www.travelers.com/cyber-insurance>

Cybersecurity Basics. (2020). NSIT FrameWork. Retrieved from <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf>

Nohe, P. (2019, May 8). Autopsying the Marriott Data Breach: This is why insurance matters. Retrieved September 10th, 2020, from <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/>

JLT. (2019, January 8). Marriott breach to test insurance response: Cyber. Retrieved September 11th, 2020, from <https://www.jlt.com/en-bh/insurance-risk/cyber-insurance/insights/marriott-breach-to-test-insurance-response>

Connor, Hayes. (2020). Marriott International Data Breach. Retrieved September 12th, 2020, from <https://www.hayesconnor.co.uk/marriott-data-breach/>

Strawbridge, G. (2020, January 9). Five Best Practices to Deal with a Data Breach. Retrieved September 12th, 2020, from <https://www.metacompliance.com/blog/five-best-practices-to-deal-with-a-data-breach/>

Burke, D. (2019). Cyber Insurance 101: The Basics of Cyber Coverage I Woodruff Sawyer. Retrieved September 14th , from <https://woodruffsawyer.com/cyber-liability/cyber-basics/>

Tittel, K. L. (2016, May 04). What is cyber insurance and why you need it. Retrieved from <https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html>

Cyber security basics. <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf>