Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

A Strategy to Get Started with a Cybersecurity Program: What would a Data Breach Cost you?

Patrick Rost prost@dopkins.com

Published February 3, 2021 – This is the latest in Dopkins series of Cybersecurity posts. These blogs will introduce various topics, related terms, importance of reviewing the topic and hopefully raise some questions you should be asking.

With an average cost of a data breach in the United States at a staggering $8.64 million in 2020, allocating a budget to identify and prevent a data breach are more critical than ever. Although the largest incidents make headlines, businesses of all size are subject to cyber threats. In this post we examine ways to mitigate your risk.

Read our other recent issues covering:

- **Working from Home (December/January 2020)**
- **Cybersecurity Awareness Training (November 2020)**
- **Data Backups (October 2020)**

There are many questions and concerns when reviewing your company's Cybersecurity plan and budget. One of them should always be "What would a data breach cost us?" Answering this question will help put your budget and efforts in perspective to make sure you are spending enough time and allocating enough budget to identify, prevent and, if needed, respond to a data breach.

Before looking into the costs, let's first define a data breach. A **data breach** is a security incident where information is intentionally or unintentionally accessed, stolen, or used by an unauthorized party. Note that it is considered a breach if information is **accessed** by an unauthorized party. This means when a user has access to your system, but never exfiltrates data, it is still a breach.

Let's start by breaking down the factors that contribute to the cost of a breach.

Lost Business Costs

Research performed by the Ponemon institute, an independent research company, and IBM (https://www.ibm.com/security/data-breach) found that in 2020 lost business accounted for nearly 40% of the average cost of a breach. Further:

- Customers lose faith in the company when they are notified of the breach or hear about it in the news and may look to end the business relationship.
- Potential customers will likely look to another company that they feel can protect their data better.

Time is Money: Costs related to identifying and containing the breach

The 2020 study also discovered that the average time it took to identify and contain a breach was 280 days. Responsiveness is definitely a contributing factor to recovery: companies who were able to contain in fewer than 200 days saved an average of $1 million. Also, note there will be additional costs such as attorneys' fees. You may also incur legal costs to pay settlements due to federal and state laws (Health

Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), NYS SHIELD Act, etc.) that regulate the disclosure of a breach and may require settlements to be paid. Business operating globally may face similar laws in other countries such as the European General Data Protection Regulation (GDPR) and United Kingdom's Data Protection Act (DPA). These laws typically add regulatory fines that are calculated per breached record as well as fines if they determine the proper protections were not in place.

Based on the Ponemon/IBM research, the average cost of a data breach globally in 2020 was $3.86 million in US funds. However, costs to United States based businesses faced the highest average cost at a staggering $8.64 million. Health care entities faced the highest industry average cost at $7.13 million. Unfortunately, recovery is not a fast process: approximately 40% of costs are incurred after the first year, 15% are incurred after the second year, and further costs extend beyond year two.

While the global average cost is $3.86 million, the cost of a breach also varies based on size of the company. Companies with fewer than 500 employees still face a staggering average cost of $2.35 million globally while companies with 5,001-10,000 employees have the highest average at $4.72 million globally.* **These statistics reflect that companies of all sizes can be breached and incur a large cost.** Even though smaller companies have lower averages, cyber criminals recognize the security controls may be easier targets to breach and remain at high risk of an incident.

What's causing the breaches?

The research by Ponemon and IBM also report on threat vectors responsible for breaches. They found that compromised credentials are both the most frequent and most costly threat vector, stressing the need for secure passwords. Following compromised credentials in frequency is cloud misconfiguration, vulnerability in third-party software, and phishing.

How do you prevent a breach?

In the scenario that a breach occurs there are several factors that can mitigate, or amplify, the cost.

Mitigating: Incident Response Testing is the leading mitigating factor, saving businesses an average of $295,267 during a breach. Other mitigating factors are Business Continuity Plans ($278,697 average savings), Employee Training ($238,019 average savings), and Encryption ($237,176 average savings).

Amplifying: Complex Security Systems were the leading amplifying factor, costing businesses an average of $291,870. Other amplifying factors are Cloud Migration ($267,469 average cost), Security Skills Shortage ($257,429 average cost), Compliance Failures ($255,626 average cost), and Remote Workforce ($136,974 average cost).

Ultimately, the best way to avoid these costs are to avoid a data breach altogether. But, in the event an incident occurs, your best recourse is to plan now to mitigate the factors and minimize the risks to your business.

If you would like to have a conversation and discuss ways to mitigate the risk of a breach contact Patrick Rost (prost@dopkins.com). Check out our STARTegy page for more information about our Strategy for Getting Started with Information Security.

See our previous blogs that cover topics relating to the above factors in mitigating/amplifying the cost of a breach: Data Backups, Cybersecurity Awareness Training, and Working From Home.

*(*Keep in mind that these numbers are all global averages that sit lower than the US average*.)