DYOPATH
Driving Your Organization's PATH to IT Success

Three Top Cybersecuity Mistakes You Might be Making...

And what to do about them

There are two types of organizations in this world; those that have experienced a cyber attack and those that haven't....YET. The bad actors are really good; really good at being bad and they are getting better every single day. While there is not simply one big step you can take to ensure you're protected from every threat in the digital landscape, here are three mistakes organizations are making every day and tips to avoid them so you can stay safer.

1. Assuming You Won't Be Targeted

Because we see stories on a weekly, if not daily, basis about large organizations being compromised by cyber criminals, many smaller organizations feel as though they are too insignificant to be targeted. Unfortunately, nothing could be farther from the truth. In fact, according to Verizon's 2022 Data Breach Investigations Report, 46% of cyber-attacks are targeted at organizations with less than 1,000 employees. Attackers often focus their efforts on smaller organizations precisely because they often have weaker cyber postures.

If you are a small business, you might have neither the budget nor the resources to implement a SOC (Security Operations Center) or SIEM (Security Information Event Manager), but there are a few things you can do and not break the bank.

a. Install an anti-virus solution that will defend against most types of malware. There is a litany of these tools on the market like CrowdStrike, Norton, Kaspersky (paid) and Windows Defender, Avast, Bitdefender (free) to name a few.
b. Install a firewall either hardware- or software-based to provide an added layer of protection to your network from unauthorized users. Again, there are a multitude of vendors providing this technology like Cisco and Fortinet, et al.

2023 DYOPATH All Rights reserved. Reproduction is prohibited without written permission.
solutions@dyopath.com
1.866.609.PATH

2. Neglecting Employee Cyber-Awareness Training

Humans are the weakest link in any organization's cybersecurity defenses, it's just a fact. According to Trend Micro, 91% of successful breaches start focused on people. And, as social engineering attacks become increasingly refined, the weakness continues to be exploited.
Imagine every employee in your organization getting an email that states:
WIN $10,000 TODAY!!! Click HERE for $10,000!!!

How many of them would do it? Even if you have a relatively tech savvy team, it only takes ONE of them to click for $10,000 (even if they're just checking that it's NOT real 😕) to release whatever malware is buried in that link onto your network. And that is an example of just one of the multitude of ways bad actors are trying to leverage your end-users to gain access to your infrastructure.

There is no way to overstate how critical end-user cybersecurity awareness training is for organizations of all sizes. There are a number of organizations, like KnowBe4, who specialize in cyber awareness training/coaching. Whether you partner with a cyber training organization or do it yourself, here are a few steps you can take:

a. Train users to recognize, and how to defend against various social engineering schemes (phishing, baiting, etc.). Make this training compulsory!
b. Simulate attacks to see who bites.
c. Continue training for those who take that bait.

2023 DYOPATH All Rights reserved. Reproduction is prohibited without written permission.
solutions@dyopath.com
1.866.609.PATH

3. Failing to Regularly Update Software & Hardware

This is the least sexy of all the issues on this list, but it makes it no less real. Software vulnerabilities are a common way attackers gain access to organizations' systems. When a weakness is discovered, either by the manufacturer or by cybercriminals who launch zero-day attacks, manufacturers make the vulnerability public along with the patch to address the issue. When you don't update your software in a timely fashion, you leave yourself open to attacks that could have been easily prevented.

And that, my friends, is only half the battle. As software and operating systems continue to evolve to address ever-increasing cybersecurity threats, you must ensure your servers, laptops, desktops can support the latest versions of these programs. If your workforce is on-prem this can be manageable. While hybrid and mobile workforces present bigger challenges to keep hardware current, they also exponentially increase the importance of why it needs done; even if one old computer gets infected, your entire network could go down.

While it is easy to limp along on technology that's 'good enough,' it might cost you in the long run. Following are a few basic things you can do to alleviate this risk:

a. Implement a patch management practice in which you develop and religiously follow a repeatable cadence and process to discover, remediate, and document vulnerabilities and the patches applied to address them.
b. No matter how many other things you have to spend funds on, refresh your hardware at least every three years. Some experts recommend doing so every two years; you can determine what makes the most sense for you and your organization; just make sure you do it!

Cyber threats are going to get worse before they get better, so please use these tips to keep yourself, your people, and your organization protected. The work you are doing is too important to leave to chance!

Thank you for taking the time to download and read this guide. I know you are dealing with many things every day in your organization. Please know that I and my team at DYOPATH are sincerely here to help you with any IT related challenges you're facing.

Book an Exploratory Call with me and we'll spend some time uncovering your issues and determining if and how we can support you, your team, and your efforts.

2023 DYOPATH All Rights reserved. Reproduction is prohibited without written permission.