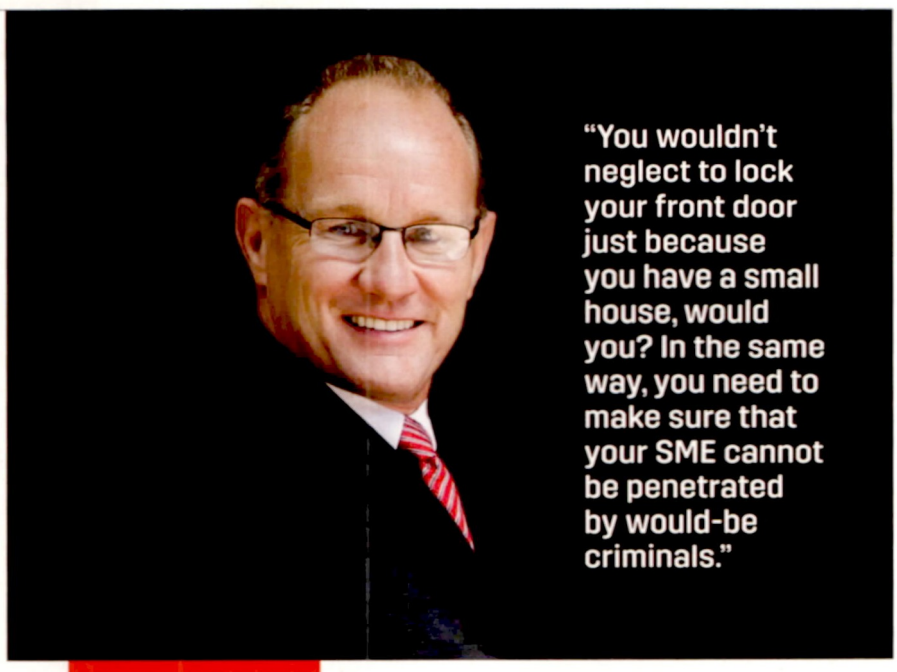
Publication: ENTREPRENEUR
Page: 51-52
Date: Mon 01 Oct 2018
AVE (ZAR): 44955.81



CYBER SECURITY

HOW SECURE IS YOUR BUSINESS?

As an SME owner, you may consider cybercrime a concern reserved for larger players. In fact, the opposite is true. **BY PIETER SCHOLTZ**

This year's attack on one of South Africa's largest financial institutions brought cybercrime into the spotlight. But, while this was an instance where the victim of the attack impacted thousands of people – employers and clients alike – the reality is that cyber criminals are, in fact, more likely to strike at small businesses. A 2017 report by Verizon noted that 61% of data breaches were carried out on small businesses. While these are global figures, South African businesses are no better off: 29% of respondents in the *Global Economic Crime and Fraud Survey 2018*, conducted by PwC, reported that they have been targeted by cybercriminals in the past two years.

WHY SMEs?

One of the reasons SMEs are at risk is because of their relatively lax approach to cybersecurity. Many owners of start-ups feel that they're under the radar for cybercriminals, especially when there are larger companies with greater assets that are surely more attractive.

Because of this, they invest less than they should on cybersecurity measures. From a cybercriminal's perspective, this makes them a prime target: on the one hand, they have more digital assets than most individuals, but on the other, they haven't taken the same amount of care to protect them as large company would.

WHAT ARE THE RISKS?

There are several different kinds of cybercrime, but those most commonly affecting SMEs include:

- **Malware:** Software like spyware, ransomware and control and command can be embedded in your system – without your knowledge – via infected emails or media like USB sticks. From there, they can track information on your system, or disrupt your operations. Occasionally, they demand payment.
- **Cryptocurrency attacks:** Distributed Denial of Services (DDoS) are becoming increasingly common. In these cases, criminals cause cryptocurrency systems to crash until they are paid a ransom.
- **Data breaches** see criminals targeting a company's database of customer information. These attacks are

particularly damaging because of the sensitive nature of the information. If this falls into the public domain, companies stand to lose credibility and may lose further business because of their tarnished reputations.

WHAT CAN YOU DO?

Now you know the risks and understand that the size of your business is no protection against cybercriminals, it's time to take action.

- **Be aware.** Your very first step should be to ensure that your employees also understand the risks and, more than this, that they understand the signs of malware and how it is spread.
- **Don't skimp on cybersecurity.** Think of it this way: you wouldn't neglect to lock your front door just because you have a small house, would you? In the same way, you need to make sure that your SME cannot be penetrated by would-be criminals. An anti-virus programme is your first line of defence. Make sure you instal a reputable one and update it as required; after all, an out-of-date programme is just as ineffective as a non-existent one. You then need to instal a firewall. This ensures that your network is safe at all times. It's also important that employees who are working remotely cannot log into the network unless they are working on a secure VPN. Next, turn your attention to your website. Are there any weaknesses that leave you and your customers vulnerable to attack? Remember to check in from time to time to make sure that there are no new developments in this regard. Finally, back-up all data on your system regularly. The loss of information can have devastating effects for a small business, so physical back-ups (checked to make sure the data is not infected) can provide invaluable protection in the case of a breach.
- **Practice, practice, practice!** Implement a drill so that you know what to do in the case of an attack.
- **Invest in insurance.** If you experience a data breach, you may find yourself liable for legal fees and other losses. Ask your insurance company about specific policies to protect you against such eventualities.

PIETER SCHOLTZ is the Co-Master Franchisor in Southern Africa of ActionCOACH

Visit www.actioncoach.co.za