sciendo

Scientific Bulletin
Vol. XXVII, No. 1(53), 2022

INTERSECTIONS OF TELEMEDICINE / TELEHEALTH AND CYBERSECURITY: THE AGE OF RESILIENCE AND COVID-19

Kim L. BROWN-JACKSON
kLbrownjackson13@gmail.com

CAPITOL TECHNOLOGY UNIVERSITY, GREATER WASHINGTON, D.C.

ABSTRACT:

The telemedicine and telehealth industry regenerates to fast-track the COVID-19 pandemic. Preliminary 2020 data suggests a 2,532 % surge in healthcare aid provided equated to the 2019 March through June timeframe. While telemedicine technology offers a variety of benefits, it is vulnerable to cyber threats. Countrywide stay-put mandates swiftly intensified telemedicine/telehealth from an auspicious novelty to becoming fundamental precedence. The industry is consistently besieged by a deluge of convalescents, restrained supplies, allotting, and additional encounters because of COVID-19. Cybersecurity leaders and healthcare establishments had to promptly change their IT resources, timetables, and work ranges to leverage prevailing technologies and propel healthcare providers and convalescents, adapted to the novel healthcare delivery services and enhanced changes. Telehealth, an integral part of delivering convalescent care, has multiplied healthcare offerors' digital traces and cybersecurity hacks, as evidenced through endpoint security and the amplification of conclusions per telemedicine/telehealth sphere. COVID-19 reveals the junctions of cybersecurity and telehealth as a worst-case scenario for modernistic interpretations regarding healthcares' cybersecurity guidance. The findings of this research provides awareness to understand if leaders at all levels aid in preventing cyber-attacks, thwarting ransom attacks, and indicating that healthcare organizations must adopt a cyber resilience plan.

KEYWORDS:

Cybersecurity resilience, leadership, telemedicine, telehealth, COVID-19 pandemic

1. Introduction

The telemedicine and telehealth industry continues to expand and accelerate in the current pandemic. Healthcare's expected revenue of $3.5 billion by 2022 might exceed these projections when combining both telemedicine and the burgeoning use of telehealth (Brown-Jackson, 2017). Camlek (2020) project a seven-fold telehealth advance by 2025.

DOI: 10.2478/bsaft-2022-0001
© 2017. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

The data shows that the COVID-19 pandemic exposed the urgent necessity regarding investment into community-health infrastructure, to better watch and attend to imminent public-health threats, and to increase insurance coverage and health care access (Bailey, 2021; De Salvo et al., 2019; Maani & Galea, 2020; Schuchat, 2020). Telemedicine provides various advantages, yet, it is susceptible to cybersecurity menaces akin to information technology (IT) services (Sykes, 2019). Stay-put requirements all across the country intensified telemedicine/telehealth to an indispensable precedence (Zielinski & Marino, 2020). New numbers from CMS offered data showing 34.5 million telehealth services were provided 2020 from March to June (Jercich, 2020a). Initial data from CMS proposed a 2,532 % surge in services contrasted with 2019 March to June (Jercich, 2020b). FAIR Health research indicates a 4,347 % increase in overall telehealth payment requests to insurers in the private space, 2019-2020 (FAIR Health, 2021). The CMS projected right at 13,000 telemedicine/telehealth weekly appointments prior to COVID-19 and minimally 10 million total, which is around 625,000 per week from early March through mid-August (Verma, 2020). The question is why is this important? Security challenges are persistent and lasting as organizations implement a hybrid work strategy to support apportioned labor force giving rise to complex amplified risk for protected health information (PHI) (Douglas & Thomas, 2020; Morris-Reade, 2021).

Healthcare organizations should continue to focus on cyber resilience. Notwithstanding new risks from telehealth vendors, the healthcare industry enhanced its security posture by elevating to the ninth position in eight reviewed industries (up from 10th in 2019) (PR Wire, 2020). The increase of telemedicine/telehealth sphere findings and elements such as end-to-end security relegate provider data and patient information at risk (Drees, 2020).

Healthcare continues to endure damages from cyber menaces. The average cost is $7 million for each breach over and above par of the worldwide average (Zorabedian, 2020). The data shows that cybercriminals are continuing to penetrate healthcare systems, and these organizations are not maintaining cybersecurity resilience strategies (Collier et al., 2020; Davis, 2021; Perlroth & Satariano, 2021). Cybersecurity breaches have abrupt consequences for healthcare offerors and are frequently besieged with ransomware attacks. Significant to know is that healthcare providers focus on cyber security attackers and possess valuable mines of PHI. Their volume and magnitude have frequently rendered them slow to adapt to securing health care data.

Currently, all 50 states have broad and restrictive data infringement notification laws (Garrison & Hamilton, 2019). The year 2003, the initial proposed federal data infringement law was recommended to Congress; however, the recommendation failed to leave the Judiciary Committee (Garrison & Hamilton, 2019). Concerning is that there is not a federal law on data infringement notifications. Needed is the comprehension of cyber resiliency. Cyber resilience is the ability to continuously supply the envisioned result regardless of the adverse cybersecurity actions (Accenture Federal Services, 2018). Note that cyber resiliency is not a substitute for cybersecurity, but is a great companion.

2. Method and design

This cybersecurity/telemedicine/telehealth article, is written with a qualitative method and literature review design.

Academic fee-based databases, the internet, and interviews with experts were used to retrieve literature. The literature review will thoroughly appraise the data gathered by detecting gaps in present understanding and evaluating areas of debate. In addition, this literature review will provide the literature in an organized manner.

Academic fee-based databases included as Academic Search Premier (EBSCO), Business Source Premier (EBSCO), Ebook Collection (EBSCO), (EBSCO), and First Research, MEDLINE, PubMed, Science Citation Index, Embase, ProQuest Dissertation Database, ABI Inform Complete (ProQuest). Association fee-based database included American Telemedicine Association (ATA). Other internet search engine included Agency for HealthCare Research and Quality (AHRQ), Healthcare.gov, Department of Health and Human Services (telehealth, rural health), Telehealth Resource Centers.org, Google Scholar, Health Services/Technology Assessment Texts (HSTAT) databases (US National Library of Medicine, National Institutes of Health (NIH), and MedlinePlus to retrieve peer-reviewed literature. This article assesses the literature and blend data from the literature into a brief accounting, specifically cybersecurity resilience and cybersecurity leadership, crossroads with telemedicine of the main points of leadership. The key data are established from numerous databases. This research method supported this researcher's confidence regarding the initiation of the information examined and the exactness of the documents.

3. Connecting healthcare security and resilience in a Cyber World

What is resilience in the cybersecurity and COVID-19 pandemic sphere? The USA's healthcare sphere is wrestling with a stretched work capacity and progressing digital technology worries and fears (Masood & Egger, 2020). The breakdown of organizations to provide and propose adequate IT security controls as a critical foundation advances to advanced persistent threats (APT) and have the propencity to lead to organization debilitation (Dawson et al., 2021). A intense knowledge of IT security is salient for cybersecurity leaders. Liken to the Presidential Policy Directive 21(PPD-21) Critical Infrastructure Security and Resilience, cybersecurity trailblazers' objectives must wrap to diminishing vulnerabilities, recognizing and disordering threats, curtailing effects and accelerating response and recovery labors linked to critical infrastructure (Holt et al., 2015; Obama, 2013). One need is to review how artificial intelligence (AI) and augmented reality (AR) serve as technological companions bracing patient care security and monitoring, scrutinizing influences on people and inclusive healthcare organizations, plus tackling the manner in that augmented command of AI and AR might direct healthcare leaders' at all levels decisions and further the total patient encounter (Burton, 2021).

This article adopts the concept of organizational resilience and its relationship to the logical dialogue of ideas and opinions analyses to examine the adoption of telemedicine and telehealth innovations to include changes needed for the COVID-19 pandemic. Data shows that resilience denotes the capability of diverse people, groups, or organizations to acclimatize rapidly to alterations in their surroundings (Burton, 2019; Cho, 2007; Horne et al., 2011; Mallak 1999). Let's break down the categories of resilience.

3.1. Interpreting cyber resilience for telemedicine and telehealth

Telemedicine and telehealth technology usage is increasing exponentially to enhance access to healthcare in remote, rural, and underserved locations, thus spreading specialize healthcare (Brown-Jackson, 2017; Taylor & Burton, 2018). Telehealth continues to increase healthcare providers' anytime and anyplace footprint. Telehealth, the delivery of clinical care, continues to lessen the uneconomical application of health care resources, enhance access to the best accessible patient care resources, and diminish inconsistency about standards of care (ATA, 2012a; IOM, 2012). Technologically, the move to disruptive telehealth innovation, is a

concerted effort to amplify the power of technology novelties and improvements (Brown-Jackson, 2017; Grady, 2014; Kirkner, 2010). This disruptiveness references the change and the exodus from the customary patient – medical provider face-to-face relationship (Grady, 2014; Kirkner, 2010).

Telemedicine allows health professionals to deliver treatment to patients remotely, which is particularly beneficial in rural areas, where individuals are distanced from healthcare facilities (ATA, 2021). This technology has the capability to withstand challenges both in developed, and developing countries. Yet, vulnerabilities are inherent in the technological platform, with telemedicine exposed to external attacks, mainly cyberattacks.

Interaction and digital exchanges through video chat mobile applications are susceptible to cyber threats, whether listening or theft of non-secured information networks. What makes telehealth and telemedicine systems to cybersecurity hack is the movement of data across networks and the combination of numerous networks and technologies. Patients can access data from their devices to see personally identifiable information (PII) and PHI, however, their devices may or may not have sound security protection. This type of data is sold on the black market and command extraordinary prices. Keep in mind the healthcare facilities must keep data protected even at the approximate costs of installing an electronic healthcare record system are $15,000.00 to $70,000.00 per provider (HealthIT.gov, 2014) with an average multi-physician practice cost of $162,000. Needed by all organizations is cyber resilience.

Diverse definitions for resilience and resiliency are used by different communities of interest – National Security (WH, 2010), critical infrastructure (NIAC, 2010), critical infrastructure security and resilience (Obama, 2013), DoD cybersecurity (DoD, 2014), network engineering (Sterbenz, 2006), resilience engineering (Madni, 2009), and Homeland Security (Risk, 2010). Cyber resiliency (also referred to as cyber resilience) definition of the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources is uniform with the given topics. What is known is the term cyber resilience is not an alternative name for cybersecurity. Cybersecurity centers on realizing the security aims of concealment, truthfulness, and convenience to suitable levels, commonly by applying an alalgamation of boundary defenses and internal controls (IDR; Dawson et al., 2021; Martin et al., 2017; Muller, 2020). Juxatapose, the aims of cyber resiliency – forestall, endure, recuperate, and progress – are resultant of the control of resilience engineering. Cyber resiliency goals are principally applicable as related to missions in the setting of their reliance on cybermeans.

3.2. Impacts of COVID-19 pandemic and connectedness to resiliency

Comprehension is that the world cannot return to pre-COVID-19 pandemic business as usual behaviors (United Nations Educational Scientific Organization (UNESCO), 2020a). Seventy-five percent of experts were optimistic about the long-term effects of COVID-19 on their business models (Research 2 Guidance, 2021). The insights elucidate that more than 77 % of experts are more painfully aware of the pandemic's impacts regarding sustained long-lasting changes compared to their initial beliefs in 2020 (67 %) (Research 2 Guidance, 2021). The growing usage of digital tools for telemedicine, remote patient monitoring, and self-management will be expected to progress, even as the world recovers from the devasting pandemic (2021 Global COVID-19 Survey, 2021). Unmet data management necessitates demonstrating how data was and continues to be organized during the onslaught of the

COVID-19 pandemic. The data shows that telehealth vendors' rapid adoption and onboarding leave providers and patient data at risk (Security Scorecard, 2020).

Virtual first care, digital healthcare in practice, can offer massive improved clinical and health economic outcomes, access to an improved overall patient experience (ATA, 2021; Digital Medicine Society, 2021) through adopting a cybersecurity framework that delivers a structure, practice, and procedure for protecting critical digital assets (Syafrizal et al., 2020). The probable implications of virtual first care wrapped in cybersecurity are adding a methodology, layer of protection, and strategy that entrenched healthcare delivery systems as healthcare organizations baked in cybersecurity resilience. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called covered entities. Privacy security was established to secure individuals' electronic protected health information (e-PHI) (Security and Privacy, 2022; The Security, 2010, 2013).

3.3. Leadership: connecting telemedicine, telehealth, change, and cyber resilience

Cybersecurity concerns have to be addressed when planning, designing and developing telemedicine programs. All telemedicine partners: the payer, the provider or health system, and the telemedicine service provider must safeguard the security of their area of the system. All programs should also align with a security framework (i.e., the National Institute of Standards and Technology [NIST] Cybersecurity Framework) or the Health Sector Coordinating Council Health Industry Cybersecurity Practices (HSCC HICP) (which aligns to the NIST CSF). Leadership's guidance to connect telemedicine, telehealth, and cyber resilience represents the change that can cause opposition and disagreement from stakeholders and other supply chain partners – internal and external (Pellathy & Slank, 2020). The indication of change is disturbing because it can enact essential or minor disruptions in operations (Cohen & Kotter, 2005) and systems affecting other business functions (Helfat et al., 2009; Senge, 2014). Change management is sometimes undervalued due to stakeholders who resist change (Cohen & Kotter, 2005). Cybersecurity leadership must understand the difference, and so must all individuals within the organization to effect a positive outcome on current and future mindsets on resistance to change (Burton, 2017). When all are engaged in the process, with subject matter experts (Müller & Pfleger, 2014), and through an up and down leadership approach, change will be more respected and accepted.

Cyber resiliency planning and implementation must be communicated throughout the organization and understood by leaders at all levels (Kozina & Barun, 2016) with elucidation of assumptions and expectations. Telemedicine and telehealth cyber resiliency must consider human capital, IT, locations, patient care, and health outcomes and manage cost wrapped in a quality solution. Cyber resiliency planning has to be consistently reviewed to verify that it remains compliant, effective, and efficient (Metricstream, 2021; World Economic Forum, 2020). Cyber resilience must be a business continuous improvement process to learn from past breaches and errors and then prepare for gap management (Burrell, 2021; Burton, 2019).

3.4. Components of cybersecurity resilience

Cybersecurity resilience has four components. See the components in Figure no. 1:

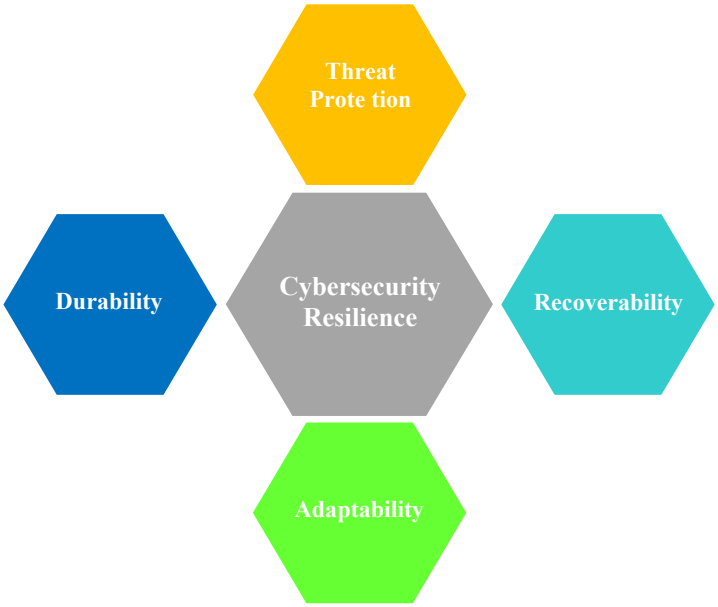


Figure no. 1: Cybersecurity Resilience Components
(Source: Author)

3.4.1. Threat protection

As technology evolves, cybercriminals magnify their reach. Security policies and procedures are necessary, and steps must be planned to guard healthcare organizations against various threats.

3.4.2. Recoverability

Recoverability must be recognized after all data breaches. Healthcare organizations should have a system for complete data backups on a diverse network. Team members at all levels should comprehend the processes and be well-rehearsed. Dependably, there must be post-breach incidence practice to maintain the resiliency plan.

- Resiliency has to remain as a practice. The plan must be updated regularly.
- All the team members must practice their step-by-step simulation. Such practice and rehearsal actions will serve to reinforce organizations' cybersecurity resilience.

3.4.3. Adaptability

Organizations must establish and remain adaptable. Cyberattacks are happening daily; therefore, organizations must be able to handle all issues readily. Adaptability is exhibited in organizations' strategic plans to utilize urgent actions and recover from all unforeseen attacks.

3.4.4. Durability

Durability has to be measured on an unceasing basis. Healthcare organizations have to remain capable of effectively returning to ordered business processes after a cybersecurity hack. By applying needed process and system augmentations and consistently informed and updated reporting and practices, organizations' cyber resilience will enhance (RSI Security, 2020).

4. Conclusions

People, process, and technology are the crux of cyber resilience. Ensuring the appropriate mix of people, processes, and technology enables healthcare organizations to attain adequate cybersecurity resilience. Training leaders at all levels consistently will work to diminish most threats. A void in training and testing will continue to lead to ill-informed employees, vulnerabilities, and weaknesses in the operations. Ensuring

proper change management will support employees' understanding and buy-in of the cybersecurity changes positively affecting resilience. The people who lead the organization should require some program for educating these people and raising awareness of things associated with cyber resilience (Burrell, 2021). The overall process must be well-designed to reduce risks and affect positive change. IT is not the responsibility of IT; it is a business concern that affects all employees (Nobles, 2018).

Preventing cyber-attacks and thwarting ransom attacks is the utmost of importance. Data fraud, theft, and cybersecurity attacks are among the top five most immense risks on the world stage. This issue is because of cyberattacks' massive overall business impact (Franco et al., 2020; World Economic Forum, 2020). Salient to understand is that cybersecurity resiliency is required to withstand capabilities offered by cyber resources despite the incidents of threat actors. The bases of the attacks deliberated by cybersecurity resiliency precisely comprise the APT, which is excessively more complex and adept than more conservative cyber hackers – distinctive criminals, bad actors, or insiders. Advanced ongoing threats cannot continually be kept at bay or readily identified and separated from that system, irrespective of the excellence of the system design, the practical efficiency of the security constituents, and the dependability of the particular constituents (NIST 80039).

The adoption of a cyber resilience plan is a conduit for improving a leader's approach to cyber resilience. There are healthcare organizations with documented and practiced cyber resilience strategies, yet they are not as effective. No matter the reason, the excuse of an ill-documented and practices plan cannot persist. Current and possible risks must be reviewed and documented through risks assessments. Assessments must review all aspects of the operation associated with cybersecurity. This work occurs through consistent and well-developed communication plans. All organization members must know their parts in the resiliency plan and remain current with the information. Consistently prioritizing threats to manage risks associated with cybersecurity is a must. Key stakeholders have to understand answers to the following questions. What could be any probability of each risk's occurrence? What is the impact (e.g., financial loss; data lost) of all the risks? Training must remain at the forefront. Leadership at all levels must focus on decreasing chances and apply required actions. After all else is in place, organizations must include a cybersecurity resilience insurance policy (Burton, 2021).

REFERENCES

Accenture Federal Services. (2018). *The nature of effective defense: Shifting from cybersecurity to cyber resilience*. Author. Available at: https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en/Accenture-Shifting-from-Cybersecurity-to-Cyber-Resilience-POV.pdf

American Telemedicine Association (ATA). (2013). *Telemedicine Case Studies*. Author. Available at: www.americantelemed.org

American Telemedicine Association (ATA). (2021, June 15). *IMPACT announces new definition of virtual first care at ATA 2021*. Author. Available at: https://www.americantelemed.org/member-partner-news/impact-announces-new-definition-of-virtual-first-care-at-ata-2021/

Bailey, S.R. (2021, February 10). *Pandemic exposes dire need to rebuild public health infrastructure. American Medical Association*, available at: https://www.ama-assn.org/about/leadership/pandemic-exposes-dire-need-rebuild-public-health-infrastructure.

Brown-Jackson, K.L. (2017). *Disrupting and retooling: A model for an effective community-based telehealth program*. The National Graduate School of Quality Management, ProQuest Dissertations Publishing, 28144638.

Burrell, D.N. (2021). *Cybersecurity leadership from a talent management organizational development lens*. [Unpublished Exegesis]. Capitol Technology University.

Burrell, D.N., Aridi, A.S., & Nobles, C. (2018). The critical need for formal leadership development programs for cybersecurity and information technology professionals. Reading: *Academic Conferences International Limited*, available at: https://www.proquest.com/conference-papers-proceedings/critical-need-formal-leadership-development/docview/2018926662/se-2?accountid=167615

Burton, S.L. (2019). Grasping the cyber-world: Artificial intelligence and human capital meet to inform leadership. *International Journal of Economics, Commerce, and Management, Vol. 7, Issue 12*, 707-759.

Burton, S.L. (2020). Protection via business impact analysis in a cyber world: A 3-Part series. In Latifi S. (eds) *17th International Conference on Information Technology-New Generations (ITNG 2020). Advances in Intelligent Systems and Computing, 1134*. Springer, Cham, available at: https://doi.org/10.1007/978-3-030-43020-7_1

Burton, S.L. (2021). *Artificial intelligence (AI) and augmented reality (AR): Disambiguated in the telemedicine/telehealth sphere*. DOI: 10.2478/bsalt-2021-0001.

Burton, S.L. (2017). *Transitioning to I can from I can't*. Lulu Publications.

Camlek, V. (2020). *Telehealth – A technology-based weapon in the war against the Coronavirus. Frost & Sullivan*, available at: https://store.frost.com/telehealth-atechnology-based-weapon-in-the-war-against-thecoronavirus-2020.html

Collier, K., Dilanian, K., & Winter, T. (2020, October 30). *More hospitals hit by ransomware as feds warn about cyberattacks*. NBC News, available at: https://www.nbcnews.com/tech/tech-news/more-hospitals-hit-ransomware-feds-warn-about-cyberattacks-n1245292

Cho, S. (2007). *A contextualist approach to telehealth innovations (Order No. 3292697)*. Healthcare Administration Database. (304877569). Available at: https://www.proquest.com/dissertations-theses/contextualist-approach-telehealth-innovations/docview/304877569/se-2?accountid=167615

Cohen, E. (2019). *Global life sciences & healthcare. Appian*. Available at: https://appian.com/blog/2019/four-challenges-facing-the-life-sciences-industry-in-2020.html

Kotter, J.P., & Cohen, D.S. (2005). *The heart of change field guide*. Boston, MA: Harvard Business Press.

Daemmrich, A. (2017). Invention, innovation systems, and the Fourth Industrial Revolution. *Technology and Innovation, Vol. 18, Issue 4*, 257-265. doi:http://dx.doi.org.proxy.cecybrary.com/10.21300/18.4.2017.257

Davis, J. (2021, March 5). FBI probing 2 hospital ransomware attacks; hackers remove health data. *Health IT Security.* Available at: https://healthitsecurity.com/news/fbi-probing-2-hospital-ransomware-attacks-hackers-remove-health-data

Dawson, M., Bacius, R., Gouveia, L.B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review, Vol. 251, Issue 101*, 69-75. DOI: 10.2478/raft-2021-0011.

DeSalvo, K., Parekh, A., Hoagland, G.Wet. et al. (2019). Developing a financing system to support public health infrastructure. *American Journal of Public Health, Vol. 109, Issue 10*,1358-1361

Douglas, C., & Thomas, H. (2020, October 21). The pandemic affecting the healthcare sector-a call for amending the HITECH Act. *CPO Magazine*. https://www.cpomagazine.com/cyber-security/the-pandemic-affecting-the-healthcare-sector-a-call-for-amending-the-hitech-act/

Drees, J. (2020, May 19). Telehealth to grow nearly 65% in 2020, report finds. *Becker Hospital Review*, available at: https://www.beckershospitalreview.com/telehealth/telehealth-to-grow-nearly-65-in-2020-report-finds.html

FAIR Health. (2021). *Monthly Telehealth Regional Tracker*. Author. Available at: https://www.fairhealth.org/states-by-the-numbers/telehealth

Franco, E.G., Schwab, K., Brende, B., Dusek, M., & Howell, L. (2020). *The global risks report 2020. World Economic Forum*. Cologny/Geneva, Switzerland. Available at: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Garrison, C., & Hamilton, C. (2019, January 02). A comparative analysis of the EU GDPR to the US's breach notifications. *Information & Communications Technology Law, Vol. 28, Issue 1*, 99-114. doi:10.1080/13600834.2019.1571473. hdl:10535/10737. ISSN 1360-0834

Healthcare & Public Health Sector Coordinating Councils. (2020, May). *Health Industry Cybersecurity Tactical Crisis Response Guide (HIC-TCR)*. Author. Available at: https://healthsectorcouncil.org/hic-tcr/

Healthcare & Public Health Sector Coordinating Councils. (2021, April). Health industry cybersecurity-securing telehealth and telemedicine (HIC-STAT). *Author.* Available at: https://healthsectorcouncil.org/securingtelehealth/

Horne, III, J.F., & Orr, J.E. (2011). Assessing behaviors that create resilient organizations. *Employment Relations Today, Vol. 24, Issue 4*, 29-39. https://doi.org/10.1002/ert.3910240405

Holt, B., Evernham, A. Armstrong, S., Boling, C., Butler, O., Coleman, C., Meehan, H., Morrison, W., Mulligan, M., Scarola, M., Weese, M., & DePersia, T. (2015). *Presidential Policy Directive 21 Implementation: An Interagency Security Committee White Paper*. Available at: https://www.cisa.gov/sites/default/files/publications/ISC-PPD-21-Implementation-White-Paper- 2015-508.pdf

Illusive. (2021). *The top threats targeting pharma and life sciences*. Author. Available at: https://go.illusive.com/top-pharma-life-sciences-threats-whitepaper

Isenberg, R., Kristensen, I., Mihir, M., & Weinstein, D. (2021, June 30). *Building cyber resilience in national critical infrastructure. McKinsey & Company*. Available at: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/building-cyber-resilience-in-national-critical-infrastructure

Jercich, K. (2020a, October 21). CMS reports 34.5M telehealth services delivered March through June. *HIMSS HealthcareIT News.* Available at: https://www.healthcareitnews.com/news/cms-reports-345m-telehealth-services-delivered-march-through-june

Jercich, K. (2020b, November 2). CDC: Telehealth visits more than doubled in March 2020. *HIMSS HealthcareIT News.* Available at: https://www.healthcareitnews.com/news/cdc-telehealth-visits-more-doubled-march-2020

Kozina, M., & Barun, A. (2016). Implementation of the business impact analysis for the business continuity in the organization. *Varazdin Development and Entrepreneurship Agency (VADEA), Varazdin*. Available at: https://proxy.cecybrary.com/login?url=https://search-proquest- 419 com.proxy. cybrary.com/docview/1793195819?accountid= 420 144459

Maani, N., & Galea, S. (2020 June). COVID-19 and underinvestment in the public health infrastructure of the United States. *The Milbank Quarterly, Vol. 98*. Available at: https://www.milbank.org/quarterly/articles/covid-19-and-underinvestment-in-the-public-health-infrastructure-of-the-united-states/#_edn7

Madni, A.M., & Jackson, S. (2009 June). Towards a conceptual framework for resilience engineering. *IEEE Systems Journal, Vol. 3, Issue 2*, 181-191. DOI: 10.1109/ JSYST.2009.2017397.

Mallak, L.A. (1999). Toward a theory of organizational resilience. *Management of Engineering and Technology, 1999. Technology and Innovation Management.* PICMET '99. Portland International Conference on, Portland, OR, USA, 223.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ: British Medical Journal (Online), Vol. 358.* Available at: http://franklin.captechu.edu:2123/10.1136/bmj.j3179

Masood, T. & Egger, J. (2020). Adopting augmented reality in the age of industrial digitalization. *Computers in Industry*, 115. Available at: https://doi.org/10.1016/j.compind.2019.07.002

Metricstream. (2021). *Cyber resilience best practices: Connecting the dots beyond cybersecurity*. *Author*. Available at: https://www.metricstream.com/insights/best-practices-cyber-resilience.htm

Morris-Reade, R. (2021). New research finds 93 % of security leaders don't repeat to the CEO. *Security Brief New Zealand.* Available at: https://securitybrief.co.nz/story/new-research-finds-93-of-security-leaders-don't-report-to-the-ceo

Muller, S.R. (2020). A Perspective On the intersection of information security policies and IA awareness, factoring in end-user behavior. *Proceedings of the International Conference on Research in Management & Technovation*, 137-142. DOI: 10.15439/2020KM1

Müller, A., & Pfleger, R. (2014). Business transformation towards sustainability. *Business Research, Vol. 7, Issue 2*, 313-350. DOI:http://dx.doi.org/10.1007/s40685-014-0011-y

National Institute of Standards and Technology (NIST). (2014, February 12). *Framework for improving critical infrastructure security, Version 1.0*. Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology (NIST). (2018, April 16). *Cybersecurity framework v1.1*. Author. Available at: https://csf.tools/reference/nist-cybersecurity-framework/v1-1/

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica – Journal of Business and Public Administration, Vol. 9, Issue 3*, 71-88. Available at: https://doi.org/10.2478/hjbpa-2018-0024

Obama, B. (2013, February 12). *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience*. Presidential Policy Directive (PPD) Series. United States. White House. Available at: https://www.hsdl.org/?view&did=731087

Pellathy, D., & Stank, T. (2020, July 09). Commentary: Cybersecurity safeguards should extend to supply-chain partners; companies must treat cybersecurity as a supply chain as work changes under the coronavirus pandemic create new vulnerabilities, say two supply-chain educators. *Wall Street Journal (Online)*. Available at: https://www.proquest.com/newspapers/commentary-cybersecurity-safeguards-should-extend/docview/2421518350/se-2?accountid=167615

Perlroth, N. & Satariano, A. (2021, May 20). Irish hospitals are latest to be hit by ransomware attacks. *NY Times.* Available at: https://www.nytimes.com/2021/05/20/technology/ransomware-attack-ireland-hospitals.html

PR Wire. (2020, September 10). *SecurityScorecard names telehealth biggest healthcare threat in new report*. Author. Available at: https://www.prnewswire.com/news-releases/securityscorecard-names-telehealth-biggest-healthcare-threat-in-new-report-301127130.html

Research 2 Guidance 2021. (2021 June). *2021 Global COVID-19 Survey*. Author. Available at: https://research2guidance.com/

RSI Security. (2019, August 14). *What is cyber resilience and why is it important?* Author. Available at: https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/

Schuchat, A. (2020). Public health response to the initiation and spread of pandemic COVID-19 in the United States, February 24 – April 21, 2020. *MMWR Morbidity and Mortality Weekly Report 2020*, *Vol. 69, Issue 18*, 551-556. DOI: http://dx.doi.org/10.15585/mmwr.mm6918e2

Security and Privacy, 45 C.F.R. (§) Part 164 Subparts A and C. (2022).

Sterbenz, J.P.G., Hutchinson, D., Cetinkaya, E.K., Jabbar, A., Rohrer, J.P., Scholler, M., & Smith, P. (2010, March 17). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks, Vol. 54, Issue 8*, 1245-1265. Available at: https://doi.org/10.1016/j.comnet.2010.03.005

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, Vol. 12, Issue 3*, 417-432. Available at: https://www.proquest.com/scholarly-journals/analysis-cybersecurity-standard-framework/docview/2483980790/se-2?accountid=167615

Sykes, N. (2019, April 25). Cybersecurity: What every telemedicine practitioner needs to know. *Arizona Telemedicine Program*. Available at: https://telemedicine.arizona.edu/blog/cybersecurity-what-every-telemedicine-practitioner-needs-know#:~:text=But%20because%20of%20the%20nature%20of%20the%20platform,health%20professional%20via%20a%20mobile%20app%2C%20for%20instance

Taylor, C., & Burton, S.L. (2018). *Advanced certified telemedicine/telehealth professional (A-CTTP)*. Lulu Publications.

The Security Rule, 45 C.F.R. (§) Part 160. (2010).

UNESCO. (2020a). *Education in a past-COVID-19 world: Nine ideas for public action*. Available at: https://en.unesco.org/sites/default/files/education_in_a_post-covid_world-nine_ideas_for_public_action.pdf

Verma, S. (2020, July 15). Early impact of CMS expansion of Medicare telehealth during COVID-19. *Health Affairs Blog*. doi: 10.1377/hblog20200715.454789

White House (WH). (2010, May). *White House, National Security Strategy*. Available at: https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

World Economic Forum. (2020). *Global risks report 2020: An unsettled world*. Available at: https://reports.weforum.org/global-risks-report-2020/chapter-one-risks-landscape/

Zielinski, L., & Marino, D. J. (2020). How to leverage the telemedicine surge to create a profitable telehealth model. *Healthcare Financial Management, Vol. 74, Issue* 6, 36-40.

Zorabedian, J. (2020 July 31). Facing growing cyber risks, here's how organizations are mitigating the cost of a data breach. *Forbes*. Available at: https://www.forbes.com/sites/ibmsecurity/2020/07/31/facing-growing-cyber-risks-heres-how-organizations-are-mitigating-the-cost-of-a-data-breach/?sh=49579fcb4025