Cybersecurity in Medical Private Practice: Results of a Survey in Audiology

Josiah Dykstra
Designer Security, LLC
Severn, Maryland 21144
Josiah@DesignerSecurity.com

Rohan Mathur
Designer Security, LLC
Severn, Maryland 21144

Alicia Spoor
Designer Audiology, LLC
Highland, Maryland 20777
Alicia.Spoor@DesignerAudiology.com

***Abstract*—Despite well-documented cyber threats to patients' protected health information (PHI), sparse evidence exists about the state of cybersecurity behavior of health care workers and medical private practices. There is evidence of insecure behavior in hospital settings, even though specific insights about private practice are still absent. In addition to mandatory standards for securing PHI, such as the Health Insurance Portability & Accountability Act (HIPAA), small business viability and their patients' security and privacy are critically dependent upon technology availability and reliability.**

In this survey of 131 clinical audiologists we show that many lack time, staff expertise, or funds to deploy adequate cybersecurity that prevents and mitigates threats to security and privacy. We find widespread deployment of HIPAA-compliant cybersecurity, including antivirus software and individual logins. Only 9.9% of participants reported at least one data breach in 2019, significantly less than the average for small businesses and health care providers, and only 24.4% reported having cyber insurance. Practice owners view patient data as well protected and unlikely victims for cyber attacks and breaches. These results have important implications for cybersecurity products and services, and to medical professionals who must acknowledge the acute importance of cybersecurity in securing protected health information and mitigating risks. Small business private practice health care providers who are particularly sensitive to the impacts of cyber attacks and must prioritize and adopt countermeasures that decrease the risks to patients and their own businesses.

I. Introduction

The delivery of modern health care is tightly and undisputedly intertwined with technology. Digital devices and electronic data introduce new challenges and opportunities to ensure that patients and medical institutions are viable in delivering health care outcomes with desired patient security and privacy. Despite cyber threats to patients' protected health information, sparse evidence exists about the state of cybersecurity behavior of health care workers and medical practices, especially in private practice.

Medical private practice is a particular type of small business with unique characteristics and needs. A private practice is a business setting that is independent of external ownership or control, such as by a parent company or hospital. The business may be owned and managed by one or more practitioners. Doctors may choose to work in private practice for the benefits of individual freedom and closer relationships with patients. At last count by the American Medical Association's Physician Practice Benchmark Surveys in 2016, 55.8% of physicians are working in practices wholly-owned by physicians [1]. This makes medical private practice a substantial and important population for which to understand specific needs for cybersecurity.

Private practice often intersects between two business sectors: small business and health care. Small business health care providers are equally vulnerable as other health settings but particularly sensitive to the impacts of cyber attacks. In addition to mandatory standards for securing protected health information (PHI), such as the Health Insurance Portability & Accountability Act (HIPAA), small business viability is critically dependent upon technology availability and reliability. With a single provider, the downtime from technology failure and attack means the business cannot provide care or bring income to sustain it. Technology and cybersecurity today require time, expertise, and funds to prevent and mitigate threats against people and business goals.

Audiology is a branch of science and medicine devoted to hearing, balance, and related disorders. Audiologists are medical professionals who are trained to diagnose, manage, and treat hearing or balance problems, and proactively prevent related damage. In 2019, the Bureau of Labor Statistics (BLS) reported 13,590 audiologists in the United States [2]. Audiologists, as with other medical specialists, practice in a variety of business settings. BLS reports that 27% of audiologists are employed by "Offices of physical, occupational and speech therapists, and audiologists" which includes private practice [3]. According to the American Speech-Language-Hearing Association, approximately 42% of private practice audiologists are self-employed [4]. Similarly, in a 2019 survey by the Academy of Doctors of Audiology, 8% of respondents reported being full-time private practice owners/partners, 8% as full-time private practice employees, and 1% as full-time private practice in a non-profit [5]. Among physicians, the American Medical Association also found that 40% worked in practice that were both small (10 or fewer physicians) and physician-owned [1].

Audiology, like other medical practices, is heavily reliant upon technology for business and health care delivery. At the forefront of hearing health care are digitally-enabled treatments, including high-tech hearing aids and cochlear implants, which are programmed and controlled with software,

978-1-7281-4146-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CIC50333.2020.00029

mostly on Microsoft Windows-based platforms. A key piece of equipment in evaluating hearing acuity is the audiometer, commonly computer based. Results and records are increasingly stored as electronic health records (EHR) in an online office management system (OMS) [6]. Patient appointments may be made online or by phone, and communications with patients or other medical professionals occur by email, text, phone, and fax. Providers use a mixture of business and personal mobile devices that include Android and iOS platforms. Billing and insurance reimbursement are routinely electronic. Without these technologies, the business is crippled and health care is diminished.

This study presents the findings of a survey of cybersecurity behavior in private practice settings, using audiology as the case study. The results offer two key contributions. First, they reveal real-world evidence of the adoption, spending, priorities, and technologies in use for cybersecurity in the practice. This behavior has pronounced implications for patient security and privacy. The results offer insights for better cybersecurity in all fields of medicine and specialty care. Second, the study serves as a baseline of cybersecurity today to measure change over time in the field, and against which to compare other branches of medicine.

The remainder of this paper is organized as follows. Section II presents relevant related work. Section III describes the methods of the study. In Section IV we present the results. Section V discusses the results and implications to cybersecurity and medicine. Finally, Section VI concludes the paper and offers some areas for future work.

II. Related Work

Previous studies have shown that data breaches are especially prevalent and damaging in health care. In a 2017 survey of health care executives, 47% reported a HIPAA-related security violation or breach in the past two years [7]. For the past ten years in a row, health care continues to incur the highest average breach costs ($7.13 million) and highest average time to identify and contain a breach (329 days) [8].

While research such as [9] has explored attitudes and challenges of cybersecurity and cybersecurity breaches in health care, less study is done about real-world behavior and solution adoption. Several studies have identified that individual clinicians view good cyber hygiene as interfering with the delivery of medical care, and some employ security workarounds [10], [11], [12]. In a 2018 meta-analysis of 472 English-language journal articles on cybersecurity and medicine, researchers found that that majority of the articles were focused on technology and not on *in situ* behavior [9]. This gap may be due to the operational or sensitive nature of health care settings and data.

One dissertation closely examined knowledge among audiologists in Ohio regarding HIPAA rules, regulations, and requirements [13]. Respondents included 66 licensed audiologists across all settings, including 12.1% in private practice. The findings revealed that participants possessed limited knowledge and understanding about HIPAA privacy and security regulations, and the majority were unable to correctly identify examples of PHI. Although the focus was on awareness and training rather measuring compliance or security implementation, these results could result in practitioners insufficiently prioritizing or implementing cybersecurity.

Hospitals and other large health institutions struggle with security and privacy [14], but they have comparatively greater resources than small medical clinics who lack the necessary cybersecurity expertise and attention despite similarly high risks. As far back as 2000, the average cost of HIPAA compliance per hospital ranged from about $670,000 to $3.7 million [15]. According to Gartner, health care providers today spend on average around 5% of IT budgets on security [16], trailing the mean of 16% across all industries [17]. The average annual spend on cybersecurity across all businesses with 1-9 employees is $13,000 [18].

There is sparse research about cybersecurity in small business beyond industry surveys on breaches. In 2019, the Ponemon Institute reported that 66% of small and medium-sized businesses experienced a cyber attack or data breach [19]. Hiscox found that 47% of small businesses had at least one cyber attack in the past year [18]. The 2018 Verizon Data Breach Investigations Report found that 58% of data breach victims were small businesses [20].

Time, knowledge, and financial cost are among the constraints to cybersecurity suggested in prior research of resource-limited populations [21]. Chen and Benusa offered recommendations for small business healthcare providers, most notably to understand regulatory requirements, followed by self-assessment and risk analysis [22]. Beautement, Sasse, and Wonham proposed a Compliance Budget to reason about actual and anticipated costs and benefits of compliance to individual employees and to the organization [23]. In their interviews, participants highlighted that lost time was directly detrimental to business. Many other variables contribute to constraints on cybersecurity behavior, including decision and alert fatigue studied in the usable security community [24].

III. Methods

A 24-item, multiple-choice and short-answer questionnaire (Appendix A) was developed and pretested with a trial group of three audiology practices. The questionnaire was advertised by email to all 936 American audiology members of the Academy of Doctors of Audiology (ADA) on June 24, 2020. Participation was voluntary, and no compensation was offered to participants. Anonymity was maintained for all participants and individual responses. The content of responses covered business and cybersecurity practices in the workplace. Unanswered questions were not included in the analysis.

Data recorded in the survey included practice demographics: state, number of providers, years of practice, revenue, IT and security spending. Technology adoption was measured by the number of desktop computers, laptops, tablets, smartphones, wired telephones, and security products such as antivirus. Practice-wide security was determined by asking about certain procedures, such as individual logins and security training.

Participants were asked about their individual password practices, including the length of their work email password and number of times the password was changed in 2019. Past and future breach information was obtained by asking for the number of times the practice was hacked or the victim of a data breach within the past 12 months and the likelihood of a hack or data breach in the next 12 months. Respondents were asked to identify barriers to security, and to select how they would use $1,000 to address one cybersecurity project.

IV. Results

A total of 131 respondents completed the survey. Respondents came from practices across 37 states. A total of 79.7% (104/131) were private practice owners. The median number of hearing health care providers in each practice was two, and 65.9% (87/131) of practices had been providing patient care for more than 11 years. The median number of desktop computers reported was four and the median number of laptop computers was two. The median number of tablet computers reported was zero.

A total of 79 respondents (60.3%) reported 2019 gross practice income less than $1 million. Overall, 42.9% (55/128) spent $1,000 to $9,999 on all IT equipment including contracted technical support. Another 38.3% (49/128) spent more than $10,000. As a subset of IT spending, nearly half (60/132, 45.5%) spent less than $500 on security.

Respondents were asked "Which of the following practices are implemented in your business?" for nine common implementations of HIPAA technical controls that aid in securing PHI. Results are shown in Figure 1. For password behavior, respondents changed their passwords on average two times in 2019. The average length of users' work email password was 11 characters.

More than 90% (120/130) reported zero instances of cyber attack or data breach within the past 12 months. Most respondents reported the likelihood that their practice will be the victim of a cyber attack or data breach in the next 12 months as not at all likely (40 [31%] of 130) or slightly likely (33 [25%] of 130). When asked to rate their overall protection, 44% (58/131) responded good or very good.

V. Discussion

This study showed a range of cybersecurity adoption and behavior among private practices in protecting patients' health information. In this section, we discuss key themes from the results and implications for health care and cybersecurity.

Indications of HIPAA compliance. Respondents reported behavior and technology implementations that are moderately compliant with HIPAA-required and best practice cybersecurity measures. Most of the items measured are explicitly or implicitly required by the HIPAA Security Rule, including unique user logins which were reported for 83.2% (109/131) of respondents [25]. Only 32.8% (43/131) reported data encryption on all devices, which is also mandated by HIPAA. Other deployments, such as secure WiFi, are not explicitly required but are commonly implemented as technical safeguards.

Because prior research has found knowledge lacking about HIPAA, we hypothesize that practitioners may not associate their active security measures with a specific HIPAA requirement. If they do understand HIPAA, they may need help determining how to implement it in practice. Technical expertise may be required, for example, to "implement a mechanism to encrypt and decrypt electronic protected health information," even if encryption is available in the operating system [26].

Password Behavior. Respondents reported password behavior exceeding minimum recommendations. For instance, respondents' average password length was 11 characters, while the National Institute of Standards and Technology (NIST) recommends a minimum of eight characters, and research studies find an average password length between 8 and 10 characters [27]. We observed that 16 users (12%) changed their password four times, which could indicate common but outdated business policies to change passwords every 90 days. In 2017, NIST updated their guidance and no longer recommends changing passwords at regular intervals [28]. The HIPAA Security Rule is not prescriptive about password length or frequency of changes, although longer passwords are more secure against malicious password guessing. Regardless, compliance is an insufficient measure of cybersecurity [29].

The survey did not explore other relevant aspects of password behavior, including password sharing, password reuse, or workstation locking. Strong passwords, if used routinely, could suggest the opportunity for more usable authentication alternatives in order to decrease the time and effort of users. The medical community may be unaware of HIPAA-compliant alternatives to passwords such as biometrics.

Cybersecurity resource allocation. Spending on countermeasures appears misaligned with risks to patient PHI and less than industry averages. This study showed that 79.8% of respondents cited "Not enough expertise" as a reason preventing better cybersecurity. At the same time, 45% spent less than $500 including contracted support in 2019 (Figure 2). The difference is particularly striking in offices with one provider. Of the 33 single-provider offices spending less than $500, only 12 (36.3%) cited "not enough money" as a limitation to better security. Rough estimates suggest costs well exceeding $500 annually for basic security such as antivirus subscriptions and managed software updates. Software updates and upgrades are recognized as the top mitigation to manage cybersecurity risk [30]. Each doctor, patient, and computer in the workplace, furthermore, contributes to raising the level of risk and security spending should scale likewise. For example, every device storing or accessing PHI must be continually maintained and defended. Linear spending was not observed.

Those spending more than $500 showed higher adoption of cybersecurity in all areas measured (Table I). They were significantly more likely to have written password policies and cyber insurance. Many of the behaviors require low fixed cost (e.g. creating a password policy) or negligible direct cost (e.g. individual computer accounts). Although $500 was used as a differentiator for behavior in this study, it is not necessarily the

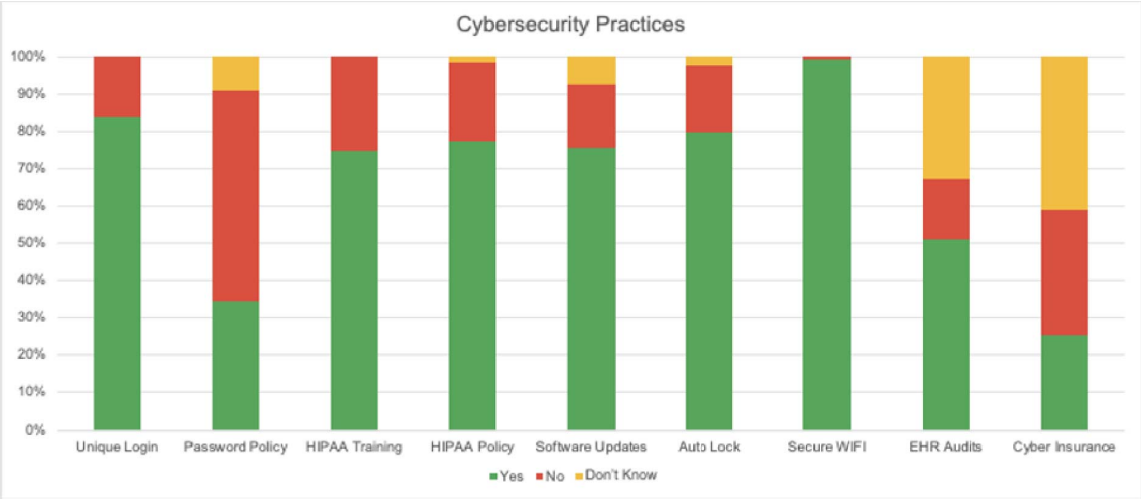

Fig. 1. Responses across all participants as to whether or not their private practice implements various cybersecurity practices.

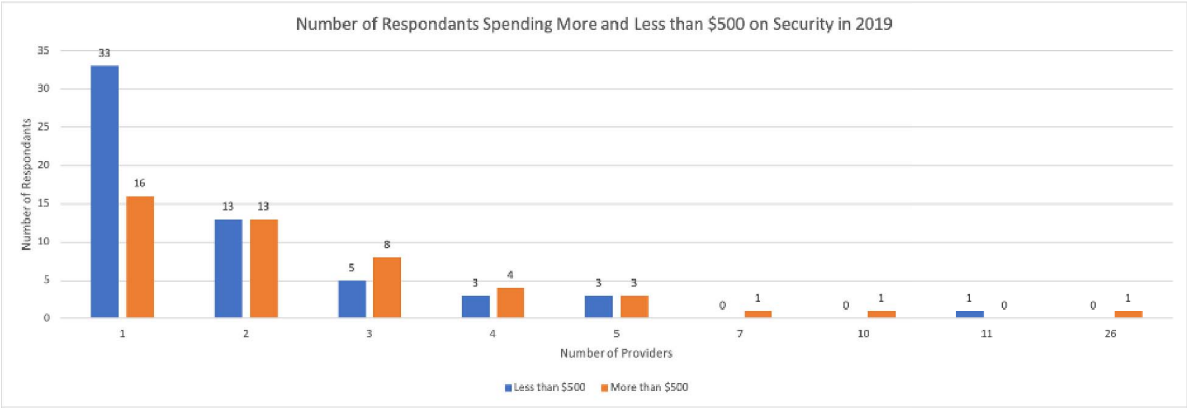

Fig. 2. Number of respondents who spent more and less than $500 on security in 2019 by number of providers.

precise amount necessary for strong and compliant security.

Perceived cybersecurity preparedness and risk. This study suggests that clinicians have an inaccurate understanding of their cybersecurity preparedness and risk. Our finding that 9.2% of respondents were the victim of a cyber attack or data breach in 2019 is significantly inconsistent with other research showing 66% of small businesses reporting an attack in the past 12 months [19]. The overwhelming majority of physicians have similarly experienced a cyber attack [31]. Therefore, it appears that respondent practices are better protected than average or unaware of attacks. Respondents overwhelmingly assessed low risk for future incidents and data breaches. Even so, 54 (43.5%) selected risk assessment as their desire if they had $1,000 to address one cybersecurity project (Question 22).

When asked to identify limitations preventing better cybersecurity, the top three responses were: expertise (79.8%), money (24.0%), and time (22.1%). In response to Question 15, those who performed security-related tasks included the practice owner (62.9%), contracted technical support (50.0%), employees (26.5%), and others such as a spouse (12.1%). We were surprised that expertise was the greatest limitation, given the availability of cybersecurity professionals who provide such services and consultation. This implies that providers might prefer to conduct cybersecurity tasks internally, or have insufficient understanding of the risks. Research supports this "flashlight in a dark room" theory, where limited knowledge illuminates only a narrow scope of the problem in a dark room of cyber risk, resulting in unknown yet accepted risk exposure [32]. Education about threats and mitigations and usable security may help overcome the limitation of expertise.

Those in the cybersecurity research and development communities should be cognizant, sensitive, and transparent about the time, money, and expertise required for users in health care. The availability of automated and hands-off security mechanisms, such as automatic software updates, may be of particular benefit to resource-constrained small medical businesses. Further study is needed to evaluate usability, and where appropriate automation or deliberate friction may improve health and security outcomes.

	Spent <$500 on security (n=59)	Spent ≥$500 on security (n=49)	P Value
Employees receive routine HIPAA security training	39/59 (66.1%)	40/49 (81.6%)	<0.001
The practice has a written HIPAA security policy	44/59 (74.6%)	42/49 (85.7%)	<0.001
The practice has a written password policy	17/59 (28.8%)	26/49 (53.1%)	<0.001
The practice has cyber insurance	10/59 (16.9%)	19/49 (38.8%)	<0.001
Software updates and patches (e.g. Windows updates) are applied automatically or within 30 days of release	42/59 (71.2%)	42/49 (85.7%)	<0.001
Work computers automatically timeout or logoff after a period of inactivity	43/59 (72.9%)	43/49 (87.8%)	<0.001
Each employee uses their own unique login and password for computers in the office	46/59 (78.0%)	43/49 (87.8%)	<0.001

TABLE I
CYBERSECURITY BEHAVIOR OF RESPONDENTS WHO SPENT LESS THAN $500 ON SECURITY IN 2019 AND THOSE WHO SPENT MORE THAN $500

VI. CONCLUSIONS AND FUTURE WORK

Patient-centered care is a hallmark of modern medical practice, which means that medical care is respectful of, and responsive to, patient preferences, needs and values, and ensuring that patient values guide all clinical decisions [33]. This is proven to produce better outcomes than without it [34]. The principle of human-centered or human-driven cybersecurity, however, is still emerging. The cybersecurity community must continue advances and partnerships in technical and non-technical risk mitigations that respect the primary goals of private practice providers and the cybersecurity challenges highlighted in this study.

One of the greatest opportunities to aid the private practice community with better cybersecurity protection is individualized risk assessments. Respondents in this survey explicitly desired that service, and it is a necessary prerequisite to selecting or deploying any appropriate cybersecurity solutions. Private practice risk assessment demands respect for, and responsiveness to, business preferences in addition to knowledge of medical-specific needs and regulations.

There were several limitations of the study. Our survey did not seek to evaluate participants' mental models, which could help explain some behavior. Next, because the survey considered the number of providers as a metric of business size, it was not possible to assess whether the total number of employees influenced cybersecurity policies and behavior. Also, while this study is not representative of all audiologists or the entire U.S. health care system, we have no reason to believe that the trends we observed would be significantly different in other private practice settings. Cross-sectional studies across medicine are needed for validation, and longitudinal studies are necessary to measure change in cybersecurity posture over time.

This study shows that audiology private practices lack cybersecurity expertise and devote insufficient resources to defenses commensurate with potential risks and magnitude of harm. Proper defenses can help prevent, detect, and mitigate cyber attacks against sensitive patient and business data and the technology underpinning the clinic. All medical professionals must acknowledge the acute importance of cybersecurity in protecting patient information, and devote resources to mitigating risks. Private practice clinics in particular exhibit the constraints of small business and burden of compliant security and privacy for sensitive health information.

ACKNOWLEDGMENTS

The study team would like to thank the Academy of Doctors of Audiology for their support with data collection. We thank the anonymous reviewers for their constructive comments which helped to improve the manuscript.

REFERENCES

[1] C. Kane, "Updated data on physician practice arrangements: For the first time, fewer physicians are owners than employees," May 2019. [Online]. Available: https://www.ama-assn.org/system/files/2019-07/prp-fewer-owners-benchmark-survey-2018.pdf

[2] U.S. Bureau of Labor Statistics, "Occupational employment and wages, may 2019: 29-1181 audiologists," July 2020. [Online]. Available: https://www.bls.gov/oes/current/oes291181.htm

[3] ——, "Occupational outlook handbook, audiologists," Sept. 2020. [Online]. Available: https://www.bls.gov/ooh/healthcare/audiologists.htm#tab-3

[4] American Speech-Language-Hearing Association, "ASHA 2018 Audiology Survey: Private Practice," Mar. 2019. [Online]. Available: https://www.asha.org/uploadedFiles/2018-Audiology-Survey-Private-Practice.pdf

[5] American Academy of Audiology, "Compensation and benefits survey," 2019.

[6] L. B. K. Hill, "Go paperless! Bridging the gap between audiology and electronic medical records," Mar. 2019. [Online]. Available: https://www.audiologyonline.com/articles/go-paperless-bridging-gap-between-24426

[7] KPMG. (2019) The health approach to cyber security. [Online]. Available: https://institutes.kpmg.us/content/dam/institutes/en/healthcare-life-sciences/pdfs/2017/cyber-report-healthcare.pdf

[8] IBM Security. (2020) Cost of a data breach report 2020. [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

[9] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J. Med. Internet Res.*, vol. 20, no. 5, p. e10059, May 2018. [Online]. Available: https://doi.org/10.2196/10059

[10] M. P. Jarrett, "Cybersecurity—a serious patient care concern," *JAMA*, vol. 318, no. 14, pp. 1319–1320, 2017.

[11] R. Heckle, "Security dilemma: Healthcare clinicians at work," *IEEE Security & Privacy*, vol. 9, no. 6, pp. 14–19, 2011.

[12] R. Stobert, D. Barrera, V. Homier, and D. Kollek, "Understanding cybersecurity practices in emergency departments," in *Proc. 2020 CHI Conf. on Human Factors in Computing Systems*, ser. CHI '20, Oahu, Hawai'i, 2020.

[13] A. C. Antalovich, "Privacy and Security in the Clinical Audiology Setting: Ohio Audiologists' Knowledge of the Health Insurance Portability and Accountability Act," dissertation, Ohio State University, 2016.
[14] S. Uwizeyemungu, P. Poba-Nzaou, and M. Cantinotti, "European Hospitals' Transition Toward Fully Electronic-Based Systems: Do Information Technology Security and Privacy Practices Follow?" *JMIR Med. Inform.*, vol. 7, no. 1, p. e11211, Mar. 2019.
[15] P. Kilbridge, "The Cost of HIPAA Compliance," *The New England Journal of Medicine*, vol. 348, no. 15, pp. 1423–4, Apr. 10 2003. [Online]. Available: https://www.proquest.com/docview/223931939?accountid=14696
[16] L. Schencker, "Hospitals' spending lags on digital security," Mar. 2011. [Online]. Available: https://www.courier-tribune.com/news/20190311/hospitals8217-spending-lags-on-digital-security
[17] IDG Communications, Inc., "2020 State of the CIO," Jan. 2020. [Online]. Available: https://resources.idg.com/download/2020-state-of-the-cio-rl
[18] Hiscox Ltd., "Hiscox cyber readiness report 2020," June 2020. [Online]. Available: https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf
[19] Ponemon Institute. (2019) 2019 global state of cybersecurity in small and medium-sized businesses. [Online]. Available: https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf
[20] S. Widup, M. Spitler, D. Hylender, and G. Bassett, "2018 Verizon Data Breach Investigations Report," 2018.
[21] A. Demjaha, S. Parkin, and D. Pym, "You've left me no choices: Security economics to inform behaviour intervention support in organizations," in *Proc. 9th Int. Workshop on Socio-Technical Aspects in Security 2019*, ser. STAST 2019. Springer, 2019.
[22] J. Q. Chen and A. Benusa, "HIPAA security compliance challenges: The case for small healthcare providers," *Int. J. of Healthcare Management*, vol. 10, no. 2, pp. 135–146, 2017.
[23] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proc. 2008 New Security Paradigms Workshop*, 2008, pp. 47–58.
[24] B. Stanton, M. F. Theofanos, S. Prettyman, and S. Furman, "Security fatigue," *IT Professional*, vol. 18, no. 05, pp. 26–32, Sept. 2016.
[25] HIPAA Security Rule, "45 CFR § 164.312(a)(2)(iv)," 2011.
[26] HIPAA Technical Safeguards: Encryption and Decryption, "45 CFR 160, 164, subparts A and C," 2011.
[27] S. Pearman, J. Thomas, P. E. Naeini, H. Habib, L. Bauer, N. Christin, L. F. Cranor, S. Egelman, and A. Forget, "Let's go in for a closer look: Observing passwords in their natural habitat," in *Proc. 2017 ACM SIGSAC Conf. on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 295–310. [Online]. Available: https://doi.org/10.1145/3133956.3133973
[28] P. Grassi, E. Newton, J. Fenton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y.-Y. Choong, and M. T. Kristen Greene, "NIST Special Publication 800-63B," June 2017. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html
[29] R. Stevens, J. Dykstra, W. K. Everette, J. Chapman, G. Bladow, A. Farmer, K. Halliday, and M. L. Mazurek, "Compliance cautions: Investigating security issues associated with us digital-security standards," in *Proc. Network and Distributed System Security Symposium*, ser. NDSS, San Diego, CA, Feb. 2020.
[30] National Security Agency, "NSA's Top Ten Cybersecurity Mitigation Strategies," Mar. 2018. [Online]. Available: https://media.defense.gov/2019/Jul/16/2002158046/-1/-1/0/CSI-NSAS-TOP10-CYBERSECURITY-MITIGATION-STRATEGIES.PDF
[31] T. Burki, "The dangers of the digital age," *The Lancet Digital Health*, vol. 1, no. 2, pp. E61–E62, June 2019.
[32] G. Auger, "Flashlight in a dark room: A grounded theory study on information security management at small healthcare provider organizations," dissertation, Dakota State University, 2019.
[33] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: The National Academies Press, 2001. [Online]. Available: https://www.nap.edu/catalog/10027/crossing-the-quality-chasm-a-new-health-system-for-the
[34] M. Stewart, J. Brown, A. Donner, I. McWhinney, J. Oates, W. Weston, and J. Jordan, "The Impact of Patient-Centered Care on Outcomes," *The J. of Family Practice*, vol. 49, pp. 796–804, Oct. 2000.

APPENDIX A

Q1. Which one of the following best describes your involvement in a private practice?

- Private practice owner
- Employee in a private practice owned by an audiologist
- Employee in a private practice owned by non-audiologists (e.g., physicians, manufacturers, commercial entities)

Q2. What state is your practice located?

Q3. How many licensed hearing healthcare providers work in your practice (including all locations)?

Q4. How many years has your practice been providing patient care?

- 0-3
- 4-5
- 6-10
- 11+

Q5. What was the gross revenue for your practice in 2019?

- Less than $149,999
- $150,000 to $349,999
- $350,000 to $499,999
- $500,000 to $999,999
- $1,000,000+
- Don't Know

Q6. How much did your practice spend on all equipment (e.g. computers, audiometers, etc.), software (e.g. antivirus, Microsoft Office, etc.), online services (e.g. email, EMR/EHR/OMS, etc.), phones, and contracted technical support in 2019?

- Less than $999
- $1,000 to $9,999
- $10,000 to $49,999
- $50,000 to $99,999
- $100,000+
- Don't know

Q7. What subset of the spending in Question 5 did your practice spend on security in 2019, including software (e.g. antivirus, backup services such as Carbonite) and hardware (e.g. video cameras, firewall)?

- Less than $99
- $100 to $499
- $500 to $999
- $1,000 to $4,999
- $5,000 to $9,999
- $10,000+
- Don't know

Q8. How many LAPTOP computers are used for work-related services?

Q9. How many TABLETS are used for work-related services?

Q10. How many DESKTOP computers are used for work-related services?

Q11. How many SMARTPHONES are used for work-related services?

Q12. How many WIRED TELEPHONES are used for work-related services?

Q13. Which of the following are utilized in your practice? (All devices, Some devices, No Devices, Don't know)

- Anti-virus
- Firewall
- Backup to cloud
- Data encryption (does not include login passwords)
- Owner-reviewed software for monitoring employee online activity

Q14. Which of the following practices are implemented in your business? (Yes, No, Don't know)

- Each employee uses their own unique login and password for computers in the office
- The practice has a written password policy
- Employees receive routine HIPAA security training
- The practice has a written HIPAA Security Policy
- Software updates and patches (e.g. Windows updates) are applied automatically or within 30 days of release
- Work computers automatically timeout or logoff after a period of inactivity
- Password-protected wifi
- Audit trails are kept for access and changes to ePHI records in EMR/EHR/OMS
- The practice has cyber insurance

Q15. Who performs security-related tasks, such as installing software updates? (check all that apply)

- Owner
- Employee
- Contracted technical support
- Other (e.g. spouse)

Q16. In the year 2019, how many times did you change the password to your work email?

Q17. How many characters is your current work email password (e.g. ResoluteChild5 is 14 characters)?

Q18. How many times was your practice hacked or the victim of a data breach within the past 12 months?

- 0
- 1-4
- 5-9
- 10+

Q19. What is the likelihood that your practice will be hacked or be the victim of a data breach in the next 12 months?

- Extremely likely
- Very likely
- Moderately likely
- Slightly likely
- Not at all likely
- Don't know

Q20. In your opinion, how would you rate your protection against data breaches and hacking?

Q21. If not Excellent in Question 20, what limitations are preventing better protection? (Select all that apply)

- Not enough time

- Not enough money
- Not enough expertise
- Not enough access or permissions
- Other

Q22. Imagine that you had $1,000 to address one cybersecurity project. On which of the following would you use it?

- Secure Email
- HIPAA Training
- Policies and Procedures
- Risk Assessment
- Patch/Update Computers
- Data Backups
- Other

Q23. Is there anything else you'd like to tell us about cybersecurity in your practice?

Q24. We would like to follow-up by phone with a small number of people to ask a few additional questions. If you are willing to talk with us for 30 minutes in the next few weeks, please provide a contact name and phone number.