The Pulse of a Nation: A Study on the Cybersecurity Issues Plaguing the Healthcare Industry

William R. Angel III
College of Education, Criminal Justice, and Human Services
University of Cincinnati
Cincinnati, Ohio, United States of America
angelwr@mail.uc.edu

***Abstract*—In this paper, I study how medical records are being used by cyber-criminal for financial gain and patient manipulation. I studied what kind of criminal organizations may be involved in these operations and confirmed incidents from the black market. I conducted a literature review which generated several sources from online databases. I determined five major criminal factions that are most likely to use compromised medical records, determined possible motivations and looked at several cases of medical records being sold on the black market. The healthcare industry's digitization efforts have left it tremendously ill-equip to combat emerging threats. It is evident that the healthcare industry must take extreme measures in order to counteract the evolving threat landscape. It is my hope that the findings of paper will being to shed light on these issues and help healthcare professionals understand what kind of threats the industry is facing.**

Keywords—EHR (Electronic Health Record), Healthcare, Dark Web, Cybersecurity

I. INTRODUCTION

Cybersecurity is quickly moving into the spotlight for nearly all organizations on a global scale. It is now widely accepted that being involved in a data breach is not a matter of "if" but "when". Therefore, organizations in every industry must prepare and develop advanced countermeasures to fight the growing threat of cyber-attacks. Healthcare is one of, if not, the most critical industries in our society today. The responsibility to keep financial, personal, and medical information safe from malicious actors now falls into the hands of our healthcare providers. This industry is faced with a rapidly growing attack surface, a very public history of major data breaches and a plethora of other flaws in the its approach to cybersecurity. Thus, we are seeing that the healthcare industry is extraordinarily ill-equipped to combat emerging threats.

Every year, articles and reports are published covering a wide array of cybersecurity issues to watch out for in the healthcare industry. Each of these publications covers several topics giving a brief summarization of each item and often leave readers with more questions than answers.

The purpose of this study is to discuss a critical cybersecurity issues in the healthcare industry. The goal is to better understand why healthcare has become such a large target for cyber-criminals, who these potential actors are and how the industry is being exploited. Specifically, we will discuss what kind of information is stored in medical records, who may be targeting this information, why these records are valuable targets for cyber-criminals, and how it is being leveraged on the black market. We will look at specific cases of healthcare records on the black market to highlight the consequences such cases can have on the industry.

II. METHODOLOGY

A. *Method Background*

The purpose of this study was to discuss critical cybersecurity issues in the healthcare industry. The goal was to better understand why healthcare has become such a large target for cyber-criminals and how they use stolen medical data to exploit individuals and organizations alike. The vast majority of people know that healthcare is experiencing these security issues but do not understand why. In this paper, I attempt to address this knowledge gap. The research questions proposed in this paper are:

- What kind of information is stored in medical records?
- Who may be targeting this information?
- Why these records are valuable targets for cyber-criminals?
- How it is being leveraged on the black market?
- How can we mitigate this risk in the future?

I have outlined the steps taken to conduct investigation and draw conclusions from these research questions in the Literature Review of this paper.

III. LITERATURE REVIEW

A. *Literature Identification and Collection*

The key terms 'black market', 'breach report', 'cybersecurity', 'dark web', 'data breach', 'electronic health records', 'fraud', 'healthcare', 'insider threat', 'medical records', 'threats', 'security awareness' and 'security education' were used to identify and collect relevant literature for this study. These terms were searched for either independently or in conjunction through online search engines or electronic scholarly databases.

In this study, we relied on a distinct online search engine, Google, to collect literature. Scholarly databases used to collect literature for this study included UC Libraries, PubMed and Google Scholar.

Several industry and academic resources were leveraged in this study including IBM, Verizon, Beazley, McAffee, Protenus and the Identity Theft Resource Center. Academic institutions referenced in this study include the ESSEC Business School and Harvard University.

B. *Literature Analysis*

The literature review generated multiple sources that are noted in this paper's References section. It was vital that this study's literature collection and results focused on current industry trends and data. Thus, only literature published between 2014 and 2018 was taken into consideration.

IV. DATA ANALYSIS AND RESULTS

A. *What are Electronic Health Records?*

Electronic Health Records (EHRs), also known as Electronic Medical Records (EMRs), are the digitized versions of a patient's medical charts. EHRs are designed specifically to provide authorized users the ability to instantaneously access and manage medical records for patients across healthcare organizations. These authorized users can be anyone from doctors, nurses and pharmacists to an agent at your healthcare insurance provider. Rather than just containing medical records, EHRs are intended to collect a broad array of information including but not limited to the following:

- Medical History
- Diagnoses
- Current and Past Medications
- Immunization Dates
- Allergies
- Lab Data and Imaging Reports
- Demographic, Financial and Insurance Information
- Social Security Number

B. *Who is Targeting the Healthcare Industry? What are their Motivations?*

The healthcare industry is a critical infrastructural element to nations worldwide. The idea that the entire healthcare industry is a web of smaller interconnected-organizations has resulted in the

industry becoming its own greatest enemy relative to cybersecurity. These organizations come in all shapes, sizes and functions while catering to the specific needs of the citizens in which they are built to serve. Due to this wide range of function, not all organizations face the same threats nor do they know who their adversaries are. Rather than identifying specific threats, a poorly constructed veil is placed over these organizations as a security "catch all".

Identifying threats that are most relevant to specific organizations is vital for the healthcare industry to evolve to the growing threat landscape. The ability to shift focus from combating irrelevant or absent adversaries to identifying the most likely threats and putting measures in place to counteract their efforts could be a monumental shift in the security of healthcare data. There are several possible actors (Figure 1) who could benefit from healthcare breaches such as:

- Individuals/Small Groups
- Political Groups
- Organized Crime
- Terrorists Organizations
- Nation State Actors

However, the ability to simply recognize who potential threats may be is not enough. Healthcare providers must be able to recognize what the primary goals or most likely targets of these groups are to best assess which threats need to be prioritized within their organization.

Individuals/Small Groups are historically opportunistic attackers who are typically motivated by financial gain and ease of access in compromising a system. These attacks could be considered one of, if not, the most common attacks in the healthcare industry. A 2016 study by the IBM Managed Security Services group concluded that 68% of all network attacks targeting healthcare organizations were carried out by insiders. These attacks originating from both malicious and inadvertent actions albeit. A study by Protenus, Inc. in 2016 resulted in data that shows out of all healthcare incidents included in said study 192 were the result of insiders. Of these findings, the compromised patient records due to insider-error was comparable to that of insiders with malicious intent once significant outliers were removed (Figure 2).

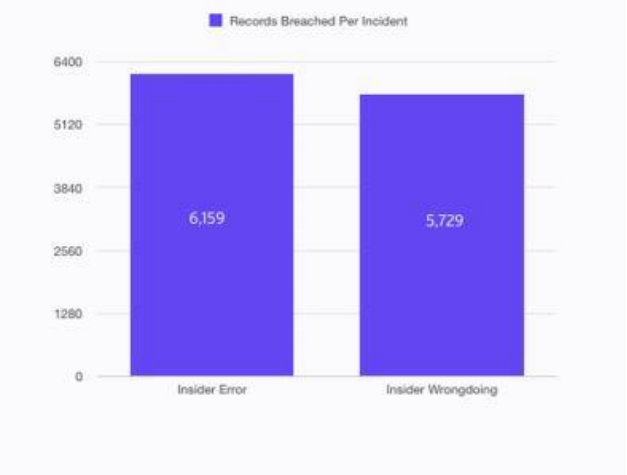


Figure 2: Average Number of Patient Records Breached by Insider Incident Type

Political groups are most notably credited with conducting targeted attacks against public figures. These attacks can include but are not limited to blackmail, extortion, public discretization and embarrassment. In 2016, fake medical records for Hillary Clinton began to circulate throughout the internet in an attempt to derail her credibility in the 2016 Presidential Elections. These documents stated that Clinton had been diagnosed with "complex partial seizures" in addition to "early-onset subcortical vascular dementia". While these documents were proved to be fake the incident is a great example of how compromised medical records can be used to impact public figures.

Organized crime covers a broad array of targeted and untargeted attacks to attain financial gain or physical harm to targets.

However, the most critical threats to the healthcare industry are considered to be Terrorist and Nation-State groups. The sole goals of these groups are to inflict harm and spread fear to both individuals and large groups of people. Cyber warfare is an increasing threat in our society today and the next major attack against the United States is likely going to be a cyber-attack. Therefore, preparedness and means to counteract these groups should be taken with upmost importance.

Figure 1: Possible Malicious Actors Involved in Healthcare Breaches

C. *Why are Medical Records such Valuable Targets for Cyber-Criminals?*

Medical records hold an intrinsic value in our society today. EHRs are one of, if not, the most extensive records of a person's identity today. Thus, they hold a tremendous non-monetary value. Since these records cannot be changed when compromised, like that of credit cards, they are considered much more valuable to every patient and criminal in possession of such data.

Compromised medical records can give cyber-criminals leverage against individuals or groups of people in targeted or untargeted attacks. Due to their longevity, compromised medical records can give malicious actors a nearly unlimited time frame to benefit from their newfound knowledge which makes healthcare data far more valuable than credit cards data. There are countless attack possibilities for attackers after acquiring medical records such as:

- Financial Gain
- Blackmail/Extortion
- Advance of Political Agendas/Career Assassination
- Public Humiliation/Discretization
- Infliction of Physical Harm/Fear through Modification of Medical Records
- Fraud/Identity Theft

Aside from these non-monetary factors, financial gain is the most prevalent motivation for hackers and other malicious actors to act on compromised medical records. Thus, we are seeing a new trend in motivation and consequence for medical record sales on the black-market (Figure 3). The FBI reported in an unclassified private industry notification that the black-market rate for EHRs, even partial, was steady at approximately $50 in 2014. A number substantially higher than the $1 per record seller rate for stolen Social Security Numbers or credit cards. Further investigation confirmed that depending on the source, nature and amount of records being offered led seller rates to go anywhere from $2.50 to $500 per record.

However, there is some logic behind this large price range. On the lower end of the spectrum, in the $2.50 range, records tend to be very minimal in quality and content. Whereas the higher range, around $50-100, records likely have much richer and more valuable content. We see that individual or bulk records have reported in the range of hundreds of dollars are more likely to contain information pertaining to specific or high-profile targets.

Reports as recent as 2018 have shown that the market value for medical records has been steadily decreasing. The black-market has become so saturated with healthcare data that the prices are declining. This is a major cause for concern due to the larger market making healthcare records available for a larger margin of buyers and the influx of breaches making this market saturation possible in the first place.

Figure 3: Financial Gain Leads to New Market Trends for Medical Records

D. *How are these Records being Leveraged on the Black-Market?*

The market for stolen medical data on the dark web is much larger than I previously realized. After reading several reports, security blogs, and evaluating countless healthcare news outlets I learned about this very real market. In my investigations, I discovered some use cases of The Real Deal which is a dark web marketplace. The Real Deal is one of the confirmed dark web markets where "Thedarkoverlord" operates. This seller is notorious for providing healthcare data on the dark web. He has advertised healthcare databases amassing 400,000 records (Figure 4), 45,000 records (Figure 5) and 200,000 records (Figure 6) in some cases. These databases included patient names and addresses, Social Security Numbers, birthdates, primary and secondary healthcare insurance

provider data and much more that would be attractive to potential buyers.

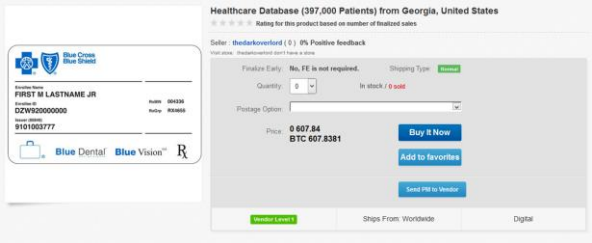


Figure 4: Screenshot from Dark Web of 400,000 Patient Database for Sale

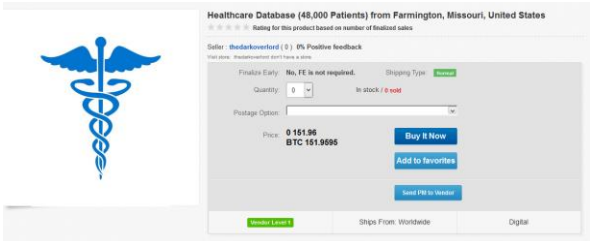


Figure 5: Screenshot from Dark Web of 45,000 Patient Database for Sale

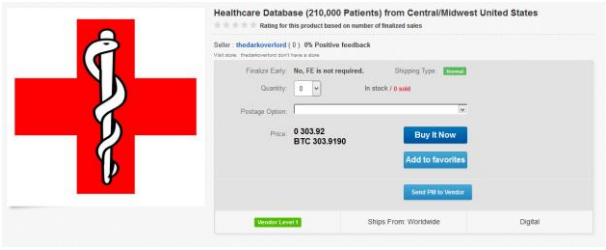
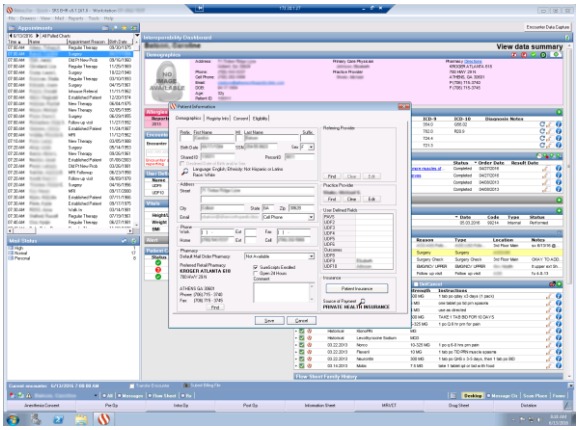


Figure 6: Screenshot from Dark Web of 200,000 Patient Database for Sale

These databases originated from locations such as Farmington, Missouri; Atlanta, Georgia; and a healthcare provider from the Midwest, United States that has yet to be named. “Thedarkoverlord” noted that the 200,000-patient database from the Midwest “was retrieved from a severely misconfigured network using readily available plaintext usernames and passwords.”.

“Thedarkoverlord” went further in giving proof of the data’s integrity by providing screenshots of activity within the victim system’s databases (Figures 7 & 8). He stated that he used “an exploit in how companies use RDP. So, it is a very particular bug. The conditions have to be very precise for it” Aforementioned screenshots provide information such as past medical appointments, demographics, allergies, and prescribed medications. This has provided us with a perfect example of past discussions on malicious actors. It could be the case that the hacker did not want to collect this data to exfiltrate for financial gain but would rather target a specific patient’s medical records. The manipulation of one patient’s medical records, such as omitting an allergy, could compromise a patient’s health and lead to serious medical issues or even death.



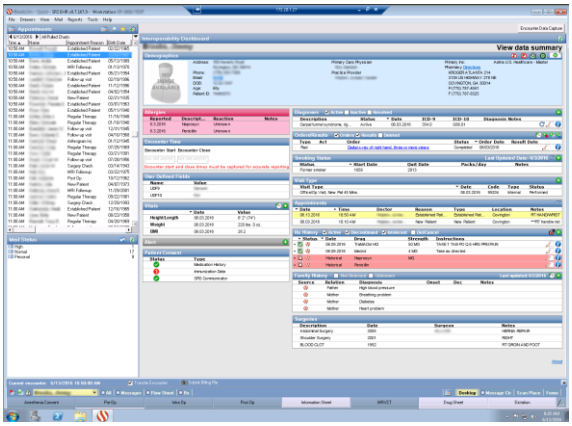


Figure 7 & 8: Screenshot from Dark Web of Compromised Patient Database Backend for Sale

Later advertisements by the same seller gave wind to one of the largest medical data dumps to date. “Thedarkoverlord” put a 9.3 million patient record database (Figure 9) up for sale on The Real Deal from a major healthcare insurance organization. The seller declined to confirm or deny the database’s relation to the Anthem breach which occurred around the same time of this data hitting dark web marketplaces. The data was retrieved by exploiting a 0-day remote desktop protocol (RDP) vulnerability in a Windows Server 2008 R2 system and was on sale for a staggering 750 bitcoins or $485,000. This database included data such as full names and addresses, email accounts, phone numbers and other critical information such as patient birthdates and social security numbers.

Investigation into the validity of the data was also performed and it was found that some data, such as addresses or phone numbers, was outdated and no longer useful. This is not surprising since many companies refrain from purging old data. However, SSNs and birthdays never change and can be used in identity theft and insurance fraud.

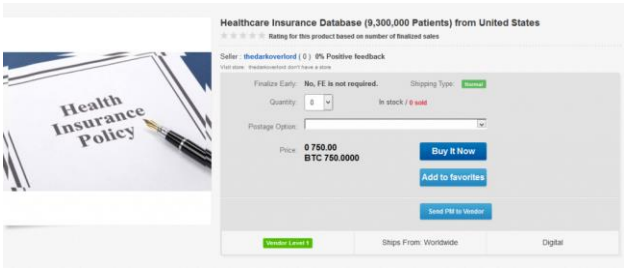


Figure 9: Screenshot from Dark Web of 9.3 Million Patient Database for Sale

E. *Industry Statistics*

In order to get a better idea about the overall state of the industry I gathered statistics from several firms about the cybersecurity landscape in healthcare.

According to a study of 91 healthcare organizations by the Ponemon Institute, 69% of these organizations believe they are more vulnerable to a data breach than other industries. This is a result of a lack of security vigilance and funding in healthcare organizations as the focus is on saving lives and medicine rather than IT. Additionally, there is a lack of qualified IT security personnel in these organizations.

Furthermore, over the past two years, 89% of aforementioned healthcare organizations have experienced a data breach resulting in lost or stolen patient data. 60% of who reported that they conduct vulnerability assessments most often do so on an annual or ad hoc basis (Figure 10). This means that 40% reported no vulnerability assessments take place and the other 60% conduct these assessments so rarely that by the time a vulnerability is recognized and patched it may already be too late. 69% of healthcare respondents also recognized insider threats as the top security issue their organization worries about.

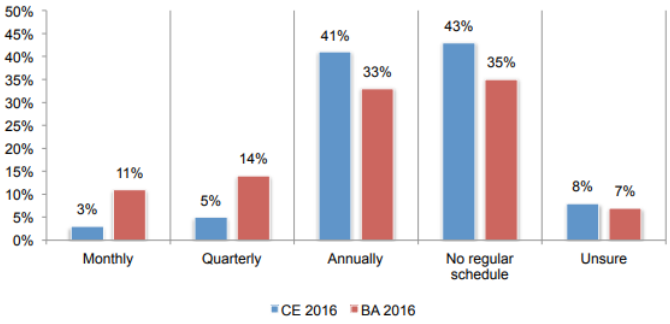


Figure 10: Vulnerability Assessment Statistics from the Ponemon Institute

V. CONCLUSION

The widespread adoption of Electronic Health Records is revolutionizing the way healthcare organizations interact with each other and its patients. However, they are exponentially increasing the industry's attack vector while failing to address fundamental security issues as digitization occurs such as vulnerability management and staff security education.

The transition from paper to electronic-based medical records is attracting the masses of the criminal underworld. What was once never possible is now only a few keystrokes away and that is the ability to inflict direct harm to the health and well-being of individuals or groups of people around the globe.

Modifications of EHRs is just one of the countless possibilities now available to a motivated party to incite fear, cause harm, and benefit financially at the expense of others. The monetary value for medical records on the dark web has been trending downwards in recent years due to market saturation. This increase in breaches and data available for consumers at even lower prices leaves the gates open for a wide array of new clientele. Thus, historically lower prices and more potential for return makes medical records a much more plausible option for cyber-criminals than credit cards. Additionally, we are past the age when you could only make someone's bank account suffer through the internet. We are now seeing confidential information being leveraged against groups or individuals directly affecting their health and well-being.

VI. Recommendations

The issue of measuring assets and determining vulnerabilities seems to be nonexistent in the healthcare industry. In order to mitigate risk in the organization, more money must be allocated to fund security efforts. Outside of patient health, information is healthcare's most valuable asset. Organizations must think about if the costs of reducing breaches really outweigh the benefits of decreasing their attack vector and overall risk.

Additionally, security education amongst staff must come into the forefront. Medical staff members are highly educated individuals who should have no problem picking up some cybersecurity education through training and awareness classes. Fostering a security minded culture is the first step to ensuring that assets and patient data is safe.

Another item is that in order to protect themselves from malicious actors organizations must determine what kind of threats they are up against. With a more focused approach on who the most likely adversaries are organizations are more likely to have better measures in place to deter them. Collaboration with government and security specialists could prove monumental in determining how to best mitigate risk with electronic health records.

VII. References

This section is dedicated to providing references to the resources leveraged in the completion on this study.

[1] Illuminweb.com. (2018). [online] Available at: http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf [Accessed 10 Apr. 2018].

[2] InCyberDefense. (2018). Medical Data Being Sold on the Black Market. [online] Available at: https://incyberdefense.com/news/medical-data-sold-black-market/ [Accessed 7 Apr. 2018].

[3] Securityevaluators.com. (2018). Securing Hospitals. [online] Available at: https://www.securityevaluators.com/wp-content/uploads/2017/07/securing_hospitals.pdf [Accessed 2 Apr. 2018].

[4] Francis, R. (2018). Healthcare records for sale on Dark Web. [online]
CSO Online. Available at: https://www.csoonline.com/article/3189869/data-breach/healthcare-records-for-sale-on-dark-web.html [Accessed 22 Mar. 2018].

[5] InCyberDefense. (2018). Medical Data Being Sold on the Black Market. [online] Available at: https://incyberdefense.com/news/medical-data-sold-black-market/ [Accessed 7 Apr. 2018].

[6] Market, 2. (2018). Healthcare Security $65 Billion Market. [online] Cybercrime Magazine. Available at: https://cybersecurityventures.com/healthcare-cybersecurity-report-2017/ [Accessed 12 Apr. 2018].

[7] Morgan, S. (2018). Healthcare cybersecurity spending to exceed $65B over the next 5 years. [online] CSO Online. Available at: https://www.csoonline.com/article/3252343/cyber-attacks-espionage/why-healthcare-cybersecurity-spending-will-exceed-65b-over-the-next-5-years.html [Accessed 12 Apr. 2018].

[7] Calyptix Security. (2018). Healthcare Data Breaches Expected to Dominate 2017. [online] Available at: https://www.calyptix.com/hipaa/healthcare-data-breaches-expected-to-dominate-2017/ [Accessed 12 Apr. 2018].

[8] Phe.gov. (2018). 2017 Report. [online] Available at: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf [Accessed 11 Apr. 2018].

[9] Idtheftcenter.org. (2018). 2017 Annual Data Breach Year End Review. [online] Available at: https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf [Accessed 10 Apr. 2018].

[10] Verizonenterprise.com. (2018). 2018 Data Breach Investigations Report. [online] Available at: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf [Accessed 11 Apr. 2018].

[11] Your Bibliography: Blogs.harvard.edu. (2018). STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS. [online] Available at: http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf [Accessed 11 Apr. 2018].

[12] Jim Avila, Marshall, S. and KAUL, G. (2018). $60 Billion Medicare Funds Improperly Paid, Report Finds. [online] ABC News. Available at: http://abcnews.go.com/Politics/medicare-funds-totaling-60-billion-improperly-paid-report/story?id=32604330 [Accessed 13 Apr. 2018].

[13] Farley, R. (2018). Fake Clinton Medical Records - FactCheck.org. [online] FactCheck.org. Available at: https://www.factcheck.org/2016/08/fake-clinton-medical-records/ [Accessed 13 Apr. 2018].

[14] Healthit.gov. (2018). What is an electronic health record (EHR)? | HealthIT.gov. [online] Available at: https://www.healthit.gov/faq/what-electronic-health-record-ehr [Accessed 15 Apr. 2018].

[15] Deep Dot Web. (2018). New Breach: 655000 Healthcare Records (Patients) Being Sold. [online] Available at: https://www.deepdotweb.com/2016/06/26/655000-healthcare-records-patients-being-sold/ [Accessed 14 Apr. 2018].

[16] Deep Dot Web. (2018). New Breach: Healthcare Insurer Database Of 9.3M Records Being Sold. [online] Available at: https://www.deepdotweb.com/2016/06/28/now-9300000-healthcare-insurance-database-sold/ [Accessed 14 Apr. 2018].

[17] Mcafee.com. (2018). Health Warning Report. [online] Available at: https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf [Accessed 11 Apr. 2018].

[18] www-01.ibm.com. (2018). Security Trends in the Healthcare Industry. [online] Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03123USEN [Accessed 4 Apr. 2018].

[19] Beazley.com. (2018). 2018 Breach Briefing. [online] Available at: https://www.beazley.com/documents/Whitepapers/201802-beazley-breach-briefing.pdf [Accessed 13 Apr. 2018].