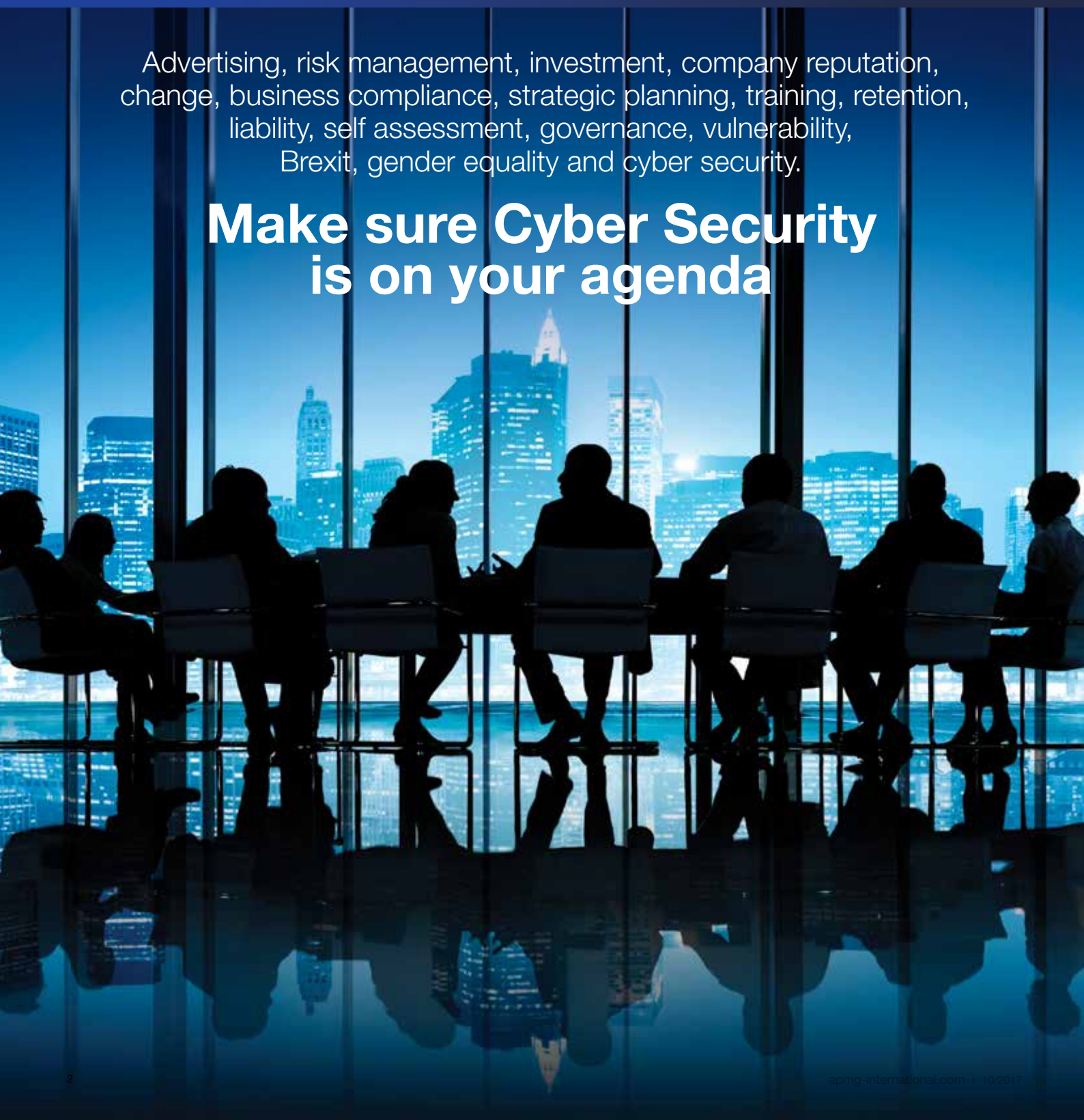
APMG International

Cyber Security

Author: Andy Taylor - Lead Assessor, APMG International

Advertising, risk management, investment, company reputation, change, business compliance, strategic planning, training, retention, liability, self assessment, governance, vulnerability, Brexit, gender equality and cyber security.

Make sure Cyber Security is on your agenda



Cyber Security Spending

Spending money on cyber security, we are told, has become the most important investment a company can make. It is said that companies large and small are not investing the right amount or, indeed, in the right things. Finance Directors are under even more pressure than usual to release funds and provide the necessary injection of cash to enhance the cyber security of their organisations in the face of an increasingly unpredictable world.

The effects of Brexit, the drop in the value of the pound, the drop in the price of oil, the instability in countries large and small from unexpected election results, terrorism, immigration, and other similar events have all led to even greater demands on the already stretched finances of organisations. So how should financiers decide whether to invest in cyber security and, if so, how much and where?

What Are The Options?

The plethora of spending options is frightening even to those who have an understanding of cyber security technicalities. To the less well informed, including those for whom it is not their direct responsibility, the range of technical gizmos, software, systems, courses and other opportunities on which to spend is baffling and worrying. Make the wrong choice and the reputation of the company could be totally destroyed by a data breach which releases millions of customers' private information onto the dark web for sale and misuse. For the finance director to be instrumental in the breach could have a terminal effect on their current prospects, not to mention future careers.

Fear uncertainty and doubt (FUD for short) has sold many things over the years and cyber security is no more immune from its effects than anything else in business. Seemingly daily we can read stories of breaches or the latest way of "preventing any breach ever". The actual effects of breaches are hard to define and even harder to quantify and that in itself makes it very difficult to do the usual cost/benefit analysis for any investment in security. Making the company "more secure" is impossible to define and equally impossible to quantify even for the most experienced cyber security professionals.

What Is The Problem?

If we take a position that says cyber attacks are inevitable, are increasing in both frequency and technical complexity, and are going to affect all organisations of all types, sizes and locations (and plenty of evidence supports this view) we can then begin to make some sense of the cyber world. It is then possible to look at the situation in a way that allows finance directors (and others who should be interested) to make reasoned and appropriate judgements of investments to ensure the organisation does not suffer a major security breach.

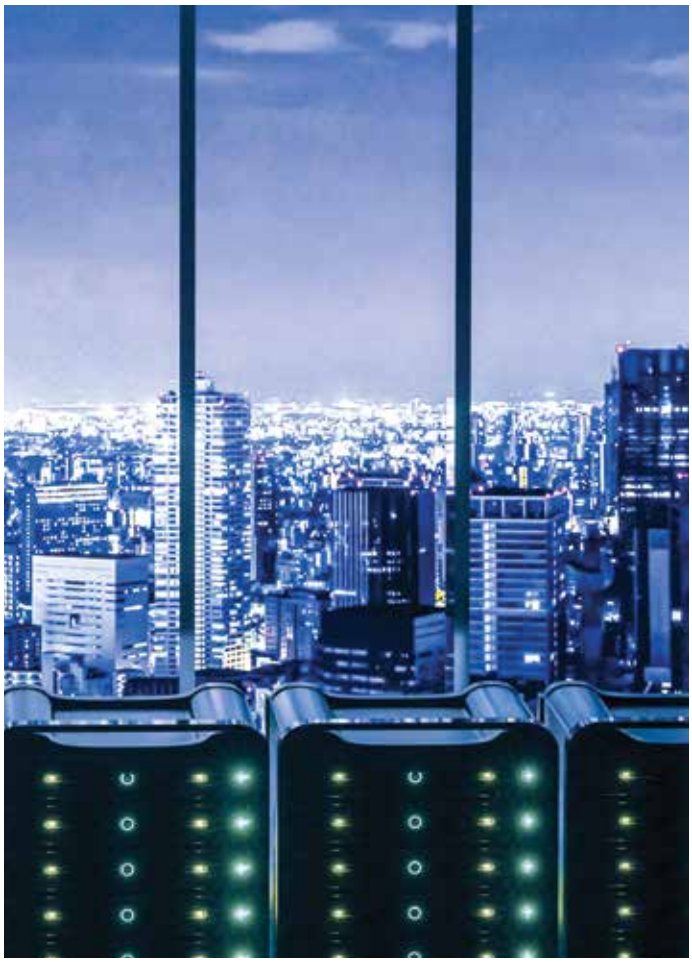
There is strong evidence from GCHQ, from the NSA in America, the Australian Cyber Security Centre and elsewhere that there is a comparatively small number of security controls which have a huge impact on the effective security of an organisation. GCHQ, now under the guise of the National Cyber Security Centre (NCSC), issued the "10 Steps to cyber security" to the top companies in the UK. Similar schemes exist in other countries but all reflect the fact that this small number of technical controls have a hugely positive effect on the overall security of an organisation. In the UK this was further emphasised when the Cyber Essentials scheme was launched which reduced these controls down to five, a number that the NSCS believe every single organisation in the country should be able to implement effectively. "That final word – effectively – is though the crucial point. Too often organisations have implemented controls and perhaps even achieved certification against an international standard such as ISO27001 to "prove" they are doing security properly. The problem is that implementing most cyber controls effectively cannot be done just by putting in extra security guards or fences as you might with the physical security. It needs processes that are defined, tested, monitored and continuously improved. This requires high levels of effective service management in the IT world using ISO20000 or ITIL or the equivalent".

"The majority of successful cyber attacks are not that sophisticated but can cause serious commercial damage. By getting the basic defences right, businesses of every size can protect their reputation, finances and operating capabilities."

Ciaran Martin, CEO of the National Cyber Security Centre

How To Check Spend Effectiveness?

To assess if this is working effectively requires a different kind of assessment, a maturity assessment rather than an audit which is really little more than a spot check of things working on a specific day. Dr Ian Levy, Technical Director of the NCSC, at the Crest/IISP Congress in April 2017 made the comment that; "Pentesting provides a security snapshot which is both its strength and weakness. While it is good at finding unexpected vulnerabilities, in some cases, savvy sys admins are turning off problematic services when they know a pentester is coming to avoid a negative report." Maturity assessments can take time but will ultimately be a much better indicator of effective security working appropriately. The legislative world is also heading this way with the General Data Protection Regulations (GDPR) from the EU demanding much more in the way of record keeping of the way things are done, together with the appropriate history, rather than merely proving they have been present on a specific audited day or the day the incident occurred.



What Is The Future?

The current thinking in the security world is making much more of two specific aspects of security. The first is the ability to respond and recover to a cyber event in a very timely manner. In order to be able to do that, the security systems in place must be monitoring activity in a meaningful way on a continuous basis. Without this there is no chance of seeing unusual activity which in turn could lead to a breach or other security incident. The respond and recover action requires controls to be agile, to be able to be reconfigured, stopped, started or otherwise used to address the current issue when an incident is seen. No longer is "fit and forget" an appropriate option (in the unlikely event that it ever was for cyber security).

The second aspect is that of cooperation. No organisation can consider itself to be an island in this inter-connected world and fostering links with any other organisation, be it in the same sector, the same geography or using the same technology, is critical to successful defence against cyber attack. Information sharing partnerships are slowly growing and are the future for good security. There is a strong pool of evidence that it works – the criminals themselves. They share, work in partnership, specialise in their strengths and buy-in expertise from others in order to achieve their nefarious aims in any way they can. The defenders must do the same and need to make it even more effective if they are to win. Governments can play their part in this and in the UK the NCSC has supported the Cyber Information Sharing Partnership (CiSP). Some specific sectors such as banking are beginning do the same but it needs to grow more quickly and be much more effective if it is to make the difference between successful attack and successful defence.

What About The Supply Chain?

The links between large and small is also a vulnerability that must not be overlooked. The supply chain for any large multi-national is likely to spread across thousands of companies in multiple jurisdictions. Checking the strength of the supply chain is critical and could be very expensive. Small companies, thinking they are too small to attract the attention of attackers, are realising they too are a vulnerability in the supply chain that has to be properly protected. One method being used is a straightforward maturity assessment of the supply chain members which can be performed at differing levels dependent on the level of security assurance required by the parent company. The Ministry of Defence's Defence Cyber Protection Partnership (DCPP) is a very good example where every company who wants to trade with the department must undergo a maturity assessment ranging from the very basic Cyber Essentials up to a full Cyber Defence Capability Assessment Tool (CDCAT) review with perhaps full certification against a recognised standard.

Why Maturity Assessments?

A maturity assessment of the cyber security controls in place in an organisation can provide the information and evaluation that allows finance directors to make decisions on where and on what to spend the company's resources. An assessment such as this should ensure that the controls in place are working effectively thereby making further investment both sensible and appropriately directed. There is little point in spending money on the latest software to monitor traffic on the firewall if users are sharing passwords and sending sensitive company information out on unencrypted emails.

This type of assessment can be done by CDCAT®, a tool developed by the Defence Science and Technology Laboratory (Dstl), for the Ministry of Defence, which is now available commercially through APMG International. It is a quick process (usually less than three hours for an assessment of any system) and will provide a comprehensive report of not only where there are weaknesses to be addressed, but also how to address them and an indication of the potential costs of not fixing them. This allows senior managers to review their cyber expenditure in a very cost effective way, to then decide where to spend more (or less perhaps) and to have confidence that the way money has been spent is delivering effective cyber security.

APMG International is a certification body ensuring that appropriate quality is at the heart of way things are done. They run schemes on behalf of the NCSC to assess and certify high quality cyber security professionals and cyber security training. They are the certification body for schemes such as Cyber Essentials and ISO27001 as well as providing maturity assessments using CDCAT.

APMG International™ CDCAT®

Email CDCAT@apmginternational.com to arrange a demonstration.

CDCAT® is the registered trade mark of The Secretary of State for Defence, Dstl