Microsoft

INTCOMEX CLOUD

General Security **Recommendations**

Businesses can no longer afford to take cybersecurity for granted. You can't read the news without seeing a splashy headline about a successful hack or data breach at a well-known company. However, this isn't just a problem for large enterprises—increasingly small and medium-sized businesses are becoming targets of cybercriminals and need to take steps to improve their security.

Yet it can be hard for small and medium-sized businesses to right size a security strategy for their unique business. We believe a good place to start is by answering these four questions:

- **How secure are your users and accounts?**
- **How protected are you from threats?**
- **How safe is your data?**
- **How effectively are you managing security?**

The Microsoft Security Assessment can help you discover where you are vulnerable and provide personalized recommendations to improve your security posture. Keep reading for a peek at some of our key learnings from the assessment.

How secure are your users and accounts?

In today's modern workplace, employees work from anywhere on any number of devices. This has been great for personal productivity, but has also created more possible points of entry for hackers to break in. One of the biggest challenges is to make it easy for your users to connect to the resources they need, from the devices they prefer, while balancing security for your company and its assets.

There are many ways to protect your accounts, but make sure you include Multi-Factor Authentication (MFA), as no password is foolproof. MFA is safer because it requires two forms of authentication to gain access. For example, you can require that users sign in with a password plus either a code generated by an application or a biometric, like fingerprints or facial recognition. Products such as Microsoft 365 Business make it easy to enable MFA for your email, file storage, and productivity apps, adding another layer of defense to your organization's assets.

How protected are you from threats?

The latest figures show that cybercriminals are increasingly targeting small and medium-sized businesses alongside big businesses. Forty-one percent of businesses with fewer than 250 employees reported an attack in the last 12 months. Fortunately, there are practical things you can do to reduce your vulnerability, and every step makes a huge difference.

Two recommendations that are low cost, or even free, include maintaining software upgrade cycles and conducting regular employee training. If you don't require that employees keep software updated and patched, consider starting. Whether it is for the operating system, servers, devices, applications, plug-ins, or any other technology, updates will reduce security vulnerabilities. You can also increase your security posture through regular employee security training. The onboarding process is a good opportunity to share cybersecurity practices, but don't stop there. Consider putting a regular security training program in place to remind employees how to detect and report suspicious links, attachments, and emails; avoid malicious websites; and download only verified applications.

How safe is your data?

One of your most valuable assets is your data. Data includes everything from a private document, to personal identifiable information, to sales projections, and more. In all cases, it will be damaging to individuals and your business if it gets into the wrong hands. You need to protect sensitive data where it lives and while it travels.

One way to safeguard critical documents is with encrypted access. Document-level protection helps guarantee that only authorized users can read and inspect privileged data, even when it is sent outside of your organization. This level of protection is available in certain products, such as Microsoft 365 Business, which also includes the ability to notify and educate users when they are working with sensitive data.

How effectively are you managing security?

A strong defense is more than just a set of tools and practices. You need a thoughtful approach to how you manage security. Effective security management will give you visibility into vulnerabilities across all your resources, and it will encourage consistency across your security policies. With a strategic approach you will better understand your current risks and be able to identify opportunities to increase your protection.

A critical component of security management is periodic reviews of user access to data, devices, and networks. People, roles, and responsibilities change over time, which is why it's good to know what roles have access to what resources. You can use this review to make sure that users have the right level of access, for the right time period, based on their role. For example, someone in HR might need to access the financial services database during a specific project. You can also make sure those that have left your organization or changed role have been de-provisioned, and you can investigate any suspicious activity that is detected.

Evaluate how well your businesses is protected

Unfortunately, it is not just the big brands that must combat cyberattacks. Small and medium-sized businesses are also at risk. We've given you a sampling of our recommended security best practices, but there is still more you may want to consider. The security assessment can help you evaluate holistically how strong your current defenses are and provide specific actionable recommendations that you can put in place to increase your confidence and reduce your vulnerabilities.