Self-Assessment: Cyber Security Planning

ENTERPRISE INTEGRATION

Creating an Information Security Plan begins with an honest look at the current state of your network. This baseline will form the basis of your ongoing work to develop a Data Security Plan.

Thinking about your current IT systems and policies, rank your organization's handling of each of these areas.

We can't find talented tech people who also fit our team

Your data and the systems that contain them should be encrypted when possible. Only users with a legitimate business need should be able to access these systems.

Your Score (1-5) ☐

Systems are Patched and Updated Regularly

Most system penetration occurs when cybercriminals exploit vulnerabilities that have already been fixed by the publishers. Your IT staff should be aware of software and firmware patches for every device on your network.

Your Score (1-5) ☐

Your Users are Aware of Social Engineering Attacks

Cybercriminals like to take advantage of the fact that unwitting employees are likely to err on the side of being helpful and providing access when asked. Your employees should receive regular training and guidance on recognizing and stopping this type of attack.

Your Score (1-5) ☐

You Have Cyber Insurance

Cyber Insurance can pay for damages and liability caused by your loss of data or service interruption due to a cyber-attack. To qualify for coverage, you will generally have to have a complete Data Security Plan in place.

Your Score (1-5) ☐

IT Risk Assessment is Complete

The first step to developing a Data Security Plan is to do a formal analysis of the IT assets. Then you will examine each possible threat to these assets and codify the likelihood of you being affected by these threats, along with the possible damage. This forms the basis of your risk factors.

Your Score (1-5) ☐

Data Security Policy is Developed

Based on the Risk Assessment, you will create a plan to eliminate or reduce each of the major risk factors that could affect your business.

Your Score (1-5) ☐

Data Security Policy is in Place

Your organization has taken the steps necessary to enact the Data Security Policy, including activities such as inventories and user training. You also have added or assigned people who are personally responsible for assuring that the policy is being followed.

Your Score (1-5) ☐

Users Have Been Educated on the Policy

The users, who can be both your best weapon and biggest vulnerability when it comes to cyber security, have been fully trained on the policy and they are able to follow it as part of their day-to-day work responsibilities.

Your Score (1-5) ☐

Your Self-Assessment Score

Under 15: You are at the beginning stages of a Data Security Plan and you will definitely benefit from obtaining some help to jumpstart your efforts.

16-25: You have some idea of the threats you face and how to combat them, but you haven't yet taken enough concrete steps in the right direction. Guidance and fresh perspective from an outside source will help considerably.

26-35: You are on your way to securing your IT systems. Following through on your plans will help you create a full Data Security Plan. Seek out some expert advice to hone the work you've already done.

36-40: You're already there. Some outside guidance on your annual review and improvement sessions will help make sure you have covered any new threats that arise.