CUT THROUGH THE NOISE

John Gilbert *reports on the importance of reducing the vulnerability of organisations to cyber crime and fraud*

Security managers need to be aware of the threats that exist both today and in the future

Cyber crime and fraud are a growing threat to UK organisations. According to figures published by the Department for Digital, Culture, Media and Sport (DCMS), 32 percent of businesses have suffered at least one cyber attack or breach within the past 12 months. And, worryingly, there were 4.6-million incidents of fraud and computer misuse last year, which accounts for a massive proportion of the overall 11-million crimes reported. What's clear is that organisations are not doing enough to protect themselves. In an age where businesses are forced to become digital-by-default, standing still is not an option.

Thanks to new technologies such as Artificial Intelligence and the Internet of Things, the threat landscape is constantly evolving with malicious actors attempting to bypass stronger security measures. While we're likely to see new threats enter the space, we can also expect to see the same – albeit more intelligent – cyber attack types in the future. Phishing, for example, will become harder to distinguish, while password hacking and social engineering will continue to cause disruption unless users get smarter at security.

Disruption can come in many forms. In fact, financial loss, reputational damage and compliance issues can all ruin a business. Figures show that the average cost of a cyber breach or attack is a conservative £4,180, which could be detrimental to smaller businesses – a market that makes up a whopping 99.9 percent of the UK's business population.

So, what's the answer? First, security managers need to be aware of the threats that exist both today and in the future. A significant proportion of malicious attacks happen through phishing, so learning to spot a fake email is a good starting point. As many organisations know, this means checking the sender is valid, not opening any untrustworthy attachments or links, and sharing across the business if a large-scale attack is identified. Sharing with colleagues is incredibly important because it only takes one mistake from an employee to spread a virus through the network. Ultimately, everyone needs to be security conscious.

The problem is that the world of digital security can be confusing and overwhelming to organisations – especially those smaller businesses because they simply can't afford to employ security managers or even outsource security to a third-party provider.

Second, and this might sound obvious, everyone needs to get smarter about password security. A review of the 100,000 most common passwords – created by the UK's National Cyber Security Centre (NCSC) – reveals how common passwords can easily be guessed by cyber criminals – or simply plucked from databases of stolen information.

More than 23.2-million accounts use "123456" as the password while 7.7-million go for "123456789". Other regularly used passwords include "qwerty, which appears 3.8-million times, followed by "password" (3.6-million) and "111111" (3.1-million).

TWO-FACTOR AUTHENTICATION

While we can't change attitudes towards password protection instantly, we can encourage better use of two-factor authentication as an additional layer of security. This could be an SMS code to a phone, a hardware security token or a mobile authentication app. Hardware security keys offer the highest levels of online security, enabling users to log into many services with just one key and without the need to retype a code time and time again.

Again, there's a problem. It can be incredibly difficult for businesses to find a digital security provider they can trust to deliver a product or service that meets their needs. There is simply too much choice. The cyber security market is booming and there are no signs of it slowing down, which will only increase complexity for businesses when making important decisions about security products and services. In fact, separate figures from the DCMS show that the cyber security market in the UK alone has grown by over 50 percent in the last five years, generating almost £6-billion in revenue. It's no wonder some SMEs hold off on making an investment or, worse still, invest in the wrong (and usually costly) solution.

More guidance and support is therefore needed, which is exactly why the Police Digital Security Centre (PDSC) and the British Standards Institution (BSI) have joined forces to develop a new certification scheme for digital service providers. It will help SMEs reduce their vulnerability to cyber crime and promote the fact they take their cyber security seriously.

The scheme will regulate digital security providers by introducing a framework and certification process much like the 'Secured by Design' accreditation associated with physical security products. Since its inception in 1989, this accreditation has been improving the physical security of buildings using products, such as doors, windows, locks and walling systems that meet strict security requirements set out by the Police Crime Prevention Initiatives (PCPI). The results have been phenomenal, raising the awareness of the importance and benefits of security throughout the standards and construction industry. Over the last 30 years, more than one million homes have been built to 'Secured by Design' standards and there has also been an overall reduction in property crime of 60 percent.

THE UK CYBER SECURITY MARKET HAS GROWN BY OVER 50 PERCENT IN THE LAST FIVE YEARS

Building on the success of the 'Secured by Design' initiative and the experience gathered by the PCPI over these three decades, the PDSC is uniquely placed to deliver a consistent approach for the delivery and implementation of cyber crime advice.

As a not-for-profit organisation owned by the police, the PDSC works across the whole of the UK in partnership with industry, Government, academia and law enforcement agencies as well as big businesses and their supply chains, Business Improvement Districts (BIDs), local Governments and crime reduction partnerships. The PDSC is purely focused on supporting small and medium-sized businesses across the UK (and consumers alike) to improve their resilience against the most common types of cyber crime and fraud.

Put simply, its new certification can help SMEs cut through the noise and find the most appropriate digital security products and services for their individual needs, keeping them safe in an increasingly dynamic and dangerous cyber threat landscape.

To deliver on its objective, the PDSC put in place a model for recommending a range of trusted digital security providers. As its partner, the BSI put together a clear assessment framework and certification process – named the Digital Security Provider (DSP) scheme – to ensure all recommended digital security providers meet certain standards.

To achieve this level of trust, organisations must be checked for: financial solvency, ensuring that their business continuity is solid; staff skill sets to demonstrate they are skilled across their areas of expertise; criminal background – all front-facing staff undergo a baseline security check against police records, with more thorough screening available for organisations working with particularly vulnerable or high-security end users; and a 'Secured By Design' approach to their products or services.

The combination of two well-known and trusted brands will help police forces signpost smaller organisations towards a list of digital security

providers that have successfully achieved the DSP certification by consistently demonstrating compliance. It will also help police forces champion organisations that have successfully achieved the Digitally Aware or Digitally Resilient certificates from the PDSC, which can be achieved once they have the necessary steps to protect themselves against the most common types of breach or attack.

As an organisation, Yubico shares the same vision for a safer, more secure internet for everyone. In order to create the standardised model of accreditation, the PDSC approached the company in the early development phase as a valued partner to help support businesses in the fight against the rise in cyber crime.

FIGURES SHOW THAT THE AVERAGE COST OF A CYBER BREACH OR ATTACK IS A CONSERVATIVE £4,180

Founded in 2017, Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts. It is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, with the company's technology deployed by millions of users in 160 countries.

It's this reason that the PDSC invited Yubico to advise and inform how the framework would be shaped for future applications, with a view to being one of the early adopters of the scheme for its two-factor authentication device, the YubiKey.

As a result of this collaboration, there is now a police and BSI-endorsed scheme in development that will give organisations – and individuals – reassurance that every accredited service provider is a robust, reliable and trustworthy partner supplying specialist digital security products or services. It gives a clear answer when individuals and organisations ask who they should talk to about a particular cyber security challenge.

MUCH-NEEDED CLARITY

The new scheme will bring clarity and consistency for end users as well as being a powerful way of making it crystal clear which organisations have invested in highly skilled staff and adopted a 'Secured by Design' approach. The scheme is expected to be a great success, with dozens of companies already interested in gaining an accreditation.

The PDSC will continue to work closely with Yubico, alongside UK businesses and other security service providers to build a comprehensive and scalable accreditation to be rolled out nationwide. The PDSC is looking to launch the DSP scheme in early 2020, with Yubico expected to be one of the first accredited providers endorsed by the BSI.

To summarise, a standard that aims to reduce the vulnerability of organisations to cyber crime and fraud has been a long time coming. The PDSC has taken great strides in protecting SMEs and, if the PCPI's success is anything to go by, its hard work will pay off ●

John Gilbert is GM and Regional VP of Sales at Yubico, focusing on providing secure multi-factor authentication solutions to help enterprise organisations protect access to user accounts.

Hardware security keys enable users to log into many services with just one key and without the need to retype a code time and time again

Picture credit: Yubico