HOME CYBER DEFENSE
ARE YOU SAFE FROM CYBER CRIME?
ALERT

Issued 8/3/17

Ransomware Shuts Down 1 in 5 Small Businesses After it Hits

When it comes to ransomware, it only takes one person to cripple the kingdom. That's the assessment of cybersecurity company Malwarebytes, which has found as many as one third of small-to- medium-sized businesses were hit by ransomware last year, and that "the human factor" is increasingly behind large-scale outages.

The findings come as part of Malwarebytes' Second Annual State of Ransomware Report, which showed that, of the 32 percent of companies hit by at least one malware attack last year, one fifth had to completely stop operations immediately. The figures paint a grim picture of digital security in the modern era, at a time when malware attacks routinely make news headlines, and ransomware (malicious software that infects systems and demands a ransom to regain access to encrypted files) has the power to bring everything from home computers to the world's biggest companies into the digital dark ages.

A quarter of businesses experienced more than 20 ransomware attacks in 2016, and in many cases, Australian and British businesses were the worst culprits. Australian figures released yesterday show 31 percent of Aussie businesses didn't know how they were attacked (compared to 9 percent in the US) [PDF]. Forty-six percent of Australian companies and 43 percent of

British companies paid the ransom (compared to 21 percent in the US). And even after paying, 40 percent of Australian and 46 percent of British businesses still lost their files (US: 32 percent). According to Malwarebytes Senior Systems Engineer Brett Callaughan, ransomware is a massive cybersecurity problem, but it often comes down to poor human behaviour, rather than poor security software. "People [behind the ransomware attacks] are going to more of the human factor now," he said. "A lot more attackers are becoming aware of the fact that they can make small amounts of money at a grand scale very quickly if they completely automate this.

The attackers we're seeing are extremely sophisticated -- they're not fussed about creating a file and making something look real. "They'll just go after the user and they'll spray and pray. If you hit 100,000 email accounts and 10,000 hit the button and you're charging $200 a piece? That's a significant amount of income right there from doing very little." If in doubt, do not click -- lest you be the one that knocks everything offline.