10 Steps to Prevent a Data Breach

Thomas Noden

[Thomas Noden](https://blog.verif-y.com/author/thomas-noden)



In today’s data-driven world, data breaches are becoming more commonplace and can affect hundreds of millions, if not billions, of people at a time. As digital transformation has increased the sheer amount of data moving, [data privacy](https://blog.verif-y.com/2021/01/29/the-current-state-of-privacy) risks and the amount of data breaches have consequently risen due to attackers exploiting the data-dependencies of our daily lives.

The best way to protect against the cost associated with data breaches is to **prevent them**. However, before you can prevent a data breach, you need to understand them. Data breaches occur when cybercriminals access data and sensitive information. According to the [2021 Cost of a Data Breach Report by IBM](https://www.ibm.com/security/data-breach), the average total cost of a data breach has risen from $3.86 million in 2020, to $4.24 million in 2020, the highest average ever recorded in the 17 year history of the report. In addition to the fines associated with data breaches, there is also the incalculable damage to the organization’s reputation. This isn’t including the loss of time it takes to resolve the data breach.

**The 5 most common types of data breaches**

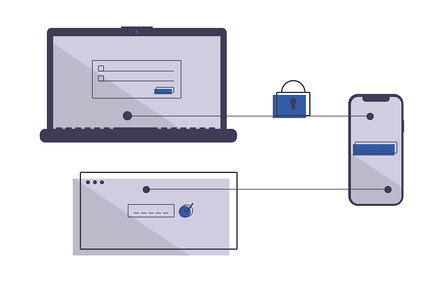
**Physical Breaches**

Stealing paperwork, laptops, phones, or storage devices. They could also access physical assets and copy them without anyone knowing they were accessed. This can also constitute as human error, the most common being if an employee/employer leaves sensitive information lying around/unprotected.

**Phishing Attacks**

Phishing attempts are rife in many organizations, which is when cybercriminals send malicious emails that look real in an effort to obtain access to sensitive data.

**Password Breaches**

Password breaches are probably the most common type of breach and happen far more frequently than you think. Many people have the same password for multiple accounts, as well as having an easily guessable password. This can be circumvented by updating passwords regularly, and to something less likely to be guessed. Alternatively, enable two-factor authentication, which will increase access security.

**Keystrokes**

Cybercriminals can insert, or email you, malware called keyloggers. This then enables them to record what you’re typing on your computer, relaying the information back to hackers to access your sensitive data.

**Ransomware**

Ransomware breaches a user’s device by notifying them that their account or system has been hacked, and their privacy is at risk. Hackers then often change the password or email address to deny access to the account. In order to secure the data again, the hackers will then ask for a monetary exchange. The more valuable the stored information is, the more money will be demanded.

**What Steps Can A Business Take to Prevent a Data Breach?**

Now that we understand the potential threats that can affect businesses, let’s delve deeper into the steps the avoid being caught out.

**Step #1:** *Develop a Strategy and Test It*

It’s important to have a strategic vision for your security strategy and develop a comprehensive plan. Often IT security teams react to issues instead of creating a proactive strategy that meets organizational risks levels.

**Step #2:** *Gain More Visibility into Your IT Environment*

To protect your organization from security threats, you need better network visibility and intelligence. In a constantly changing environment, it’s important to know what’s happening every day to remain aware, detect an issue, and subsequently prevent it from spreading.

**Step #3:** *Stay One Step Ahead of the Hackers*

A strong security posture is about continuously identifying, assessing, and remediating security risks and threats. You should prioritize your security threats. A risk is something you are not doing, and a threat is something that can exploit that risk.

**Step #4:** *Incident Management Tools*

Businesses need to be quicker in detecting and responding to threats. This can be achieved by using advanced cloud-native incident management tools (SIEM) and automated response solutions (SOAR), which restore normal service operation as quickly as possible and minimize the harmful impact on business to ensure the best quality of service.

**Step #5:** *Have, or contract, a Security Operations Centre (SOC)*

An SOC is a centralized unit that deals with security issues on an organizational and technical level. This can be done either in-house, or contracted out, to help monitor and manage security to reduce the risk of a breach. An SOC tracks user behaviour and looks for unusual activity using artificial intelligence and machine learning.

**Step #6:** *Make Cybersecurity a Board Priority*

Cybersecurity needs to be a board priority, and the company needs to know much how it will cost to mitigate security risks and how much a data breach could cost the organization.

**Step #7:** *Train Your Employees on Cybersecurity*

Schedule and conduct cybersecurity awareness training for all employees, including emphasis on potential pandemic impacts. Cybersecurity must come from the top and must be embraced by all employees to be effective.

**Step #8:** *Prepare for The Worst*

With hackers becoming more sophisticated and targeted, it’s important to protect your company from a ransomware attack and have systems in place.

**Step #9:** *Back Up Your Systems*

Ensure business continuity and disaster recovery plans are up to date and include specific procedures. Too often, leaders view High Availability and Disaster Recovery solutions as a “nice to have” not a “need to have.” That’s both unfortunate and risky.

**Step #10:** *Consider Outsourcing Your Security*

Research shows that companies who outsource endpoint protection have lower malware infection rates. It’s important to work with a partner who has a macro and micro view of cybersecurity.

*For more information on the best way to prevent a data hack of Personally Identifiable Information,*[click here.](https://www.verif-y.com/services/identity-verification/)