# 3 Big Examples of Cyber Attacks Against Major Business (And How You Can Protect Yours From Disaster)

World-renowned businesses are not safe from cyber attacks. In fact, in this presentation, we're going to take a look at three major businesses that have fallen victim to them. You might even recognize some of these brands. So, without further ado, let's get right to the list and provide you with these three examples and how you can protect your own business from cyber attacks as well.

## Target Data Breach

First, we'll take a look at a cyber attack in 2013 when Target's data was breached. At the time, it was one of the most significant breaches in history. Hackers found vulnerabilities in the company's point-of-sale systems and, as a result, were able to steal credit card and debit card information from well over 40 million customers. Target took a $202 million hit in financial losses, and many customers seemed to lose trust in the brand.

So, what does this mean for your business? If you use point-of-sale or similar systems, keep them updated with the latest security patches. Additionally, you should isolate different parts of your network to limit the spread of attacks. Finally, implement security tools that will promptly detect and respond to suspicious activities.

## Equifax Data Breach

The next data breach occurred in 2017 with Equifax, one of the largest credit reporting agencies in the world. Cybercriminals found a vulnerability in their web application, which led to the exposure of the personal information of over 150 million people. As a result, Equifax settled over $1.4 billion in fines and payments to those affected. Their reputation also suffered a major blow.

This is why every business needs to assess and address vulnerabilities in their computer systems as soon as possible, especially if you regularly use web applications. We must stress the importance of employee training to reduce the risk of human error, which accounts for 90% of cyber attacks. You should also take encryption seriously, especially when handling sensitive data.

## Sony Pictures Entertainment Hack

The final cyber attack we'll examine is the Sony Pictures Entertainment hack in 2014. The attack resulted in the leak of sensitive company information, including employee data, confidential emails, and unreleased movies. Many believe the attack was politically motivated, particularly by a foreign power opposed to the United States. Nonetheless, it cost the film company millions of dollars.

The lessons you need to learn and apply to your business include ensuring access controls are properly set up so employees can only access parts of the data, not everything that is stored. Additionally, it's important to implement regular backups to secure and update data, mitigating data loss during an attack. Lastly, consider implementing an incident response plan to take specific actions if a cyber attack occurs.

## Final Thoughts

Thank you for checking out this presentation. We hope you take the necessary measures to protect your business's computers from cyber attacks. These three major examples have shown the serious impact a cyber attack can leave behind. These were major, recognizable businesses that lost millions of dollars and the trust of many customers, among other damages. Do your part to maintain and preserve the trust of your customers by protecting the sensitive data in your computer systems that keep your business running.