FORTRA

10 Data Security Worst Practices and How They Could Lead to Data Breaches

Introduction

Take it from us: for just about any organization, cybersecurity is challenging. The cyber threat landscape is evolving and growing more advanced by the day, and as your organization grows, you may find the number of attack vectors within your organization is growing, too.

Data loss as a result of a breach is the last thing you can afford, but with so much information available on how to best address your security vulnerabilities, it's understandably difficult to know where to start. Instead, we're going to take a different approach.

Take steps to avoid a disastrous data breach by exploring the following data security worst practices, understanding why they need to be avoided, and learning what you can do to better protect your sensitive data.

1 Not Establishing, Enforcing, and Updating Corporate Data Security Policies

Before allowing their employees to begin handling sensitive data, organizations must first ensure they've established a comprehensive set of corporate data security policies. The purposes of such policies are to standardize the handling of data throughout its entire lifecycle and create enforceable security rules and procedures for employees to follow. As an organization grows and the cyber threat landscape continues to change, these policies can be updated to accommodate for new vulnerabilities.

At its most basic level, corporate data security policies often include more stringent password management. But as these policies grow more intricate and specific, they can detail precisely how an organization's data is to be created, collected, stored, transferred, and disposed of. Creating and standardizing safe data security practices both on the employee and technology levels can help your organization to prevent a data breach before one ever occurs.

RELATED READING: Corporate Data Security Policy: What, Why, and How

2 Lack of Employee Awareness and Training

While creating corporate data security policies is certainly a great place to start to avoid costly data breaches, if your organization's employees aren't aware of those policies or properly trained to follow them, then you are still at a high risk of a data breach. In fact, Verizon's 2021 Data Breach Investigations Report found that 85% of breaches have a human component, and IBM's 2021 Cost of a Data Breach Report found that breaches caused by social engineering cost an average of $4.47 million. Other related attack vectors with a human element, such as a lost device, compromised credentials, and phishing attacks, can cost between $4.11 and $4.65 million on average.

Most employees are not trained cybersecurity experts, meaning awareness campaigns and proper employee training are paramount in preventing data breaches. By offering frequent, recurring training sessions, resources that outline data security protocols, and testing employees' susceptibility to attacks, organizations can be more certain their employees will more consistently follow corporate data security policies.

3 Not Properly Securing Your Organization's Remote Environment

By creating comprehensive data security policies for your organization and complementing those policies with employee training, you will already be on a good path toward securing your sensitive data. A newer problem has emerged as a result of the ongoing wave of digital transformation, though: unsecured remote work. A 2020 Malwarebytes Labs Report, which surveyed 200 IT and cybersecurity decision-makers, found that nearly 20% of organizations experienced a data breach as a result of a remote worker.

Training employees to follow proper data security protocols within the bounds of an office is not necessarily an easy task, and organizations are finding it even more difficult to secure employees' at-home offices. Common issues like the use of unsecured personal and/or mobile devices, accessing data through unsecured Wi-Fi networks, phishing and other malware, and unencrypted file sharing have become even more problematic with the shift to remote work. Each of these issues now requires specific attention when crafting your organization's security policies and training remote employees.

4 Misclassifying Your Organization's Data

If your organization has addressed the first three worst practices on this list, then they've already covered most of the bases to prevent a breach as a result of human error. What could be seen as one of the final steps in this effort, though, is to help deter the misclassification of your organization's data by opting for the use of data discovery and classification solutions.

Organizations are handling more data than they ever have before and because many of them are forced to comply with stringent data security laws and regulations like GDPR, PCI DSS, HIIPA, and others, it can be easy for an employee to mistakenly allow information protected under such regulations to slip through the cracks. The misclassification of data could result in a person or entity's sensitive information getting into the wrong hands, and for your organization, that could mean accruing liability and receiving hefty regulatory fines.

Data classification solutions can automate the process of identifying and labeling your organization's data, meaning employees will always know what kind of data they're handling, can determine who is authorized or unauthorized to see that data, and can avoid an accidental breach as a result of sending sensitive information to the wrong person.

RELATED READING:

DLP or Data Classification First?

5 Employing a Perimeter/Firewall-based Security Model

When thinking about the traditional concept of data security (and security in general), it's easy to think of a perimeter-based security model. Like how castles had moats and modern communities have gates, networks often have a firewall. But as business growth and digital transformation open more ports in organizations' firewalls, attack vectors increase along with the risk of a breach.

While including a firewall within a greater data security strategy is not necessarily a bad thing, organizations should instead opt for a zero-trust approach to data security. Rather than assuming a user attempting to access information is trustworthy, a zerotrust framework never assumes trust. Instead, this framework assumes anybody attempting to access an organization's sensitive information could be a bad actor or cybercriminal and that a breach may already be in progress.

6 Granting Full Network Access Upon Authorization

When an organization uses a perimeter-based security model, like a firewall, things can become particularly problematic when they also have what is known as a "flat network." In this case, once a user is granted access to an organization's network, they are essentially given access to the entire network and all of the data stored on it rather than individual network zones. If that user turns out to be a cybercriminal that gained access with stolen credentials, the extent of a data breach could be massive and catastrophic.

Rather than storing sensitive data in a flat network, a zerotrust framework allows organizations to segment their network and grant users the least amount of access possible. For example, an employee that works in your organization's marketing department should not necessarily be granted access to information only relevant to the organization's HR department, where personal identifiable information (PII) may be stored. By segmenting the network, that marketer (or anyone posing as them) will only be allowed access to access data relevant to them and their position in the organization.

7 Failing to Secure Your Organization's Cloud Ecosystem

Organizations are increasingly incorporating cloud solutions into their workflows and daily operations for the sake of ease of use. Such solutions eliminate the need for organizations to purchase hardware and software, speed up workflows, and make collaboration more efficient.

Oftentimes, organizations will use applications from public cloud providers like AWS, Microsoft Azure, and Google Cloud that come with security measures already embedded in their infrastructure. While this pre-existing security sometimes deters organizations from implementing cloud applications with security at the forefront of their minds, in reality, misconfigurations are precisely what can lead to a costly data breach. Ensuring your organization's cloud applications and overall cloud ecosystem are secure is key to helping the cloud work in your organization's favor rather than against it.

RELATED READING: Keeping Cloud Security Top Priority in Your Digital Transformation

8 Sending Unprotected Data to External Vendors

If you've already tackled everything on the list up to this point, then you've already taken several steps to address potential data breaches as a result of human error and inadequate network security. Perhaps by this point, you have decided to implement a data classification solution to examine your data, you've switched to a more secure zero-trust framework, and possibly even added a secure managed file transfer (MFT) solution to your workflows to securely send data to your partners and customers.

Regardless of how protected your data is when it's within the bounds of your organization, though, you may find that you lose control over its protection as soon as it's sent to an external vendor. Simply sending data to the wrong recipient can result in a breach if your data isn't wrapped in protection itself. This issue can be solved by layering a digital rights management (DRM) tool like Vera on top of your existing security measures, which allows organizations to have the highest level of visibility and control over their data no matter where it travels.

9 Failing to Adopt Modern Technologies

By now, you'll find that your organization is operating much more securely. Not only is your overall work environment more secure, but your organization's sensitive information is protected both on the application level and the data level. Even then, though, a common vulnerability that can slip through the cracks is outdated hardware and software.

According to Ivanti's 2021 Ransomware Spotlight Year End Report, 56% of older vulnerabilities that were discovered prior to 2021 continue to be exploited by ransomware groups, indicating that many organizations are failing to recognize and/or patch vulnerabilities in their systems.

Even when vulnerabilities are found in their systems, it isn't uncommon for organizations to maintain an "if it ain't broke, don't fix it" mindset, which can show itself in several different forms. Perhaps you and your organization use software that hasn't seen a security patch in years, or maybe you use old printers that aren't password-protected. Even if updating these technologies costs your organization some money upfront and causes a bit of a headache with its implementation, a data breach will almost certainly cost far more.

10 Not Monitoring Network Activity and Security at All Times

While regaining cybersecurity confidence is certainly a good thing, confidence should never be confused with invincibility. The cyber threat landscape is only becoming more and more advanced as time goes on and even the most secured systems can experience a breach.

While preventative measures are certainly important to reduce the risk of a breach before it ever happens, it is just as important to maintain good security hygiene by monitoringnetwork traffic and conducting regular security scans.

Turn Your Worst Practices into Best Practices with Fortra's Data Security Solutions

While it's true that we want to help you avoid these data security worst practices, we want to take things a step further.

Our data security solutions work to protect your data throughout its entire lifecycle, complement the various technologies you already use in your daily workflows, and remain flexible enough to grow and change with your organization.

To find which solutions will work best for you, read our Data Security Use Cases Guide for more information, and when you're ready, speak with one of our experts to help you get started.

Chat With Us

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

© Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

fta-corp-gd-1022-r1-79d