Understanding Data Privacy: Why it's Not Just for Big Companies

In 2019, over 100 million people had their personal information compromised by a hacker who exploited misconfigured AWS databases. This hacker, using a simple scanner, accessed open databases without proper authentication and managed to breach 30 organizations, including Capital One.

You might recall the 2019 Capital One breach, which exposed millions to potential financial harm. Capital One faced severe consequences, with an $80 million fine and an additional $190 million to settle customer lawsuits.

This incident highlighted the importance of cloud security for all kinds of businesses. No matter the size, losing $270 million is a big hit to any company. This event showed us that relying on default security settings isn’t enough. We must take a proactive approach to safeguard our data.[5]

Why Data Privacy is Important for Business Owners

Your business is your passion and your livelihood. You've invested so much time, effort, money, and heart into making it thrive, so it’s important to keep it safe. When people use your product or service, they need to trust that their personal information is safe.

Adopting strong data privacy practices not only helps you protect your business but also ensures you meet legal requirements, earn your customers' trust, and gain an edge over your competitors. Here are some key reasons why making data privacy a priority is a smart move for your company:

Legal compliance

Nobody wants to face a lawsuit, right? Data privacy helps you stay compliant with regulations and shields your business from potential legal trouble. If you ignore these requirements, you could face hefty fines and negative public attention. In some cases, you might even have to halt your data processing activities.[3]

Trust and reputation

Adobe found that seven out of ten consumers prefer to buy from brands they trust. Building that trust isn’t just about offering great service and a fantastic customer experience, it’s also about how you handle customer data. By creating a safe and transparent online environment, you not only enhance your customers' confidence but also add real value to your products and services. When customers feel secure and valued, they're more likely to stick around and choose your brand time and again.[1]

Competitive advantages

Many business owners don't realize how much value there is in prioritizing customer data privacy. When you show your customers that protecting their privacy is a top priority, it helps them feel a stronger emotional connection to your brand.

Think about it: if you bought something online and then found unexpected charges on your card, would you ever shop with that company again? Probably not! By making your customers' privacy a top priority, you build their trust and loyalty, which gives your company a real edge over the competition.[4]

Practical Steps for Implementing Data Privacy Measures

Accidents can happen, but it's up to you to do everything you can to ensure strong data privacy practices. It might feel like a big responsibility, and we totally get that! Don't worry, here are some practical steps to guide you through the process and make it a bit easier.

Choose a reliable service provider

It might seem like a no-brainer, but starting with the right provider is crucial for securing your data. When choosing one, look for features like secure data storage, encryption, and strong access controls. Also, make sure the provider follows the latest security standards and regulations. These steps are your first line of defense in keeping your data safe!

A few things you can do to ensure a service provider is reliable include:

- Review the privacy policy, security policy, and terms of agreement to see how the company handles and protects data. This information can usually be found on a company's website.
- Conduct a third-party risk review to request information about the service provider's security policies to thoroughly understand how data is protected. This review is typically more in-depth and done on an annual basis to ensure compliance of the service provider is properly maintained.

Understand your role in your security practices

When it comes to managing your data, it's important to know who's in charge of what. Usually, your cloud provider handles the security of the infrastructure, but you're responsible for keeping your data safe once it's on that infrastructure. Understanding your role and taking the right steps to protect your data is key to keeping everything secure.

Use file-level encryption

Many providers offer encryption for data both in transit and at rest, which is very convenient! But to boost your security even further, it's a good idea to consider adding extra file-level encryption as well. You can do this by encrypting your data before uploading it to cloud storage.

If that's not feasible, another option is to "shard" your data. This is where you split it up and store it in different locations. This way, even if hackers get access, it's much harder for them to piece everything together.[2]

Use strong credentials and authentication

Strong credential policies and tight access permissions are essential to keeping your company's data safe. Strict permissions ensure that users and apps can only access the data they actually need, while strong credential policies help prevent hackers from exploiting any permissions they might get.

Passwords are your first line of defense against unauthorized access, but they can still be compromised. That's where multi-factor authentication comes in. It adds an extra layer of security by requiring users to provide additional forms of verification, like a password plus a passcode. This makes it much harder for anyone to access your data without proper authorization.

Implement access control

Access controls help keep sensitive data in cloud services safe by limiting who can see and use it. The key is to follow the principle of least privilege, giving users only the minimum access they need to do their jobs. This way, you keep your data more secure and reduce the risk of unauthorized access.

Monitor cloud activity and security posture

Frequent monitoring is crucial to spot and stop unauthorized access to your data. Most cloud service providers offer monitoring tools that can alert you to any suspicious activity. It's also important to regularly check cloud logs and audit trails to catch any potential security threats early on.

Train your employees

As a business owner, it's up to you to make sure your team understands the security risks of storing data in cloud services. Providing regular training on best practices for data security and how to report any suspicious activity is key. Keeping everyone informed helps protect your data and strengthens your overall security.

How Cybersecurity Connection Can Help

Data privacy is a critical concern that goes beyond the boundaries of large corporations — it impacts individuals and small businesses alike. Personal information is becoming increasingly valuable, so protecting privacy is essential to avoid misuse and security breaches.

At Cybersecurity Connection, our assessment services can help you identify which data controls your security is lacking. We use this information to put together a priority list of which controls need to be remediated first. Additionally, if you lack data handling policies, we will also help develop those policies to fit your organizational needs and regulatory requirements.

Schedule a consultation with our team today and discover how we can transform your organization with cutting-edge solutions. Let’s transform your approach and lead the way to a stronger, more secure future.

References

1. Adobe (2021, November 4). *7 in 10 Customers Will Buy More from Brands They Trust; Abandon Those They Don't*. Adobe Experience Cloud Blog. Retrieved August 29, 2024, from https://business.adobe.com/uk/blog/perspectives/7-in-10-customers-will-buy-more-from-brands-they-trust-uk#:~:text=Customers%20buy%20more%20from%20brands,t%2C%20according%20to%20Adobe%20research
2. Cloudian (n.d.). *Data Protection in the Cloud: Challenges and Best Practices*. Retrieved August 29, 2024, from https://cloudian.com/guides/data-protection/data-protection-in-the-cloud-challenges-and-best-practices/
3. Cussol, E. (2023, September 1). *6 Reasons Why Data Privacy Is Important For Businesses*. Termly. Retrieved August 29, 2024, from https://termly.io/resources/articles/why-is-data-privacy-important/#why-is-data-privacy-important
4. DiSabito, A. (2022, October 18). *6 Ways to Make Data Privacy Your Competitive Advantage*. Validity. Retrieved August 29, 2024, from https://www.validity.com/blog/6-ways-to-make-data-privacy-your-competitive-advantage/
5. Seals, T. (2022, June 20). *Capital One Attacker Exploited Misconfigured AWS Databases*. Dark Reading. Retrieved August 29, 2024, from https://www.darkreading.com/cyberattacks-data-breaches/capital-one-attacker-exploited-misconfigured-aws-databases