12 Best Practices to Enhance Organisational Cybersecurity Hygiene

With the evolving cyberthreat landscape, lack of cybersecurity professionals and limited resources to manage an infinite amount of threats, securing the modern enterprise requires a clear strategy. Microsoft recommends 12 best practices to help organisations elevate their digital defence.

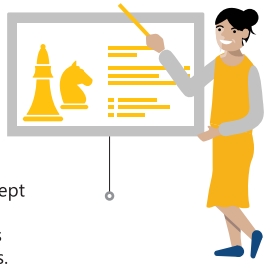
Business Leader

1 Participate in threat intelligence and cybersecurity knowledge-sharing

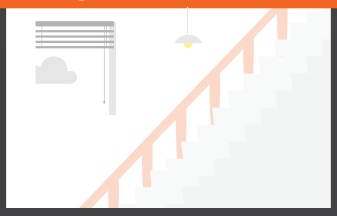
Engage with the Cyber Security Agency of Singapore, Chief Information Security Officer communities and CERTs to exchange threat intelligence and cybersecurity knowledge to keep abreast of the cybersecurity developments and best practices.

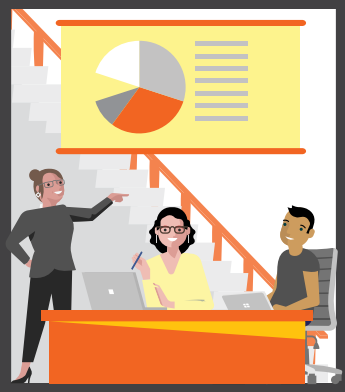
2 Position cybersecurity as a joint leadership priority

Engage your organisation's leadership and board in the development of cybersecurity strategy and crisis management exercises. This ensures they are kept updated on the organisation's cybersecurity posture, and builds trust among key decision-makers.



Organisation





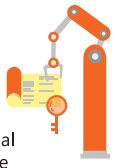
3 Build a security-minded culture

Cybersecurity is everyone's business. Building a culture that encourages individuals to play a role in organisational security enhances readiness to protect, detect and respond to cyberthreats.

4 Train cybersecurity talents

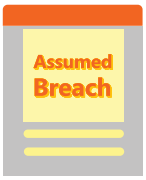
With up to 3,400 cybersecurity professionals required in Singapore by 2020, organisations need to play an active role to continuously train their staff to ensure that their cybersecurity knowledge and skills are up-to-date.

5 Leverage AI and machine learning



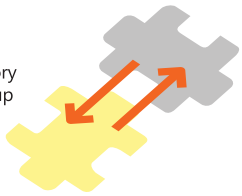
With talent in short supply, organisations can use artificial intelligence (AI) and machine learning to analyse data at scale, augmenting human investigators in detecting, investigating and responding to threats over a wider risk area.

6 Adopt an assumed breach security approach



As the attack surface broadens, leaders should adopt an "assumed breach" approach to security. Developing a security playbook and implementing crisis management practices will empower organisations to be better prepared for future attacks.

7 Set up a shared responsibility model for compliance



With changing compliance and regulatory requirements, organisations should set up a shared responsibility model with security vendors to clearly define the control boundaries, and ensure that there are no overlaps or gaps.

Individual

8 Ensure personal cyber hygiene

Cybersecurity hygiene is everyone's responsibility. Make use of security solutions and keep your software and operating systems updated to elevate your defence against cyber threats.

9 Use software only from trusted sources

Software from untrusted sources, like pirated software, are often laden with malware that poses a security threat. Use only software from trusted sources and suppliers to minimise the risk of cyberattacks.

10 Ensure good credential management

Choose a strong and unique password for each of your accounts, and never reveal your credentials to anyone. When available, use multi-factor or biometric authentication to enhance security.

11 Backup files

Make sure that important files are backed up on a trusted cloud platform to minimise the impact on daily work in the event of a security breach.

12 Stay vigilant

Be wary of where you are transmitting sensitive information. Make sure this is done on a secured, private device and on a trusted network instead of a public Wi-Fi hotspot.

For more information on how to secure the modern enterprise in a digital world, visit aka.ms/security

Microsoft