Quiz

How secure are you?

interlink® CLOUD ADVISORS

Take this 10-question quiz to find out if you are safe and secure, or if your organization is at risk to become a cybercrime victim.

1 Do you have a Single Sign-On (SSO) identity framework?

- Ⓐ Yes, an Active Directory or Azure Cloud ID
- Ⓑ Yes, we have single sign-on from another system in place
- Ⓒ No, we do not use a centralized identity system or have single-sign on deployed

Pro Tip:

Explore Azure Active Directory and Identity Protection to deploy centralized cloud based identity for your userbase. If possible use Multi Factor Authentication (MFA).

Pro Tip:

Explore Azure cloud offerings to get your business set up with proper backup and recovery functions so you can ensure data and services are backed up and always available.

2 Which of the following is true about your Disaster Recovery program?

- Ⓐ All critical systems and data are automatically backed up and are tamperproof
- Ⓑ Our IT guy regularly conducts business continuity exercise drills
- Ⓒ We use a cloud based recovery service like Azure Site Recovery

3 Do you monitor for unauthorized intrusion activity?

- Ⓐ Yes, we do have an intrusion detection system (IDS)
- Ⓑ Yes, our IT guy monitors for cyberattacks daily, somehow
- Ⓒ No, we cannot monitor for such activities

Pro Tip:

We can help design an IDS solution and tune detection to fit your network and business needs.

Pro Tip:

You need to define a security policy based on ISO 27001 to ensure compliance and alignment to best practices. We can help you write one and get compliant!

4 Do you have a security policy in place?

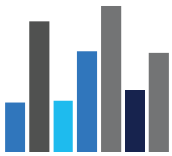
- Ⓐ Yes, we do have a comprehensive security policy endorsed by management
- Ⓑ Yes, someone wrote a policy for us to follow
- Ⓒ No, we do not have a complete security policy

5 How do you connect your company to cloud services?

- Ⓐ We use VPN and/or SSL to securely access hybrid cloud services
- Ⓑ We connect to the cloud via the Internet
- Ⓒ We do not use cloud services at this time

Pro Tip:

Evaluate Azure Virtual Network and Office 365 secure portal solutions for secure connectivity to the cloud.



Pro Tip:

Let us help you design a comprehensive data and information protection solution. Azure and Office 365 can help provide technology for both!

6 How do you monitor for data leaks?

- (A) We do have a comprehensive data protection program in place with rule detection logic
- (B) Word of mouth, someone reported it
- (C) We cannot track or monitor for data leaks

7 How long does it take to deploy critical security updates to software?

- (A) It takes us 5-30 days and we strive to patch quickly
- (B) We need 30+ days because it is a lot of work
- (C) We have to patch? Don't systems patch themselves!?

Pro Tip:

Updating systems on time and taking the practice seriously is paramount to the security of your environment.

It sounds simple, but in business environments there are a lot of factors at play that could delay even critical updates. Explore the adoption of Azure Cloud and PaaS and focus on running your applications in an always up-to-date environment.

Pro Tip:

Define roles and responsibilities and look for a technology such as Azure AD, and deploy access control features to effectively manage authentication and authorization to resources.

8 How do you limit access to resources?

- (A) We have access control defined based on roles and responsibilities in AD groups
- (B) Everyone asks everyone for access to everything
- (C) We don't have any real means to reliably restrict access to services and data beyond authentication

9 Do you perform vulnerability assessments on your environment?

- (A) We have a vulnerability management program and assessment technology in place
- (B) We let our IT admin run some scans at times or wait for others to expose our gaps
- (C) We do not have a vulnerability scanner or process

Pro Tip:

Identify a vulnerability management service that has cloud and internal offerings to be deployed in your network. Consult with us to set up and tune the scanner and train your IT pro to handle vulnerability reports. It requires management commitment to remediate discovered issues.

Pro Tip:

Obtain a comprehensive solution for all systems. Patch your systems and apps regularly to ensure propagation of malware using old bugs will not go far. Be aware of zero-day potential risks by following our bug reports and awareness campaigns.

10 Are you prepared to deal with ransomware attacks and demands?

- (A) We patch our systems regularly, remediate any potential risks quickly and have regular backups
- (B) We have purchased enough Bitcoins to pay for ransoms, so we're not worried if it happens
- (C) We are not prepared to handle malware and ransomware attacks at this point

Protect your organization from unnecessary security risks. Most organizations don't take action on cybersecurity until it's too late, but a security breach could cost millions, drive away customers, disrupt your business, and become a PR nightmare. If your answers to this simple security quiz have raised concerns about your cybersecurity, contact us to learn how Microsoft 365 can help protect you against today's evolving security threats.

www.interlink.com | 800-900-1150 | hello@interlink.com

interlink® CLOUD ADVISORS