P&N
Postlethwaite & Netterville

Cybersecurity Basics: 5 Things You Should Do Now

By Michael Richmond

Sometimes, you have to back up and consider the fundamentals before you get knee-deep in complex strategy and controls. Start-up companies, small family offices, non-profit organizations and companies that lack dedicated IT employees are particularly at risk of falling behind in basic cybersecurity practices. If your organization hasn't assessed its IT policy in a few years, or lacks much protection beyond an antivirus program that may or may not be up-to-date on every machine, you need to check off a few beginning cybersecurity tasks in the short-term.

Step 1: Take inventory

Account for every company desktop, laptop, mobile device, server, network, and cloud service—even those not currently in use. Knowing exactly what technology resources you have is the first step toward filling any security gaps.

Step 2: Ensure that security tools are up and running

Check each device and resource that you identified in Step 1. Does it have antivirus software, firewalls, and other security coverage installed? Has anything been turned off by a local admin? Has malware slipped in and disabled security features? Visibility is key when verifying that your security program works. You need to have confidence that the current security process you have are functioning the way you intended. Make sure every asset is protected by advance endpoint software and all applications and operating systems are patched with the most recent updates to resolve any known vulnerabilities.

Step 3: Audit user settings

Making sure that the right people have access to the right information (and that the wrong people do not) is a basic step toward securing your organization's data. Check every user account to ensure that periodic password changes are enforced, you are aware of any total-access administrator permissions, and that any accounts belonging to former employees are shut down.

Step 4: Establish and enforce your IT policy

If you don’t have an IT policy in writing, it’s time to create one. Are employees allowed to use personal devices for work? What information is okay to share publicly? What websites and apps are employees allowed to access? An IT policy sets expectations for employee behavior. Have you implemented the necessary technology to apply your policies? Enforcing your policy consistently throughout your organization is key to mitigating risks.

3-2-1 Backup Rule: *Maintain at least **three** total copies of your data. **Two** copies are local but on different devices, and at least **one** copy is saved off-site.*

Step 5: Backup, backup, backup

Regularly backup data from all computers so that if any one machine is compromised, important information is accessible. Consider copying your critical data to an off-site or cloud storage location and leverage the 3-2-1 rule. Backups should be performed automatically if possible, and should occur as often as needed considering how much data you can afford to lose in the event you need to rely on those backups.

What’s next?

Every organization has to start somewhere, but these five steps are just the beginning of a robust cybersecurity plan. Safeguarding your data and systems requires the right tools, training, and ongoing vigilance. Our Technology Services team can help you catch up to modern cybersecurity practices with IT policy assessment or creation, vulnerability and penetration testing, employee education, and ongoing threat monitoring. You don’t have to be a cybersecurity expert if you have the support and resources of an experienced partner.