Copernican Journal of Finance & Accounting

2017, volume 6, issue 3

e-ISSN 2300-3065
p-ISSN 2300-1240

Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63–73. http://dx.doi.org/10.12775/CJFA.2017.017

Marta Meisner*
Nicolaus Copernicus University in Torun

FINANCIAL CONSEQUENCES OF CYBER ATTACKS LEADING TO DATA BREACHES IN HEALTHCARE SECTOR

Keywords: cybersecurity, data breach, healthcare.

J E L Classification: G32.

Abstract: Healthcare sector is identified as particularly vulnerable to digital data breaches and damages caused by illegal use of personal and confidential information. Facing such dangerous threat medical entities need to estimate financial consequences of potential cyber attack leading to a breach of patients' data. The paper's aim is to provide an overview of the consequences of digital data breach in healthcare sector and their financial impact – comparing Polish and global perspective. The research method used was analysis and comparison of international literature, reports, case studies, statistics concerning data breaches in healthcare sector as well as new legal regulations applicable in European Union. The results of the research show that estimations of total digital data breach costs vary widely among various reports and analysis. The main reasons are application of different methods of estimation and lack of complete and reliable databases due to insufficient disclosure of cyber incidents. In addition, the most important conclusion of the paper is that there is an urgent need to conduct research concerning probable data breach costs in Polish healthcare sector, since studies pursued by renowned organisations have not covered Poland so far.

Date of submission: December 15, 2017; date of acceptance: December 30, 2017.

* Contact information: marta.a.meisner@gmail.com, ul. Krasińskiego 25/8, 87-100 Toruń, Poland, phone: +48 660 773 077; ORCID ID: https://orcid.org./0000-0002-4145-3482.

Introduction

Healthcare industry has moved beyond the stage where all patients personal data were stored within paper-based systems, which – although reduced the exposure of data – did not bring enough effectiveness for communication, transfer of documentation and general workflow (Health Care Industry Cybersecurity Task Force, 2017, p. 10). To overstep these limitations healthcare sector enters the phase of electronic healthcare records being the main source of information. In Poland these changes are introduced mainly following legal acts and recommendations of European Union organs. It is not questioned that digitalization of documents and deeper digital connectivity is essential in order to deliver effective and safe medical services, however it has to be balanced with the need to provide proper protection of IT systems (Health Care Industry Cybersecurity Task Force, 2017, p. 9).

Healthcare sector is one of the most frequently attacked – in 2016 it was ranked on the 9th place on the list of most targeted industries and on the 5th place in number of data breaches (SecurityScorecard, 2016, p. 5). Medical entities have, thus, urgent need to effectively estimate costs they would have to bear in case of potential materialisation of digital data breach. Unfortunately, in this case financial management is a challenge since there are limited sources of data, cyber incidents – even if discovered – are rarely reported and results of researches conducted vary widely.

Research methodology

For the purposes of this article critical analysis of international literature, reports, case studies and statistical data concerning data breaches in healthcare sector has been conducted. Additionally, the research involved study of law regulations and institutional recommendations of European Union and Polish organs regarding cybersecurity and digital health data.

Healthcare sector vulnerabilities to cyber threats leading to data breach

Reports and analysis indicate that within healthcare sector data breaches are, beyond ransomware, the greatest threat, which (apart from names, birth dates,

contacts) involve the most sensitive personal data – medical information (SecurityScorecard, 2016, p. 2; Romanosky, 2016, p. 122; Lloyd's, 2017, p. 15). As healthcare information cannot be altered after data theft, its permanence is reflected in the black market price – higher in comparison with e.g. credit card data or social security number (Luna, Rhine, Myhra, Sullivan & Kruse, 2015, p. 6; Fuentes, 2017, pp. 10–12; Mansfield-Devine, 2017, p. 15).

Cyber crimes on personal data may result in severe financial losses for their victims (Accenture, 2015; Mansfield-Devine, 2017, p. 15). According to analysis digital personal information of more than 25 million people will be stolen from their healthcare providers between 2015 and 2019, leading to more than 6 million identity thefts and almost USD 56 billion out-of-pocket costs payed by the victims (Accenture, 2015).

Digital data breaches are caused mainly by: malicious or criminal attack, glitch of IT system or human error (Ponemon Institute, 2017, p. 7). The majority of data breaches is caused by malicious actions (Romanosky, 2016, p. 122; Ponemon Institute, 2016, pp. 1, 6) of either internal (e.g. employees abusing their access) or external character (outside agents using stolen login details or computing devices, social engineering or hacking: exploiting weak credentials, using malware or presence of system vulnerabilities) (Luna et al., 2015, p. 4). External incidents dominate (Ponemon Institute, 2016, p. 2) and as many as 45% of analysed healthcare organisations points cyber attackers as the source of digital data breach incidents that worries them most (Ponemon Institute, 2016, p. 3).

Cybersecurity is even more endangered every year with the Internet of Things (IoT) spreading in medical industry. Common use of optimised and automated IT processes and interconnected systems, particularly based on IoT, creates Smart Hospitals (ENISA, 2016, p. 9). The digitisation in healthcare sector is generally promoted in European Union, mainly through the concept of eHealth. In addition, in Poland on 20 July 2017 the Act on Information System in the Healthcare Sector from 2011 has been amended so that as from 1 January 2019 healthcare entities are obliged to prepare certain medical documentation in electronic form. It all results in expansion of health information attack risk (ENISA, 2015, p. 26; Health Care Industry Cybersecurity Task Force, 2017, p. 17).

In order to regulate, harmonise and update standards of data protection two new pieces of legislation will soon apply to EU member states: the European General Data Protection Regulation (GDPR) and the Network & Information

Security (NIS) Directive. The GDPR (enforceable from 25 May 2018), directly binding and applicable in all EU member states, is intended to strengthen protection of personal data i.a. by providing tools such as: an obligation to notify about security breaches (Articles 32–34); fines (Article 83); individuals' right to claim compensation for both financial loss and non-material damages (Article 82). In 2018 also NIS Directive, focusing on essential services operators including healthcare providers, will be incorporated to national legislations (deadline: 9 May 2018). In November 2017 Polish Ministry of Digitisation published a draft of National Cybersecurity System Act, which incorporates NIS Directive regulations and provides i.a. a requirement to report all significant cyber incidents (Article 12) and sanctions (Article 57).

Fortunately, the need to invest in cybersecurity seem to be understood by the majority of healthcare providers as 69% of them believe healthcare sector is at greater risk of data breach than other industries and 67% states that recent massive data breaches affected their security practices (Ponemon Institute, 2016, p. 3).

Financial impact of digital data breach for healthcare providers

Due to insufficient amount of quality data and a huge number of factors that has to be taken into account, estimating data breach costs is an ongoing struggle. While determining the cost of data breach the Ponemon Institute suggests relying on the number of individual records compromised (in 2017 an average global cost of a record was USD 141) (Ponemon Institute, 2017, p. 1). Alternatively, Sasha Romanosky from RAND Corporation suggests basing on correlation between data breach costs and annual revenue of attacked organization and proves that recent data breaches have cost companies 0.4% of their annual revenue (Romanosky, 2016, p. 122). Bearing in mind various methods of estimating the costs and incomplete sources of data researchers rely on, differences in results should not surprise. The Ponemon Institute researches shows that the mean total cost of data breach is decreasing: being USD 4 million in 2016 and USD 3.6 million in 2017 (Ponemon Institute, 2017, p. 1); in the 2016 RAND study the mean total cost is estimated at USD 6 million (Romanosky, 2016, p. 129); in the NetDiligence 2016 analysis the mean total cost is USD 0.67 million, but almost USD 6 million for large companies (NetDiligence, 2016, p. 2).

Costs resulting from data breach are usually borne in two phases: immediate (first hours, days or weeks of data breach response) and delayed (costs be-

ing long-lasting business consequences of a cyber attack) (Deloitte, 2016, p. 2; Lloyd's, 2017, p. 22). Certain expenses are almost unavoidable, direct and fairly easy to quantify, while other remain intangible, largely dependent on the sector and region of operating as well as nature of the attack, and may be spread over many years following data breach (Deloitte, 2016, p. 4). Below, main costs that healthcare entity would have to incur in case of cyber data breach are presented and briefly described.

Forensic investigation. Immediately after a data breach is discovered or even suspected the main task is to determine what has actually happened. Professional third-party services are usually essential to help a healthcare organization conduct an accurate investigation. Such assistance is most often time-consuming, costly and charged on hourly basis (according to Zurich Insurance Company fees vary between USD 100 and USD 1,000 per hour) (Zurich Insurance Company, 2014, p. 7). In its report Deloitte estimated that six weeks of engaging a team of five experts would cost approximately USD 600,000 (Deloitte, 2016, p. 20).

Breach notification. When it is known whose data has been breached, healthcare entity should notify those individuals. In European Union the GDPR will unify among EU members states the notification requirement as Article 34(1) obliges the controller of data (e.g. healthcare entity) to communicate without undue delay affected individuals about personal data breach whenever the breach is likely to result in a high risk to their rights and freedoms. Notifying the victims also helps preserve good reputation among individuals and avoid customer churn. Notifying one victim may cost between USD 5 to USD 50 per notice (Zurich Insurance Company, 2014, p. 7).

Post-breach patient protection. Additional services, such as credit monitoring and identity theft protection may help keeping patients safe from potential unauthorised use of stolen data. According to the research conducted in the U.S. by the Ponemon Institute the majority of respondents stated that medical data breach victims should be protected for at least 2–3 years, however 64% of healthcare entities do not offer any post-breach protection services (Ponemon Institute, 2016, p. 6). Such additional protection is not yet a common practice, but is a good tool to reduce the probability of being sued or at least to limit the damages. Researches show that typical costs are USD 10–30 per victim, however only 9% of affected individuals in fact registers for offered identity theft protection services (Deloitte, 2016, p. 20).

Attorney fees and litigation expenses. With the development of data protection legislation and social awareness – the affected individuals tend to bring claims more often seeking compensation for both financial losses and emotional distress resulting from data breach (Lloyd's, 2017, p. 28). Sometimes the costs of legal claims against healthcare provider may be recovered through litigation against an attacker; however it is most often both uncertain and long-lasting process. As NetDiligence report presents in 2016 the average cost for legal defence was USD 130,000 (the median was USD 16,000) and the average legal settlement cost – USD 815,000 (the median was USD 250,000) (NetDiligence, 2016, p. 3).

Regulatory compliance. If a healthcare entity fails to fulfil legal requirements (concerning application of preventive measures or post-incident conduct), it exposes itself to risk of potential regulatory fines. In EU member states GDPR introduces sanctions up to EUR 20 million or 4% of the annual worldwide turnover (whichever is higher) in case of infringement of indicated provisions. The ability to impose penalties is also provided by NIS Directive and in Poland the draft of National Cybersecurity System Act in case of non-compliance with certain provisions gives authorities right to impose fines up to PLN 200,000 (Article 57). With ever-growing scrutiny of authorities in the field of personal data protection, more severe regulatory penalties may be expected in the following years (Deloitte, 2016, p. 21).

Cybersecurity improvements. To prevent similar cyber incidents in the future, actions aimed at increasing security should be undertaken. Most often these are technical improvements to the IT infrastructure, controls system, capabilities of monitoring and other processes (Deloitte, 2016, p. 21). Also cybersecurity training for personnel should be provided, especially when the cause of a vulnerability enabling data breach was human error. The expenses for cybersecurity improvements are impossible to predict generally, since the standard of protection varies widely and the scope of improvement depends on individual cyber risk management strategy.

Loss of reputation and patients churn. In the aftermath of a data breach mitigation of potential damage to the healthcare entity reputation is crucial. A massive personal data breach may trigger not only aversion of victims, but generally – the public, which may require involving professional help of public relation experts (Zurich Insurance Company, 2014, p. 7). Deloitte estimates the cost of a 4-week PR campaign following a cyber attack at USD 400,000 on average, while extended 1-year campaign at USD 1 million (Deloitte, 2016,

p. 21). If PR actions are ineffective, medical entity may experience decline of brand value and patients churn leading to a revenue loss. According to analysis from 2015 in 5 following years healthcare providers may lose as much as USD 305 billion in cumulative lifetime patient revenue due to patients churn resulting from medical identity theft (Accenture, 2015). While it may be hard to imagine massive patients churn from public hospitals in Poland, especially where there is no alternative available locally (e.g. one cancer treatment centre in region), negative consequences of a data breach may be very severe for private medical entities.

Other potential costs. The Deloitte analysis shows that it is not uncommon for insurers to increase, even double, premium in case of purchasing or renewing cyber risk insurance after a cyber incident. Sometimes policyholder may even be denied an insurance offer until certain conditions, such as technical improvements or introducing cyber incident response plan, are met. Also banks may perceive medical entities that recently experienced cyber attack as high-risk borrowers, which can lead to increase of interest rates for borrowed capital while raising debt or renegotiating the terms of the existing one (Deloitte, 2016, p. 22).

While abovementioned renowned researches have not covered Polish healthcare market so far, one may try to make a general estimation of potential costs that cyber data breach in Polish hospital would entail. In 2016 in Poland there were 186,607 beds in 957 hospitals, which means that in average one hospital had about 195 beds (GUS, 2017, p. 81). According to Polish Central Statistical Office in 2016 bed occupancy ratio was 66% (GUS, 2017, p. 92) and the number of patients using one hospital bed was in average 45.3 (GUS, 2017, p. 89). In consequence, the average number of patients, whose data a hospital collected, was almost 6,000 per year. While patients medical records are stored in healthcare entities for many years, a data breach resulting in theft of personal records of e.g. 3,000 people is highly probable. The costs of such breach may be estimated properly only by calculation prepared for a specific entity. Nevertheless, in order to show potential financial consequences of a rather small data breach, hypothetical costs estimation basing on the results of aforementioned renowned researches are shown in the table below.

Table 1. Hypothetical financial cost of cyber data breach in Polish hospital

Type of costs	Potential scenario	Estimated costs	Estimated costs in PLN*
Forensic investigation	3 weeks of engaging 3 experts (each working 8h/day). Rates: USD 200 per hour.	200 USD x 8h x 3 experts x 21 days = 100,800 USD	348,223.68 PLN
Breach notification	Notification of 3,000 patients. Cost of notification: USD 10 per victim.	3,000 patients x 10 USD = 30,000 USD	103,638 PLN
Post-breach patient protection	Post breach protection cost at the level of USD 15 per victim. Only 9% of victims – 270 patients – registered for such services.	270 victims x 15 USD = 4,050 USD	13,991.13 PLN
Attorney fees and litigation expenses	Costs of legal defence (USD 16,000) and cost of settlement in a class action civil lawsuit (USD 250,000).	16,000 USD + 250,000 USD = 266,000 USD	918,923.60 PLN
Regulatory compliance	The attacked hospital, i.e. the controller processing personal data, failed to notify about data breach as required in Article 33 of GDPR. Fine: EUR 2,000,000 according to Article 83 of GDPR. The data breach also showed that the hospital (being essential services operator) had not remedied non-compliance found during former audit. Fine: PLN 50,000 according to Article 57 of National Cybersecurity System Act (currently in draft version).	2,000,000 EUR + 50,000 PLN	8,341,400 PLN + 50,000 PLN = 8,391,400 PLN
Cybersecurity improvements	Cyber attackers gained access to patients data using presence of hospital system vulnerabilities. Cost of cybersecurity improvements: PLN 1,000,000.	1,000,000 PLN	1,000,000 PLN
Loss of reputation and patients churn	The attacked hospital was public healthcare provider and, despite loss of reputation, patients churn was almost unnoticeable.	–	–
Other potential costs	The hospital was refused to obtain insurance against cyber incidents, unless further cybersecurity improvements are made. Cost: PLN 300,000.	300,000 PLN	300,000 PLN
Total:			**11,076,176.40 PLN**

* 1 USD = 3,4546 PLN; 1 EUR = 4,1707 PLN (NBP, 2018).

Source: own study.

As the costs of data breach differ among countries (Ponemon Institute, 2017, p. 5), financial consequences of such incident in Poland would be most probably much lower than e.g. in the U.S. (due to i.a. IT experts and lawyers rates or awarded legal compensation for damages). In addition, potential regulatory

fines imposed under GDPR or NIS Directive regulations are becoming very important while estimating data breach costs. Taking into account the aforementioned factors, the total cost of a data breach affecting only 3,000 people at the level of PLN 11 million is not an impossible scenario.

Conclusions

While global digitisation of medical data and spreading application of IoT are obviously a tremendous achievement for healthcare sector treatment capabilities and operational effectiveness, they also open more possibilities to the attackers. Cyber data breach has become one of the most serious risks for healthcare sector with financial consequences that may exceed the capabilities of unprepared medical entities.

In order to properly manage financial risk related to data breach caused by cyber attack, healthcare providers have to be aware of potential costs they would have to incur in case of a successful cyber attack. Unfortunately, researchers still struggle with accurate data breach costs estimations, as many data breaches are not reported or their details are not available. Researches are, thus, conducted basing on partial data, surveys pursued among medical entities, patients or insurers and with use of diverse methods of costs estimations. This is why results of various organisations' studies concerning data breach threat and its financial impact on healthcare sector differ so much.

While there already are numerous researches conducted globally, the analysis of digital data security and financial scale of breaches in healthcare sector in Poland is a great scientific challenge. Hopefully future international researches will take also Polish market into account. Also, legal requirements to report major cyber incidents may help create reliable database for further studies. Proper perspective – both local and international – is needed, since otherwise preventive measures and data breach response plans prepared by healthcare providers may turn out to be completely inadequate.

References

Accenture (2015). Insight Driven Health. Digital Health, https://www.accenture.com/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf (accessed: 05.12.2017).

Act on Information System in the Healthcare Sector of 28th April 2011, Dz.U. 2011 nr 113 poz. 657 z późn. zm.

Deloitte (2016). Beneath the surface of a cyberattack, A deeper look at business impacts, http://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf (accessed: 24.10.2017).

Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

ENISA (2015). Security and Resilience in eHealth. Security Challenges and Risks, https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services (accessed: 06.11.2017).

ENISA (2016). Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures, http://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals (accessed: 06.11.2017).

Fuentes, M. R. (2017). Cybercrime and Other Threats Faced by the Healthcare Industry, http://documents.trendmicro.com/assets/wp/wp-cybercrime-and-other-threats-faced-by-the-healthcare-industry.pdf (accessed: 06.11.2017).

GUS (2017), Health and Health Care in 2016, http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5513/1/7/1/zdrowie_i_ochrona_zdrowia_w_2016.pdf (accessed: 17.01.2018).

Health Care Industry Cybersecurity Task Force (2017). Report on Improving Cybersecurity in the Health Care Industry, http://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf (accessed: 06.11.2017).

Lloyd's (2017). Closing the gap. Insuring your business against evolving cyber threats, http://www.lloyds.com/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap (accessed: 24.10.2017).

Luna, R., Rhine, E., Myhra, M., Sullivan, R. & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, 24(1), 1–9. http://doi.org/10.3233/THC-151102.

Mansfield-Devine, S. (2017). Leaks and ransoms – the key threats to healthcare organisations, *Network Security*, 2017(6), 14–19. http://doi.org/10.1016/S1353-4858(17)30062-4.

National Cybersecurity System Act (draft), http://www.gov.pl/documents/31305/0/projekt+ustawy+z+za%C5%82%C4%85cznikiem+-+do+uzgodnie%C5%84+%281%29.odt/d330ca24-b76f-f772-5e42-317dbb798cbd (accessed: 28.11.2017).

NBP (2018). Table No. 001/A/NBP/2018 from 2018-01-02, http://www.nbp.pl/home.aspx?navid=archa&c=/ascx/tabarch.ascx&n=a001z180102 (accessed: 02.01.2018).

NetDiligence (2016). 2016 Cyber Claims Study, http://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf (accessed: 06.11.2017).

Ponemon Institute (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, http://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf (accessed: 06.11.2017).

Ponemon Institute (2017). 2017 Cost of Data Breach Study. Global Overview, http://www.ibm.com/security/data-breach (accessed: 06.11.2017).

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Romanosky, S. (2016). Examining the costs and causes of cyber incidents, *Journal of Cybersecurity*, 2(2), 121–135. http://doi.org/10.1093/cybsec/tyw001.

SecurityScorecard (2016). 2016 Annual Healthcare Industry Cybersecurity Report, http://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Healthcare_Report_Final.pdf (accessed: 15.11.2017).

Zurich Insurance Company (2014). The good, the bad and the careless. An overview of corporate cyber risk, https://www.zurich.com/en/knowledge/articles/2014/12/the-good-the-bad-and-the-careless-an-overview-of-corporate-cyber-risk (accessed: 14.11.2017).