littlefish
Cyber Security Services

Cyber Certifications
Gold Dust or Fools Gold?

www.littlefish.co.uk/futurethinking

Contents

Cyber Certifications
Gold Dust or Fools Gold?

Do certifications really protect you from modern cyber threats?

Katy Hinchcliffe
Head of Cyber Security
Littlefish

How safe is your business? More pertinently, how safe are the IT systems, infrastructure and data on which your business depends? This is the question which any organisation has to ask itself in 2020 and the answer to the question – if it's asked and dealt with honestly – is sadly often 'Not as safe as we would like to think it is'.

There are many reasons for this, not least the ever changing nature of the threat from cyber criminals, fuelled by the irony of the fact that every technological step forward which makes an organisation easier to run and security controls simpler to maintain, also arms the hackers and criminals with ever more sophisticated means via which to counteract those security controls. Another major factor which leads to many organisations being nowhere near as well protected as they might assume is, paradoxically, the number and perceived effectiveness of the many cyber certifications and compliances which now operate across a range of industries and technology sectors. Often seen as the gold standard, certifications such as Cyber Essentials, Cyber Essentials Plus and ISO 27001 are, all too often, the benchmark against which organisations measure their cyber security and, having been met, are treated as a panacea. The question which needs to be asked is whether, in a landscape of ever changing security requirements, with factors such as cloud computing, AI and the Internet of Things (IOT) altering and expanding the nature and number of threats to be dealt with, a single certification – or even a set of overlapping certifications — can still be considered the ultimate resolution to the issue of cyber security. This paper looks at the general scale and nature of the global cyber-crime risk, the specific factors which newer technologies are introducing to the equation and, most vitally, the steps which need to be taken over and above gaining mainstream cyber certifications in order to safeguard an organisation. To put it simply, in a world where Mark Zuckerberg can discover that his Twitter and Pinterest accounts have been compromised (according to the hackers involved this was largely due to having a password consisting of 'dadada'), can anyone feel relaxed about their security because they've ticked the right boxes for the next 12 months? Given that many certifications are a legal requirement within certain sectors or

"Often seen as the gold standard, certifications such as Cyber Essentials, Cyber Essentials Plus and ISO 27001 are, all too often, the benchmark against which organisations measure their cyber security and, having been met, are treated as a panacea."

across specific geographical entities, the idea of setting them aside completely is an obvious non-starter. Nor would it be recommended, since a certification such as Cyber Essentials provides a robust and measurable baseline from which to build a comprehensive cyber security policy. The idea of building a comprehensive policy upon the foundation of a certification is at the root of an effective approach to security – the certifications gained should act as a starting point but not an anchor, providing the platform from which to respond in an agile and intuitive manner to changing threats.

For many organisations the prospect of having to go above and beyond the certifications they have may seem daunting, in terms of budget, manpower and effort. The wider problems facing the cyber security industry underline this point. Survey after survey places cyber security at or near the top of the issues rated as most important by the C-suite, and yet across the cyber security industry as a whole there is a crisis in recruitment, skills and this is surely the bottom line – the ever increasing number and scale of data breaches. We'll be looking at the issue of breaches – their nature and what it says about relying on certifications – in more depth later in this paper, but the topic of the cyber security skills shortage is worth considering briefly now as it highlights one of the reasons why many organisations might feel content to rely on ticking the boxes of a certification. The question of the investment needed to enhance security measures is fairly easy to answer in terms of the financial and reputational damage which any hacking event or data breach could cause, but the task of finding the right people to take advantage of that investment is somewhat more problematic. According to the 2019 $(ISC)^2$ Cyber Workforce Study – the $(ISC)^2$ being an international, non-profit membership association for information security leaders with more than 140,000 members – the number of unfilled cyber security positions globally is currently a huge 4.07 million, up from 2.93 million in 2018. This is a result gathered by surveying 3,237 individuals responsible for security/cyber security in North America, Europe, Latin America and Asia-Pacific, so can be taken as highlighting a global phenomenon. The reasons for this labour shortage could be traced back to a lack of training provision for what is a highly complex and technical role and a dearth of industry-wide consistency in aspects such as the individual certifications and qualifications needed, but at the root of the problem is the

fact that, in historical terms, cyber security is still an extremely new industry. The first computer virus was created as long ago as 1971, when the internet existed only in its most primitive evolutionary state as the Advanced Research Projects Agency Network (APRANET), a network of computers created by the US Defence Department. Known as the Creeper, it was a worm, a type of virus capable of replicating itself and spreading across systems, but was harmless in nature, and it wasn't until 1983 that the first US Patent for cyber security was granted. For the record, this was U.S. Patent 4,405,829, granted for a 'cryptographic communications system and method', namely the kind of algorithm which forms the bedrock of modern cyber security.

The point of this short history lesson is to underline the degree to which cyber security – even when compared to the IT industry as a whole – is a field in its relative infancy. It may seem like a rather arcane measure of the maturity of a field of operations, but the fact that the UK's Chartered Institute of Information Security only received its royal warrant in 2019 (compared say to the Soap makers Company which has been around since 1638 and the Royal Medical Society dating from 1773), demonstrates that this is

> *"Survey after survey places cyber security at or near the top of the issues rated as most important by the C-suite, and yet across the cyber security industry as a whole there is a crisis in recruitment, skills and this is surely the bottom line – the ever increasing number and scale of data breaches."*

> *This means that widely accepted, road tested definitions of the right and wrong way to approach the industry have yet to be established, honed and passed from practitioner to practitioner. The certifications this white paper is examining have arisen, in no small part, from the vacuum created by this absence.*

a field of expertise which is still in its earliest incarnation. This means that widely accepted, road tested definitions of the right and wrong way to approach the industry have yet to be established, honed and passed from practitioner to practitioner. The certifications this white paper is examining have arisen, in no small part, from the vacuum created by this absence. Given the overwhelming importance of IT infrastructure — not only individuals and organisations but also to the coherent functioning of any modern developed state — it is hardly surprising that governmental bodies have attempted to provide a base level of competence and good practice to safeguard the structures they rely upon. The downside of this is the temptation to take these certifications as anything more than a base level, in the manner of a car owner assuming that passing their MOT means that they don't have to worry about servicing or maintaining their vehicle in any other way for another 12 months. A measure like ISO27001 is as much a signifier of the failure of the market to ensure cyber security provision as it is a solution to that lack of provision. As more and more organisations embrace digital transformation the necessity of moving beyond certification and toward a genuine gold standard – one which is tailor made for each individual organisation – will only increase.

The Scale of the Problem

One of the key indicators of the relative ineffectiveness of standard compliance in the battle against cyber-crime lies in the number, scale and nature of the data breaches which occur on an all too regular basis. The growth of digital transformation and the rise of big data have played a part in ramping up the numbers – in as much as there is simply an exponentially larger amount of data to be targeted on a year by year basis – but the rising line traced by any graph of data breaches you might choose

to create, demonstrates the simple truth that in the war between digital organisations and cyber criminals the cyber criminals are staying several steps ahead.

According to data aggregating platform Statista, the number of data breaches reported in the US has been rising pretty much year on year since 2005. In that year, 157 data breaches were reported, with 66.9 million records being exposed. By 2014 the number of breaches had risen to 783, an increase of almost 500%. In the two years to 2017, however, breach is almost bound to lead to under reporting if organisations feel able to keep the details under wraps.

Anatomy of a Data Breach

Despite the rise in the number and scale of data breaches over the years, the breach which is still generally described as the largest in history took place in 2012 and impacted upon credit reporting agency Experian. The figure of 200 million records being exposed is often cited, but this is actually the maximum number of records stored in the data base, which was breached, and the actual number of records exposed in the breach has never been established but is likely to be much lower.
A brief examination of the way in which the breach occurred is highly instructive, in that it highlights the ways in which even the largest and most tech savvy organisations can fall foul of lax security if they think of themselves as being sealed within their own silo of compliance and certification. The interaction with third and even fourth parties which the gathering and use of data imposes on virtually any organisation opens up an entirely new front in the struggle for cyber security and renders the monolithic and unchanging nature of a tick-box certification less than adequate for the task in hand. In simple terms, while your working methods may comply with the highest levels of security, you have to work in a way which assumes that your partners don't have the same high standards. In many cases, the assumption is that if a third party meets certain levels of compliance then their security systems can be relied upon, but the nature of the Experian data breach demonstrates that this is not necessarily the case.

> *One of the key indicators of the relative ineffectiveness of standard compliance in the battle against cyber-crime lies in the number, scale and nature of the data breaches which occur on an all too regular basis.*

In March 2012 Experian acquired Court Ventures, specialists in the aggregation of information on individuals available in public records. When this acquisition was made Court Ventures themselves had a contract with a further company, U.S Info Search, which allowed U.S. Info Search to access the data gathered in order to track the addresses of individuals with an eye to determining which specific court records to review.
The statement released by Experian at the

time the breach became public knowledge explains what happened next:

"After Experian's acquisition of Court Ventures, the U.S. Secret Service notified us that Court Ventures had been and was continuing to resell data from a U.S. Info Search database to a third party, possibly engaged in illegal activity. The suspect in this case posed as a legitimate business owner and obtained access to U.S. Info Search data through Court Ventures prior to the time Experian acquired the company."

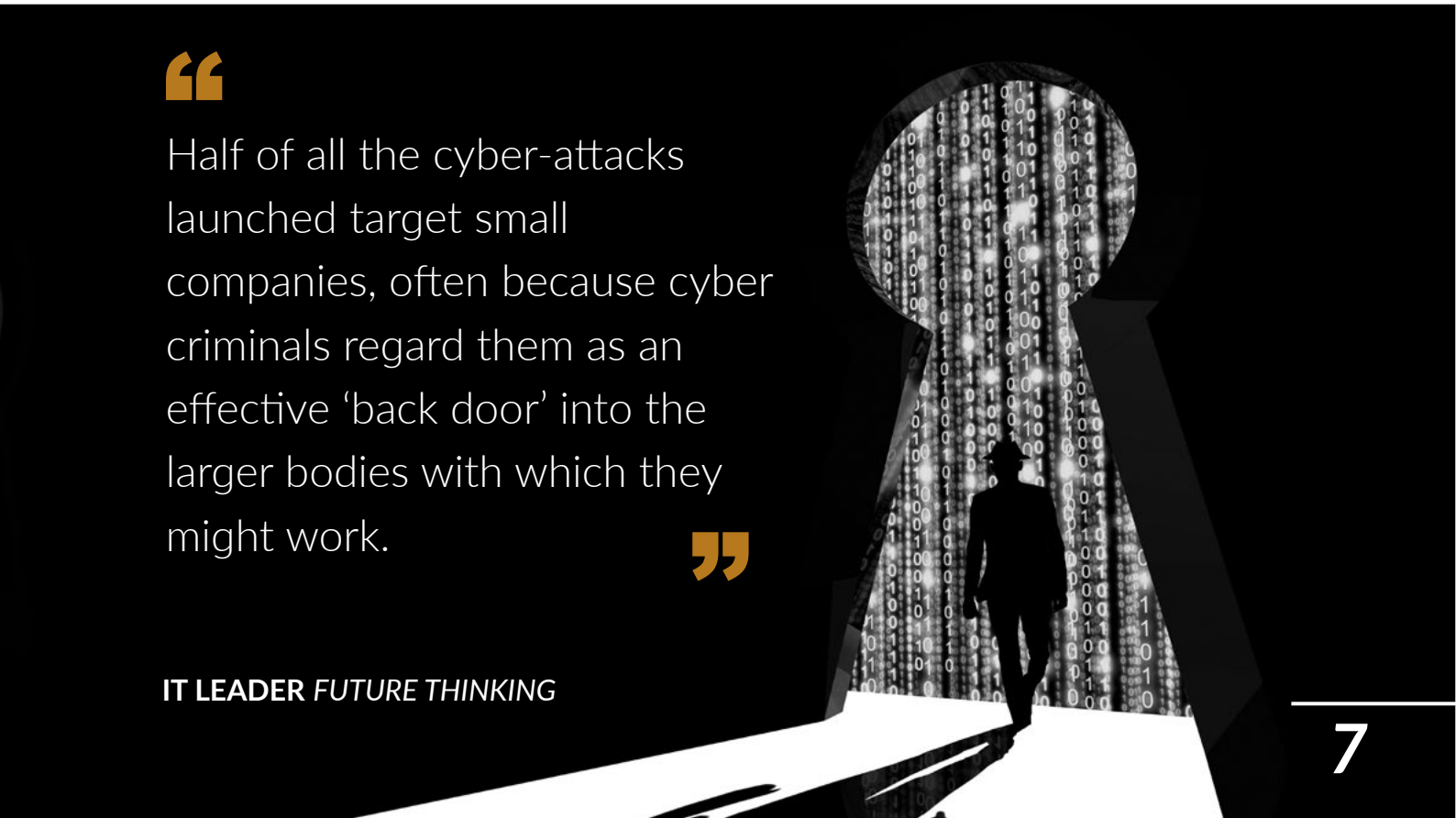
In slightly more detail, it emerged that one of these third parties was a so-called 'Vietnamese fraudster service' which sold the information – including financial details and Social Security numbers – to customers often intent on identity theft.

What the Experian breach demonstrates is that even complying with the strict legal requirements in place for working in the financial sector, it is no guarantee of high security standards.

Once the data which your organisation relies upon has to pass through two or more external bodies, the risk of security breaches begins to ramp up, and the responses in place need to be fluid and agile enough to deal with a threat coming from a number of different directions.

Once the data which your organisation relies upon has to pass through two or more external bodies, the risk of security breaches begins to ramp up, and the responses in place need to be fluid and agile enough to deal with a threat coming from a number of different directions.

Half of all the cyber-attacks launched target small companies, often because cyber criminals regard them as an effective 'back door' into the larger bodies with which they might work.



The Cyber Security Challenge

If you've yet to be impacted by cyber security issues, and have the relevant accreditations in place, it can be easy (and a little comforting) to assume that the problem is hyped up somewhat by businesses keen on selling their personal solutions, and that as long as you have a firewall and anti-virus downloads in place your systems will be safe. Statistics gathered from around the world, coupled with accounts of issues faced by some of the largest, most successful and most technologically advanced companies in existence, tend to undercut any such complacency however:

1. Hackers around the globe create something in the region of **230,000 malware** samples every single day.

2. The average data breach of an organisation remains unnoticed for up to **6 months** after it takes place.

3. Since 2016, an average of **4000 ransomware** attacks have taken place every day.

4. **91% of cyber-attacks** involve the use of 'spear phishing'. This is a highly targeted form of phishing which makes use of information about the target themselves to create specific and personal attacks which are more likely to cut through.

5. The FBI estimate that by the end of 2019 a business was being attacked by ransomware every **14 seconds**, down from every **40 seconds** in 2016.

6. The anti-phishing system operated by the Kaspersky cyber security platform was triggered approximately **247,000,000 times during 2017**.

7. According to Verizon, **30% of phishing emails** are opened by users, and **12% then go on to click** on the infected link or attachment.

8. According to Juniper Research, the amount lost as a result of cybercrimes during 2019 **hit $2 trillion**.

The State of Play in 2019

The issues around compliance, and the way in which it doesn't guarantee security, are clearly highlighted by accounts of the biggest security breaches of 2019. Some of these cases feature organisations whose pre-eminence is based upon their aptitude for working at the cutting edge of technology, while others involve public bodies with legal obligations to reach specific standards of digital security. In all cases, compliance fell well short of equalling security.

WhatsApp

In May 2019 hackers succeeded in installing surveillance technology on user's phones via WhatsApp. Although the Financial Times reported that the spyware in question was originally designed by Israel's NSO group, a technology company which specialises in providing "authorized governments with technology that helps them combat terror and crime", the firm denied any involvement. Given that an even more recent case has involved Jeff Bezos, founder of Amazon and probably the richest man in the world, having his phone allegedly hacked via a WhatsApp message sent from the personal account of the crown prince of Saudi Arabia, the fact that WhatsApp is compliant with the strict data handling rules in place across the various geographical areas within which it operates, has clearly not been enough to guarantee security.

Apple iPhone

For the two years leading up to 2019 Uighur Muslims in China were targeted by an attack on iPhones. The hack was highly sophisticated in nature and was finally discovered not by the security people at Apple but by researchers working in Google's Project Zero. They found that users who visited specific websites had their phones infected with spyware which impacted every aspect of the software, providing access to messages, passwords and location data. The highly specific nature of the websites in question led to the conclusion that the attack was probably backed by the Chinese state, in an effort to monitor the minority Uighur Muslim population within the country. When the attack was discovered, Apple attempted to minimise any reputational damage by announcing that the problem had been patched within 10 days of being discovered, and that it had only been associated with 'a few dozen' sites. Although this attempt to minimise any reputational damage is understandable, it doesn't take into account the fact that the 'few dozen' sites had been specifically targeted for a reason, and that the speedy patching followed a 2 year period during which the issue went unnoticed. The final issue, of course, is that the security measure put in place by Apple weren't able to spot the issue, and it had to be picked up by a third party.

"They found that users who visited specific websites had their phones infected with spyware which impacted every aspect of the software, providing access to messages, passwords and location data."

> *It's fairly safe to assume that anyone making use of software developed and supplied by Microsoft would do so under the impression that the security measure in place were as strict as possible, and yet the fact that such a risk was still present illustrates the degree of vigilance which always has to be maintained.*

US Customs and Border Protection

In June 2019 hackers managed to break into a data base of images gathered by US Customs and Border Protection. According to a Washington Post report, the breach could have impacted the data of as many as 100,000 travellers, and this data included photographs of traveller's faces and vehicle licence plates. Responding to the news, Customs and Border Protection stated that a subcontractor supplying the technology for reading licence plates had been responsible for the breach.

Quest Diagnostics

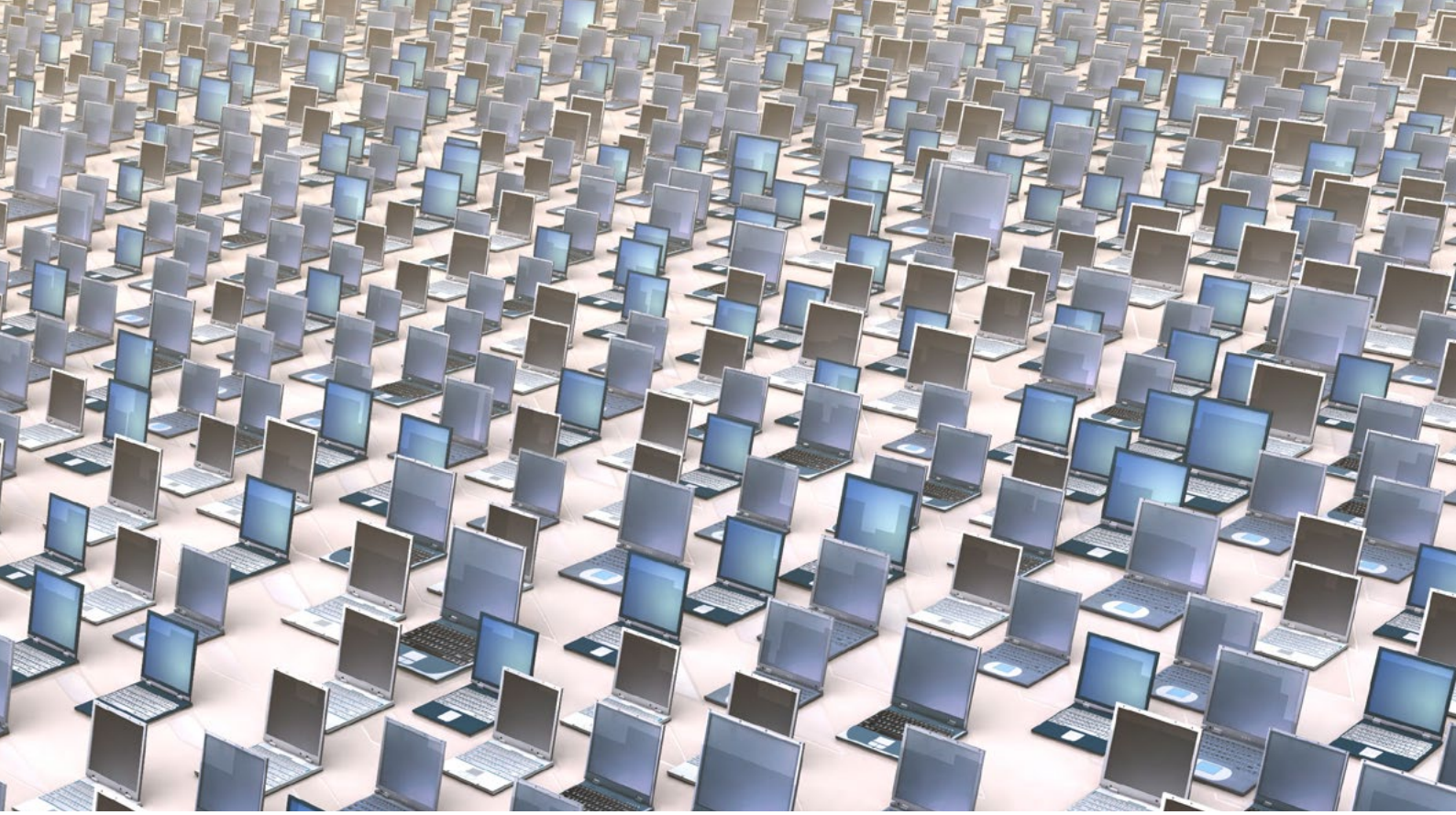
The clinical laboratory Quest Diagnostics announced, in June 2019, that an unauthorised party had accessed data relating to almost 11.9 million patients. The information in question included details such as credit card information and social security numbers. Not only was the breach large scale, but the laboratory announced that the unauthorised user had been able to access the information in question for a period between August 1st, 2018 and March 30, 2019. Once again, the parent company, Quest, blamed the breach on a third party, in this case a debt collector called American Medical Collection Agency (AMCA).

According to Bloomberg, the impact of this revelation on AMCA was huge – they quickly lost the four largest clients it dealt with and filed for Chapter 11 protection with the intention of liquidating.

Microsoft

Having dealt with Apple and WhatsApp it seems only fair that tech giant Microsoft should also take its place in the 2019 data breach hall of shame. In April the company discovered that hackers had infiltrated the development tool Visual Studio, placing backdoors in the tool which enabled them to hack video games companies which used the tool. According to Wired magazine, this breach resulted in 92,000 computers running malicious versions of the games in question.

It's fairly safe to assume that anyone making use of software developed and supplied by Microsoft would do so under the impression that the security measure in place were as strict as possible, and yet the fact that such a risk was still present illustrates the degree of vigilance which always has to be maintained.



Asus is the fifth largest manufacturer of computers in the world, and in March of 2019 Kaspersky announced that hackers had been able to hack as many as tens of thousands of computers, infecting them with malicious software via the online automatic update service provided by the company. Although the issue was discovered in 2019, the problem probably dated back to sometime in 2018. According to Wired magazine, the attack was probably the work of Barium, the China-based group also thought to be behind the Microsoft Visual Studio hack.

An overview of these cases prompts two observations. The first is that the attacks generally fall into two different camps. Some, such as the WhatsApp and Microsoft hacks, are highly sophisticated hacks designed to defeat the advanced security measures put in place by some of the most technologically advanced companies in the world. Others are somewhat simpler and manage to circumvent the security which might be in place at the upper levels of an organisation by attacking it via a third party. This was the case with Quest and US Customs and Border Protection, both of whom reported that the breach had originated via subcontractors, while in the case of iPhones, on the other hand, the targeting was done via completely external websites. The follow on from this is that working with third party providers, websites or tools which meet all the necessary compliance standards is no guarantee that systems won't be breached. Asking a sub-contractor if they've been deemed to meet a set of behaviours set out in a certification such as the NIST Cyber framework, is no substitute for interrogating the measures they have in place in greater depth.

More than anything else, the culture of an organisation needs to be established in order to ensure that it has the right attitude toward cyber security. Are members of staff routinely trained in the changing nature of the threat and do the separate silos of the company work in a unified manner in order to maintain security across the board? Presented with these questions, as we've seen, the NHS in England would fail any cyber security test another party put to it, and yet it would, if asked, be able to point to the accreditations it works within.

To take a more extreme example of this phenomenon, the company Apple is proud to boast, on its own website, of the following security certifications:

ISO 27001 and 27018 Certification

Apple has received ISO 27001 and ISO 27018 certifications for implementing an Information Security Management System (ISMS) for the infrastructure, development and operations supporting the products and services: Apple School Manager, iTunes U, iCloud, iMessage, FaceTime, Managed Apple IDs, Siri and Schoolwork in accordance with the Statement of Applicability v2.2 dated 5/11/2018. Apple's compliance with the ISO standards was certified by the British Standards Institution. The BSI website has certificates of compliance for ISO 27001 and ISO 27018.

Common Criteria Certification

The goal, as stated by the Common Criteria community, is for an internationally approved set of security standards to provide a clear and reliable evaluation of the security capabilities of Information Technology products. By providing an independent assessment of a product's ability to meet security standards, Common Criteria Certification gives customers more confidence in the security of Information Technology products and leads to more informed decisions.

Through a Common Criteria Recognition Arrangement (CCRA), member countries and regions have agreed to recognise the certification of Information Technology products with the same level of confidence. Membership along with the depth and breadth of Protection Profiles continues to grow on a yearly basis to address emerging technology. This agreement permits a product developer to pursue a single certification under any one of the Authorising Schemes.

Previous Protection Profiles (PP) were archived and have begun to be replaced with the development of targeted Protection Profiles focusing on specific solutions and environments. In a concerted effort to ensure continued mutual recognition across all CCRA members, the International Technical Community (iTC) continues to drive all future PP development and updates towards Collaborative Protection Profiles (cPP) which are developed from the start with involvement from multiple schemes.'

The page then goes on to list a number of Common Criteria certifications for aspects of its service including mobile devices, browsers and application software. In addition, it offers up an impressive list of countries and regions which have approved Apple devices for government use. The governments in question include the Australian government, the UK government, the German government and the US government. Under each there are details of how each of the governments has certified Apple products as being safe to use with data of specified levels of sensitivity, and the impression, as a whole, is of a company which has covered it's security bases and can point to the evidence to demonstrate this.

None of which, of course, stopped the Chinese government from being able to hack into the phones of Uighur Muslims for a period of two years.

Standards Explained

Having examined the role which standards and certifications play in creating the security landscape within which we all have to operate, it may be useful to give brief details of what some of the more popular standards consist of:

Cyber Essentials Scheme

This is backed by the UK government and sets out security standards which, if applied correctly across an organisation, should ensure protection against the lowest level of cyber threats. Gaining the certification is mostly a matter of filling in questionnaires. Once gained, particularly by smaller companies, it will doubtless reassure customers that cyber security is something you take seriously.

The IASME Governance Standard

This standard, Information Assurance for Small and Medium Enterprises, also developed by the UK government, is intended to go a step further than Cyber Essentials and includes an assessment based upon GDPR requirements. It is risked based and may demonstrate a more rigorous approach to cyber security and gaining IASME may help in terms of being able to take part in government supply chains.

ISO 27001

ISO 27001 is an internationally recognised standard for information risk management. It offers guidance on selecting effective and proportionate protection for data and defines the policies, processes and standards a business should adopt.

Cloud Controls Matrix (CCM)

The Cloud Controls Matrix (CCM) is aligned with ISO 27001 and covers three areas – cloud architecture, operating in the cloud and governing in the cloud. It provides a structure for information security tailored to the cloud environment and can be used to strengthen the security of your cloud environments.

ISO 22301

IOSO 22301 is a standard which goes beyond merely protecting a business and preventing cyber attacks and deals with minimising the impact of any attacks which do happen and recovering as quickly and fully as possible. Working through the accreditation will enable you to identify the critical assets you depend upon and put into place measures which will make sure these assets are still available if a cyber attack takes place.

PCI-DSS

PCI-DSS is the Payment Card Industry Data Security Standard, designed to ensure that companies which store, process or transmit credit card information maintain a completely secure environment. It applies to companies of any size which accept card payments, and it fulfils a dual role. In the first instance it reassures customers that you have adequate security in place. Secondly, a company which suffers a data breach and isn't PCI-DSS compliant runs a far greater risk of being fined.

Minimum Cyber Security Standard

This standard has been developed by the Cabinet office, working with the National Cyber Security Centre (NCSC), and sets minimum requirements for all departments, agencies and suppliers. It is broken into categories such as identify, protect, detect, respond, and recover and is intended to grow and develop over time as new threats and vulnerabilities emerge.

Other certifications and accreditations include the NIST Cyber framework and the SANS CIS top 20 critical security control set. Although each is different and offers varying levels of protection and higher or lower standards which have to be met to be compliant, they all basically offer a framework which can be used to build a cyber security policy around. Clearly, this is not a bad thing in itself, and having a set of clear guidelines and questions to ask when putting a policy together can provide a roadmap in the first instance and a reference point for future revisions. To question the validity of certifications and accreditations is not to dismiss them altogether. Indeed, many are legal requirements for working within certain sectors, and so not adhering to them is a complete non-starter. The question is actually more of a question about the overall cyber security policy of an organisation. Do you view accreditation as the starting point for an in-depth examination of your cyber security needs and responses? If so, there's every chance you'll be able to put together a robust and effective security policy. If, on the other hand, you gain an accreditation and think 'job done', then there's a huge risk that you'll be caught out in the manner of Experian, Apple, the NHS, the US Government and countless other smaller organisations which doubtless

assumed that, because they and their suppliers or sub-contractors were covered by the relevant accreditations, they were working in a completely safe environment. It has to be remembered that the aim of compliance standards is to ensure that everyone who meets them has reached a minimum standard across the board, and that it can only ever offer a snapshot of how secure an organisation was at the time the standard was met. Genuine security, on the other hand, has to be capable of shifting and responding to newly emerging threats or vulnerabilities on an on-going basis.

One of the major differences between compliance and genuine risk management is that the former is prescriptive whereas the latter is predictive. Becoming compliant involves adhering to a set of rules and regulations which have already been put in place by external arbiters. Risk management, on the other hand, is less reactive and more strategic, being based upon analysing your IT landscape in order to predict problems before they occur and put protections and plans in place, utilising innovation and fresh thinking if need be.

Another risk of focusing too strictly on compliance is that it tends to divide an organisation into separate silos. GDPR, for example, deals specifically with the protection of data, while PCI-DSS handles the payment regime and ISO 22301 is about disaster planning. Each can be effective in its own right, but each also mainly concerns a certain part of an organisation, meaning specific individuals and departments concentrating on individual areas of cyber security. Moving beyond compliance and into genuinely effective risk management means installing a culture across the organisation, however, so that these silos break down and a threat or vulnerability which emerges in one section of an organisation is instantly transmitted across the rest of that organisation. Ticking the boxes of a certification will often be the job of those officially charged with 'risk management' within an organisation. If the right communication structures are not in place, the messages taken on board by the cyber security department via the accreditation process won't be disseminated across the rest of the organisation. This presents a dual risk – firstly that the measures which the cyber security

team maintain are in place are not, on the 'shop floor' so to speak, actually functioning as they should. Staff armed with the day to day task of working with systems and processes may be more aware of the vulnerabilities of those processes than someone taking a top down view with an eye to crossing items off a list of requirements. The second risk is that the effective measures outlined in the accreditation process won't become firmly embedded in the organisation. By breaking down the silo of risk management and making it a concern for everyone in the organisation, you create an environment in which risk and security become part of the conversation around everything, from procurement to sales, and research and development.

The main issue with compliance as a controlling security outlook is that the battle being waged for cyber security is a classic case of asymmetrical warfare. On the one hand we have compliance standards which are large, set in stone (regular reviews notwithstanding) and come as a one size fits all solution. Cyber criminals and hackers, on the other hand, whether purely criminal or government sponsored, rely on being reactive, nimble, and flexible, basing their approach on staying one step ahead of the latest security by developing effective uses for the latest technology. The irony of the rush to embrace this latest technology is that each technology, as it emerges, opens up a whole new field of risk. Many will be sold on the promise of greater security, and will indeed offer security advantages, but the same features that an organisation will seize upon to enhance their processes will be prized by hackers for making their activities easier. It's useful to examine technologies such as cloud computing, the Internet of Things, Robotic Process Automation (RPA) and AI in terms of the emerging security risks which they carry with them – including some real-world cases of breaches – and the steps which might be taken to lessen these risks. It's also worth noting that newly emerging risks such as these are unlikely to be dealt with by accreditations and certifications as they now exist. By their very nature, such tools are a response to established threats, and by the time something like RPA becomes a fixed part of such processes there's a risk the damage will already have been done.

> *By breaking down the silo of risk management and making it a concern for everyone in the organisation, you create an environment in which risk and security become part of the conversation around everything, from procurement to sales, and research and development.*

> *The irony of the rush to embrace this latest technology is that each technology, as it emerges, opens up a whole new field of risk.*

The CLOUD

The Capital One Financial Corp store their client's data on the Amazon.com Cloud platform, and it was this platform which, on July 30, 2019, was subject to a major breach which potentially exposed 106 million customers.

The hack involved a former Amazon cloud employee taking advantage of what was described as a 'poorly configured firewall' and was taken by some experts as indicating that Capital One may have switched to cloud storage without ensuring that sufficient safeguards were in place.

More than 104,000 Social Security numbers and 80,000 bank account details were exposed during the hack. This case highlights the need for all security processes to pay due attention to the potential for insider threats when developing the protocols, processes and plans for switching to cloud storage, or indeed for providing that cloud storage.

PCM

As if to highlight the potential vulnerability of the cloud the next case features PCM, a significant provider of cloud services. In July 2019 the company underwent a series of hacking attacks which infected their cloud services with malware able to collect login credentials, including usernames and passwords. In this case the issue was spotted before any personal information had been able to be gathered, but PCM had to inform clients of the attack and take the reputational hit associated with it.

There's a little doubt that the cloud represents the future of computing, but the rush to embrace it shouldn't blind organisations to the risk that security provisions often lag behind process and convenience. If a company like Amazon can find its cloud computing platform compromised then the average smaller organisation will have to treat the cloud computing services, they use as a potential source of risk, rather than taking their security at face value.

The INTERNET of THINGS

Industry experts Gartner predict that by 2020 there will be more than 14 billion IoT devices operating in homes and businesses. Given that this is viewed in some quarters as an underestimation of the numbers, the announcement made by Microsoft at the 2019 Black Hat conference in Las Vegas should give all concerned pause for thought. The announcement involved the discovery that a Russian hacker group had been using vulnerabilities in devices such as a voice over IP phone, a Wi-Fi office printer and a video decoder to gain access to enterprise networks. This story highlights the reality that the firmware — the software which provides low level control for the hardware of an IoT device — represents a point of attack which is often left relatively unprotected. Gaining access to a poorly secured IoT device enables hackers to then make the sideways step into the wider network of an organisation. The vulnerabilities exhibited by the latest generations of firmware can include the following:

Unauthenticated access – it's surprisingly common for firmware to allow access without authentication. If authentication is required it is often relatively weak, being single factor and password based, or utilising cryptographic algorithms which are vulnerable to attack.

Backdoors – hidden backdoors are often included in firmware with the intention that they should only be accessed by people with the right authentication. In most cases this will be customer support operatives. The risk, however, is that skilled hackers generally tend to make pretty short work of finding these 'hidden' back doors.

Passwords – the firmware in the majority of IoT devices makes use of either hard-coded passwords that users can't change or default passwords which users rarely get around to changing (the entire phone hacking scandal was predicated on this tendency to not bother changing default passwords). In 2016 a botnet called Mirai managed to infect 2.5 million IoT devices globally, using default passwords to do so. Once in the devices, the botnet used them to launch a DDoS attack which took down organisations including Netflix, Amazon and the New York Times.

Organisations concerned about the integrity of their IoT devices can take a few relatively simple steps to enhance security including:

1. **Upgrading the firmware and changing all default passwords.**

2. **Pulling together an inventory of all IoT devices on the network to create a full picture of the possible risk.**

3. **Contact the manufacturers to see if they've acted to counteract common IoT vulnerabilities, and insist they introduce secure coding practices.**

Practical examples of the vulnerabilities inherent in some IoT devices include the case of CNN, in 2019, using the specialised search engine Shodan to access a number of camera feeds in user's homes. From the family in Australia to a man making his bed in Moscow and a woman feeding her cat in Japan, none of them seemed at all aware that they were being filmed. CNN reported than none of the cameras hacked into featured even the most rudimentary security checks. An even more worrying case was confirmed by the US Food and Drug Administration (FDA) in 2017, when it announced that some implantable cardiac devices used to monitor patient's heart functions and minimise the risk of heart attacks could be hacked into and that the hackers could administer shocks, control the pacing and deplete the battery.

In some ways the use of AI to aid cyber security runs the same risk as gaining certifications – namely that it can encourage a false sense of security.

AI

The heart of AI is machine learning, the ability of a system to develop and enhance its 'intelligence' by observing patterns in data and developing an understanding of what those patterns mean. In terms of cyber security this means that the system can train itself to spot a specific action taking place when processes are running, see that action repeated on the wider network, a specific computer or a combination of both, and recognise that this is a sign that a cyber-attack has taken place and preventative steps need to be taken. The fact that this process is being repeated millions of times per second across an entire network means that AI should offer a simple and massively effective weapon in the war against hacking.

The sheer intelligence of AI can be used by the hackers to work against it, however, by 'teaching' it misinformation which disrupts the algorithms used to make decisions. Sophisticated hackers could insert fake data into a database and that information would 'teach' the AI system that personal information being copied was just a normal aspect of the operation of the IT systems rather than an anomaly which needs to be flagged up.

This example demonstrates the degree to which the battle against cyber-crime is as much a question of understanding tactics and psychology as it is a technological challenge. Hackers don't have to have the skill, funding or time to develop a means of by-passing the AI, they instead partner with it, tweaking what it knows about the system in a way which will enable them to act with impunity.

An experiment which took place at Kyushu University in Japan in 2017 demonstrated that an AI image detection system – often heralded as the long term replacement for passwords – could be tricked by changing just a single pixel in an image, a change that would be invisible to the naked eye. Even more striking was that the AI in question was tricked without the scientists knowing anything about the inner workings of the system or the Deep Neural Network (DNN) as it's known. Using only the probability functions – the tools used to teach the machine learning – they were able to trick the AI into thinking that an airplane, a car, a cat, a bird, a deer, a truck, a frog, a horse and a ship were, in fact, all pictures of a dog. This highlights one of the risks of AI, a risk which it shares with virtually every emerging technology. The risk is that the 'wow factor' of the technology, to coin a phrase, makes the people using it less likely to interrogate its effectiveness and reliability. In simple terms,

the very fact that an AI system can now undercut and surpass the well-worn technology of passwords and other forms of authentication can blind users to the possibility that it might be less than perfect. If it can do something as advanced as use your face in order to open files, processes or systems then surely the security aspect can be taken for granted. As the Kyushu University experiment shows, this can be far from the case.

Another tactic is to 'train' the AI system to see the abnormal as normal. This involves hackers inserting signals and processes which won't have any actual effect upon the IT system – and so won't be spotted by any users – but will train the AI to see such activities as a normal part of the system. Once this has been achieved, the hackers can attack the system using the same signals and processes, safe in the knowledge that the AI will regard them as being the norm.

Another tactic involves what is sometimes called "bobbing and weaving," where hackers insert signals and processes that have no effect on the IT system at all – except to train the AI system to see these as normal. Once it does, hackers can use those routines to carry out an attack that the security system will miss – because it's been trained to "believe" that the behaviour is irrelevant, or even normal.

In some ways the use of AI to aid cyber security runs the same risk as gaining certifications – namely that it can encourage a false sense of security. Having installed a hugely advanced system capable of learning as it does the job of protecting an organisation, it's all too easy to relax and assume that the technology will do all the work. The truth of the matter, as the examples we've given demonstrate, is that, powerful though the technology may be, nothing takes the place of human observation of the systems.

SUMMARY

Compliance is only ever going to be the starting point of an effective cyber security policy, not the solution. The scale of breaches which take place around the globe every year demonstrates clearly that, however widespread the uptake of certifications and other forms of compliance may be, the cyber criminals generally manage to stay at least a couple of steps ahead. The fact that some of the tech companies that helped to usher in the age of digital transformation have also found themselves falling victim to cyber-attacks underlines the fact that cyber security can never be a given. The problem is that gaining a certification can often be seen as the solution to cyber security issues rather than – as it is – simply a starting point for building secure systems and processes.

Many organisations are aware of these facts, and work to inculcate a culture across all sections of the workforce in which cyber security is placed at the centre of decision making. The problem, as can be seen by examples such as the Quest Diagnostics hack, is that digital transformation often involves working with a range of other parties in order to successfully cope with the volume of data involved. In many cases, the process of choosing an organisation to partner with will be driven by the question of certification – it saves time and money to simply ask the partner you're considering working with if they have gained ISO27001 and Cyber Essentials Plus. As we've seen in the cases of the huge ransomware attack on the NHS, however, meeting certain certification standards is no guarantee that the organisation in question isn't working with outmoded hardware, software and processes. The more partnering with other organisations becomes a core part of digital transformation, the more in-depth the investigation of any partners' cyber security approach is going to have to become.

Another core lesson of any investigation of cyber security is that technology is not going to be the saviour. Options such as cloud computing and the use of AI throw up as many problems as they do advantages, not least of which is that they encourage complacency. Cyber criminals, on the other hand, are constantly examining any emerging new technology to work out how it can be exploited to attack the systems it's intended to protect. On top of this is the problem which arises from the fact that commercial pressures can lead to organisations embracing a new technology such as cloud computing before the cyber security issues have been fully considered.

The core problem with an over-reliance on certifications to guarantee cyber security is that the biggest threat is almost always the next threat to emerge over the horizon. Being reactive in nature, codified certifications are based upon threats which are already known and quantified to a degree, but the next wave of cyber security breaches could potentially revolve around emerging threats such as supply chain and third-party attacks, the impact of 5G, which will increase the speed and volume of data theft, and the potential use of deep fakes of all kinds. By the time certifications come to deal with problems like these it may be too late for your organisation, whereas a coherent and comprehensive cyber security policy will have predicting future threats embedded in its core.


Our Cyber Security Partners
AT&T Cybersecurity Partner
Microsoft
mimecast
ALIEN VAULT
tenable network security
cisco Meraki
Bitdefender
AQUILAI
littlefish
Cyber Security Services
0344 848 4440 info@littlefish.co.uk www.littlefish.co.uk