State Privacy Office
March Privacy Tip

Best Practices to Improve Data Security

Day after day, security breaches in high-profile businesses all over the world are hitting the news. These attacks highlight the vulnerability of data and the lack of robust security strategies in organizations of all sizes. Your data security is vital to the overall well-being of your business. Your trade secrets, financial records and employee records all need protection. If compromised, you could suffer reputational and financial damages. There are steps you can take to ensure you don't become a headline.

1. Protect the data itself, not just the perimeter

Concentrating on securing the walls around your data seems to be the focus in many organizations, with almost 90% of security budgets spent on firewall technology. However, there are hundreds of potential ways to circumvent a firewall; including through customers, suppliers, and employees. All of these people have the ability to bypass exterior cyber-security and misuse sensitive data. For this reason, you need to ensure that your security efforts are focused on the data itself, not just the perimeter.

2. Pay attention to insider threats

It's easy to visualize threats originating from outside your organization, as these are often represented in news and television as the biggest and most costly ones. However, the reality is that it's your insiders that can potentially hurt you the most. Due to their nature, insider attacks can be difficult to detect and prevent. It can be as simple as an employee clicking on an email attachment they believe to have come from a trusted source and releasing a ransomware worm. These kinds of threats are the most prevalent across the world and the most costly.

3. Encrypt all devices

In today's world, more and more people are choosing to work on mobile or personal devices. How can you ensure that these devices are trustworthy? Make sure that all data is stored in an encrypted format and remains encrypted during migrations.

4. Testing your security

If you think installing an antivirus on every computer or device will protect your company from attacks, think again. As recent data breaches have shown, hiring a professional organization to conduct a security audit will always reveal weaknesses you weren't expecting. I encourage you to take a walk around your office and look at your employees' desks. I guarantee, if you look hard enough, you'll spot a password written down on a sticky note.

5. Delete redundant data

Many organizations deal with sensitive information as an essential part of their business; especially companies in healthcare, finance, the public sector and education. Ensuring information disposal mechanisms are in place helps prevent stale data from being forgotten about and stolen at a later date. Having a system for shredding, erasing or otherwise modifying redundant data to be indecipherable will go a long way to ensuring your employees don't stash it away.

6. Spending more money and time on Cyber-security

Many CIO's have admitted that spending more money and more time on data security is a must, as the lack of it continues to be the number one risk to your IT infrastructure. Many big companies with sensitive business data to protect are appointing chief security officers, often to board-level positions, with an acknowledgment that cybersecurity has to be an integral part of all business processes.

7. Establish strong passwords

Many organizations are still employing relaxed password policies, leading to simple, generic, and easy-to-hack passwords for critical accounts, which have access to the sensitive and valuable data. Implementing strong passwords is the first step you can take to strengthen your security in this area. Use reasonably complex passwords and change them at least every 90 days. Never use passwords like "12345" or "Admin1". Don't ever write down your passwords and leave them on your workstation for other people to find.

8. Update your programs regularly

Make sure your computer is properly patched and updated. This is often the best way to ensure its adequately protected. Your security applications are only as good as their most recent update. Since hackers and ransomware strains are constantly adapting to exploit weaknesses in earlier software versions, it is advisable to update these applications regularly.

9. Back up your data regularly

This should already be a crucial part of your IT security strategy. With secure backups in place, you can survive everything from accidental file deletion to a complete ransomware lockdown. As a security best practice, backup data should be stored in a secure, remote location away from your primary place of business.

10. Create a company-wide security mindset

Everyone who has a password and username is responsible for keeping data secure. IT administrators must periodically remind their managers and employees that they must not share logon information with any outside party. Data security is everyone's job and is not just limited to just a handful of employees in the IT team.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*