WHAT IS THE FINANCIAL IMPACT OF A DATA BREACH?

magna5

www.magna5global.com 844.624.6255

According to a report from IBM and the Ponemon Institute, the average cost of a data breach in 2020 is $3.86 million. This is a 10% rise over the last five years. The average cost of each lost record has gone down slightly to $146 from $150 in 2019. Despite some of these declines in the overall cost, the biggest increasing divergence was between organizations that took effective cybersecurity precautions versus organizations that didn't properly prepare.

The study also stated that the odds of experiencing a security breach are as high as 1 in 4. The question then is not so much whether or not your company will be breached, but when. In the U.S. the cost of a data breach increased 5.3%, to $8.19 million on average. U.S. businesses experienced the most expensive data breaches due to their complex regulatory landscape.

"Data breaches and the implications associated continue to be an unfortunate reality for today's businesses," said Dr. Larry Ponemon, Chairman of the Ponemon Institute. "Year-over-year we see the tremendous cost burden that organizations face following a data breach. Details from the report illustrate factors that impact the cost of a data breach, and as part of an organization's overall security strategy, they should consider these factors as they determine overall security strategy and ongoing investments in technology and services." In order to understand the extent of the risk that can result from data breaches, it is important to take into account the full financial impact that these data breaches can have.

Recent Data Breaches in the Headlines

If these statistics aren't enough to scare you, just look at some of the past data breaches that have hit major organizations. For example, in October of 2013, a data breach affected at least 38 million Adobe customers. It was discovered that sensitive customer information was stolen including credit card information and passwords. As a result of this data breach, Adobe paid $1.1 million in legal fees and about $1 million to customers.

Another data breach incident happened at the Aetna insurance company last year in Ohio. The company began investigating a potential security issue on April 27th. On May 10, they determined that a data breach had occurred affecting 1,700 customers with personal information exposed such as name, Aetna member identification number, provider information and claim payment amount.

Equifax experienced a breach in 2017 that exposed sensitive data for as many as 143 million U.S. consumers. This security breach was undetected for a longer time than the credit bureau originally thought. Equifax claimed that it first learned of the breach on July 29. But according to the Mandiant Report, cybercriminals had been roaming undetected inside Equifax's network since March. Equifax didn't disclose the cyber attack until September. It took 141 days for Equifax to discover that they had been hacked.

It is not only large companies that experience data breaches though. According to a Verizon survey published in their 2017 Data Breach Investigations Report, 61% of the victims of breaches in 2016 were businesses with fewer than 1,000 employees. Experts say that small companies are being targeted more because they do not have the high level of security that big corporations do.

Why is the cost of a data breach so high? Below is a breakdown of common costs companies will face after a security breach.

Loss of Productivity, Downtime & Remediation

Preventative measures are no longer enough, it's also necessary to have the right detective tools and an incident response team for maximum protection against data breaches.

When an organization gets hit with a cyber-attack, downtime is inevitable and this always negatively impacts productivity. Most often, a company must shut down its systems, putting a halt to its business. This also causes serious revenue loss in most cases as well. If a business gets disrupted during busy season, the cost could affect more than half the company's annual income.

Downtime can lead to financial loss, reduced customer satisfaction and damage to a company's reputation. However, the faster the data breach can be identified and contained, the lower the cost will be. Companies that respond quickly to a data breach experience significantly fewer costs. According to the IBM Security and Ponemon research, it now takes a combined 280 days to identify and contain a breach. The report found that organizations that were able to detect and contain a breach and under 200 days spent on average $1.1 million less.

Loss of Data

Data loss alone can severely damage a company's business. Many times, businesses struggle to stay open after they experience the loss of sensitive and mission-critical information. This loss can significantly impact an organization's bottom line and brand reputation.

According to a survey of IT pros from over 300 organizations conducted by Barkly, Numbers: Must-Know Ransomware Statistics, less than half, 42%, of cyber-attack victims, were able to fully recover their data after a malicious event, even with backup. Common reasons for this are incomplete backup and recovery processes including unmonitored and failed backups, loss of accessible backup drives that were also encrypted and loss of between 1-24 hours of data from the last incremental backup snapshot.

The more records that are lost, the higher the cost of the data breach. According to IBM Security and the Ponemon Institute, the average total cost ranged from $1.9 million for incidents with less than 10,000 compromised records to $6.3 million for incidents with more than 50,000 compromised records.

Damaged Reputation & Loss of Customers

When a company experiences a cyber-attack or any kind of data loss they normally experience loss of reputation as well. When such situations occur, what matters the most is how quickly and efficiently a company can recover from a cyber-attack and be back up and running.

Another serious problem resulting from a data breach is loss of customers. The loss of less than 1% of an organization's customer base is equal to a total cost of $2.6 million on average; IBM Security and the Ponemon Institute research found. Among the industries with the highest churn are financial, health and the service industry.

High-profile data breaches are even more inclined to negatively impact consumer trust in major brands. In a survey of 2,000 adults across the U.S. by independent technology market research specialist, Vanson Bourne, Beyond the Bottom Line: The Real Cost of Data Breaches, 76% of consumers would be likely to move their business away from companies with a high record of data breaches and negligent data handling practices. Consumers are more willing to take legal action against companies if their personal information was stolen and could be used for criminal purposes.

After major data breaches, despite the efforts of organizations to provide free services or other compensation, the damaged reputation remains for a long time. Consumers expect companies to take security seriously, keep their personal information safe and make investments to prevent any cyber-attacks that could happen now or in the future.

Legal, Regulatory & Notification Costs

After a data breach, an organization can face costly fines and other legal charges. Data breaches can attract fines from the Federal Communications Commission, Federal Trade Commission, Health and Human Services, the Payment Card Industry Data Security Standard and other regulatory agencies.

Adobe, Target and Home Depot are just a few of the numerous organizations that have had class-action lawsuits filed against them because of a data breach. Some companies have had to pay upwards of $10 million to settle.

Most U.S. states require private and public sector entities to notify individuals of security breaches of information involving personally identifiable information. Federal regulations such as PCI, HIPAA and GDRP, also require disclosure to consumers whose data has been breached.

Legal, regulatory and notification costs can include:

- The engagement of outside experts to help determine all regulatory requirements and to help facilitate a response
- Extra postal expenditures
- The set-up of inbound communication lines
- Additional help desk activities
- Special investigative activities
- Remediation
- Legal expenditures
- Product discounts
- Investment in identity protection services
- Regulatory interventions

The United States spends the most on post data breach response versus other countries. According to a Dashlane blog, the average U.S. business paid $1.56 million in post data breach response costs.

5 Steps to Lower Data Breach Costs

While many organizations can't afford to pay the high price of a data breach, there are a few measures they can take to minimize the cost and impact of a data breach. Below is a list of 5 key considerations your organization should take to minimize data breach cost.

Implement a 24/7/365 Incident Response Team

An experienced team of security experts can help you identify and contain an attack faster and therefore, minimize costly downtime. They can also perform preventative tasks to harden your network for a tighter security posture to protect you now and in the future.

Detect Solutions for Quicker Response

The faster a company identifies, contains and removes the attacker's access to its critical information, the more successful it will be. Implementing a detection solution along with an incident response team, can help quicken your response time to an attack. An intuitive detection solution will include multiple security essentials (Intrusion Detection, SIEM, Behavioral Monitoring, etc.) in order to correlate attack information and achieve actionable data.

Prepare for a Crisis in Advance

Companies must have a risk plan in place to understand how to be effective and efficient in a crisis. Your security team should have a concrete plan in place that outlines the chain of command along with what steps need to be taken immediately following a crisis. Also, organizations should educate their employees on the security crisis plan and what information they can or cannot share publicly before a crisis occurs.

Keep Your Organization Compliant

When it comes to your organization's security, it is better to plan ahead. It is crucial for an organization to prevent compliance breaches with continuous monitoring of internet exposed systems, accurate risk assessments, vulnerability scans and verified remediation tactics. These processes will help an organization to know what assets are at risk and prevent any critical issues. When you are regularly fixing issues and maintaining compliance, you are able to avoid hefty regulation fines.

Perform Regular Backups

An organization must use a reliable data backup service to complete regular backups of their critical information. This will ensure the protection and availability of data at all times even in the face of human error, accidental deletion, stolen endpoints or ransomware. These backups should be stored in an off-site location that allows for a clear line to the recovery process.

"Having access to an internal or outsourced incident response team has been the top cost reducing factor for three years running," said Dr. Larry Ponemon, Chairman, The Ponemon Institute. "An incident response team typically accelerates the time frame in which security events can be contained, which is a significant factor in reducing the overall cost of a breach. Extensive use of encryption and employee training can also help reduce the cost."

If this all sounds like a tall order for your organization, consider working with an MSP like Magna5. We can perform all of these tasks for you in the most cost efficient and effective way possible.

About Magna5

Magna5 is a nationwide provider of network services, unified communications, infrastructure technology and managed services. By bringing together enterprise-class platforms from leading providers and a 24/7/365 Operations Center, Magna5 has the unique ability to leverage leading software, carrier diversity and customize solutions that drive value to customers and vendors alike.

In working with private and public businesses of all sizes, from government agencies to manufacturing organizations, small businesses and large-scale operations, we believe that focusing on the needs of our clients through a boutique approach to customer service is key. With more than two decades of experience in the telecommunications and managed services industry, we've acquired the experience to understand the needs of your organization, the changing landscape of providers and diverse technologies to deliver targeted, strategic solutions that make a difference.

Whether you need voice solutions, managed services, security services or are looking to move to cloud-based infrastructures, Magna5 helps your business make smart connections.

CONTACT US

Corporate Office
3001 Dallas Parkway, Suite 610
Frisco, Texas 75034
844.624.6255
www.magna5global.com