ACHIEVING AN ADAPTIVE APPROACH TO INFORMATION SECURITY IN A DIGITAL WORLD

Jason Connolly, director of Next Generation IT, examines developments in security

In the old days, we used to take a binary approach to security - it was either blocked or allowed. A good example is social media in the workplace, where your choice was simple, you were either blocked from social media or allowed to use it. I remember when using social media was frowned upon in the workplace, but now businesses without an online presence are disappearing fast. So, what does this mean for businesses in terms of security?

Firstly, traditional security, such as firewalls and anti-virus software, no longer work as the only defence in the new digital world. Infrastructure and perimeter protection alone will not ensure accurate detection and cannot protect against insider threats or attacks.

So, what is the answer? Running new digital components will no doubt create complexity in our environment, so we must continuously adapt. Taking a continuous, adaptive approach to information security pushes organisations to embrace new thinking in how they manage data, people and services. However, businesses have limited resources and therefore, the focus should be on the biggest threats, implementing a top down approach. If we were to mitigate every security risk, we would probably have to close off all routes of communication, especially the more modern ones, as well as invest huge amounts of money in IT security. For most, if not all organisations this is just not possible.

So, what do we do? Well, this is where it gets a little complicated. Technology is not as black and white as it used to be. We need a principle-based approach that allows for continued innovation and adaptation. We also need analytics, teamed with a balance of automation and manual intervention. Add these together and you have a force multiplier that will help scale protection and manage risks efficiently, without creating an unaffordable overhead. Do it well and you'll not only remain relevant, but ahead of the competition.

Artificial Intelligence and machine learning are also new and emerging technologies that provide companies with a more realistic and holistic view on security. There are many new ways to control the lifecycle of information, such as sharing your company's system directly with a customer by creating a tailored set of permissions. When you consider these controls as part of a solution to the same problem, they become a powerful toolset that should bring new levels of protection and new levels of freedom.

Therefore, the message is simple, embrace new technology and new ways of working, do not use security as an excuse not to innovate and take a risk based approach to your use of digital services. The ability to adapt is important in business and new digital opportunities are forcing businesses into making decisions, especially as customers are becoming more tech-savvy and more demanding. For example, many companies tell me that their clients want them to use Dropbox. Add this to the counter position of new regulation and standards, such as GDPR and it is easy to see that the only healthy option for a modern business is to take a top down approach. So, start with the board, educate them or bring in the skills necessary to understand this new world. The director, be it non-executive or executive, must be fully aware of the digital world and the risks and opportunities it brings.