6 Sensible Cybersecurity Strategies

In today's economy, businesses cannot afford to operate without an online presence. On the other hand, the moment you expand your reach into "the cloud," even if you limit your digital activity to email and a simple website, your private data becomes a target for cyber criminals.

According to a report published by the Identity Theft Resource Center (ITRC) and CyberScout in January 2017, the number of reported data breaches in the United States rose from 780 in 2015 to a record high of 1,093 in 2016. In IBM's 11th annual Cost of Data Breach Study, the average consolidated total cost of a data breach in 2016 came to $4 million.

Underestimating the importance of cybersecurity can be financially devastating. Consequences can include lawsuits, server and website repair costs, increased public relations expenses, and loss of future business due to reduced confidence in your brand.

Fortunately, there are some simple, internal measures you can take that can significantly reduce your risk. Here are six simple strategies for protecting your confidential data that you can implement right away.

1: Put your cybersecurity in the hands of an expert.

This would seem to be a no-brainer, but you'd be surprised how many businesses blindly purchase security software that's not a good fit for their data or leave their security measures entirely up to an outside firm.

Mike Sentonas, vice president of technology strategy at CrowdStrike, said, "It's not always about buying the latest and greatest widget. Sometimes, it ends up there. But it shouldn't be the starting point."

Appointing a dedicated cybersecurity expert within your organization allows you to analyze your company's needs and establish protocols that fit the type of data you're protecting and the way in which you use the Internet. According to Sentonas, "Businesses need to first think about what assets they're trying to protect from cyber threats, as opposed to blindly buying the latest security products."

2: Emphasize cybersecurity as a key component of your culture.

Companies that handle cybersecurity matters behind closed doors may be inadvertently sending their employees the wrong message. Your staff needs to know that you take security seriously and that you consider employees to be a critical line of defense against data breaches.

Your cybersecurity expert can play a key role in emphasizing the need for security within your ranks. He or she can personally explain internal security measures to your staff and follow up to make sure they're abiding by established guidelines.

This hands-on approach both demonstrates to your employees that you take cybersecurity seriously and allows you to head off potential breaches before they'd ever reach an outside security firm's notice.

3: Train employees to uphold your cybersecurity measures.

A 2016 Gallup survey found that approximately half of all employees feel that they don't completely understand what's expected of them at work. One reason cybersecurity measures are often ineffective is a lack of clarity among the staff members who interact with your data on a daily basis.

Set up regular training initiatives with all employees that not only cover your company's security policies but share examples of cyber threats in the news.

Many individuals see hacking as a nebulous, "it can't happen to me" crime. Mike Buratowski, vice president of cybersecurity services at Fidelis Cybersecurity, pointed out that, "Although people don't need to be paranoid, they do need a healthy sense of awareness that cyberattacks are real and often involve hackers trying to exploit gullible victims. For example, employees are often quick to respond to email phishing schemes, thinking the message came from a legitimate source."

4: Protect yourself from accidental security breaches.

Don't leave things like password strength and email protocols to chance. In addition to regular training, make sure employees have written descriptions of their responsibilities when it comes to cybersecurity and establish consequences for violations.

Secure passwords

Although given enough time, most hackers can crack just about any password, the following tips will help make sure your employees' passwords are difficult to hack, which will encourage cyber criminals to move on to easier prey.

- Passwords should be reset every few weeks.
- Passwords should contain combinations of uppercase and lowercase letters, numbers, and symbols; administrative passwords should be particularly complex.
- Never set simple passwords like "Password01" or "Admin123." Hackers try these first because they frequently work.

Secure communications

If your employees interact with each other or with clients or vendors via cell phone, make sure the data those devices can access is restricted. It's also a good idea to have a policy in place that defines under what circumstances your IT department can access employee mobile devices for security purposes.

When it comes to email, use two-factor authentication to protect employee accounts. Two-factor authentication requires another step besides a password to access the account. This means that even if a hacker figures out an employee's password, he or she still can't get into your system without the second step – a fingerprint or a text to the employee's phone, for example.

Other steps you can take to protect information shared via email are encryption and expiration dates.

With encryption, even if your email account is compromised, the hacker will be unable to read anything he or she finds there. Expiration dates automatically delete emails after a designated time period, ensuring that information you've sent outside of your network is less likely to be found by criminals who manage to hack into the recipient's account.

5: Protect yourself from deliberate security breaches.

Although you'd like to assume that all security breaches are the work of wily criminals hacking away in far-off basements, 55 percent of cyber attacks are inside jobs.

Make sure only those employees who require access to sensitive data to do their jobs have access to it and audit employee activities regularly to confirm compliance with security regulations.

Additionally, make sure your IT department is prepared to immediately revoke access to accounts and data when an individual leaves your employ or if anything suspicious comes up during one of their audits.

6: Keep multiple, secure backups of your data.

One tactic cyber criminals use to leverage their access to your data is called “cyber blackmail.” In this strategy, hackers remove your data from your servers and then demand a monetary ransom to get it back.

You should always back up your data in multiple locations, at least one of which should be separate from your internal hardware.

While this won’t protect you from the other consequences of a security breach, if you back up your data in multiple locations, you’re less likely to find yourself in a situation in which a devious third party has the only copy.

Conclusion

Cyber attacks are a real threat to businesses of all sizes, and failure to take cybersecurity seriously can be a costly mistake. Fortunately, not all security measures need to be complicated. The six simple strategies listed above can serve as a first line of defense in your efforts to protect your company from cyber criminals, and they require nothing but your commitment to better security to implement.

###