YOUR RESULTS

HIGH RISK:

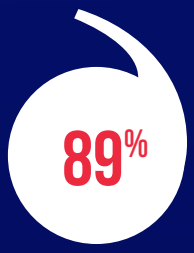
BASED ON THE INFORMATION YOU HAVE PROVIDED IT APPEARS THERE ARE SOME SIGNIFICANT GAPS IN YOUR CYBERSECURITY CONTROL

It looks like you need some guidance to walk the walk, we're here to help. This report will outline some of the potential risk factors, but for a more comprehensive analysis contact CSO Group for a obligation free meeting. We'll break down the threats and demonstrate how they relate to your business functions, and show you how effective management, and strategy can mitigate many of the risks you're currently facing.

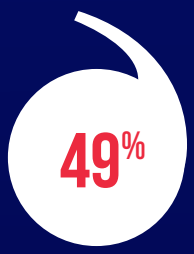
It is worth-while noting that the most likely reason for an attack is intelligence gathering? According to Symantec's Internet Security Threats Report (ISTR) for 2017, that could mean theft of documents and intellectual property, or it could involve snooping on your staff and customers. With this in mind, attackers will do everything they can to avoid discovery and can sometimes succeed in staying on a victim's network for months at a time.

Not all attacks will shut your network down, many are much more covert. It's important to protect your business because data breaches and privacy of customers are a business's responsibility to manage. Following the introduction of the Australian Notifiable Data Breaches (NDB) Scheme, the Office of the Australian Information Commissioner (OAIC) has released its second quarterly report, which uncovered 242 reported data breaches between April and June 2018. Of these, 89% of data breaches involved individual's contact details, 49% involved financial details and 39% involved identity details. And the damage? Of the 242 data breaches, 51 affected only one individual – but 6 affected more than 10,000 individuals.

DID YOU KNOW



of data breaches involved indivduals contact details



of data breaches involved indivduals financial details

HUMAN ERROR ACCOUNTED FOR 36% OF DATA BREACHES IN THE LAST QUARTER

It's important that cybersecurity is on the radar of all employees, because cybercriminals often rely on humans to open the door to their organisation. The ISTR states that spear-phishing emails are the number one means of attack. This means a well-crafted email, sent to an unsuspecting staff member is a very likely source of compromise and can be the trigger to a potentially serious security breach. Interestingly, this view is supported by the NDB report which stated that human error accounted for 36% of data breaches in the last quarter, where vulnerabilities involving a human factor were exploited.

It's about taking steps to protect the future of your business, and CSO Group can help you approach this in a holistic way, so it permeates from top to bottom. By assessing your business and how the right cybersecurity can help strengthen it, you'll be safeguarding the value of what's already been created. Your relationships, your reputation and your potential for further growth. Get in touch with CSO Group to find out exactly what walking the walk means for your organisation.

ARE YOU TAKING STEPS TO PROTECT THE FUTURE OF YOUR BUSINESS?

If you see the value in assessing cybersecurity with a business-centric approach, get in touch with CSO Group to find out exactly what walking the walk means for your organisation.

info@csogroup.com.au