10-Step Cybersecurity Checklist

Your cybersecurity strategy doesn't have to break the bank, and you don't have to be an expert yourself or employ a team to manage it. By taking some basic measures, you can protect your assets, reputation and customers and help your business thrive.

Presented by

mailguard

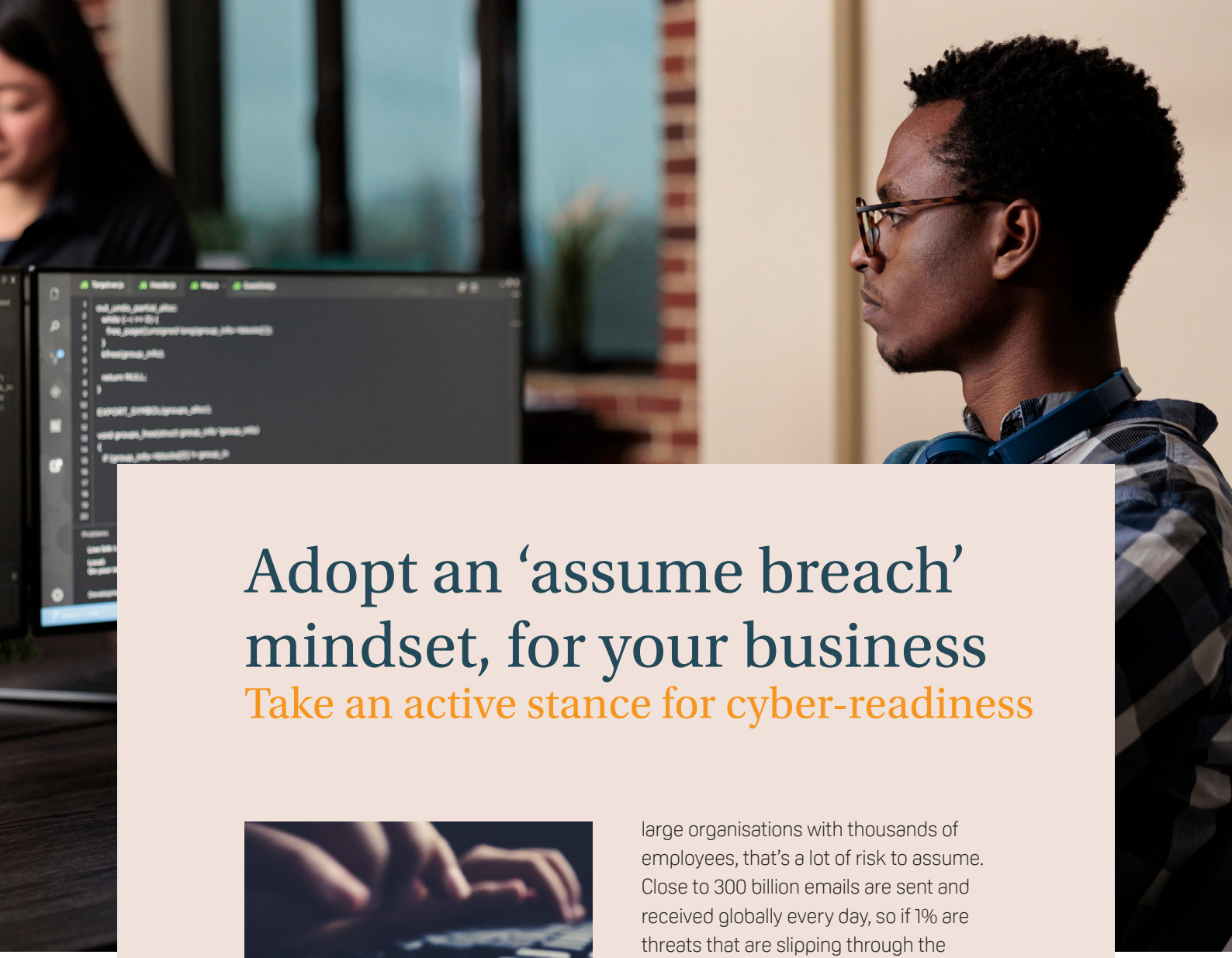
Cyber ready?

The spectre of a cyberattack continues to loom large for every business, and the problem is only getting worse. As it stands, the industry is worth more than $1.2 trillion - a number which is expected to grow to $6 trillion by 2025.

The digital threat landscape is constantly evolving, as is the scale, speed and sophistication of cyberattacks. With workforces more remote than ever, the attack surface has expanded, meaning more vectors to defend and greater vulnerability.

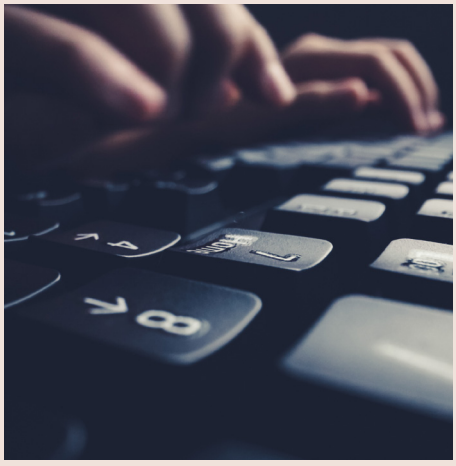
And, hackers have become even more relentless, thanks to ransomware-as-a-service and phishing kits, their attacks continue to be more advanced, quicker to execute, and harder to defend against. Add to that, sophisticated organised crime groups, and transnational nation-state sponsored bad actors, and it's a frightening climate for any business.

And as the range of vectors continues to expand, the ubiquity of email means that it is still the number one source for cyberattacks. Last year phishing scams claimed four times more victims than any other cybercrime type in the U.S., and Business Email Compromise (BEC) attacks were by far the most financially damaging, costing victims almost $2.4 billion.



Adopt an ‘assume breach’ mindset, for your business

Take an active stance for cyber-readiness



As 91% of successful cyberattacks result from human error, cybercriminals go straight to the source through email.

When you consider that on average, we each receive more than 100 emails per day, even if your defenses are 99% effective, that’s still a threat a day that’s slipping through. And for large organisations with thousands of employees, that’s a lot of risk to assume. Close to 300 billion emails are sent and received globally every day, so if 1% are threats that are slipping through the cracks, then that’s 3 billion opportunities for a compromise.

We see high-profile cases of cyberattacks and data breaches in the media daily, but cybercriminals don’t discriminate. Businesses of all sizes are at risk and need to take preventative measures to ensure the safety of their data and systems.

Don’t assume that an attack won’t happen to your business. It can and it will. How you defend against those attacks is vital. While it is almost impossible to prevent all cyber risks, basic security practices can make an enormous difference.

10 Steps to improve your cybersecurity

01 Ensure all devices, software, and apps are up to date

Outdated software can leave your device vulnerable to attacks. As soon as an update appears, make sure to install it – or better yet, turn on automatic updates. Software and application updates contain important security fixes that can help keep your devices safe from cyber criminals.

02 Practice good password hygiene

Make sure passwords are hard to guess, using a combination of letters, numbers, and special characters, and make sure they're unique. You can also use passphrases rather than singular words. Password managers are a great option to store and generate passwords securely and help users to fill them in automatically, which takes the pressure off having to memorise them and encourages healthier password habits.

03 Mandate multi-factor authentication (MFA)

MFA is one of the most effective ways of preventing unauthorised access on your accounts. It can involve using methods such as biometrics, one-time passwords, and authenticator apps, in addition to (or sometimes instead of) your password.

04 Regularly back up important files

Backing up to a cloud is a good start, but it's important to ensure that at least one back up is offline on an external device. The 3-2-1 strategy recommends having at least three copies of your data, two local (on-site) but in different storage formats, and at least one copy off-site to assist with disaster recovery.

05 Take a defense-in-depth approach to email security

90% of cyberattacks begin with an email, and no one vendor can be relied upon to detect and stop every threat. If your business is using Microsoft 365 or Google Workspace, add a specialist cloud email security solution like MailGuard to your security stack.

06 Perform periodic cyber-risk assessments

They can help your business identify it's cyber strengths and weaknesses and can help you to get your systems back online quicker if you're attacked. You can use the Australian Government's Cyber Risk Assessment Tool as a starting point.

07 Secure your devices and network

Invest in anti-virus software, VPNs, firewalls, and email security. Strengthening the security of your devices and accounts is crucial in protecting your business from attacks but doesn't have to cost an arm and a leg.

08 Establish a human firewall in your business

Ensuring that the employees in your business form a 'security first' culture is critical in adding an extra layer of defence against cyberattacks. In order to do this, they need to be adequately informed and trained. Learn more about creating a human firewall here.

09 Engage with vendors to understand their security practices

Supply chain attacks are attractive to cybercriminals because they can impact a number of businesses at once. Speak with third-party suppliers to ensure that they are complying with cybersecurity standards and are capable of keeping your data safe.

10 Revise and update cyber policies continuously

The cybersecurity threat landscape is always evolving. Your policies need to take emerging threats into consideration in order to protect your business and customers.

Presented by mailguard

Other Resources

Businesses need to be proactive in their approach to strengthening their cybersecurity position. We encourage you to speak with your Partner for advice that's relevant to your business. They will be able to assist you in identifying weaknesses in your security stack and help you mitigate risks.

Speak to those within your business to leverage their experience and help them to understand and formulate cyber policies, and to recognise key business risks.

Business owners should seek the most current and thorough advice, like the ones below.

Essential Eight

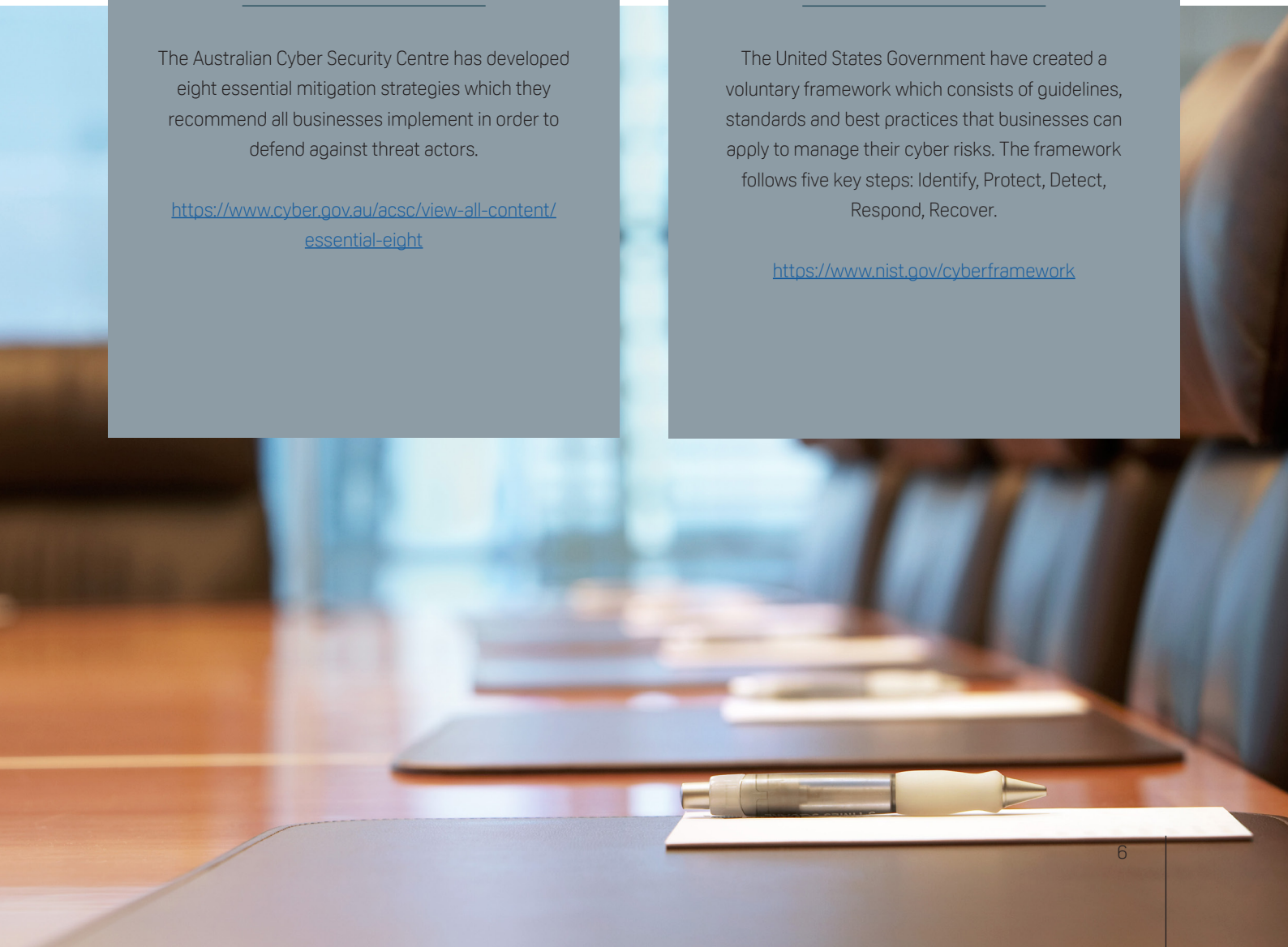
The Australian Cyber Security Centre has developed eight essential mitigation strategies which they recommend all businesses implement in order to defend against threat actors.

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

NIST Framework

The United States Government have created a voluntary framework which consists of guidelines, standards and best practices that businesses can apply to manage their cyber risks. The framework follows five key steps: Identify, Protect, Detect, Respond, Recover.

https://www.nist.gov/cyberframework



If sophisticated, email-borne cyberattacks are a problem for your business, don't wait until it's too late. Speak to your IT Partner about using MailGuard to defend your inbox.

MailGuard delivers category leading, cloud-based email security that anticipates, predicts, and learns from emerging threats, such as phishing, ransomware & BEC, keeping email users safe from harm up to 48 hours ahead of rivals.

FIND OUT MORE
expert@mailguard.com.au
1300 304 430

Presented by

mailguard