dohertyassociates
IT SUPPORT. BEYOND THE CALL

# Fixing the weakest link in IT security:

## How to address the workforce behaviours putting your business at risk

# Contents

# Introduction

It's natural to worry about external threats – historically, humans have been inclined towards an 'us vs them' kind of attitude, and it's not that much different when you examine cyber security practices in businesses.

Here, thoughts and actions revolve around potential threats coming in from the outside world – bringing to mind the idea of a hooded and hunched mastermind operating in a darkened room, exploiting technical loopholes to break into private networks and snatch company data.

The reality, however, is that most data is compromised in less sinister and arguably much simpler ways. Instead of looking outward, we should be examining the vulnerability on the other side of the fence: from inside our organisations, where workforce behaviours are leaving gaps in security.

It isn't technology, but humans who are the weakest link in IT security. Employees are easily fooled by social engineering attacks like phishing scams, are often careless because they care more about getting their jobs done quickly than acting in a secure way, and are sometimes simply unaware of the new risks presented by trends like cloud, BYOD and remote working.

> “Intentional attacks are frequently seen to succeed because of human error. This is the most common single factor that businesses see as having led to their most disruptive breach... ”

Cyber Security Breaches Survey 2016

Perhaps the biggest challenge to businesses is that technology is advancing too quickly for companies to keep up with relevant cyber training. In the UK, there’s a growing shortage of IT security skills, making expertise hard to come by, even for large and well-resourced organisations. The 2017 WannaCry attack is testament to this - if the world’s largest healthcare establishment is susceptible to breaches, where does this leave other companies?

In this guide, we look at some of the steps businesses can take today to begin fixing the weakest link in their IT security.

# Document and data security

A lack of security on the document level, combined with insecure and ad hoc working practices, is one of the biggest sources of cyber risk for many businesses. This is an issue especially for “knowledge workers” within organisations, such as solicitors and barristers, who need somewhere to store information and business-critical data but may not have a process in place to ensure they do so securely.

Often, these workers will make use of files such as Word documents, PowerPoint presentations and Excel spreadsheets – which are easy to misplace or lose control of. Forwarding an email attachment to the wrong person, or saving a confidential file on a portable USB that is then lost, for example, is potentially disastrous.

# How can company data be protected?

There are a number of technological solutions that can help businesses manage their documents and keep them from prying eyes regardless of where they end up. For example, placing encryption around emails and documents which forces users to enter their credentials will keep people from outside of the organisation from gaining access.

In some cases, there may also be an argument that an extra layer of security is required in the form of remote-wipe functionality, or a "kill-switch". Passwords, after all, can be cracked (or given away voluntarily), and some data protection laws and regulations may also stipulate that data is deleted after a certain timeframe – something that isn't simple to do if that data is spread across multiple documents on multiple devices.

# Device security

Device security for businesses was once relatively simple – all work computers, mobiles and tablets were left in the hands of an IT team who were responsible for software patches and updates, installing and updating security solutions like anti-virus, and preventing unauthorised configuration changes and the use of unsafe applications. The advent of Bring Your Own Device (BYOD), however, has thrown a spanner in the works, where employees prefer to use their own personal mobiles and laptops, and are not so willing to hand over control to IT for security.

As such, organisations are both under pressure to support more flexible working practices, whilst ensuring that data is kept secure. This is a particular cause for concern for small businesses, who worry that strict security policies will disrupt the balance of the friendly and flexible atmosphere they wish to create for workers.

However, the dangers of poor device security must be taken seriously. Alarming findings by EE reveal that:

- One in five (19 percent) of employees say that they have lost mobile devices used for work on a work night out.

- One in six (16 percent) have left their devices on public transport.

- Devices are also commonly left in taxis and public toilets.

The consequences of an unlocked iPhone being picked up by a member of the public could prove to be catastrophic for a business – they could easily gain access to confidential company documents that could put both the business and clients at risk.

## How can businesses improve device security?

It's common that remote-wiping is proposed as a possible solution, but it is often met with resistance because people don't want to lose personal data, such as irreplaceable photos of their children and family.

However, many modern enterprise mobility management solutions now allow organisations to segregate work related data from personal data. The result is a separate and secure mobile environment that exists purely for work data, with the option to implement additional security measures on top, such as multi-factor authentication and encryption.

So, even if a worker loses their phone in a taxi, the next person who picks it up will never be able to access any confidential business data without the correct credentials.

# Network security

The rise of remote working has meant that employees are putting business data at increased risk by using unsecured Wi-Fi networks. Although connecting to the internet at a local coffee shop doesn't sound particularly dangerous, the reality is that it's very easy for sensitive data to be intercepted in transit if wireless encryption is not in use.

And this is just one example of a network security risk. Elsewhere, one of the most common methods used by hackers to gain access to an organisation's sensitive data is to compromise a single device and then gradually widen their foothold across the business network.

So, if an employee-owned laptop is infected with malware and then used to connect to other network resources, there may be a domino effect where other devices and servers become vulnerable as a result.

The 2017 WannaCry attack offers an example of this in action: the ransomware was reportedly able to spread across unpatched devices on the same network regardless of whether users acted in a way that put themselves at risk.

## How can we avoid network security risk?

Businesses should take the time to make employees aware of the risks that connecting to public networks bring, and place limits on the use of personal mobile phones within the company network.

Other practical solutions include:

- Document-level security – placing encryption, such as passwords, around client-sensitive and business related documents
- Application-level firewalls
- Anti-virus
- Network monitoring  – continuously monitoring the network for any suspicious activity

# Security training

> In these smaller organisations, cyber security typically sat alongside IT and was in many cases left to the IT enthusiasts within the business. This could lead to a sense of assumed technical knowledge, where the person left in charge would implement what they could from what they knew, but would not necessarily know much about cyber security (as opposed to IT in general)

Cyber Security Breaches Survey 2016

Even with all of the above solutions in place, a sophisticated social engineering attack (e.g. spear phishing and whaling) can still give hackers enough of a foothold to bring a business to its knees.

As mentioned earlier, technology is advancing too rapidly for businesses to keep up, leaving large gaps in knowledge about how to remain secure in the new digital age, especially when cyber security is being left an in-house IT technician or other non-specialist who may not have the skill or expertise to protect you properly.

This is why end-user training remains a vital link in the chain of security. Businesses must be able to clearly outline their cyber security strategy, and continuously revaluate their worker's knowledge, as putting security into practice is a task for every single individual.

Ultimately, employees want to get their job done. If businesses are able to offer them the right tools, (such as cloud, BYOD and remote working) alongside the right training, workers will be empowered to complete their tasks with efficiency, as well as security.

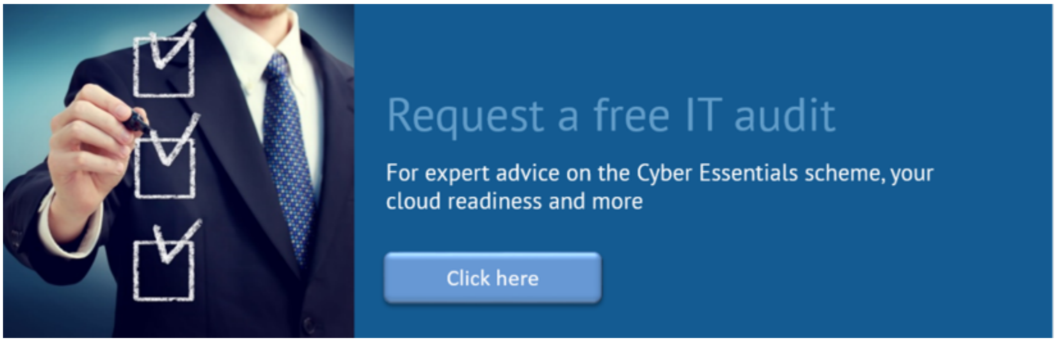
## What makes a great security training programme for knowledge workers?

- Optimised length and depth of sessions
- Power-user sessions
- Self-service password reset/intranet resources
- Unlimited access to IT support

# About Doherty

Founded in 1991, Doherty Associates is an IT support and managed services company that has embraced cloud solutions since they were in their infancy. We focus on implementations of Microsoft cloud services, including Office 365 and Azure, as we believe they represent some of the most flexible, user-friendly, secure and innovative cloud solutions for SMEs on the market. This focus has enabled us to achieve Microsoft Gold Partnership and pass on the benefits that this status brings to our customers.

As an IT support company based in London but with a global presence, we are on hand to help you day and night, with a dedicated team to monitor our systems 24/7 and ensure protection against any kind of cyber security attack.



Request a free IT audit

For expert advice on the Cyber Essentials scheme, your cloud readiness and more