Wavelink
Global Technology | Local Knowledge

# MEDIA RELEASE

## How to combat human error in cyber risks

According to the Office of the Australian Information Commissioner, more than one third of companies that had data breaches in the past quarter passed on private customer information because of simple human mistakes. This won't come as a surprise to many in the security industry; human error has long been known to be the weakest link when it comes to IT security, and it's time for businesses to act on this vulnerability, according to Wavelink.

Hugo Hutchinson, Wavelink's national business development manager for Fortinet, said, "Businesses need to have the right protection measures in place but, if that doesn't include educating employees about the ways they can mitigate risk, then the business is likely to fall victim to an attack no matter how good their technology is. It's therefore crucial for businesses to understand the ways in which employees contribute to risk and, therefore, how to combat this."

Wavelink has identified five ways employees contribute to security risks:

### 1. Lack of attention

Employees are busy trying to do their jobs. Social engineering campaigns known as phishing attacks use this to their advantage. They send emails that look like they're from a legitimate source, tricking employees into paying money into accounts, providing password details, or divulging other sensitive information without realising they've been hacked.

### 2. Lack of understanding

When employees are trying to be productive, they can feel stymied by good security policy if they don't understand why that policy is in place. They can look for workarounds that help them move faster but open up the organisation to risk. For example, they may use Dropbox or another unsecure service to share documents instead of sharing them through secure channels. Or they may share passwords with others to expedite a project. It's essential to ensure that employees understand the reason for security policies that they may find cumbersome to increase the chance that they'll comply.

### 3. Lack of hygiene

Good security hygiene demands that employees don't connect unsecured devices to the network, don't insert unknown USB drives into laptops, and don't click on suspicious links in emails. Yet, every day, organisations catch their employees doing all of these things. Doing so opens up the company network to attack, so it's imperative to put in place specific policies around these actions and communicate them regularly and clearly to employees so everyone knows what not to do.

### 4. Lack of complexity

One of the weakest links in an organisation is passwords. Staff members can become overwhelmed with the number of unique passwords they need to remember, so they opt for simplicity when it comes to updating their passwords. This could mean they use the same password across multiple accounts, or that they use easy-to-guess passwords. This makes it easier for cybercriminals to gain access to the network posing as an authorised user, which can make it harder to detect and remediate the attack. Employees must use complex, hard-to-crack passwords, change them regularly, and use multi-factor authentication when it's available.

### 5. Lack of device management

Wavelink
Global Technology | Local Knowledge

# MEDIA RELEASE

Bring your own device (BYOD) policies have been appreciated by employees who prefer using their own device for work. However, this can blur the lines between personal information and corporate information. And, if the employee downloads or accesses sensitive customer information on their own device, it creates potential for non-compliance with privacy legislation. Companies that do allow BYOD must ensure that devices are properly secured and segmented on the network, and must insist that employees protect these devices with biometric security and remote wiping features. Better yet, companies should consider providing purpose-built devices for employees to eliminate the risk posed by employee-owned devices.

Hugo Hutchinson said, “Being aware of these people-based risks is the first step in mitigating them. Organisations must embark on a sustained, consistent campaign of staff education to ensure that employees know their role in keeping the organisation secure. Regular reminders and updates on security will help keep this important issue top of mind for team members, so companies can reduce the risk of falling victim to cyberattacks that prey on human weakness. Minimising user risks, when combined with implementation of the appropriate network security measures will ensure the highest degree of protection in an increasingly risky environment.”