pointnorth networks, inc

3 Most Common Cyber Security Mistakes and How to Fix Them

www.pointnorth.net

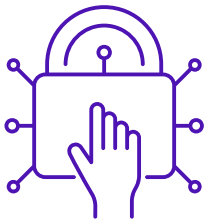
Cyber-attacks continue to grow, and small and medium businesses that don't properly secure their digital assets are exposing themselves. From business reputation or monetary loss, the cost of a cyber-security mistake is high. Ultimately the goal is to protect our confidentiality, privacy, and finances. Sometimes the means we use to protect our cyber-assets are more vulnerable than the data itself. Have you ever thought about the security mistakes you could be making but aren't able to recognize? Well, now is the time. Find out the 3 most common security mistakes you didn't know you were making and take steps to eliminate them today.

Mistake 1

Organizations do not properly secure their IT infrastructure. It is imperative to implement asst management systems, policies and procedures, and strong user authentication mechanisms.

Fix

- Conduct an audit of all technology solutions, user accounts, and roles. Repeat this process on a quarterly basis (at least).
- Disable accounts upon employee technology offboarding, or update permissions and access upon role change.
- Use a password manager to create strong, unique passwords per technology solution and enable multi- factor authentication (MFA) on the password manager. Do not allow storage of credentials in web browser.
- Enable MFA on all accounts, especially on email and cloud-based services.
- Monitor accounts for exposed credentials using free or commercial tools.
- Conduct phishing simulations and training campaigns for your staff.
- Avoid shared accounts. MFA is designed for a single user. As a result, it is difficult to manage on shared accounts.

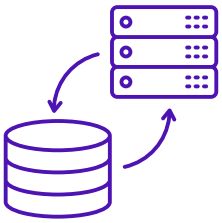


Mistake 2

When a breach occurs, many organizations are not properly covered financially. Cyber Security Insurance is an important component for recovering from a security incident.

Fix

- Invest in cybersecurity insurance, but do not publicize it.
- Understand prior acts, exclusions, and timelines for each of these policy areas.
- Run a ransomware attack tabletop scenario with your managed service provider and insurance carrier to understand the limits of coverage based on a real-world scenario.
- Extortion coverage should cover your business into the low to mid-six figures.
- Verify that the insurance carrier will pay for a preferred incident response and forensics provider, or become
- Verify that there are no wartime exclusions with your carrier.



Mistake 3

When you need to recover data from ransomware, backups are a crucial part of the recovery process. Unfortunately, some organizations find out too late that their data backups aren't up to date, or don't exist at all. Protection of backups is an important part of the recovery process.

Fix

- Act on your vendors' recommended guidance or best practices for the protection of your backup technology.
- Move away from shared login accounts on appliances and technology portals.
- Enable MFA on access to technology portals and appliances.
- Store copies of backups offsite, or in an isolated network or file share location that is inaccessible from servers or workstations, thus making backups harder to access, encrypt, or destroy.
- Monitor and alert for backup deletion. Some vendors offer "soft" delete so backups are not immediately removed. Understand your vendors' capabilities.
- Test your backups. Determine how long it takes to do a restore, and set accurate expectations should the need arise.


pointnorth
networks, inc