Is Cyber Security still a Maze?

I attended Infosec2018 this week at London Olympia. It was a vibrant event as you can imagine with every exhibitor enthusiastic to promote their wares. They were also eager to grab your details with their ‘GDPR compliant’ badge scanner. As a technologist of too many years to mention (I started in IT when 5-inch floppy discs were the rage), what really dawned on me is that it is understandable why many small businesses are not fully engaging in a comprehensive cyber security strategy.

There are many vendors with absolutely great solutions targeted at fixing some particular problems or protecting a specific area of potential exposure. And of course, there were many GDPR compliant or GDPR enabling solutions on view. The information security landscape is increasingly becoming more challenging as technology becomes more pervasive, as the cyber attack surface increases and as the sophistication and scale of

attacks also increases to match.

Cyber Security really needs to be demystified to a large extent to make it more accessible to organisations. What would have really been a helpful approach from vendors would be a means of sharing a common language of Cyber Security. A means of easily identifying where each vendors solution sits in the Cyber Security stack and what it talks to vertically and horizontally.

This would be akin to placing their offering in a Cyber Security jigsaw puzzle so that organisations can clearly see where it sits, what problems it solves and importantly what problem it doesn't solve. Such an approach would make it easier for decision makers to engage and fully commit to adopting and implementing a comprehensive strategy for effective Cyber Security.

It has been an ongoing bug bear of mine that businesses don't easily have a conversation about their security needs. There are some obvious reasons for this such as lack of resource, lack of understanding or no buy-in at senior management level. There is also a tendency to not want to do anything because "we've been OK so far despite all the doom and gloom".

This was reinforced in a very enlightening conversation I had with the team at the National Cyber Security Centre (the public face of GCHQ). They strongly advocated that cyber security ownership now has to be at CxO level of organisations. It will only be taken seriously, and the right strategy and resources effected when CxOs understand the

business imperative of getting this right and the consequences of not doing what needs to be done.

He lamented the fact that too many organisations are sitting back and waiting until it’s too late before they do something.

He also advised rightly so that it was not actually so difficult to achieve a respective level of Cyber Security. The NCSC have published guidelines on this in terms of 10 Steps to achieve Cyber Security and this really is very straightforward practical actionable guidance.

I must say of all the people I spoke to during the day at Infosecurity, he was the most impassioned and engaged individual (long live our public services).

On a final one of my reasons for going to InfoSec was to research products that I think are unique and can fulfil customer needs. I actually met a supplier that has been named Cool Vendor by Gartner. Being my usually cheeky self I said “you guys don’t look cool”, however after spending some time understanding what the product is able to do to expose Cyber Security gaps, I am convinced that every organisation connected to the Internet needs such as service. Literally within seconds of clicking a button you can test for a range of exposures and vulnerabilities. Lack of visibility is a challenge we all face when it comes

to digital communication but it is actually ‘cool’ if you can see your exposures and do something about them before it’s too late. We are in the process of signing up with this cool vendor and will bring you news about the service in the near future.