JUNE 12, 2019

BY: Dan Kiehl

It seems like every day in the news you read about another data breach. According to a study published by IBM, an organization has a 27 percent chance of suffering a breach of at least 1,000 records. There have been so many data breaches in the past several years that now it seems commonplace.

> "According to the Privacy Rights Clearinghouse, there have been 9,033 data breaches made public since 2005—and those are just breaches that were reported in the U.S. or affected U.S. consumers. Spread out over the last 14 years, that averages out to about 1.77 breaches a day. All told, there were at least 11.6 billion records lost in those breaches."

Many experts today believe that consumers are now suffering from "data breach fatigue." Instead of being outraged, consumers either feel despondent or apathetic—often choosing to not discuss it with their friends or family. If pressed, most consumers will say that they care; however, a recent study by the Ponemon Institute found that 32 percent of data breach victims took no action to protect their data after a breach, and 55 percent took no action to guard against identity theft. It's clear that our actions don't match our words when it comes to data breaches.

Given the relative apathy of consumers and the likelihood that all organizations will eventually become the victim of a breach, it's inevitable that businesses will choose to not dedicate an adequate amount of resources toward their cybersecurity programs. However, becoming the victim of a cybersecurity incident often results in the company having to pay substantial direct and indirect costs.

Costs to Consumers and Businesses

The costs of a significant data breach in the United States is astounding. According to the study published by IBM, the average cost of a breached record for a U.S. company was an astounding $233, and the average total cost of a data breach in the United States was nearly $8 million. These costs were demonstrated to an extraordinary degree in the 2017 Equifax breach of approximately 143 million records. Since that time, reports indicate that Equifax has paid a total of $439 million in costs, which include security upgrades, credit monitoring services, legal fees, as well as fines and settlements from scores of lawsuits.

Not only do organizations pay an exorbitant amount of direct costs as the result of a breach, but cybersecurity incidents can also affect an organization's bottom line through indirect costs. Before it was revealed that Yahoo! suffered a mega-breach of approximately 500 million accounts in 2013 and 2014, Yahoo! was set to be purchased by Verizon for

approximately $4.8 billion. After the breach, Verizon purchased Yahoo! for approximately $4.48 billion. This breach, which did not include sensitive information such as payment card or bank information, cost Yahoo! $350 million. Worse yet, this amount did not include costs related to legal fees, fines, breach notifications, and various corrective actions. Given the astronomical costs of a data breach, it's important to discuss some quick action items that companies can take to help them guard against such incidents.

Effective Strategies for Preventing Breaches

What can be done to protect your customers' information? While the answer is always going to be "adopt a best-practices information security program such what is stated in the NIST 800-53 framework," there are some immediate action items that can be undertaken to mitigate against the risk of being the victim of a material breach.

First, approximately 25 percent of data breaches are the result of well-meaning employee mistakes such a falling for a phishing scheme or inadvertently disclosing sensitive data. To guard against these mistakes, organizations should provide basic security awareness training to information system users, including managers, senior executives, and contractors as part of initial onboarding training. Companies should provide this training within 60 days of onboarding. The organization's workforce members should also be provided with refresher training on an annual basis.

Second, organizations should ensure that their patching practices are up to speed. Within the past couple of years, studies have shown that inadequate patching of information systems have been one of the main causes of data breaches. For new systems, the organization should ensure that the latest patches are installed on the systems so that those systems comply with the organization's hardened system configuration. For those systems that are considered critical, organizations should patch those systems within one month of that particular patch's release.

Finally, it's important to be aware of who is doing what within the information system. Companies should ensure that an audit logging mechanism is running on the information system and also that the mechanism cannot be disabled by users. This audit logging solution should log, among other things, all user access to the sensitive information environment as well as invalid access attempts. The logging mechanism should identify the user and record the type of event that was performed as well identify the affected data, component or resource. Logs should be reviewed daily, and when suspicious activity is discovered, the organization should address the incident according to the organization's incident response policy. Many incidents last for months or years due to administrators not actively monitoring the system activity on a daily basis. By monitoring the system activity, companies can greatly reduce the severity of the incident should it occur.

While cybersecurity incidents have become commonplace in today's information security landscape, the costs incurred by companies that have been breached have demonstrated the need for continued cybersecurity vigilance. By training their workforce, patching their systems, and monitoring the activity that takes place on the information system, companies can reduce the risk of an incident as well as lessen the severity should one occur.