How to Create a Cybersecurity Policy for Your Organization

Tags: cybersecurity, security policy | Categories: File Security

The cyberattacks and data breaches that make the news are usually the ones that happen at big corporations like TJX or Home Depot. But every organization, large or small, needs to be concerned about cybersecurity.

According to Symantec's 2016 Internet Security Threat Report, 43 percent of cyberattacks in 2015 targeted small businesses—up from just 18 percent in 2011. Hackers might be starting to understand that even though small and mid-sized businesses may not have as much valuable information available to steal, they are also less likely than their large counterparts to have strong security measures in place.

An attack is usually devastating to a small company. The U.S. National Cyber Security Alliance found that 60 percent of small companies are unable to sustain their businesses over six months after a cyberattack. If you don't want your organization to be put out of business by a hacker, it's time to improve your security posture. The first thing to do is develop something that most of the big companies already have: a cybersecurity policy. Here's how:

Step One: Secure Senior Management Buy-in

If you're in IT, you could probably tell most of your fellow employees a thing or two about security best practices. But in order to have the resources to design the policy and the authority to enforce it, you need management on your side.

It may help to point out that if you don't have a cybersecurity policy, it could open you up to legal liability. For example, if you don't want your employees connecting to your network with their own devices but you haven't told them not to, what happens when an employee's device with corporate data stored on it is lost? Your first reaction may be to remotely wipe the device—but can you legally do that without a written and user-acknowledged policy?

Step Two: Determine Your Security Guidelines

A key reason you need a policy in the first place is that modern cybersecurity has gotten very complex. There are a lot of details to keep track of, even for a small organization, and the landscape is constantly changing as both cybersecurity technology and cyber criminals become more advanced. Only you know your organization's unique needs, but some things you might want to keep in mind include:

- Which industry regulations do you need to comply with?
- What data do you need to protect and how should it be stored and transferred?
- What business software needs to be maintained and updated to stay secure?
- What do you expect of all employees in terms of choosing passwords, appropriate internet use, remote network access, email guidelines, etc.?
- Who will manage and maintain the cybersecurity policy?
- How will you enforce the guidelines (what is the penalty for willful non-compliance)?

Once you have these questions answered, you should be able to draft your company's policy. Depending on your current situation, understanding your security needs could be easy or could require extensive auditing of your current assets and tools.

We've compiled a few resources that provide templates and examples of cybersecurity policies below.

- General, Network, Server and Application Security Policy Templates (SANS.org)
- Computer & Internet, Physical Security, Privacy, Planning & Procedure Templates (CSO)
- Cyber Security Planning Guide (FCC)
- 10 Top Downloadable Security Policies (ITBusinessEdge)

Step Three: Educate Your Employees

Did you know that internal actors are responsible for 43 percent of data loss? Half of this is intentional—disgruntled or opportunistic employees, contractors, or suppliers performing deliberate acts of data theft. But half of it is simply negligence. Employees don't want to change their password every month if they can stick with "password123" forever. Some of them probably don't see the problem downloading the attachment from that suspicious "urgent" email.

Communicate your new cybersecurity policy to employees, and make sure they understand the relevant details: what they are expected to do, how to do it, and what could happen if they don't. Remember that things that seem obvious to you—like how to change that password—might not be known to everyone in the company.

Some organizations regularly test their employees on their cybersecurity knowledge. Make it fun and rewarding—there should be some kind of incentive for mastering security best practices.

Step Four: Monitor and Update Your Policy

Now your cybersecurity policy is up and running! But that doesn't mean the work is over. A cybersecurity policy is a living document that needs to be updated regularly to include changes in your business, in technology, and in compliance regulations. Set a timeline for when you will re-evaluate the policy.

You'll also need to determine how you will self-audit along the way. How will you know if the latest updates to your security software have been installed or that no one changed the server settings a month ago? Ideally, maintaining compliance with your policy will not be a fully manual process.

Bonus Step: Choose Solutions that Complement Your Cybersecurity Policy

Maintaining security and compliance across your entire business and all your employees can be daunting. Fortunately, dealing with all those moving parts doesn't have to be so complicated. Implementing the right software solutions can mean that your security policy practically enforces itself.

For example, you may be checking systems manually that could be monitored automatically. And if you expect employees to update their passwords regularly, what's easier—checking if they have done it on their own or using software that requires it? Software with role-based security and audit logging will ensure that you always know who accessed or changed what, and when they did it.

Ideally, any solution you choose to implement should come from a vendor that you trust to keep the software updated to match current security threats. Needing to replace your security tools or update custom scripts makes it much more difficult to keep compliant with your own policy.

Sometimes despite your best efforts, your data is breached. Check out these resources to help you create a data breach response plan.

Latest Posts

Discover Managed File Transfer at RSA Conference 2018
March 26, 2018
Are you thinking about heading to the 2018 RSA Conference in San Francisco? GoAnywhere MFT will be exhibiting and sharing information about our secure managed file transfer solution, in addition to...

On-Premises and the Cloud: A Comparison of Two Unique Environments
March 20, 2018
On-premises. The cloud. Hybrid environments. As technology evolves and business needs grow, organizations are rapidly trying to make sense of their options. What are the benefits of running their...

The Ultimate Guide to Investing in Secure File Transfer Software
March 13, 2018
It comes as no surprise—file transfers are a critical part of each organization's operations. They can share anywhere from dozens to hundreds of thousands of documents with trading...

What You Need to Know to Prepare for GDPR Compliance
March 6, 2018
Now that we've crossed into 2018, the GDPR is only months away. Less than three months, in fact—the new EU General Data Protection Regulation becomes enforceable worldwide for any...

On the Road Again: Where to find GoAnywhere this Spring
February 28, 2018
On the road again Goin' places that I've never been Seein' things that I may never see again And I can't wait to get on the road again. Is anyone else itching to follow in Willie Nelson's...

Add a Comment

Name:

Email:

Website:

Notify of New Replies:

Add a new comment:

Post

Allowed tags: <b><i>
