Combatting cyber-attacks in the health insurance sector

Mark Deem, a partner at Cooley (UK) LLP, explains why cyber-attacks pose a major risk for the health insurance sector and outlines the steps organisations can take to mitigate against them

It is the ultimate CV: a detailed account of the vital information, which makes us who we are; a unique statement which cannot be changed; and data which potentially could map out the trajectory of the remainder of our life. A life-saver.

Equally, it is the ultimate nightmare: the same sensitive personal information - in the wrong hands - used to steal an identity and perpetrate a fraud, extort money or blackmail an individual – and all in a manner, which would remain largely undetected for a long period of time. A life changer.

With such intrinsic value, it is perhaps little wonder that medical information – a helpful collection of data about date of birth, gender, medical conditions, place of residence and possibly lifestyle information – is reported to have a value on the black market of up to ten times the value of 'pure' financial information, in the form of credit card or bank account details.

Yet, with an ever increasing number of cyber-attacks and information security lapses being reported in the healthcare industry, organisations working in or supporting the sector are slow to recognise the risk posed by the nature of the information they hold as custodian; slow to understand how the legal and commercial risks manifest themselves.

It is not just those in the front-line of delivery of medical care or providers of healthcare insurance that are vulnerable to information security breaches in this area.

Medical information

Any custodian of medical information is potentially at risk: from the insurers who have required the disclosure of medical records in order to write a life assurance policy to those who have needed the sight of those same records in order to consider the provision of key-man insurance. Each will be in possession of this valuable information and each will be of particular interest to cyber criminals.

So what measures can be implemented to try to militate against the risk?

Awareness of the risk and an acknowledgment of the value of this information is undoubtedly a major first step. But equally

important is an assessment of how this particular information - as distinct from less personal or less sensitive data - is being kept (specifically, in what format is it being retained, whether it is in an anonymised state and on which servers); who has access to the information (can all users access it? is access limited to those with administrator rights?); and for how long is the information being retained and for what purpose is it being retained.

Best practice in this regard is to ensure that, where possible, only critical information is kept and for no longer than is strictly necessary. This is especially true of healthcare information. Even then, given its sensitive nature, it should be 'locked down' as effectively as possible, with access limited to those who need to have access to it. For many insurers, the ongoing possession of medical data may not be crucial once an initial assessment of risk profile has been performed. If you don't need it, don't keep it.

Further awareness is also required as to the existence of wider vulnerabilities, which may exist in the wider computer network within insurers. Whether through budgeting restraints or as a result of business growth through mergers and acquisitions, many companies in all sectors have legacy IT systems, which themselves are opening up the business to a risk of an information security breach.

Finally, as with all information security issues, a formal incident response plan is essential. To fail to plan is quite simply to plan to fail. Be aware of what you need to do should an incident arise: pre-determine who the individual stakeholders are, know the lines of communication and understand the legal risks and issues concerning notification.

Unlike breaches involving credit card or bank account details, incidents involving healthcare information are less easily recognisable and detectable by the data subjects and the true costs of making reparation upon an incident is also very different.

Red flags, such as money being taken out of a bank account or credit being used, are not there. Changes in behavioural patterns – purchases being made in foreign countries – do not alert security teams in the same way. Indeed, many years may pass before the data subject is aware that his/her personal information has been compromised, during which time the loss and damage caused will be irreparable. Accordingly, effective detection remains primarily in the domain of the custodians of the data, who will be among the first to know that there has been an issue.

Once an issue has been identified, the cost of replacing a credit card is limited and will generally have no lasting impact on the individual, whereas reconstructing and repairing an identity is an entirely different matter.

Credit cards may come and go; medical records are for life.

Sensitive personal data, like healthcare information, is being captured and collated at an ever-increasing rate, primarily with the laudable aim of improving the provision of healthcare services. This same data is also becoming a key component in establishing and authenticating our identity as we move from a world where security focussed simply on what we knew (a password) to what we had (a token on a smartphone handset) and now to who we are.

Healthcare information and establishing an identity has never been more valuable to either the individual or the criminal. The duty on custodians of such information to hold and keep such information safe has never been more critical. ■