5 Elements of a Strong Cybersecurity Policy

THE BEST WAY TO ENSURE VALUABLE INFORMATION IS BEING PROTECTED IS BY HAVING A SOLID CYBERSECURITY POLICY.

For any company in the digital age, cybersecurity is an obvious area of concern. If your company holds any kind of sensitive or otherwise valuable information — such as identity documents, personal records or financial information — about your employees, clients or customers, these elements must be safely under lock and key, protected by responsible people.

The best way to ensure valuable information is being protected is by having a solid cybersecurity policy. This is really the first step to making sure your company abides by national and international compliance laws, and is a trustworthy and safe place to store and handle data. The following are foundational tips that will help you develop a strong cyber security policy.

Know Thyself

There are plenty of standardized, off-the-shelf cybersecurity products that anyone can buy and implement to protect their company's assets, but chances are those products will not fill the gaps you have. Security issues are different for every company, so it's important to get to know your own security potential and challenges in order to fully protect your company.

When writing a security policy, it's important to involve both IT professionals and management, so that all aspects of the company factor into the decision-making process. Get to know the kind of information your company manages, which types of information need to be private, and who needs access to what. Policies can be based on industry standard frameworks, but you should also try to fill these in with as much specific detail as you can.

Choose Infrastructure

Once you know more about your cybersecurity needs, you can start to decide on what systems to put in place. Different programs will be useful for different aspects of digital protection, so make sure your policy covers all aspects of your security matrix.

In the policy, be specific about which programs will be used and which aspects of your data will be protected. Look into potential updates to the programs to make sure the technology is current and the protection is as complete as possible. The more detailed you can be, the more prepared you will be for the worst-case scenario; for customers, it is encouraging to know that you have their security in mind.

ABC: Always Be Compliant

Depending on which industry your company operates in, there might be different laws related to data handling and security industry compliance. It's your responsibility to make sure your company's security policy abides completely by these standards, and that these standards inform the development of your policy.

Credit card information, government contracts, and medical information are three common types of data that must be handled with particular attention. For credit cards, you must be compliant with PCI (Payment Card Industry) standards; for medical information, it's HIPAA, or the Health Insurance Portability and Accountability Act; and for government contracts, security is regulated by the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR).

Responsibility and Accountability

In both infrastructure and compliance, the issue of designating responsible people is paramount. In any cybersecurity situation, whether it's daily maintenance or during an attack, it's important to know exactly who to contact and who is accountable, so this should be detailed in your policy.

Include contact information for responsible persons, so that staff, clients and customers have a direct line to the person with the most knowledge in times of a security crisis. Also make sure your policy accounts for contingencies, like listing deputies in case the key responsible person is away.

Don't Forget Your Employees

Since your company's employees are the ones handling information and dealing with your network on a daily basis, it's important to consider them when writing your security policy. It's important to analyze how employee actions could put the company at risk, and to include measures in the cybersecurity policy that safeguard against such risks.

Finally, be sure your employees understand best practices for password management and social media use, as these are the primary entryways for hackers and scammers. Include these practices in your policy, but also consider running workshops or meetings to ensure the message gets out to the staff in a meaningful, accountable way.