APMG International

Managing Cyber Risk

Written by Andy Taylor, Lead Assessor at APMG International

www.apmg-international.com/cdcat

Foreword

There is so much happening in our world today, from unprecedented political events to confusion about the direction that Europe is going in, now that the UK has voted to exit the European Union. Businesses of all size and scale have been concerned about managing change for the best outcome in this new economic environment.

One constant is the pace of change in respect of cyber-crime and the ease and speed with which criminals can anonymously make money from fraudulent commercial enterprise. Security for business today is changing from how we have traditionally regarded it. Thieves and disrupters operate in the covert world of digital interactions without borders. Whether they hold you to ransom to pay for an encrypted release key, trick you into paying them money through spoofing your emails, take your data or take control of your business by invading critical control systems…you will be affected at some stage and most of you already have been to some degree. We take physical security for granted, in the same way we have culturally adopted health & safety regimes at work. Managing cyber security is the current challenge to be addressed.

The cyber activist, whether criminal, terrorist or just an individual doing it for kicks, is winning the game. In most cases this is because we are simply not prepared for the threats they can create with ease. These people develop ways to infiltrate our lives through technology as full-time and well-funded specialists, and they are constantly finding new ways to stay ahead of the game. It is suggested that funding for the "Hacktavist" is greater than the discretionary investments that commerce usually spend on their enterprise to defend themselves against attack. Is it any wonder we are losing the fight?

Regulatory change and empowerment could have effects on the focus we put on managing our data security. We need to comply with these changes in a way that provides the best security outcome for our businesses, and not just complete a tick-box exercise. The new penalties for data loss are game changers in terms of cost to business. Most agree it is wiser to invest in defence to provide real operational business value, rather than paying fines and still having to spend operational investment on remedial actions to improve security.

The focus on operational risk management is changing and cyber security risk in some companies (though by no means all) is being placed on an equal footing with other risks. The General Data Protection Regulation (GDPR) comes into force in May 2018 and will drive change by stick rather than carrot. As a self-funding organisation the regulator will be dependent on fines to keep their operation going so expect some early casualties. Some of these will be directly associated with the simple failure to prepare ourselves against defending data loss and cyber intrusion.

One of the obvious risk management options is to insure yourself against cyber-crime either:

(a) directly, through specific cyber risk cover; or

(b) by having extensions for cyber risk to existing business insurance.

However, due to a general lack of understanding of exactly what you should insure against, it becomes even more important to understand the risk, and have knowledge that supports your strategy to self-insure by:

- accepting the risk in your overall risk management strategy;
- mitigating the risk by establishing a clear fact-based understanding of what that risk is and accepting the cost of remedial action;
- transferring the risk to insurance; or
- a combination of these.

The first priority is to understand what the risk actually is.

This paper takes a look at the practicalities of good cyber security management and what it takes to defend ourselves against cyber-crime in its most fundamental form. This may be old news to some, but how many companies who consider themselves safe from cyber-crime could undertake an independent assessment of their cyber defences and have no further actions required?

Andrew McQuade
Managing Director of Kyngswoode Services Limited

Introduction

Cyber attacks make the news headlines almost every week and many people in business will look at them and be grateful it doesn't mention their company. Many people will think that it is only a matter of time before they are hit and others will think that they are so careful spending lots on cyber security that it will never happen to them. Some people in smaller businesses and those which are perhaps more mundane in the services they offer, may believe they do not need to worry – who would bother to attack me or my business? Those who take online payments may think they are the prime target for cyber criminals but this is not necessarily the case. The attackers will go wherever they feel they can get a quick and / or high return for their minimum efforts.

There are new challenges that need to be considered by every business or organisation. The new regulations regarding the protection of personal information (the General Data Protection Regulations – GDPR) which, despite Brexit are anticipated to be implemented in the UK in one form or another, have the capacity to levy fines on those who suffer a data loss. The fines could be up to €20 million or 4% of the annual worldwide turnover of the organisation, whichever is the higher. It could also deliver criminal charges at the door of senior managers who are deemed responsible for the damage caused and that might include directors. The recent significant increase in the use of ransomware (software that will encrypt all files until a ransom is paid to release the encryption key) has affected a large number of businesses from the smallest to the largest.

There is a further major concern. The damage done by a successful cyber attack can be felt by parts of the organisation other technical issues cannot reach. Shareholders, staff, board members (especially non-executive directors), customers, clients and suppliers can all be adversely affected by a cyber attack. What might be termed consequential losses in insurance terms are very likely to far outweigh the actual cost of the attack. Insurance may cover some of this but it is most unlikely that all the costs of a major attack will be covered and so the ongoing effect on profits, share prices and the overall confidence of clients and customers could be the most significant impact.

What does this mean to me and for my organisation?

Many technical issues affect companies ranging from the seemingly standard IT issues of broken kit to damage to the water supply or a lightning strike. All of these examples are dealt with by the relevant technical team, either in-house or outsourced as appropriate. Cyber attacks are different. If the organisation suffers a cyber attack it is likely to impact everybody in the organisation to some degree. Indeed, it is highly likely that the start point of the attack may well be a member of staff, perhaps one of the directors or the temp working in the goods loading area. It is therefore the remit of every member of staff to take responsibility for their own cyber security with assistance and guidance from the technical team.

The different ways a cyber attack can be launched is often called the attack surface and it is very large and does not need to be complex. The easiest ways are often preferred by the criminals simply because they get their returns quicker. Recent ransomware attacks have been based on a spear phishing email being sent to a member of staff of a smaller organisation. The email looks genuine but has been carefully targeted at members of staff of the organisation based on some straight forward research. This research has provided enough information for the attacker to know what to address and to whom to address it in order to have the greatest chance of success.

The live link in that email, or an attachment to it, will download encryption software onto the computer which will then mean that the user no longer has any access to their files. A message will then appear on the screen requesting a sum of money to be paid (usually in bitcoins) in order for the key to the encryption to be provided allowing (in theory at least) access to the files on the computer once more.

One of the very clever parts of this crime is that the amount of money demanded is not excessive. For smaller organisations it might be no more than £100 or for larger companies perhaps a couple of thousand, enough that the senior managers say, "Oh just pay it and be done with it." Whilst this may (or may not) deliver the key, the problem is that this highlights that company to the criminals as one that does not have the right precautions in place. This in turn means the criminals are likely to return with a new demand and there are stories around of single organisations being hit several times paying out much larger sums of money than the initial attack might have cost. The simple process of having offline backups would have alleviated the issue and would have avoided the need for any money to be paid.

"Be warned, the sophistication of these attacks is steadily increasing and it is clear the best solution to addressing these type of attacks is an operational risk management capability, such as using endpoint protection with well-trained central cyber security operations staff. Using endpoint security (some software installed on the PC) that stops this type of infection being installed in the first place is the only really effective way of dealing with them. Training business users not to click on links is good but will inevitably fail at some point. For operations staff, training is an essential part of the capability mix not simple reliance on technology. Off-line back-ups are critical but using a technological protection such as link protection (e.g. TrustWave) in addition will be more cost effective in the longer term."

Martin Huddleston of Dstl

The way in which these sorts of attacks work make the whole cyber security issue everyone's problem. With the best technology available it is possible to reduce the risk of an attack like this being successful but it will never eradicate it entirely (unless there is no internet connectivity which is probably not acceptable for good business practice in most companies). Any member of staff might receive the email, indeed in a slightly more sophisticated version of this attack, after some further research perhaps on social media, the email will be sent to a junior or newly joined member of staff and appear to come from a senior manager. The email will, to all intents and purposes, look genuine. The target person will want to do the best for their employer and so will do as requested.

In a more worrying attack, the chief finance officer of a large company was emailed by the CEO and told to transfer some funds to a client's account. The transfer was done but it turned out to be fraudulent and the significant sum of money was lost[1]. Obtaining the necessary intelligence to make such an email appear genuine is not too difficult with the prevalence of personal information available through social media, Companies House and company web sites. In one interesting case access was gained to a company's information through the Managing Director's PA who routinely bought flowers for the boss from a local florist. The florist kept the details of the boss on their records which were a relatively straight forward target providing intelligence for a more sophisticated attack on the main company.

All in all, this means that cyber security cannot be seen as a purely technical issue. Whilst the techies certainly have a large part to play putting appropriate security measures in place, the behaviour of everyone in the organisation is by far still the weakest element of the defences. Social engineering to obtain personal details to either enable or at least facilitate an attack, poor practices opening suspect emails or attachments, downloading videos, documents and pictures from unknown or untrusted sources, loading viruses from USB drives they have found or obtained from dubious sources, all happen because people do the wrong thing, often knowingly so.

1.Source: https://www.theguardian.com/technology/2015/feb/05/company-loses-17m-in-email-scam

The more "traditional" cyber attack of hacking into a business network is still very common. The methods used to gain access vary from the relatively straight forward to the complex and technically difficult. The attack on Target in the USA in 2014 was based on access being obtained through a supplier to the retailer. A data connection (presumably from an infected laptop) exclusively used for electronic billing for their air conditioning system, allowed the attacker to gain access to Target's main administration network that stored the customers' personal details[2].

This highlights the importance of checking the security not only of the organisation's own systems but those of their suppliers too.

The more recent attack on TalkTalk was apparently achieved by hiding a straight forward hack behind a distributed denial of service (DDoS) attack that closed the majority of the TalkTalk system down and pre-occupied the techies in dealing with it. The effects of this attack are still being felt as this paper is being drafted but a conservative estimate puts the cost to TalkTalk at between £42 and £60 million. Whether this results in a hostile takeover, a severe dent in the profits or simply a loss of customers' confidence is difficult to determine. What is clearer is that the senior executives lost their credibility as a result of the poor handling of the events as they unfolded. Seeing the CEO of TalkTalk, Dido Harding, being interviewed and failing to answer seemingly straight forward questions about encryption, for example, highlighted the lack of preparedness that in the future is likely to attract the most serious attention of regulators and the Information Commissioner's Office. An incident response plan is an essential document that every organisation large or small must develop and then regularly exercise and update[3].

MPs said TalkTalk had not done enough to prepare for an attack on its systems and slowness to protect computer systems was weak across British industry. They recommended measures including:

- **A chief executive's pay should be based partly on maintaining effective cybersecurity to reduce the chances of a crisis[4].**
- **Companies should appoint an officer with day-to-day responsibility for protecting computer systems from attack.**
- **It should be easier for consumers to claim compensation if they are the subject of a data breach.**
- **Companies should report on their cybersecurity measures and show they have identified and dealt with weaknesses if a breach occurs.**

Dealing with the problems

The first major problem with cyber security is determining the extent of the risk and the potential impact of an attack. There is some growing evidence from attacks in the last few months and years that the cost of a successful attack is very significant for any organisation. There are examples of companies ceasing to trade as a result of an attack - such as CODE Spaces closing down because they couldn't keep up with the attacks[5]. However, others having suffered seemingly minimal effects, were those who were properly prepared and aware of the potential consequences.

The risks faced are in some ways universal. Just because the organisation makes cardboard boxes rather than offering insurance policies makes little difference to the criminal. It is true that some organisations are a more attractive target and that is, to some degree, part of the defence. Making your organisation less attractive to criminals than the one next door (talking digitally rather than geographically) is a key aspect. In the same way that a burglar alarm on a house says to a criminal this house is less attractive to burgle than the one next door without an alarm, cyber security measures should have a similar effect.

As with the management of any business risk, there are some key steps to take when considering cyber security. The first is to get a good understanding of the size of the problem and its consequences. A full business impact assessment for the information an organisation holds is a clear starting point. Understand what information is obtained, processed, stored, passed to others and ultimately disposed of. This is not about individual pieces of information so much as types. It might include for example: customer information containing personal details – date of birth and contact details - bank account details and transaction details for their purchases from the company. Having determined what is held, the value of that information must be analysed. What would it cost if the information was lost, inappropriately accessed or if it was corrupted in some way? This valuation should include, for example, recovery costs, potential fines from regulators or the courts, business interruption and compensation.

Once this is done for all the information types there should be a clear agreement on which information is the most critical to look after and a general assessment of how much risk the senior managers are prepared to accept - commonly called the risk tolerance or risk appetite. This risk appetite will be directly linked to money – the lower the tolerance of risk (the less the seniors want information to be lost) the more must be spent on security.

The cyber security world is not new and it has been working reasonably effectively for some time. So the next step is to determine what security there is already in place and how effective it is. Is it comprehensive and working well or are there some holes or weak links in the security chain? In part this can be done by a technical assessment such as a penetration test. This will determine if there are any technical holes in the defences and should provide advice as to how to fix them. This might lead to compliance with a specific security standard such as PCI DSS, ISO27001 or similar.

Compliance is good and certainly helps to develop the right security attitude and approach. There is a problem though since the tests, audits and approvals are really only valid on the day they are completed. On the day after the audit, things are likely to have changed.

2. *Source: http://www.securityweek.com/target-hvac-contractor-says-it-was-breached-hackers*
3. *Source: https://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack*
4. *Source: https://www.theguardian.com/business/2016/jun/20/talktalk-paid-its-ceo-an-extra-18m-in-2015*
5. *Source: https://www.itgovernance.co.uk/blog/the-attack-that-forced-code-spaces-out-of-business-what-went-wrong/*

There will be a new threat, a new piece of equipment, a new competitor or new senior manager with a different risk appetite. In all cases the previous certification is effectively no longer valid and must be redone. This is, however, usually too expensive and impractical.

There is an option to use a tool that determines not so much whether controls are in place but how effectively they have been implemented – a maturity assessment. The **Cyber Defence Capability Assessment Tool (CDCAT®)**, developed by the Defence Science and Technology Laboratory (Dstl) on behalf of the Ministry of Defence, is based on best practice. CDCAT can check which controls are best placed to address the current threats most effectively. Since it is a maturity assessment this will provide a very sound indication of how well those controls will protect the organisation in the future. It is also able to provide, at pace, some quantification of the financial impact of security breaches. The report from the assessment will also include best practice advice on how to fix the problems identified.

Once the assessment has been done there needs to be a plan of work, a programme or project depending on the size of the task, to deliver improved security in the areas identified as weak which therefore provide vulnerabilities. Once the work has been completed, or at least at some stage after the start, it should then be routine to recheck the maturity of the controls to see if there has been an improvement in the overall security status of the organisation. This assessment can be repeated at any stage to update the view of the organisation's security maturity, as can the review of the different information assets and the risk appetite. It is most likely that something will have changed and needs to be reflected in the business impact analysis and the risk assessment.

Since January 2015, the Cabinet Office has been using the Cyber Defence Capability Assessment Tool (CDCAT®) to deliver cyber assessments for business-critical assets across the Public Sector, including central Government assets that form part of the UK Critical National Infrastructure.

Using CDCAT, which was developed by Dstl and delivered by APMG, the Cabinet Office has been able to assess the overall cyber defence capability for a variety of different critical systems within Government. CDCAT allowed various departments to gauge how effectively they were implementing their most important security controls, and gave them a starting point for any future remedial work that might need to be considered. The Cabinet Office presented this data quarterly, via aggregate reports that allowed benchmarking across Government, showing themes and trends.

Cabinet Office funded a number of enhancements to CDCAT that provides a "Government Grade" high level view of the strengths and weaknesses across Government assets, identifying where changes may need to be made, or if modifications need to be implemented. CDCAT also enables an overall view of how effectively the budget for cyber defence is being used, which can then inform the efficient and appropriate allocation of funds.

The impact of change

In order to address the major issues in cyber security it is essential to understand that there is really no difference between the business risks that organisations face in other areas and those from the cyber threat. The analogy often used is of health and safety. A few decades ago everyone was being told to worry about health and safety – people had to be trained how to manage it, how to ensure staff were safe and educated about the benefits of the work being done. Today most organisations barely think about health and safety other than in specific high risk industries. There is no need to explain to staff or even visitors that if there is a fire there are exits and procedures to follow – it is in the culture of organisations and of most of the population. That has to be the aim for cyber security too.

In a similar way, it is second nature for boards to consider the risks from health and safety, albeit that few of those board members are specialists in the subject. The aim must be for the same level of concern and interest to be shown in cyber risk by the board members of organisations large and small. Indeed, it could be argued that the risk to the business from a cyber attack could be much greater than a health and safety incident and so the board's interest should be even greater.

The way an incident is managed is critical to the ongoing success or otherwise of the business. Poorly handled, even a relatively minor breach of security could result in major press coverage (usually adverse), significant fines by regulators and the loss of customer and shareholder confidence. Wiping the value off the share price is unlikely to be a major concern for smaller businesses but the loss of customer confidence and the drop in sales, in customers and in revenue is going to have a much larger effect where much of the worth of the company is in its client list or order book. Indeed, if the loss is of the details of those clients, the effect could be disastrous if a competitor gained those clients' details and thereby stole the business.

The regulators also have a part to play. They will naturally want to ensure that the interests of the innocent bystanders affected by a breach – customers, staff and others – are appropriately looked after by the organisations who hold data about them. The way the regulators work differs from industry to industry but the general management of information is overseen by the Information Commissioner's Office (ICO). The current Data Protection Act (DPA) introduced in 1998 is their handbook and the eight principles it sets out are the basis of all information security. The new European General Data Protection Regulations (GDPR) which are currently in the process of being implemented, will replace the DPA in one form or another regardless of the vote to leave the EU.

One of the key factors in the new GDPR is the requirement to inform those affected by a breach very soon after it becomes apparent that it has occurred, usually within 72 hours. This will have a significant impact on the way organisations monitor their security and how they handle breaches. There will always be a debate about the benefit of public notifications of breaches. Those in favour will say "naming and shaming" helps to improve standards whereas those opposed will suggest that keeping the details of a breach confidential reduces the risk of further breaches and will not affect competitiveness in the industry.

Overall the EU has come down on the side of notifications at least to those directly affected. It remains to be seen if that will include more public notifications as well but it is highly likely that a confidential notification to someone affected will very quickly get into the public domain such is the power of social media and the like today.

There is a view that says as soon as there is a public notification of a breach the value of the information stolen is significantly reduced. To take an example of the loss of credit card details, one of the more common breaches, if the details of the breach are made public then fraudsters will know they have very limited time to take advantage of those card details before the issuing banks block all transactions on the stolen cards. This does not however stop the use of those details in other ways such as identity fraud, one of the areas still increasing in frequency in recent years.

Communication has, therefore, become critical in the management of data breaches. Handled correctly, the communications can actually enhance the reputation of the breached organisation. Handled badly and the results can be catastrophic. Good communication can also lead to improvements in the security posture of an organisation. If the staff hear of breaches and the use that has been made of the data so obtained, it can have a positive effect on their own behaviours, perhaps reducing the chance of a breach in their organisation. It must always be remembered however that information alone will rarely change the behaviour of people. They need other things, such as incentives, to really change their behaviours appropriately.

Cultural adoption

Changing the culture of an organisation has always been a major issue and there has been much work done on the best way to achieve change effectively and efficiently. Overall, it must be regarded as a project or programme of work (depending on the size of the organisation), properly planned, resourced, financed and managed. It will not happen overnight and it will rarely happen without some issues.

One of the most significant factors that has been proven time and again to increase the chances of success is the senior management's active support for the change. Without senior management buy-in, it will almost certainly fail and seeing the bosses not just "talking the talk" but also "walking the walk" is critical to the expectations of success. This means then that those managers must understand what the risks are and what is to be done to reduce or mitigate them. This then comes back to the purpose of a business impact assessment and risk assessment.

It is becoming increasingly common now for someone to be appointed at board level with the title of senior information risk owner (SIRO), chief information security officer (CISO) or the equivalent. This person must be the champion for good security and must be able to explain in business terms the reasons why information security in general, and cyber security in particular, are critical to the organisation. They may have a technical background and may need to be able to discuss security measures at a technical level with those in the organisation, but overall their task is to educate and advise the board. They will be the one who is accountable for the delivery of better security and the business benefits associated with it. The principle of "make someone senior accountable for security but make everyone responsible for it" is a good starting point.

Even though they are at board level, they will not be able to accomplish the full cultural change required alone. One way of assisting them is to designate security champions or the equivalent at all levels throughout the organisation. Whilst the SIRO/CISO will be the champion at board level, they will need champions on the shop floor, in the HR department, in the IT section and everywhere else. There must be coverage of the total organisation if it is to be successful. These champions should not be technical (in security terms) and must understand how security affects the specific area in which they work. It will be a secondary role perhaps, but they will be advertised as the first point of contact for anyone with questions relating to security. They will need training and they should be provided with resources to help them achieve the aims for the security of the organisation. This might include, for example, mouse mats with security reminders, screen savers, posters, competitions, awareness days and so on. In some major organisations security is so important that they choose to have a full department just raising awareness of security issues. They will send out fake phishing emails with a live link or attachment that, if clicked on, takes the user to an in-house area where they can be reminded not to click on links, not to open attachments and so on. Repeat offenders can suffer serious consequences which could result in dismissal in appropriate circumstances.

"There are better alternatives than this cultural enforcement. There is likely to be a staff backlash from this stick-wielding method and it is, in the end, unlikely to be 100% successful. It is better to address the issue with an operational risk management capability based on a combination of skilled operations staff and technology. But there is a price to pay. Doing security on the cheap also has a price and potentially a much more significant cost in remedial actions, such as when business user training fails as it will."

Martin Huddleston of Dstl

When an organisation implements such a programme of cultural change, showing the return on the investment (in both money and time) is essential if boards and shareholders (and perhaps in the future regulators) are to be convinced of its value. Undertaking a series of maturity assessments monitoring the improvements over time, and making use of the subsequent recommendations for action to fix, could be one way to achieve this. An assessment planned in at key stages of the project or after six months of a programme being initiated could be a quick way of reporting progress. Reporting to the board, and perhaps investors where appropriate, could be a powerful tool for improving security overall.

Using a variety of messages is essential to engage staff and ensure they do not become bored or forget and revert to old ways. Whilst the main target of the information provided to them has to be the benefit to the organisation, benefits to them as individuals of not having their credit card used fraudulently, not having their identity stolen and not have their credit rating affected by a fraudulent act can also be strong motivations for staff to take more care. As the general public awareness grows in terms of the consequences of a stolen identity, card fraud and the like, their buy-in should gradually be getting easier to gain.

An excellent example of the right approach came recently from a major company where they had problems with people getting into their premises without suitable authorisation and checking. Arriving at a building with the very plausible excuse, "I'm from IT to fix a computer but have forgotten my pass" usually got them in. This was despite a major awareness campaign covering the risks of such unauthorised access and the potential consequences of it. The senior managers decided to implement a new programme so that about once a month they offered an iPad to a secretly designated employee if they could get in without a pass. Anyone stopping them would get the iPad instead. They never had another problem not least because the first person to be designated to try was the CEO who was stopped by an employee! Motivation is a very powerful change enabler. It is clearly appropriate to use both carrot and stick when deciding how to change the organisation's culture.

What could the top ten actions of a strategic change look like?

There are some clear steps to take in order to ensure the cyber security of an organisation is as good as it can be. These include, in no particular order:

1. Know your business and the digital assets upon which it depends. There needs to be a very clear understanding of the information held and its true value. This is likely to differ for every organisation and is fundamental to providing secure information management.

2. Agree an overall risk strategy that you intend to manage. The risk strategy will include ideas such as outsourcing, the use of encryption, checking on suppliers or those with whom the organisation trades electronically.

3. Include cyber defence management as an equal stakeholder in the strategy. Cyber defence management has to be pro-active and must attempt to look forward at what might affect the organisation in the future. To date many organisations have had a reactive policy or worse a passive "wait and see" policy. Moving into the realms of pro-active requires a full and detailed understanding of the vulnerabilities in the organisation based on principally the poorly implemented security controls.

4. Quantify & evaluate the financial impact of data loss or business outage for your business. A business impact assessment is the only way risk can be managed in anything like a cost effective way. It is impossible for most organisations to protect all information to the same high level that they would use for the moist valuable information. A clear understanding of the risks the organisation is prepared to accept will help to focus the mind on the more valuable and important information assets.

5. Break your strategy into the operational risk management of lifecycles covering training, equipment, personnel, information, policy, organisation, infrastructure and logistics. All these elements must be present in the organisation throughout the lifespan of any piece of information. Each needs assessment to see what is in place and what is missing. The gaps then need to be considered and dealt with appropriately and a programme of work designed and implemented to address them.

6. Assign the responsible "Champions" to each business asset and defensive strategy ensuring that their purpose is clearly business driven. As discussed earlier, the culture of the organisation must reflect the willingness of everyone to act in a secure and safe way. Local champions who can advise, guide, answer questions, feedback issues and generally be the senior managers' eyes and ears in the workforce is a very effective strategy.

7. Create the topology of what you are protecting and the dependencies of each business component. Mapping data/information flows and the security architecture will help to identify where there are issues or areas of weakness. The interconnections are often a weak point between strongholds of security. Transferring information unencrypted, even internally, might be a risk if the attacker is a disillusioned staff member wanting to do damage or make a name for themselves. Understanding the links and transfer mechanisms is a vital part of the overarching strategy. Mapping the dependencies might also highlight critical pieces of data that affect the most important processes in the organisation.

8. Benchmark against known cyber security outcomes of how well the organisation currently performs against each of these controls and publish the findings to the risk board and Non-Executive Directors. Use ISO/IEC:27001:2013 as a starting benchmark if the standard is already implemented and it is recognised within the organisation that there are limitations in maturity assessment of operational effectiveness. An assessment based on a number of the best practice models available in the UK (including ISO/IEC27001:2013), the USA, Australia and elsewhere should provide a comprehensive report on the maturity of the controls in place whilst also identifying any gaps between the current state and best practice.
9. Agree plans that include the cost to remediate problems, to transfer risk to insurance or decide what you are prepared to self-insure. Any planned improvements to security including culture change must be properly planned, managed, funded and delivered. Culture change in particular needs a well-considered and carefully designed plan with clear measurables to monitor progress. A maturity assessment of the controls as they are implemented should provide the necessary monitoring.
10. Repeat the quantification and business strategy assessment whenever the business, the systems, the threats or the vulnerabilities change. The ongoing monitoring of the state of the security of the organisations is critical. Once-a-year audits for compliance or to meet regulatory requirements are a small part of the answer but they must be regularly enhanced by frequent assessment whenever anything changes. Changes could come in the form of new threats, new attack scenarios, new technology or new risk appetite being expressed by a new manager or any number of other causes.

Maintaining the continuous improvement journey

The cyber security world will never stand still. The changes are increasing both in the frequency and in the speed with which the new threats appear. It is therefore critical to ensure the organisation's defences also improve and develop. Getting ahead of the criminals is not really an option for most organisations but at least keeping pace should be. This does involve work in order to ensure that the controls which are most significant in delivering security are well implemented at a maturity level of 4 or 5 (on a standard Carnegie Mellon type maturity scale) if real security is to be ensured. At level 5 maturity, the process will be fully optimised which means that when something happens, as it will, the process is quickly updated and enhanced to deal with the new situation. Having a security process, however well-documented, sat on the shelf gathering dust is not going to protect the organisation from threats which are continually evolving and developing.

Undertaking regular assessments against best practice will help to monitor the progress and the development and should also allow the always-limited funding to be spent most wisely in those areas delivering the most important aspects of security. An assessment must be quick if it is to be effective in helping to deliver effective pro-active security in an organisation. Ideally, in less than half a day, a maturity assessment of the effectiveness of the controls in place will be completed along with the automated production of a comprehensive action plan to address the vulnerabilities in the system that has been assessed.

Compliance may be required to satisfy the regulator or clients but an ongoing programme of maintenance and enhancement is the only way to try and ensure the security status is maintained. They can also provide key milestones for investors, boards, shareholders and other interested parties. Setting a target maturity to achieve in certain designated controls by a particular date is an excellent start and will help to convince senior managers that the investment was worthwhile.

It is almost impossible to prove a negative and so saying we have not been attacked and therefore we are safe is not a good strategy. Regular assessment against a selected best practice framework is a much better way and will provide a much more convincing argument for the board, staff and shareholders. It also helps to convince suppliers or customers that the organisation is doing all it can to look after their valuable information too and is not providing an easy backdoor into their business.

There is beginning to be a movement in the UK towards requiring cyber security as part of contractual arrangements. The UK Ministry of Defence now requires anyone wanting to work with them to have the UK government's Cyber Essentials certification. Whilst this is a high hurdle to reach it does set a minimum standard which is going to be raised as time goes on. Already the next step will be to have Cyber Essentials Plus – the more intensive version that includes some independent testing. Time will tell the next steps but the UK government in general is following a very similar path. It would be highly likely that in a few years' time, no company would be allowed to trade in the UK without proving they have an appropriate level of cyber security in place. The success or otherwise is increasingly becoming very dependent on the cyber security the organisation has in place and, more significantly, its effectiveness.

About APMG International's Cyber Portfolio

In response to mounting risks in a digital age, APMG International has designed a broad portfolio of world-class cyber security products. We've partnered with CESG to deliver their Certified Professional and Training schemes, and the Defence Science and Technology Laboratory (Dstl) to develop The Cyber Defence Capability Assessment Tool.

Find out more at **www. apmg-cyber.com**

The Cyber Defence Capability Assessment Tool (CDCAT®)

CDCAT is a comprehensive way for organisations to assess their existing cyber defences, identify vulnerabilities and see what improvements should be made. CDCAT was developed by the Defence Science and Technology Laboratory (Dstl), for the Ministry of Defence.

Find out more at **www.apmg-international.com/cdcat**

APMG International™ CDCAT®

About Kyngswoode Services Limited

As a Channel Partner to APMG International, Kyngswoode Services offers CDCAT® and CDCAT® Insurance services which provides a cyber risk underwriting report to assist brokers and underwriters establish a fact-based view of their clients' cyber vulnerabilities. This report provides evidence of the maturity of each security control, blockers to improvement and benchmarks an assessed organisation against peers and cross industry sectors. This helps brokers and underwriters achieve better cyber insurance terms for their clients.

Find out more at **www.kyngswoode.com**

FOLLOW US ONLINE

APMG International

@Cyber_APMG

apmg-international.com/news

www.linkedin.com/company/apmg-international

www.apmg-international.com