A Cost Analysis of Healthcare Sector Data Breaches

Health Sector Cybersecurity Coordination Center (HC3)
HC3@HHS.GOV
Date: 4/12/2019

Executive Summary

Data breaches can have a significant impact on both the healthcare organization attacked and the individual victims. Healthcare and Public Health Sector (HPH) sector entities face the cost of recovery, lawsuits and the public relations ramifications including loss of customers/patients. Individuals can suffer financial penalties of various sorts as well as the embarrassment of having personal information leaked. As a result, the Federal government has passed several pieces of legislation in order to help protect against and curb data breaches, including regulations and penalties for healthcare organizations that are non-compliant. Costs are either direct or indirect, and mitigation efforts can be viewed in terms of prevention (the preferred method) and post-breach cost reduction. HPH Sector entities are encouraged to factor the cost of breaches into their overall approach towards risk management for both legal and operational efficiency reasons. According to a Ponemon Institute study, the average cost of a breach for a healthcare organization is approximately $8 million, and trending upwards, while another study concluded that a total breach cost can exceed $400 per patient record exposed, elevating the importance of establishing strong risk management practices.

Understanding Data Breaches

The healthcare industry is unique in the information that it contains, the sensitivities associated with that information and the potential impacts that can occur, financially and otherwise, if such information is obtained by those not authorized to have it. Protected information in the healthcare industry is defined by U.S. law, can exist both digitally and in hard copy and has legal, ethical, and business impacts when it falls outside those protections.

Protected Health Information (PHI) is defined by the Health Insurance Portability and Accountability Act of 1996 as information that uniquely identifies the individual to whom which it is related. It also has to be generated or received by a healthcare provider and is related to a patient's medical or financial information. The key to this definition is identification of the individual. Individuals who have their data leaked face repercussions including identity theft, fraud, theft of money, and the embarrassment of having information on sensitive medical procedures leaked to the public. PHI can also be used to violate non-medical aspects of a victim's

HIPAA defines PHI as: "Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

privacy such as being to pinpoint their location, acquire information on other aspects of their life such as their employment, educational, criminal or financial records. Based on several major pieces of legislation such as HIPAA and the Cybersecurity Information Sharing Act of 2015 (CISA), the federal government has rules and regulations in place in order to keep PHI from being leaked or disclosed to unauthorized individuals. There are 18 PHI identifiers defined by HIPAA:

HIPPA PHI Identifiers		
Patient name	Dates (birth, treatment, death)	Physical addresses
Fax numbers	Social security numbers	certificate/license numbers
phone numbers	full face photos/other pictures	URLs/web addresses
E-mail addresses	health plan beneficiary information	Internet Protocol (IP) addresses
medical record #s	device identifiers and serial #s	biometric (finger, voice, etc.) info
account numbers	vehicle identification information	Other uniquely identifying info

PHI can be exceptionally valuable when stolen and sold on a black market, as it often is.[1] PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering.[2] At least one study has identified the value of a PHI record at $1000 each.[3]

Electronic PHI (ePHI) is PII that is produced, stored, transferred or received in electronic form. Due to the fact that it exists in cyberspace and in many cases, is either directly or indirectly connected to the public Internet, ePHI can theoretically be stolen by anyone around the world with access to the internet.

A **record** in the healthcare industry is information that identifies an individual and includes protected health information either in hard copy or electronic form (PHI or ePHI). Authorized access to a record is limited to the individual patient whom it is related to as well as authorized healthcare professionals in service to the individual patient. Access to a health record by anyone other than authorized individuals can often be categorized as a breach.

A **breach** is an event in which one or more records are put at risk of being exposed or have been known to be accessed to someone not authorized to have access to them, in either hard copy or electronic format. It's the potential or actual access and/or use of personal information by unauthorized individuals. It often refers to the deliberate theft of such information for the purposes of monetizing it by selling it on a black market, often on the dark web. Even if information is only exposed to an unauthorized individual and never actually exploited, it is still considered a breach. Generally, breaches occur for three reasons: cyberattack, human error or system error. A cyberattack is a deliberate attempt of a malicious individual to access data which they are not authorized to have access to. A human error is an inadvertent mistake by any internal employee of an organization, such as an accidental release of information or a misconfiguration of an information system by an IT administrator. A system error is a malfunction or some other unintended means by which an information system fails to function properly. According to a recent study, the healthcare industry was one of the top four sectors affected by breaches, according to the average cost of a breach.[4]

HIPAA § 164.402 Definition of a breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. A breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Cost of Breaches

The costs of breaches can generally be broken down into two categories: Direct costs and indirect costs. According to one research institution, "Direct expenses include engaging forensic experts, outsourcing hotline support, and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates." Direct and indirect costs incurred by an organization are added up to calculate the cost of a data breach. One study released in 2018 determined that the average total cost of a data breach across industries in the United States was $7.91 million, which is also the country with the highest per capita costs at $233.[5] Furthermore, both of these costs increased in the United States from 2017 to 2018 due to factors such as prioritizing speed of victim notifications over having a thorough and comprehensive

understanding of the scope and impact of a data breach, compliance failures, the need for consultants and potential lawsuits which all contribute to these costs.[6]

U.S. healthcare breach costs

The healthcare industry has been called a high priority for hackers for a number of reasons including the value of the data they retain, the lack of security investment in the industry and the degree of connectivity between systems. US healthcare breach costs have increased in recent years. One study determined that the cost of a single stolen healthcare record increased from $363 to $380 from 2015 to 2017.[7] Other research identified the cost of a data breach in the US healthcare industry in 2018 to be $408 per record, which made healthcare breaches the most expensive by industry, roughly double the second most expensive industry (finance, $206/record) and almost three times the average for all other US industries (see Figure 1 for further data).[8] That year, costs per record breached were as low as $75 for the public sector and ran an average of $160 per record across all seventeen industries studied.[9] This was up from an average of $141 per record in 2017 according to the same organization.[10] One examination of the largest healthcare data breaches in history revealed that the number of records exposed ranged from approximately 3.5 million to almost 80 million per breach.[11]

One study determined that the average total cost of a data breach across industries in the United States was $7.91 million, which is also the country with the highest per capita costs at $233. Furthermore, both of these costs increased in the United States from 2017 to 2018.

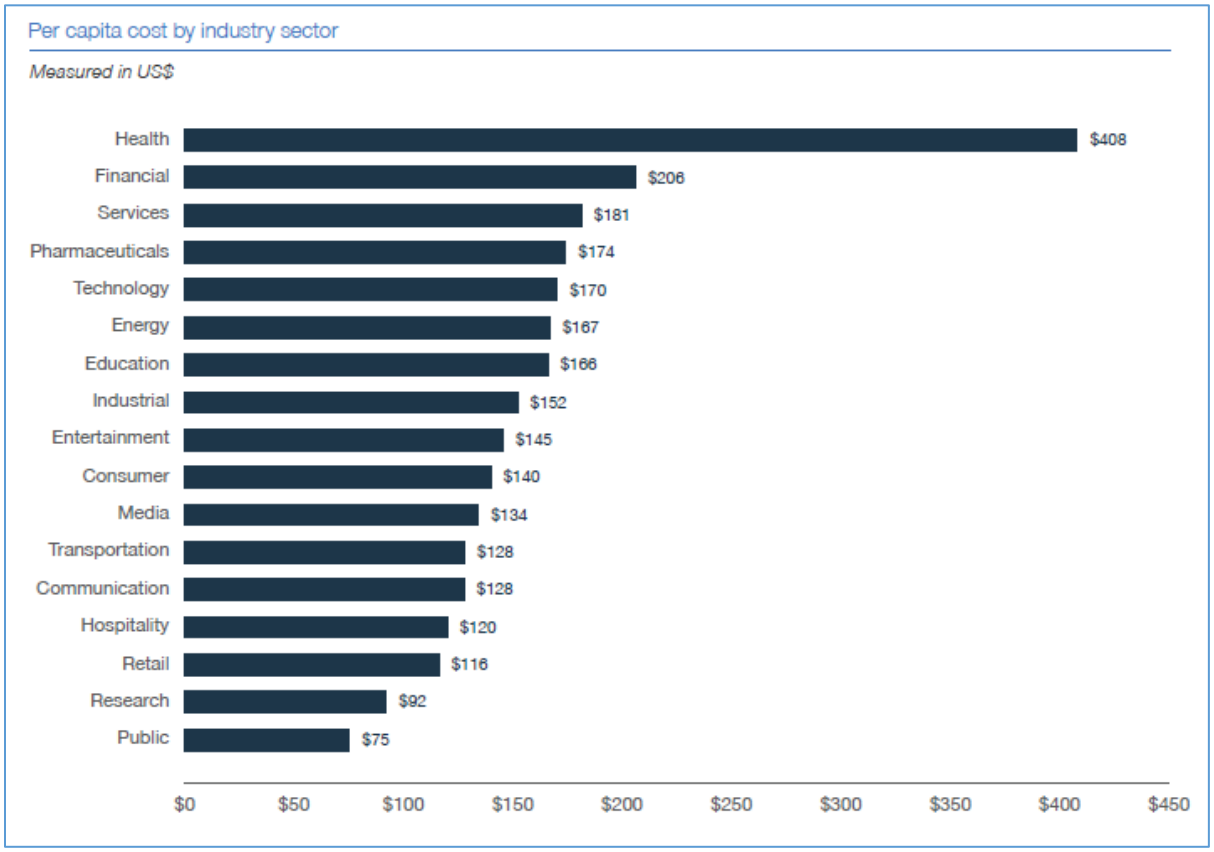

Figure 1: Per capita cost by industry sector

Breach cost breakdown

There are a number of costs associated with data breaches and two of the biggest are the time to detect, and the time to contain the breach. A Ponemon Institute study from 2018 noted that for the U.S. healthcare industry, the mean time to identify (MTTI) a breach was 255 days and the mean time to contain (MTTC) a breach was another 103 days, leaving a full year between the initial breach time and full remediation.[12] Victim notification costs contain a number of subcategories of costs that together account for another significant factor in data breach costs. As the same report noted,

> "Notification costs are the highest in the United States. These costs include the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication setups. Notification costs for organizations in the United States were the highest at $740,000"[13]

These increased costs for notification are due to the fact that the U.S. healthcare system involves the greatest amount of financial transactions as compared to any other country. In fact, while the world spends a total of approximately $6.5 trillion dollars on healthcare annually, the United States alone accounts for more than $3 trillion of this – roughly equal to the value of all other countries healthcare expenditures combined.[14] This data assists in identifying what accounts for the focus of hackers around the world as it relates to the American healthcare sector. Therefore, the increased effort and cost to protect such organizations, including but not limited to notification costs are prevalent within the industry.

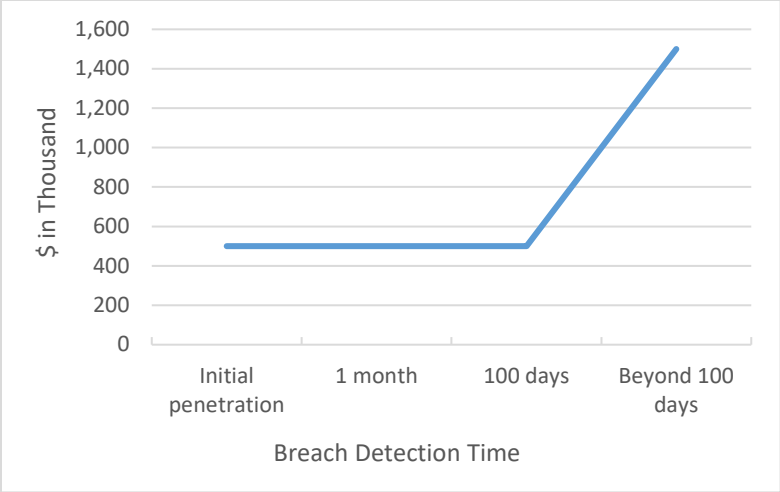

Figure 2: Cost of Breach increases by average of $1 million after 100 days of not being detected

This study also noted that companies that identified a breach in less than 100 days saved more than $1 million. This compared to companies that took more than 100 days. Furthermore, the study noted that companies that contained a breach in under 30 days, saved over $1 million as compared to those that took more than 30 days. The study also determined that the United States, along with the Middle East, spend the most on post data breach response. This includes incident handling, investigative and helpdesk capabilities, legal costs, identity protection services and other communications. Which was reported to be an average of $1.76 million in the U.S. in 2018. Another cost associated with data breaches are the unexpected loss of customers following a data breach.[15] As one study notes, "The loss of customer trust has serious financial consequences. Organizations that lost less than one percent of their customers due to a data breach resulted in an average total cost of $2.8 million. If four percent or more was lost, the average total cost was $6 million, a difference of $3.2 million."[16] Other factors associated with data breach costs are effective management of detection, escalation costs, and effective management of post data breach costs.

As previously mentioned, breaches generally occur for three reasons: cyberattack, human error or system error. Cyberattacks are the most common of them. Per Poneman in 2018, "Forty-eight percent of all breaches in this year's study were caused by malicious or criminal attacks. The average cost per record to resolve such an attack was $157. In contrast, system glitches cost $131 per record and human error or negligence is $128 per record. Companies in the United States and Canada spent the most to resolve a malicious or criminal attack

($258 and $213 per record, respectively).” Factors such as the size of the organization, the size and scope of the mission, the sensitivity of the data leaked, the amount of time the data is exposed before its properly mitigated, and the number of records are all factors in specifically determining the specific cost of a breach.

Mitigations

There are two general approaches to mitigating data breaches: prevention and cost reduction via mitigation. Optimally, a breach will be prevented before it happens. This requires standard information security practices hardening defenses and reducing the enterprise information attack surface. However, once a breach occurs, minimization, containment and recovery with minimal costs is the next best option for any organization as well as its patients/customers. These two approaches are detailed below:

Preventing Breaches

There are several methods of prevention when it comes to data breaches. First, IT security policies can help to prevent unauthorized access to systems, networks and most importantly, data. These include policies such as data loss prevention (DLP), password policies and an incident response plan. DLP applications identify, categorize and prioritize critical organizational data as well as protect data in motion, data at rest, and data at endpoints. This directly supports the overall purpose of a DLP plan which is to prevent end users from either deliberately or inadvertently disclosing sensitive data. Implementation includes; determining the critical components of an enterprise network, identifying single points of system and network failure, detailing roles and responsibilities for the team members, developing and maintaining a business continuity plan, detailing the tools, technologies, and physical resources to be utilized, maintaining a data recovery process, an internal and external communications plan, a staff training plan, and detailing both internal and external communications. Password policies are critical to ensure passwords have a minimal level of complexity, are periodically changed, and have limitations on their reuse, thus decreasing the possibility that a person or automated tool could predict them. Finally, an incident response plan provides guidance and instructions to detect, respond to, and recover from malicious activity on an enterprise information infrastructure. The detection component is critical to preventing or minimizing the effects of data breaches. Developing, maintaining, and enforcing IT security policies are one of the most important steps to preventing a data breach.

Beyond policy, there are a number of other efforts that serve to prevent data breaches. Data encryption is especially important in this regard. Encryption digitally restructures a file in such a way that only authorized parties can access it and those who are not authorized cannot, which can prevent data from being accessed even if it’s stolen. Employee training is also critical to protecting information. This should include threat awareness education and guidance for maintaining good habits when it comes to handling information. Monitoring of unintentional

mistakes via technology and processes is also recommended. Finally, monitoring should not be limited to employees and their actions. A full incident monitoring and response capability can go a long way in stopping threats at the perimeter of an enterprise information infrastructure or even after they have penetrated the network. This capability, when fully implemented, includes analysts and incident responders working on a 24x7x365 basis who support the full incident handling lifecycle (preparation, identification, containment/mitigation, eradication, recovery, Follow up).[17] Endpoint security – the protection of every system on an enterprise network with security software intended to identify, quarantine, and eradicate malicious software- is a significant component of any data breach prevention strategy.

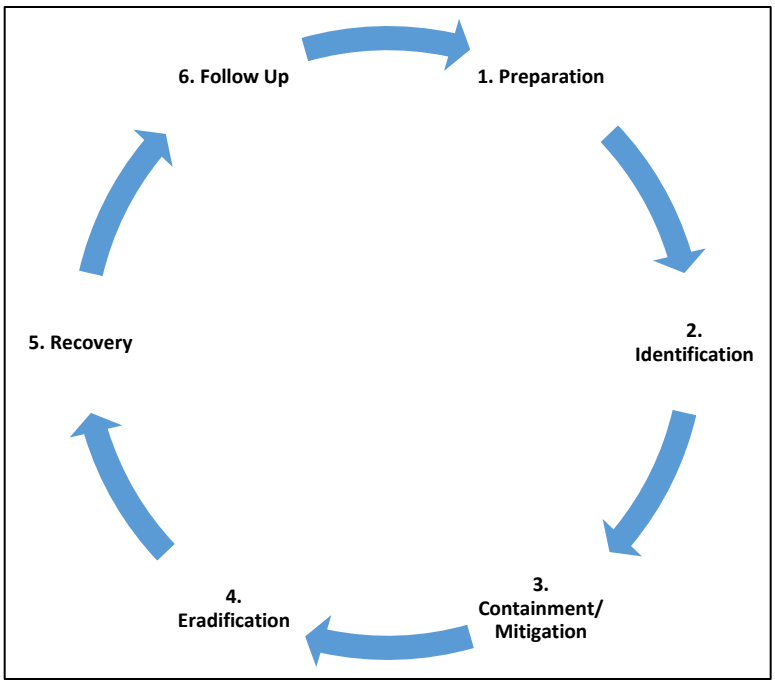

Figure 3: Incident Handling Lifecycle

Reducing costs

When attempting to minimize costs of potential data breaches, appropriate financial resources must be invested in information security programs. An incident response capability is an example of an investment that not only prevent a breach from occurring at all, but it also can save significant costs in the long run by minimizing the impact of a breach after it has happened. An incident response team can identify a breach as it is occurring and intervene to remove a threat actor's access to sensitive data. Which may improve the chances that any individual victims of a data breach can take immediate action to ensure their data isn't exploited. Encryption is a second step that can be taken which can prevent a breach from occurring, and also minimize the impact of a breach after it has happened. Data which is encrypted becomes obfuscated from any attacker who is seeking a target based on its value and it also becomes much more challenging for an attacker to sell or otherwise exploit after it's acquired. As the Ponemon Institute has noted,

> "Incident response teams and the extensive use of encryption reduce costs. In this year's research, an incident response (IR) team reduced the cost by as much as $14 per compromised record. Hence, companies with a strong IR capability could anticipate an adjusted cost of $134, down from $148 per record. Similarly, the extensive use of

encryption reduced cost by $13 per capita, for an adjusted average cost of $135, down from $148 per record."[18]

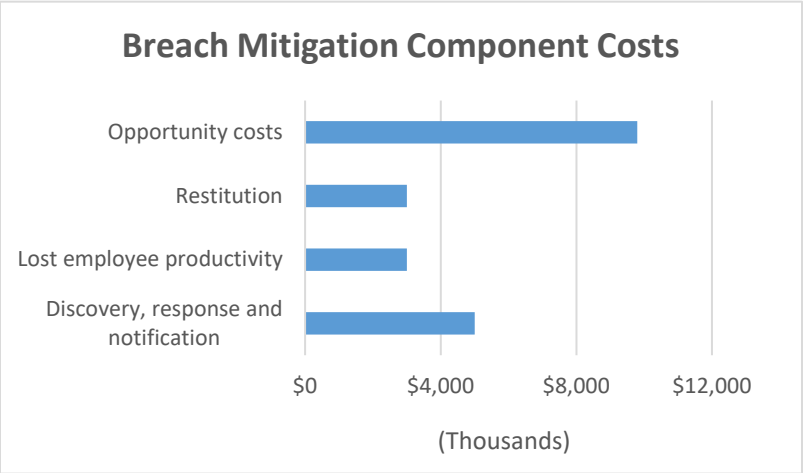

Figure 4: Breach mitigation costs based on Websense white paper and Forrester data, assuming organization suffering loss of 100,000 customer records

As the non-profit organization Cyber Threat Alliance has asserted, "Threat intelligence gathered from multiple sources, and then processed and correlated, is the most effective, valuable, and actionable."[19] Participating in a threat sharing program has also been shown to reduce the cost of a breach.[20] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency offers cyber intelligence products at https://www.us-cert.gov/ncas. The Healthcare Information Sharing and Analysis Center (H-ISAC) is another resource that can provide organizations in the healthcare industry with valuable cyber threat intelligence to prevent and minimize breaches. H-ISAC membership information can be found at: https://h-isac.org/membership-account/join-h-isac/.

Cyber insurance is also an option for reducing the costs of a breach over time. Premiums will add to operational costs, therefore it is critical that cyber insurance be fully integrated into an enterprise risk mitigation plan. Cyber insurance policies can be custom tailored to fit the needs of a specific healthcare organization, and can cover software and hardware damages as well as loss of business, costs associated with restoration of data, notification costs, and liability expenses.

Finally, employee training is a core component to any cybersecurity program but is especially applicable to preventing and reducing costs for healthcare breaches.[21] Employees play a critical role in mitigating against the effects of data breaches, and this has been noted as the top source of security incidents.[22] Employees who accessed personal patient files cost the Healthcare sector $6 million according to one study.[23] Employees should not just be reminded of the need to take organizational IT policy seriously, but an explanation as to why it's in place and what the potential consequences are if it's not followed are thoroughly important. Employees should have clearly defined responsibilities and understand the importance of protecting passwords, patching and updating all systems they use, and how to spot suspicious e-mails and other alerts.

Conclusion

Data breaches can be costly events for a healthcare organizations, due to response and recovery activities as well as business opportunity costs and the potential loss of patients. The average breached healthcare organization faces $8 million dollars in costs, or $400 per patient record. These costs are important to consider in the context of an organization's comprehensive risk management plan. In order to avoid operational and reputational impacts from breaches, organizations should consider implementing strong risk management practices to help prevent data breaches and minimize any disruptions or loss if a breach occurs. Options exist for both prevention and mitigation, and should be tailored to meet the mission of the specific organization. Adequate prevention and preparation for data breaches will protect patients, minimize direct and indirect costs, and allow for more efficient operations for a healthcare organization.

End Notes

[1] Snell, Elizabeth, Ensuring Security, Access to Protected Health Information (PHI), Health IT Security, https://healthitsecurity.com/features/ensuring-security-access-to-protected-health-information-phi
[2] Schaeffer, Juliann, PHI: Valuable and Vulnerable, For The Record, Vol. 28 No. 3 P. 18, https://www.fortherecordmag.com/archives/0316p18.shtml
[3] Yao, Mariya, Your Electronic Medical Records Could Be Worth $1000 To Hackers, Forbes, Apr 14, 2017, https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#7dccdd2d50cf
[4] 2018 Cyber Claims Study, NetDiligence, https://netdiligence.com/portfolio/cyber-claims-study/
[5] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[6] Ibid
[7] 2015 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ponemon.org/library/2015-cost-of-data-breach-global and 2017 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states
[8] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[9] Ibid.
[10] 2017 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states
[11] Lord, Nate, Top 10 Biggest Healthcare Data Breaches of All Time, Digital Guardian, June 25, 2018, https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time
[12] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[13] Ibid.
[14] Value in Healthcare, World Economic Forum, https://www.weforum.org/projects/value-in-healthcare and Munro, Dan Munro, U.S. Healthcare Hits $3 Trillion, Forbes, Jan 19, 2012, https://www.forbes.com/sites/danmunro/2012/01/19/u-s-healthcare-hits-3-trillion/#21f79b9d3da8
[15] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach (p. 25 has a relevant discussion on customer churn caused by a healthcare organization date breach)
[16] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[17] There are several similar incident handling lifecycle models used across industries, and the one recommended in this paper is based on the SANS Institute and is often utilized in the healthcare industry in particular (https://www.healthcareitnews.com/news/7-best-practices-successful-incident-response-plan), however a similar but alternative plan can be found here: https://www.cso.com.au/article/600455/six-stages-incident-response/
[18] 2019 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[19] https://www.cyberthreatalliance.org/value-collaborative-threat-intelligence-sharing/
[20] 2018 Cost of a Data Breach Stud: Global Overview, Ponemon Institute and IBM, https://www.ibm.com/security/data-breach
[21] Ibid.
[22] The Global State of Information Security Survey 2018, Price Waterhouse Coopers, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html
[23] 2018 Cyber Claims Study, NetDiligence, https://netdiligence.com/portfolio/cyber-claims-study/