10 Simple Solutions

You Can Do To Improve Your Company's Cybersecurity Posture and Culture

Edafio
TECHNOLOGY PARTNERS

Contents

Cybersecurity is no longer an option. Businesses of all sizes are increasingly reliant on the Internet and information technology systems to run their business operations. With such a dependency on technology, there is an increased opportunity for malicious entities to take advantage of system vulnerabilities. Today, businesses are just one data breach away from making headline news, resulting in severe damage to the organization's valued reputation.

Security expertise is a foundational component of Edafio's managed services offering. The three pillars of Information Security (Confidentiality, Integrity, and Availability) are at the heart of daily life at Edafio. We realize security is an ongoing and ever-evolving endeavor, which requires a dedicated team of professionals working around the clock. Many Edafio clients partner with us through our Managed Services offering to leverage and incorporate our world-class security monitoring, interpretation, and remediation skills into every thread of their IT canvas.

Advocate a Security Culture

Employees aren't going to care about cybersecurity because you tell them to - they have to want to do it. Security needs to be seen as a state of mind that is everpresent. The best way to accomplish that is to weave it into company culture from the start. Remember that your staff - will look to their leadership to emulate how they should behave. Adopting a cybersecurity culture from the ground up helps businesses integrate this mindset from the outset.

Keep Applications & Operating Systems Up-to-Date

Cybercriminals do and they look for vulnerabilities in the security of programs and take advantage of these exposures to gain access to your device.
Once they have access, they can wreak havoc on your device by enabling a keylogger to track what you type, stealing confidential information, or worse yet, installing ransomware to lock you out of your files and demand payment for access. Software developers help prevent breaches like the examples listed above by fixing vulnerabilities as soon as possible. These fixes are included in software updates. Meaning, the sooner you install your update, the less likely your system is at risk for a cyberattack.

Restrict Admin Access

Access control is essential because it is a reliable security method to control who can access a particular file, equipment or device.
The ultimate purpose of access control is to provide a level of security that reduces risk to a company by helping to keep data, devices and people secure. It should be a fundamental part of every business. Without proper access control, you could leave your staff and your company vulnerable to problems such as data loss, theft or breach of privacy and data protection laws.

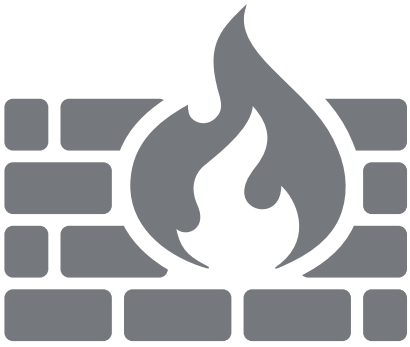
Maintain Current Back-Ups

The primary purpose of a data backup is to have a secure archive of your critical information, whether it is classified documents for your business or cherished photos, so that you can restore your device seamlessly and quickly in the event of data loss. Think of a data backup as the foundation of your digital disaster recovery plan. By maintaining current backup of your devices, you are already one step ahead of any cyber threats that might result in data loss.
Use the 3,2,1 Backup Rule:
Create three copies of your data...on at least two storage solutions...and store one of them in a remote location. 1. Back up regularly. 2. Opt for more storage. 3. Don't underestimate physical copies

Continuous Monitoring

The more complex technology becomes, the more vulnerabilities it has. As such, IT teams must confront and manage the growing security demands negated by ever-evolving digital ecosystems. Implementing continuous security monitoring (CSM) into cybersecurity plans is a logical defense technique and can transform a company's security stature.

Continuous monitoring refers to a threat intelligence technology that provides real-time visibility and feedback from an organization's digital ecosystem. This security method uses automated scanning to speed up remediation to protect your data from external threats. Databases, networks, applications, and servers across every industry can be compromised due to breaches and other cyber attacks. CSM provides a transformative resolution and is one of the most efficient and effective security tools available today.



Use Endpoint Detection & Response

Endpoints – the laptops, smartphones, and other devices we use daily – are a favorite target of cyber attackers. Endpoint Detection and Response (EDR) is one of the fastest-growing solutions aimed to provide deeper capabilities than traditional anti-virus and anti-malware solutions.

Companies today face a variety of cyber threats that traditional security products miss. Attackers have become highly proficient at outmaneuvering signature-based protections like anti-virus software. However, in contrast to other legacy solutions, EDR is most valuable during and after a breach. So, if a breach does occur, the capabilities offered by EDR greatly aid investigation and remediation efforts.

Keep Current on Emerging Cybersecurity Threats

If you want to win a battle, you have to know as much about your enemy as possible. Remaining secure in the digital age means learning to educate yourself about emerging cybersecurity threats -- ransomware is the main offender trending now, which can encrypt your hard drives and hold your data for ransom.

Consider setting aside time a few days a week to read articles to understand what's happened to others and use this knowledge to be better prepared. Google's Online Security Blog posts are reliable sources that report on general cyber industry observations to keep you in the know and are an excellent source of expert information.

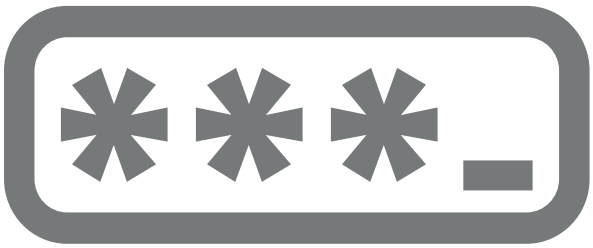
Mobile Device Encryption

With the rise in mobile devices, it makes sense that more companies are using their devices to process, store, and transmit data. But with the increased use of technology comes the increase in security issues. One common issue is stolen or lost devices. Suppose your business deals with a lot of mobile devices that carry critical data. In that case, it's a good idea to ensure none of that information falls into the wrong hands by implementing mobile device encryption.

One benefit of mobile device encryption is the sensitive information is protected. If a fully encrypted device falls into the wrong hands, the owner of the device can be sure that the data will not be used for unwanted purposes. Using mobile device encryption to secure your data correctly takes this extra step in security and protects yourself from liability.

Password Protect Your Wi-Fi Network

Mobile devices like smartphones or tablets present a security risk, given the flexibility of our modern lives. If employees can access their email, applications, or data with OneDrive or DropBox from their mobile devices, they must have a passcode. The passcode protects
information if the device falls into the wrong hands. You can even configure policies to erase the device after a certain number of incorrect attempts. It's healthy security hygiene to get in the habit of protecting all data, even if it means a bit of added work to unlock a phone or tablet.



Have a Strong Password Policy

By educating employees best password management practices is the a company's first line of defense against intruders. It is a constant endeavor to continuously improve and close holes in security and to ensure your users aren't one of them, we recommned users to:

- Log out of systems they're not using.
- Avoid writing down passwords
- Longer is Stronger: Take time and consider a strong/long password that they can remember.
- Multi-Factor Authentication
- Invest in a password manager

About Edafio

We pledge to offer you our very best. Fortunately for you, our best is the best there is.

Edafio helps to reduce risk and prepare your company against cyberattacks. It's no longer a question of whether or not you'll suffer a hacking attempt. It is now necessary to take a proactive mindset and approach.
With Edafio servicing your cybersecurity, you'll have the education, tools and people to prepare, react, and protect your - staff, assets, reputation and peace of mind.

One Team with Humility and Respect • Unquestionable Integrity • Committed to Client Success

We'd love to work with you

CONTACT US

edafio.com
info@edafio.com
501.221.4100