BlueCotton

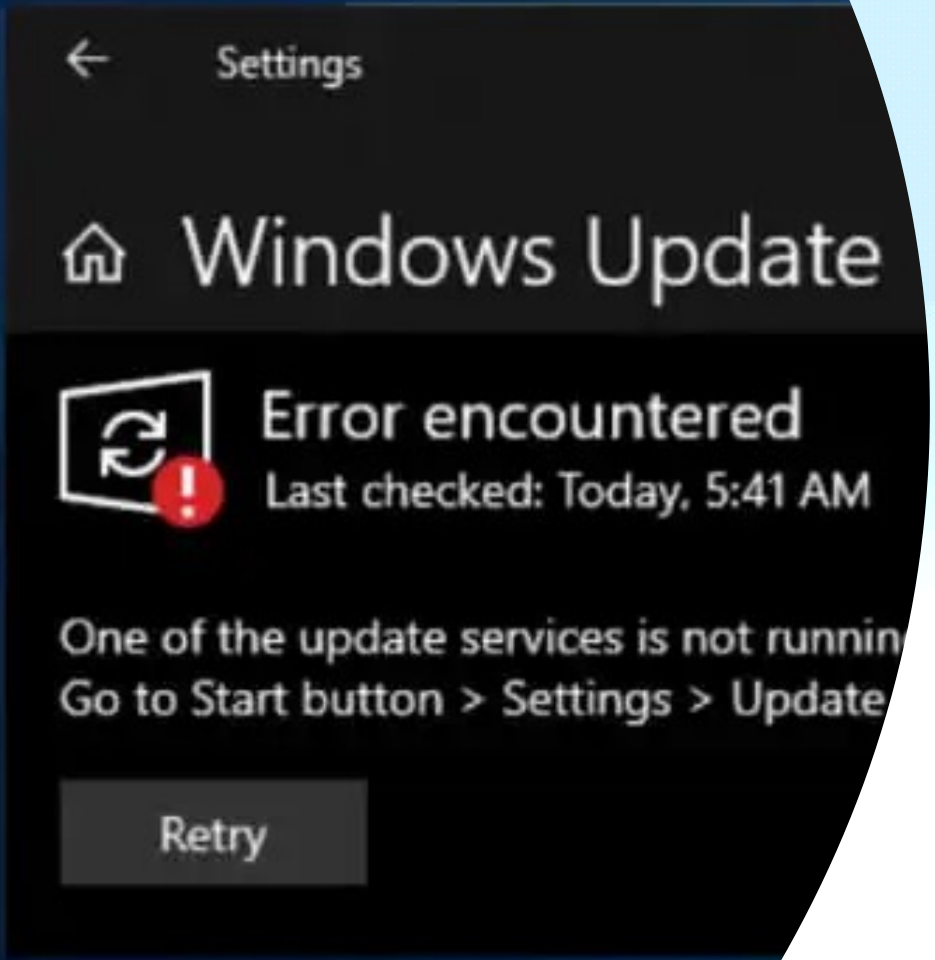
SMB 10-Step Cybersecurity Checklist

End-User Training

It's important to provide regular training to your employees on the latest trends within cyber security, so they can be more aware as they operate. Important things to cover includes phishing, password security, device security, and physical device security.

Employees need to know what potential cyber security breaches look like, how to protect confidential data and the importance of having strong passwords.

It's recommended to have organizational workshops with your company at least once every six months.



← Settings

Windows Update

Error encountered

Last checked: Today, 5:41 AM

One of the update services is not runnin

Go to Start button > Settings > Update

OS & Application Patches and Updates

The single most important—and simplest—action you can take is keeping your computers' applications and operating systems up to date with the latest security patches.

If your computers are still running on Windows XP, you are at risk: Microsoft stopped supporting this version of Windows long ago, and is no longer providing security updates.

If you do nothing else, at least update your systems with the latest versions and security patches

Strong Pa$$w@rd Policy

A password should be 16 characters or more; our password-related research has found that 45 percent of Americans use passwords of eight characters or less, which are not as secure as longer passwords.

Best Practices:

- A password should include a combination of letters, numbers, and characters.
- A password shouldn't be shared with any other account.
- A password shouldn't include any of the user's personal information like their address or phone number.
- A password shouldn't contain any consecutive letters or numbers.

Where possible, implement multi-factor authentication to further increase security.

Access Control Measures

Most users should not have administrative access to computers, networks, or applications. Limiting this access can prevent users from installing malware or accidentally turning off security measures.

Least privilege is the practice of preventing certain users from accessing certain computer processes and data by restricting their access. Typically, there are “super user” or “standard user” accounts which can define the roles that people can have.

Network Segmentation & Segregation

Your organization should have a network segmentation and segregation strategy in-place to limit the impact of an intrusion. It will ensure that the most sensitive and confidential data is not accessed.

Working with a security professional to create a secure network architecture is essential to ensure business continuity.

Staff Training

Humans are the weakest link in any security scheme.

Keep your staff vigilant with periodic training on your IT policies as well as how to spot cyber threats such as phishing.

Properly Configured Security

Layered security is implemented by having layers of security that provides different levels of protection. It's essential for your organization to use some type of layered security, such as a firewall to protect against cyber attacks.

As a best practice, it's important to have anti-virus/ malware software in place, a fire wall, and lastly an intrusion prevention system (IPS).

The implementation of layered security can be tricky, so it's best to engage with an expert before deployment.

Internal and External Vulnerability Scans

It's recommended to conduct internal and external vulnerability scans at least once a quarter to look for weaknesses in your system. The scans are implemented through a computer program to find any type of threats that could exist.

Internally these scans detect if there was harmful programs downloaded onto a computer. Or externally detect the strength of the network segmentation and segregation.

Data Backup

Regularly backing up your data to a secure, encrypted, and off-site location can aid in recovery from a cyberattack as well as other human and natural disasters.

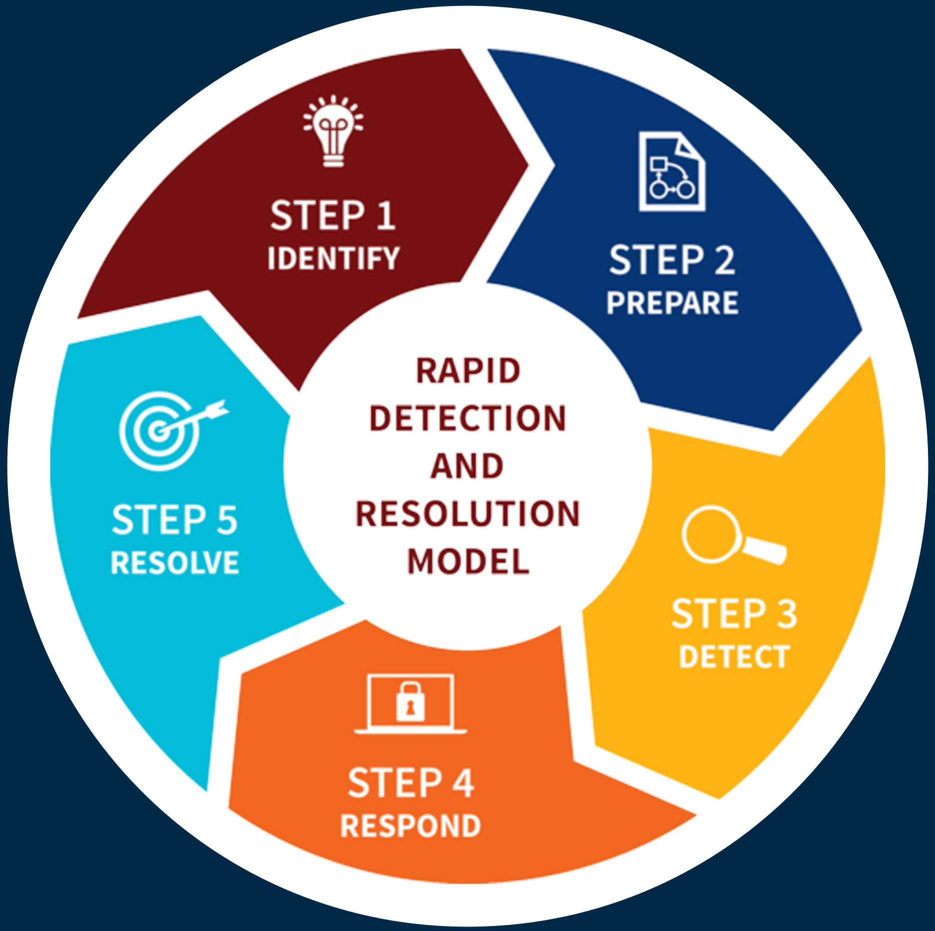
It's also essential for compliance with certain government regulations

Cyberattack Response Planning

A cybersecurity breach response plan is a regulatory requirement in several industries.

Furthermore, it identifies a clear path of what to do to mitigate the damage from a successful cyberattack and how to get your systems up and running immediately.

Defined escalation levels cater to auditor and regulatory requirements.



What's Next?

This threat assessment checklist for cyber security should help guide you towards a more secure future.

Cyber security is not easy or inexpensive, but its cost pales in comparison with that of a successful cyberattack.

If you don't have the expertise to implement these measures yourself, find a reputable, experienced cyber security service provider to do it for you.

It can mean the difference between success and failure of your business.

BlueCotton

Ready to take your SMB's security to the next level?

Contact our team for a complimentary consultation.

bluecottontech.com