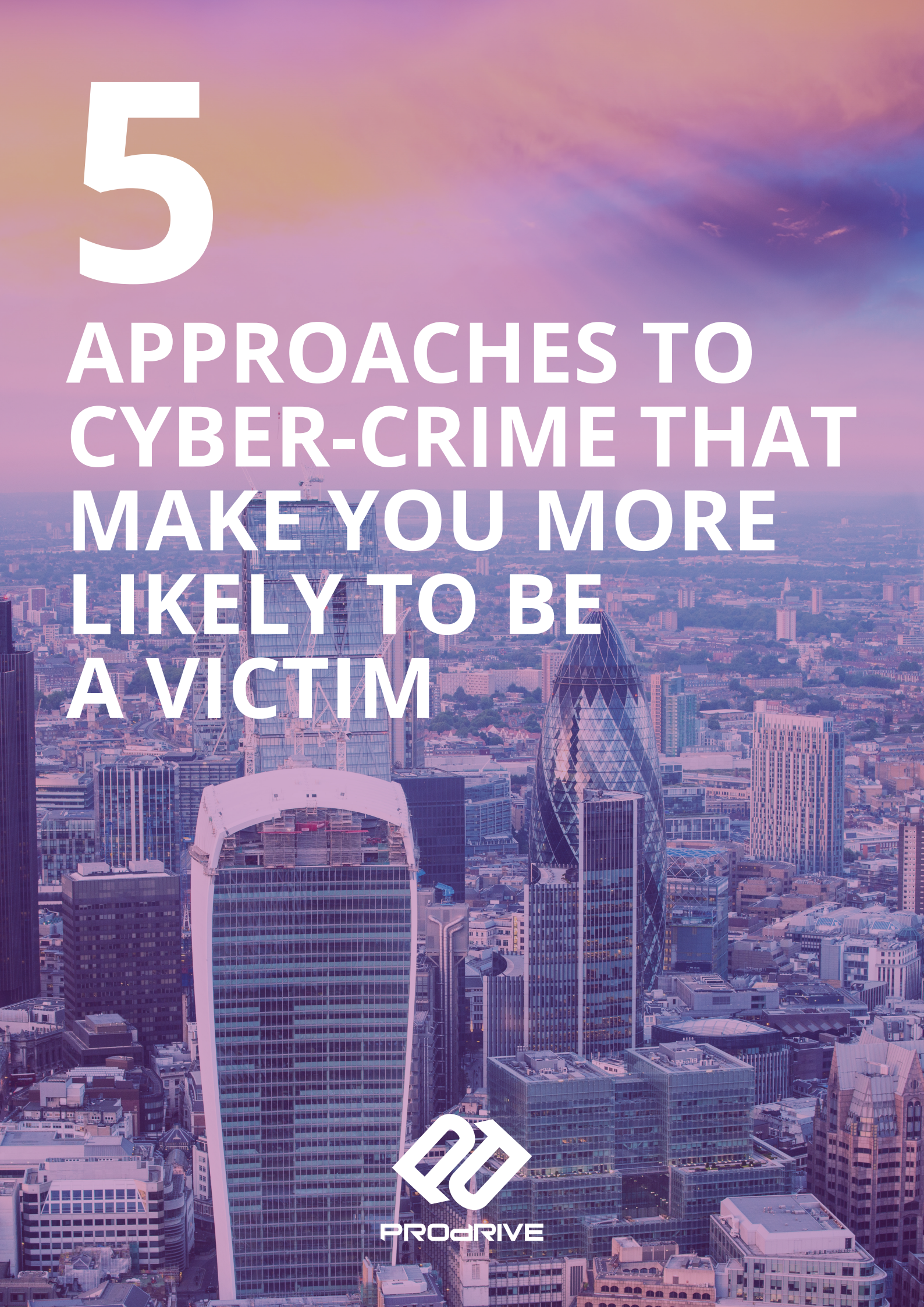
5 APPROACHES TO CYBER-CRIME THAT MAKE YOU MORE LIKELY TO BE A VICTIM



PRODRIVE

1. WE HAVE NEVER HAD A CYBER-ATTACK BEFORE SO WE ARE NOT AT RISK

Let's clear this one up first as it is fairly straightforward. 60% of UK SME businesses suffered a cyber-attack in the UK during 2016. Furthermore, we know that many businesses who have been compromised, are not actually aware that they are under attack. In fact it takes on average 229 days to detect an intrusion. So even if you believe your business has not been a victim of cyber-crime, there is still a good chance you might have been.

The cyber-crime 'economy' is growing at an astonishing rate and as a result there is virtually zero chance that the situation will improve, and every chance that it will become considerably worse. And with combination of the increasing sophistication of cyber-attacks and the fact that more and more criminal organisations are turning to cyber crime as a source of revenue, the frequency and success ratio of attacks is likely to increase.

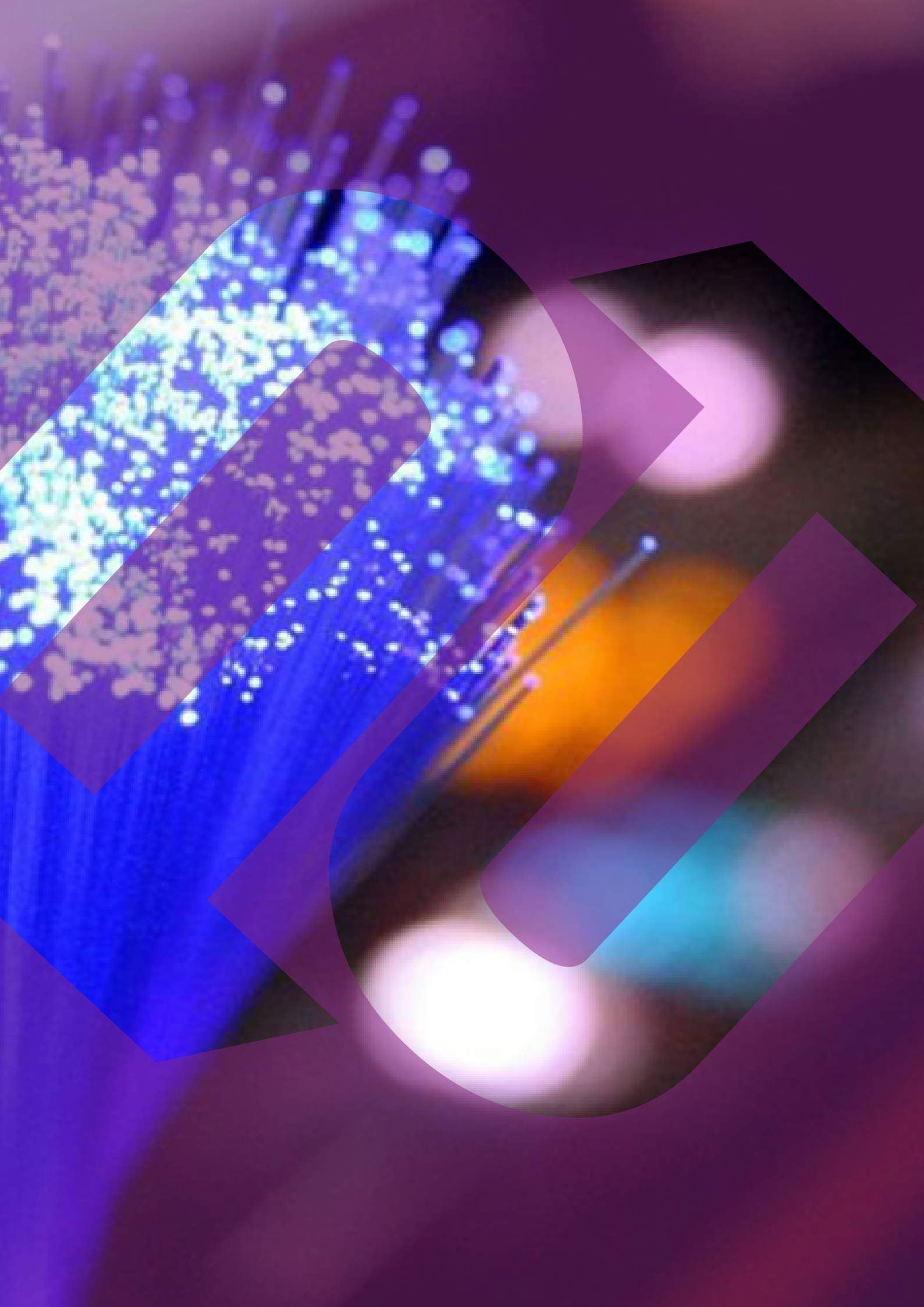
So if you have not already been a victim of cyber-crime, chances are you will be very soon.

2. WE ARE NOT A TARGET - WE'RE TOO SMALL

It certainly used to be the case that targeted Cyber Crime - where criminals specifically craft a scam or campaign of cyber-attacks ultimately to extort or steal money - used to be the domain of larger business or perhaps niche companies with valuable intellectual property.

However this is absolutely no longer the case. Larger businesses have significantly increased their cyber security budgets and consequently they are now more challenging for criminals to make money from. Smaller businesses on the other hand are typically less prepared and more likely to pay any ransom demanded. And because there are so many more small businesses then those at the enterprise level, it only takes a low percentage of success for cyber criminals to net a substantial amount of money.

Crucially though, it is because small businesses often believe they are not a target that they are in fact the ideal target.



3. IT HAVE IT COVERED

Many businesses turn to their IT, whether in house or outsourced, and task them to reduce the risk to the business from cyber-crime. Often they are given much needed budget to do this and IT wisely recommended and install some of the better security product on the market. They should have reason to feel pretty safe, shouldn't they?

Unfortunately not. Whilst technology failings can be one of the key issues that makes business vulnerable to cyber criminals, and we have seen well documented examples where poor software patching regimes have done exactly this, it is perhaps a lesser known fact that 95% of all cyber security incidents involve at least some element of human error.

So there whilst there is most certainly a place for improved technology in your cyber security plan, unless you address the human element as well you are wasting your money.

4. OUR PEOPLE ARE TECH SAVVY SO THEY KNOW WHAT THEY ARE DOING

Some businesses, particularly those in technology related sectors, have a wealth of technical knowledge within their teams. These people are very comfortable using email and similar systems and are probably aware of the some of the common forms of cyber-attack. Would it be reasonable to assume that this would reduce risk from Cyber Crime?

Whilst undoubtable there are situations where having staff who are technically savvy can help, in particularly responding to a security incident should one occur, it is unlikely to have a significant impact on reducing the likely hood of a cyber-attack occurring in the first place.

Cyber Criminals often research their targets and craft their activity to have the best success against the companies they are attacking. And the same human factors that make any person susceptible to cyber-crime apply regardless of their levels of technical knowledge.

5. WE DON'T SEE ANY VALUE IN INVESTING IN CYBER SECURITY

There is a cost to implementing cyber security improvements - of that there is no doubt. This can be in the form of bottom line expenditure or time from your staff. Either way it must be seen as an investment to protect the assets and reputation of your business. A bit like an insurance policy.

Many SME businesses still do not see investigating in mitigating cyber security as a high priority. In some cases it might not be - but until they fully understand the cost of a cyber-attack, it is impossible to make an informed decision. Unfortunately for most SMEs, they only discover the true cost of a cyber-attack once they have experienced one.

So before you decide on your cyber security budget, or decide on the internal resources you intend to allocate to it, make sure you fully understand you risk first.

HEAD OFFICE
Pro Drive IT Limited
Unit 22, Home Farm
Loseley Park
Guildford
Surrey, GU3 1HS

Sales Team
0845 507 0846

Support Team
0845 507 0845

E-mail
sales@prodriveit.co.uk