BRENNAN
People first – secure always

FAST FACTS SHEET

EIGHT TIPS TO ENGAGE EMPLOYEES IN CYBERSECURITY

Cyberattacks have increased by an astonishing 48 per cent since March 2020, with bad actors mainly targeting remote workers. Given that all successful attacks must be reported publicly, under the Notifiable Data Breaches Scheme (NBD), it is crucial that all employees are engaged in cybersecurity. Here are eight tips to protect your valuable business data, and avoid an embarrassing breach:

1. ENSURE EVERYONE RECEIVES CYBERSECURITY TRAINING

Most cyberbreaches occur because of human error due to a lack of knowledge, awareness and concern about cybersecurity, a problem we've seen heightened by the pandemic. Ongoing training through short, online modules can help employees across your organisation keep cybersecurity front of mind as they go about their day-today.

2. HAVE A CYBERSECURITY STRATEGY AND COMMUNICATE IT

Every organisation must have a cybersecurity strategy documented clearly so that all employees can easily understand it. The strategy must be communicated regularly to all teams, to help build a cybersecurity culture. The Australian Cybersecurity Centre's Essential Eight provides a framework for businesses to establish their cybersecurity strategy.

3. ADOPT A VIRTUAL FIREWALL

With employees working across multiple devices and locations, organisations need virtual firewalls that authenticate individual connections and transactions. Identity-based security and multifactor authentication can fill the gap when employees are not protected by the corporate firewall.

4. BUILD EMAIL CYBER RESILIENCE

Use threat protection software to protect employees and build email cyber resilience against spam, malware, ransomware, and phishing attacks.

BRENNAN
People first – secure always

FAST FACTS SHEET

EIGHT TIPS TO ENGAGE EMPLOYEES IN CYBERSECURITY

5. UPGRADE IT SECURITY

Legacy systems often allow cybercriminals easy access into organisations. To keep your people and business data safe, ensure security is immediately updated with new software or patches as soon as they are released.

6. ENGAGE A DEDICATED IT SECURITY PERSON OR TEAM

A dedicated IT security expert keeps cybersecurity top of mind for the organisation and its employees and helps guard against emerging cyberthreats. It's not always easy to find someone with the right skillset, therefore outsourcing this to a Managed Services Provider is an easy way to add an experienced cybersecurity expert to your IT team, without the overhead.

7. MAINTAIN DATA GOVERNANCE

To manage growing amounts and types of organisational data while ensuring compliance, use asecure data solvency and archiving platform.

8. IMPLEMENT A HOLISTIC SECURITY APPROACH

A holistic approach that combines proactive and defensive security is the most effective. This includes staff training and identity management, vulnerability management, endpoint and application security, network & data protection, security monitoring & incident response.

If you would like to get a fresh perspective on your organisation's security posture or seek guidance on how to move forward with your security strategy, get in touch to arrange a time to speak with one of our cybersecurity experts. **Call us on 1300 500 000 or send us an email.**