Health industry security downfall: Safeguarding your life but not your Personally identifiable information (PII)

15 hours ago

In a world where cyber-attacks are becoming the norm and companies are afraid to report them over fears of loss of reputation and customer dissatisfaction, many healthcare companies and insurance providers had been making the conscious decision to not report them.

Prior to GDPR, unless a whistleblower reports the attack or the attack is captured by government analysts, these crimes would go without notice for months if not years. Even then the public was rarely notified. Have you ever received notification of your healthcare provider or insurance company affected by a data breach? Did you ever want to know why they may or may not tell you?

In numerous discussions with health insurance executives and executive board members from some of the largest hospitals in North America and Europe, the following questions were posed when discussing their annual data breaches and other cyber-related concerns:

Q - Why is no money truly dedicated to cyber-security?
A - All of our funds go to medical staff salaries.
Q - If all the money goes to medical nurses and doctors, why is it that there are so many strikes and protests occurring?
A - We pay the industry standards for their skill sets.
Q - So, if not all the money goes to medical nurses and doctors, where does the money go, which could be used to provide security for patient data?
A - The money not allocated for salaries, goes to research and development (R&D) of new drugs.
Q - Actually, pharmaceutical companies and in the US, in some instances the US Government pays for the R&D, so what is the real reason why you do not offer better cyber-security of your patients' data?
A - (In the US) Payment of the HIPAA fines is cheaper than the costs to provide cyber protection at our facility.

One of the main reasons cyber-attacks on healthcare are so dangerous and troubling is because compromises often go unreported. Additionally, as much as 80 percent of the healthcare industry security breaches have hitherto remained unnoticed for months, if not years. However, another reason not known to the public, is that in many incidents, in the US federal authorities will ask that the compromise not be made public while their investigation is ongoing. This is especially troubling given the sensitivity of the data the healthcare industry maintains on individuals.

Black market prices for passports, driver's licences and even social security cards are dramatically less expensive then medical files. For example, as of September 15, 2018, the price for a social security card on the "Deep Web" was only US$ 15.00 (£10) whereas an individual's medical record was US$ 60.00 (£40). Unlike credit cards, bank accounts, or driver's licences, all of which can be replaced, closed, or changed, medical files contain more personal information about an individual, that cannot be changed or closed. That is why, criminals pay so much more for personal health information.

Think about this, would you invest in a company if you knew that the founder and CEO had an illness and was going to die within 12 months? What about an executive's child being diagnosed with a fatal disease; would you still invest in the company? How would you feel if you saw non-corroborated medical files showing injuries to a company executives' spouse (Domestic violence); would this change your perception of the company? What would happen if abortion or sexually transmitted disease treatments data was released to the public on executives from a company; what would be the reaction against those companies? All the above questions can lead to negative perceptions of the companies as well as financial loses.

While reporting to the authorities has become manadatory in Europe under GDPR, what about informing the public - are we about to duplicate the US experience? In the US citizens ask themselves, why does the US Government receive money from HIPAA fines from these healthcare cyber-incidents, yet the data which is the public's, does not equate to any financial damages being awarded to them, not even free credit monitoring? What is the reason behind it? Are they ever been notified when their health insurance carrier or medical provider files were compromised? Is the real reason neglect by the healthcare companies and insurance providers in protecting the public's data or is it that in the US the authorities have a vested interest in getting payment from these companies?

Employee actions and/or mistakes, followed by external theft and vendor issues, are the top causes leading to compromises of patient data. This can be traced back to lack of employee training, inadequate security procedures for healthcare devices, and lack of oversight for systems and devices used to share healthcare records.

Many employee compromises of patient health records occur in oral disclosures, when providing patient records to the wrong patient or using unprotected electronic devices for sharing patient records. With security software available to include two-party authentication, why is this not the basic standard when medical personnel open your file to share information? A two-party authentication would mostly prevent your personal data from being shared with people other than medical staff and/or your family.

Compromises to patient health records not only has the potential to increase the likelihood of identity or financial theft and tax fraud, but also extortion and ransomware attempts. This threat affects not only the individuals whose records were stolen but also the businesses that were entrusted with their sensitive personal data. Businesses that fall victim to data breaches experience declining stock prices and market capitalisation, loss of reputation, and potential civil litigation. Within the healthcare industry, the risk of extortion is one that is shared by both the individual and the business.

Besides employee actions and lack of training, the lack of cyber-security policies also leads to compromises in Personally identifiable information (PII). This can be seen in the lack of understanding that Wi-Fi enabled devices need to be protected from cyberattacks. These devices include:

Desktop web cameras
Printer/scanner/fax
Modems
IP KVM
Security cameras
VoIP
Enterprise network controller
Mail servers
Digital recording devices
Router
Video conferencing system
Radiology imaging software
Contact call centre
Cellular devices

Specifically, personal cellular devices and tablets that nurses and doctors currently use to share patients PII, do not have audit capability, retention of emails or more importantly, lack of universal standard security protocols from cyber-attacks. How many times have you been to an office, hospital, etc. and seen staff, nurses, doctors using these devices to play games or answer personal emails from non-work-related accounts?

A more robust training criteria must be created, enforced, with annual virtual exercises for all medical professionals and staff to ensure their understanding of cyber-attacks, vulnerabilities and why patients PII is so valuable to criminals. Not only to avoid such negative exposure but also to save money as it could end up being very costly - as the NHS has found out. If no clear mitigation strategies are implemented then these companies must be held liable for these breaches, not only to the regulatory authorities, but to all patients whose data was stolen.

Contributed by John Evans COO & Sofia Cardante, risk manager, Front Sight Protection.

**Note: The views expressed in this blog are those of the author and do not necessarily reflect the views of SC Media UK or Haymarket Media.*