EU and UK cyber security initiatives and the health sector

The healthcare sector in the UK, although so far not targeted on as significant a scale as its counterpart in the US, is attractive to cyber criminals given the value of health data. Both the UK government and EU authorities are taking action on cyber security through initiatives such as the UK's Cyber Essentials scheme and at a legislative level, predominantly through the proposed EU Network and Information Security Directive. Simon Shooter of Bird & Bird explains why the UK's NHS can be considered a major cyber target, what healthcare operators can do in terms of improving cyber security, and what's upcoming on the legislative horizon.

The woes of the TalkTalk breach are being played out in the press, with an early statement from TalkTalk indicating that the bank details and personal information of more than four million customers in the UK could have been accessed. More recently comes the sobering revelation that a 15 year old boy has been arrested in Northern Ireland in connection with the hacking attack and has been released on bail pending further inquiries. The possibility of a 15 year old prosecuting so successful a cyber attack is surely a cause for alarm.

At least NHS cyber security is not on the front page of newspapers. However, before complacency sets in it needs to be acknowledged that the NHS represents a prime cyber target and, if that is acknowledged, a significant cyber attack is a matter of 'when' not 'if.'

Why is the NHS considered a prime cyber target?

Perceived wisdom has it that the NHS is both a soft and valuable target for cyber attack. The value of cyber targets can be measured across a number of axes - the size of the aggregated pool of sensitive data and the quantum and value of intellectual property mapping against the ease of access. NHS entities hold possibly one of the largest pools of aggregated personal sensitive data in the country, combining patient data such as names, dates of birth and National Insurance numbers with significant quantities of data from NHS suppliers and partners. NHS entities also generate extremely valuable IP in terms of clinical research and development, the invention of medical devices, new forms of treatment and test data.

To put the size of the target into perspective and for the purpose of this example ignoring the IP asset value, the average cost of a person's personal details bought on the Dark Web is, according to a Whitehall security official, just under £20 a go. It can be seen that simply in terms of patient data held across the NHS system the potential value is enormous. Reuters has been reported as stating that the criminal value of medical information in the US is up to 10 times that of credit card data.

From an ease of attack perspective the NHS IT landscape is a patchwork quilt of systems and equipment, much of which is legacy and where there is a lack of integrated architecture. Add to this the incessant drive for reliance on technological solutions to achieve faster, better, cheaper goals and the myriad of connected mobile devices, the challenge to secure the technological perimeter for the NHS makes it a soft target. There is also the challenge that comes from the obvious desire to ensure that highly sensitive personal patient data is readily accessible to support clinical intervention while needing at the same time to maintain high levels of security.

Reviews of the resilience of medical devices to cyber interference in the US have pointed to a material vulnerability arising from widespread failure to seek to protect devices such as drug infusion pumps, defibrillators, X-ray machines, electronic patient record systems and the like from remote manipulation. The take home comment is that the healthcare operator systems simply need to be infiltrated, and once infiltrated access to medical devices is almost entirely unguarded.

Evidence of criminal focus on the healthcare sector

While there have been sporadic cyber attacks on NHS targets over the last few years, including the LulzSec hacks in 2011 that ended in prosecutions in 2012 and 2013, there is at present no rogue's gallery of evidence of material cyber attacks on the UK healthcare sector.

In the US, which is seen as a more mature cyber market, the picture is different. The highly publicised attacks on health insurers Premara Blue Cross and Anthem Inc. involved the accessing of 80 million records from Anthem and 11 million from Premara. Trustwave's 2015 Security Health Check Report describes a sector where in excess of 90% of the survey group agreed that criminals were targeting healthcare organisations. A study published by the Ponemon Institute records the costs to the US healthcare system this year at $6 billion with criminal attacks more than doubling in the last five years. Accenture has recently offered its projection of one in 13 patients having their personal data stolen in the next five years as a result of a data breach at their healthcare

provider, with an estimated associated price tag of $305 billion.

Government action and the impact on healthcare

The UK Government has been active in publishing the UK Cyber Security Strategy, establishing a Computer Emergency Response Team in March 2014, setting up the Cyber Security Information Sharing Partnership, having BIS, GCHQ and CPNI publish the 10 Steps to Cyber Security and setting up the Cyber Essentials Scheme. More recently the Health and Social Care Information Centre ('HSCIC') has announced that a new NHS cyber security service will be established by January 2016 - CareCERT will be run by HSCIC and is due to be phased in imminently to enhance cyber resilience across the health and social care system and to provide a resource for incident response expertise.

In the background the European Commission ('EC') has been progressing, albeit slowly, the Network and Information Security Directive ('Directive'), first published in draft in February 2013. While the scope of the Directive is currently still the topic of discussion in the European Parliament there is some hope that agreement is not a great deal further off. Once the text is finalised the Directive will have to be implemented into domestic law by the national governments of the Member States. With an estimated two and a half year implementation period it seems a national cyber law will not be in place until 2018 at the earliest.

Nevertheless, for the healthcare sector it is important to note that one key aspect of the Directive is that risk management and reporting obligations are likely to be imposed on 'market operators' where market operators are identified as operators of critical infrastructure and where critical infrastructure is defined as 'infrastructure that is essential for the maintenance of vital economic and social activities […] the disruption of which would have a significant impact in a Member State.'

Team sheets, plans and policies alone cannot deliver improved cyber readiness. Those assets need to be tested and adjusted so that they are more bespoke to each operator's needs

Healthcare has been identified as critical infrastructure. Accordingly, it is extremely likely that healthcare operators will be required by legislation to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their network and information systems and to have some level of responsibility to notify their national competent authorities of incidents that have a significant impact on the security of the critical services they support. So, what is that likely to mean and will there be any sanction for non-compliance?

It seems highly unlikely that 'appropriate and proportionate technical and organisational measures' will be laid out in any legislation and the market operators will need to determine for themselves the measures to adopt. However, the aim must be to adopt measures that are reasonable, prudent and proportionate to the risks faced by the relevant market operator. It also seems foreseeable that the legislation may borrow from the UK Bribery Act 2010 and provide a defence for market operators who can show they had 'adequate procedures' in place to protect against cyber attack.

As to sanctions, at the moment it is unclear but there have been rumours that the penalties may follow the expected position in the General Data Protection Regulation ('GDPR') with fines potentially of up to 2% of worldwide turnover. If this is the case the fines will obviously be significant.

The Directive when finally adopted into national legislation will obligate compliance on pain of sanction. The lag before this occurs provides a fine opportunity for those who are likely to fall into the sights of the anticipated legislation to put their houses in order.

The Directive will obligate action but pure common sense demands cyber security to be a board priority now in any event. The risk to valuable assets and the allure to criminals of significant aggregation of personal data which, as we have seen above, is considered significantly more valuable than pure credit card details, mean cyber security should be of the highest importance.

So what should healthcare operators be doing now?

Key assets in the drive to improve cyber readiness are having:

- a clear categorisation of cyber risks and incidents following a thorough threat analysis;
- cyber incident response teams appropriate to each categorisation of incident;
- cyber incident response plans appropriate to each categorisation of incident; and
- a cyber security policy, or policies, if it makes logical sense to have different policies that map to each categorisation of incident.

Planning and testing your own cyber preparedness is the obvious initial focus but it is important to consider weak points in your security that may be outside your immediate and complete control. For this reason the lead recommendation made above is for a thorough cyber security threat analysis to be conducted. It is a feature of quite a number of the main cyber incidents that access to the penetrated system has been obtained by contractors and

others who are 'guests' and to whom access to the system has been made available. It is perhaps surprising how often entities who routinely vet their staff by background checks seem not to bother with contractor staff and other suppliers.

It is also interesting to note that insurance industry statistics that identify the root cause of cyber incidents as being employee-related at being in 70-80% of incidents leading to claims. The cause is a mixture of disgruntled leavers and those who simply wish to cause mayhem, but it is predominantly simple human error.

Team sheets, plans and policies alone cannot deliver improved cyber readiness. Those assets need to be tested and adjusted so that they are more bespoke to each operator's needs and adapted as the analysis of the needs is continuously updated by cyber security threat analysis and cyber intelligence.

Steps to be taken to address the need to tune and improve cyber readiness assets and drive cultural change and awareness include:

- Cyber awareness training and the explanation of cyber policies, and education to support them. The level of training should be graded according to the cyber risk exposure of the relevant individuals and their roles within the organisation.
- Testing of the readiness assets. Desktop exercises, war games and other such simulations are invaluable in evaluating cyber readiness. Simulation exercises can provide assurance that the assets have good practical application and are fit for purpose; they can point out deficiencies in the assets themselves or in the human interface and they provide the best possible form of training so that the response teams can operate decisively and with confidence should an event occur.

Other regulation

Careful attention also needs to be paid to both the GDPR and the Trade Secrets Directive.

GDPR

On 25 January 2012, the EC published its proposal for a new GDPR. The proposed Regulation promises greater harmonisation - but at the price of a significantly harsher regime, requiring more action by organisations and with tough penalties of up to 2% of worldwide turnover for the most serious data protection breaches.

The GDPR is to be accompanied by a new Directive, governing use of data by public authorities for law enforcement purposes, a proposal for which was also published on 25 January.

The link to the need to take prudent measures to guard against cyber attack and the need to take measures to protect data is clear. Steps taken to improve cyber resilience will assist in meeting the harsher regime referred to above.

The Trade Secrets Directive

On 28 November 2013 the EC published its draft Trade Secrets Directive. The purpose is to seek to harmonise laws across the EU to provide an unified definition of what a 'trade secret' is, to harmonise the approach to protection and the remedies available in response to theft or unauthorised use and to homogenise the measures courts can use to prevent trade secret leaks in legal proceedings.

The importance for the purposes of this article is the clarification of the requirement that for a trade secret to be protected under the legislation requires a lawful owner of the trade secret to take 'reasonable steps' to keep it secret in the supply chain.

In this circumstance then the Directive promises new protections and opportunities for those with trade secrets. However, to take advantage of them requires the maintenance of the secrecy aspect and the taking of reasonable steps to keep trade secrets secret throughout the supply chain. PwC in its 'Key Findings from the 2013 US State of Cybercrime Survey' noted: "Previous PwC surveys support the view that the supply chain is a potential weak link in cybersecurity - both in the United States and globally […] Companies often struggle to get their suppliers to comply with privacy policies - a baseline indicator of data protection capabilities."

Having suitable cyber security measures in place will assist in evidencing steps being taken to maintain secrecy and the flow down of those steps to the supply chain will promote the demonstration of reasonable steps with regard to the supply chain.

Simon Shooter Partner
Bird & Bird, UK
simon.shooter@twobirds.com