3 Cost-Effective Methods for Securing Business Data

In the wake of numerous security breaches targeting large and well-known holders of private data, information security has become a topic of great importance to both those whose data had been compromised, and those who fear that their data (or their customer's data) could be next.

When dealing with sensitive information it is crucial that the proper precautions are taken to keep it safe and secure. While there is no one, all-encompassing solution to prevent breaches, there are simple steps that can be taken to protect against any hacker attempting to extract data from company systems. If you are exploring cost-effective methods for securing business data, it's best to start with the basics:

1. **Update Whenever Available:** Although the frequent and persistent reminders to update our business applications can be irritating at times, there is good reason that these reminders are given. Many of the updates to major software systems are security patches, aimed at fixing potential exploits. Most cyber-attacks occur due to an exploit for which a patch has already been released. Updating these systems whenever a patch is available is a simple yet effective deterrent to the average hacker.

2. **Implement Best Practices and Controls:** A simple yet surprisingly common way for a hacker to gain access to private data is through a company account. Having any data compromised because of the negligence of an employee is bound to be an embarrassment, so implementing best practices and controls is a no-brainer. Proper email filtering and timed logouts after inactivity are two key controls that are often overlooked, and it is astounding when one realizes the number of companies that do not require strong password complexity and frequent password changes. Requiring password autofill to be disabled and training employees to be skeptical of unfamiliar and public email domains are also key in ensuring data security.

3. **Choosing the Right Systems:** When choosing systems and services that handle sensitive data, it is critical to account for the security of the system. There are several different ways data can be hosted. Hybrid cloud systems, which use both publicly hosted and privately hosted integrated solutions are surprisingly vulnerable. Privately hosted cloud document management systems, whether off site or locally hosted, are not nearly as vulnerable. Even more, publicly hosted cloud-based solutions are often the safest as many times they have the most security measures in place. When transferring your data,

these systems should always use an encrypted SSL, or safe socket layer. This will ensure that while the data is traveling, it is completely indecipherable, preventing anyone who attempts to capture it without the decryption key. Another staple is a web application firewall. This will prevent unauthorized uploads and downloads aimed at jeopardizing the security of the system.

Although many of these measures may seem minute, they are overlooked quite often. Your company's data is precious. Ensuring it is guarded against the majority of attacks is not only simple - it is necessary. Contact Square 9 today to learn how our cloud hosted Enterprise Content Management solution is designed to securely capture and control all of your business-critical information.

This blog article was written by **Sam Young**, Square 9 Marketing intern. Sam delivers highly effective blog content that supports Square 9's overall marketing goals and objectives. Beyond blogging, Sam uses his analytical skills to help Square 9 propel marketing efforts through in-depth reporting and research. To learn more visit www.square-9.com.