The cyber threat to healthcare in South Africa

https://www.bsigroup.com/globalassets/localfiles/en-za/healthcare/cyber-in-healthcare-final.pdf

It will take a big leap for South Africa's healthcare sector to address cyber-attack strategies of syndicates becoming more fluent and adept at their game.

Attacks on healthcare establishments can threaten not just the integrity of systems and security of information but also the health, safety and lives of patients. It further seems as if any notion of complete cyber risk immunity in healthcare belongs to a distant future, as cybercrime syndicates keep upgrading their tactics and keep taking quick steps to thwart countermeasures.[i]

Healthcare sectors across the globe have long been hard-pressed to implement more penetrating means to counter this trend of data attackers outpacing medical enterprises.[ii] But things are happening at a snail's pace, making organisations more vulnerable to attack by the day.[iii]

In recent years, South Africa has experienced an acceleration of attacks throughout its industries.[iv] With spikes in especially the healthcare sector, our local hospitals and other medical facilities have been exposed as amongst the most vulnerable in the world.[v]

Fundamentally, healthcare in South Africa needs a decisive rethink and a deep overhaul of systems strategies to deal with this cyber risk crisis.

Digital transformation outdistancing the drive toward holistic cybersecurity

The intrinsic nature of healthcare makes the sector more likely to spend on patient care and saving lives than on cyber resilience.[vi] The same applies when considering the increased adoption of innovative technologies to expedite organisational objectives: to date, cyber security has mostly taken a back seat to improving quality and performance through digital transformation in healthcare.[vii]

It's speculated that the global digital health market's worth could reach about R6600 billion by 2025 – approximating a compound annual growth rate (CAGR) of 24.4% over the coming years.[viii]

With such escalated spending on digital technologies – and mainly due to the accelerated introduction of the Internet of Medical Things (IoMT), Artificial Intelligence (AI), data processing and analytics, telemedicine, and wearable technologies, among others – it goes without saying, organisations need to sufficiently budget for comprehensive cyber risk frameworks that provide security measures throughout their extensively connected network of systems.

Sometimes all it takes is for a syndicate to find one weakness in a network to breach important assets. Without holistic cyber protection, organisations are making themselves vulnerable to a host of threats that can cripple operational systems, have severe financial implications, corrupt patient care processes, and potentially endanger the lives of patients.

The first death indirectly caused by a cyber-attack was reported in Germany in September 2020. A critically ill patient who required emergency treatment had to be transported to another hospital after the University Hospital of Düsseldorf (UKD) was unable to receive her because of a ransomware attack that crippled its network and internal servers.[ix] The patient died as a result of the delay in treatment.

The attack compromised UKD's digital infrastructure that's central to the management and coordination of doctors, patients and processes. Hundreds of operations and other procedures had to be postponed or cancelled because of the attack. The hospital could now also only treat about half its patients, and simply couldn't take any new admissions. Eventually, it took two weeks to restore essential services and to reopen its emergency rooms. It took UKD much longer to again become fully operational. [x]

Attack targets, costs and comparisons

Besides attacks targeting operational systems or intellectual property related to medical research and innovation, patient data breaches are currently one of the predominant threats faced by healthcare.[xi] Targeted data can include patients' protected health information (PHI), patients' financial information and personal identification info.[xii]

Stolen health records may sell for 10 to 40 times more than stolen credit card numbers on the dark web.[xiii] Today, a patient's medical record could fetch anything between R1000 and R15000, even more – mostly this cost is relative to the level of sensitivity of the information.[xiv]

The cost to remediate a breach in healthcare is also three times higher than the cross-industry average.[xv] What's more, in 2020 the time it took to identify a healthcare breach averaged 329 days, whilst the average time to contain a breach was 233 days. By contrast, the data breach lifecycle of other industries averages at 228 days and 80 days, respectively.[xvi]

Attack threats in healthcare

With our healthcare sector having become such a prime target, South Africa is listed as one of the top countries in the world for the highest quantity of system breaches.[xvii]

Ransomware

Ransomware attacks on global healthcare have skyrocketed during 2020 and experts predict that things will only get worse in the coming years.[xviii] Ransomware is a form of malicious software that uses encryption technology to hold data at ransom. It can infect medical systems and data files, rendering them inaccessible until the ransom is paid. In the meantime, critical processes can be slowed down or even become inoperable.

Phishing

Phishing through email is one of the top cyber-attack methods in healthcare. It's such a lucrative attack strategy because the barriers to attack entry are low. Spammers also have a host of tools to initiate a phishing campaign, such as botnets-for-hire and Malware as a Service (Maas). One of phishing's main objectives is to obtain access to patients' protected health information (PHI) because it's become such a high-value commodity on the dark web.[xix]

Wearable and Implantable IoT Healthcare Devices

Implantable medical devices (such as cardiac implants and deep-brain neurostimulators), radio frequency identification tags, and wearable devices (such as pacemakers) are prone to severe security vulnerability. The rapid proliferation of these connected devices is redefining patient care processes, as doctors and patients are now using their smart-phones to control and monitor them.[xx] Imagine the risk when there's a zero-day exploit – patient injury or death can result and due to vendors or developers not having had the chance to fix the system's vulnerability.[xxi]

Insider threats

Not all threats are external, often the most common threat actors in healthcare are internal. Healthcare facilities, pharmaceutical companies and medical research firms are all banks of sensitive data. All it takes is for one rogue element to exploit, sell or manipulate this information. According to the 2020 Verizon Data Breach Investigations Report (DBIR), nearly half of all breaches in healthcare involve internal threat actors that target protected health information and electronic health records (EHR).[xxii]

There are of course many other major cyber threats to healthcare, and experts today agree that the best way to achieve greater cyber resilience is to adopt a comprehensive protection framework that drives a security culture through all levels of an organisation. Such a framework should be able to quickly detect a cyber disruption, minimise its impact, and ensure that operational continuity is maintained.

This is also exactly where world leader in standardisation frameworks, the British Standards Institution (BSI) can help South African healthcare facilities and companies. BSI's comprehensive information security solutions have been at the forefront of driving resilience in industries across the globe.

Establishing your journey towards cyber resilience with ISO/IEC 27001 – the international standard for Information Security Management Systems (ISMS)

ISO/IEC 27001 is an internationally recognized framework for managing information security and represents a consummate first step for healthcare organisations in South Africa. This security framework helps establishments implement, maintain and grow an independently assessed and certified Information Security Management System.

With an ISMS you're demonstrating commitment and compliance to global best practice, thereby showing that security is a primary consideration in your organisation.

How ISO/IEC 27001 can help healthcare, pharmaceutical and biotech facilities and companies build resilience:

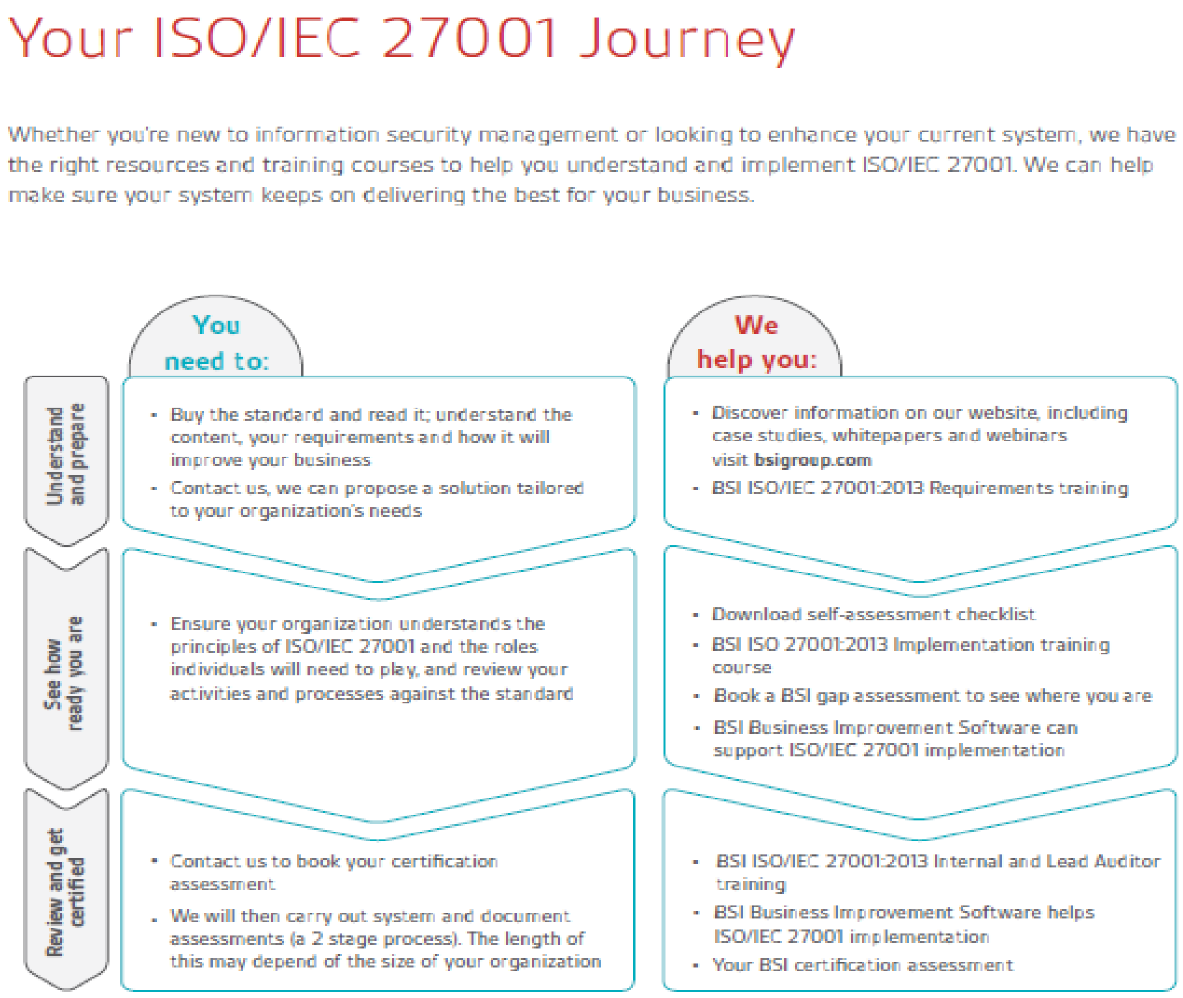
- Requires you to continually detect and evaluate information security risks and breaches and to ensure the procedures and controls you activate are sufficient to manage or minimize them
- Helps you identify all internal and external stakeholders relevant to your ISMS
- Helps establish a work environment in which there's a continuous improvement of your ISMS
- Ensures information is always protected, available, and can be accessed
- Reduces the likelihood of insider threats to security breaches
- Shows commitment to information security at all levels, whilst helping to embed an information security culture
- Requires you to communicate the ISMS policy throughout your organization, which will help you raise awareness and gain buy-in
- Creates an environment in which top management define ISMS roles and ensure individuals are competent
- Provides flexibility to adapt relevant controls across your organisation
- Helps inspire trust that data is protected, which in turn will strengthen your reputation and help cultivate patient and workforce confidence

Having your ISMS assessed by BSI, and successfully fulfilling the requirements of ISO/IEC 27001, provides you the opportunity to show your commitment to excellence by displaying the prestigious BSI Mark of Trust across your organisation.

Benefits BSI Clients get from ISO/IEC 27001 certification:

1)	We have reduced our operational risk	88%
2)	We have improved out internal business confidence	86%
3)	We have improved customer satisfaction	85%

Reference: Voice of the customer survey 2020



Your ISO/IEC 27001 Journey

Whether you're new to information security management or looking to enhance your current system, we have the right resources and training courses to help you understand and implement ISO/IEC 27001. We can help make sure your system keeps on delivering the best for your business.

You need to:

We help you:

Understand and prepare

- Buy the standard and read it; understand the content, your requirements and how it will improve your business
- Contact us, we can propose a solution tailored to your organization's needs

- Discover information on our website, including case studies, whitepapers and webinars visit **bsigroup.com**
- BSI ISO/IEC 27001:2013 Requirements training

See how ready you are

- Ensure your organization understands the principles of ISO/IEC 27001 and the roles individuals will need to play, and review your activities and processes against the standard

- Download self-assessment checklist
- BSI ISO 27001:2013 Implementation training course
- Book a BSI gap assessment to see where you are
- BSI Business Improvement Software can support ISO/IEC 27001 implementation

Review and get certified

- Contact us to book your certification assessment
- We will then carry out system and document assessments (a 2 stage process). The length of this may depend of the size of your organization

- BSI ISO/IEC 27001:2013 Internal and Lead Auditor training
- BSI Business Improvement Software helps ISO/IEC 27001 implementation
- Your BSI certification assessment

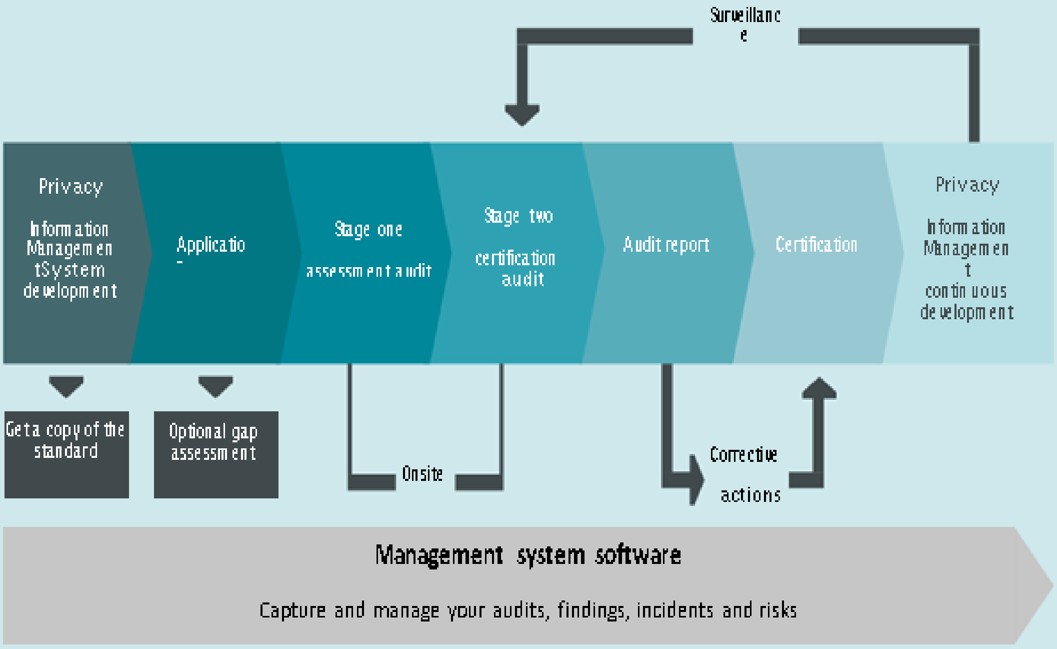
Upgrade your cyber resilience with ISO/IEC 27701

As an extension to ISO/IEC 27001, the ISO/IEC 27701 framework provides further guidance for the protection of patient information.

ISO/IEC 27701 enables your healthcare establishment to enhance its ISMS with additional requirements in order to establish, implement, maintain and continually improve your Privacy Information Management System (PIMS). The standard outlines a framework for personally identifiable information (PII) controllers and PII processors to manage privacy controls so that risk to individual privacy rights is reduced.

ISO/IEC 27701 certification journey

Whether you're new to privacy management or looking to enhance an existing information security and privacy system, certification to ISO/IEC 27701 provides confidence and trust in the way you manage privacy. It demonstrates you have taken accountability for processing PII in a secure and compliant way. No matter where you are in your journey, our team are on hand to support.



Our ISO/IEC 27701 journey builds upon ISO/IEC 27001 certification. If you're certified to ISO/IEC 27001, talk to us about the option of combined audit days.

The BSI leap

BSI is aware that achieving cyber resilience is not going to happen overnight. But by complementing your organisation's existing culture of patient care with an entrenched culture of cybersecurity – as provided by the ISO/IEC 27001 and ISO/IEC 27701 frameworks – you have taken a big step towards augmenting your information security defence system.

Get in touch with us today to discuss your plans and how we can support you on your journey towards operational excellence.

[i] Amy Baker, Healthcare Global, May 17, 2020, “An ounce of prevention: how the healthcare industry can fight cybercrime” <https://healthcareglobal.com/technology-and-ai-3/ounce-prevention-how-healthcare-industry-can-fight-cybercrime>
Nicole Wetsman, The Verge, November 11, 2020, “Waves of attacks on US hospitals show a change in tactics for cybercriminals” <https://www.theverge.com/21551050/cyberattacks-hospitals-coronavirus-deadly-tactics>
Malwarebytes, November 1, 2019, “Cybercrime tactics and techniques: the 2019 state of healthcare” <https://resources.malwarebytes.com/files/2019/11/191028-MWB-CTNT_2019_Healthcare_FINAL.pdf>
BMC Medical Informatics and Decision Making, various authors, July 3, 2020, “Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks” <https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7>

[ii] Rajiv Leventhal, February 17, 2021, “With New Attack Vectors, Healthcare Data Breaches Continued to Soar in 2020” <https://www.hcinnovationgroup.com/cybersecurity/data-breaches/article/21209658/with-new-attack-vectors-healthcare-data-breaches-continued-to-soar-in-2020>
Help Net Security, November 16, 2020 “Healthcare organizations are sitting ducks for attacks and breaches” <https://www.helpnetsecurity.com/2020/11/16/healthcare-attacks-breaches/>

[iii] O'Brien, Niki and Martin, Guy and Grass, Emilia and Durkin, M and Darzi, Ara and Ghafur, Saira, October 20, 2020, “Cybersecurity in Healthcare: Comparing Cybersecurity Maturity and Experiences Across Global Healthcare Organizations”
https://ssrn.com/abstract=3688885 or http://dx.doi.org/10.2139/ssrn.3688885October 20, 2020,
Leila Hawkins, Healthcare Global, March 17, 2021, “CyberMDX: How to prevent cyber-attacks in healthcare” <https://healthcareglobal.com/technology-and-ai-3/cybermdx-how-prevent-cyber-attacks-healthcare>
Susan Morrow, INFOSEC, May 1, 2020, <https://resources.infosecinstitute.com/topic/top-cyber-security-risks-healthcare/>
HIPAA Journal, “Healthcare Cybersecurity” <https://www.hipaajournal.com/category/healthcare-cybersecurity/>

[iv] Blue Turtle Technologies, Aug 6, 2020 “Cyber Crime: a pandemic hitting the wallet of South African business” <https://www.itweb.co.za/content/JN1gPvOYBWPMjL6m>
Accenture, “Insight into the cyberthreat landscape in South Africa”, 2019 <https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf>
Brett van Niekerk, The African Journal of Information and Communication, Dec 2017 “An Analysis of Cyber-Incidents in South Africa” <https://www.researchgate.net/publication/322455131_An_Analysis_of_Cyber-Incidents_in_South_Africa>
Gareth van Zyl, Fin24, July 7, 2016, “8.8 million South Africans hit by cyber crime – study” <https://www.news24.com/fin24/Tech/News/88-million-south-africans-hit-by-cyber-crime-study-20160707>

[v] Sameer Naik, IOL, Jan 9, 2021 “SA hospitals under further strain due to increase in cyber attacks”, comment by Anna Collard from KnowBe4 Africa <https://www.iol.co.za/saturday-star/news/sa-hospitals-under-further-strain-due-to-increase-in-cyber-attacks-efb62b96-9170-43e9-b1af-475783472ba9>

[vi] Heather Landing, Fierce Healthcare, November 23, 2020, “Could patients be at risk during a hospital cyberattack? It depends how far hackers are willing to go, expert says” <https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are>
Fred Pennic, May 16, 2018 “Global Healthcare Cybersecurity Spending Expected to Exceed $65B Over 5 Years” <https://hitconsultant.net/2018/05/16/global-healthcare-cybersecurity-report/#.YKI4YagzbIU>

Help Net Security, November 16, 2020 “Healthcare organizations are sitting ducks for attacks and breaches” <https://www.helpnetsecurity.com/2020/11/16/healthcare-attacks-breaches/>
Symantec, “Cybersecurity in Healthcare: Why it’s not enough, why it can’t wait” <https://docs.broadcom.com/doc/symantec-healthcare-it-security-risk-management-study-en>
Michael Ebert, KPMG, “Health Care and Cyber Security” p.3 <https://assets.kpmg/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf>
ir.deto, 2021 “Report: The business value of cyber security in MedTech” p.22 <https://resources.irdeto.com/assets/report-the-business-value-of-cybersecurity-in-medtech>

[vii] Various authors, more specifically comments by Andrew Bycroft, Michael Magrath, Tom Hui and David Finn. June 25, 2018, “Healthcare information security: the top Infosec considerations for healthcare organizations today” <https://digitalguardian.com/blog/healthcare-information-security-top-infosec-considerations-healthcare-organizations-today>

[viii] Business Wire – A Berkshire Hathaway Company, March 29, 2021, “Global Digital Health Market Report 2021: COVID-19 Growth and Change to 2025 & 2030 - ResearchAndMarkets.com” <https://www.businesswire.com/news/home/20210329005618/en/Global-Digital-Health-Market-Report-2021-COVID-19-Growth-and-Change-to-2025-2030---ResearchAndMarkets.com>

[ix] UKD/HHU, September 10, 2020, “Krankenhaus derzeit nur sehr eingeschränkt erreichbar – Patientenversorgung eingeschränkt” <https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt>
Catalin Cimpanu (for Zero Day), ZDNet, September 17, 2020, “First death reported following a ransomware attack on a German hospital” <https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/>

[x] Melissa Eddy and Nicole Perlroth, The New York Times, September 18, 2020, **“**Cyber Attack Suspected in German Woman’s Death” <https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html>
Wired, September 19, 2020, “A Patient Dies After a Ransomware Attack Hits a Hospital”
https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/
Reuters Staff, September 18, 2020, “Prosecutors open homicide case after hacker attack on German hospital” <https://www.reuters.com/article/idUSKBN26926X>

[xi] John Riggi, AHA Center for Health Innovation, “The importance of cybersecurity in protecting patient safety” <https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety>

[xii] Dräger, “Cybersecurity in Healthcare: Keeping Devices and Data Secure” <https://www.draeger.com/en_uk/Hospital/Cybersecurity-In-Healthcare> sub: “Do you still think hospitals don't get hacked?” Florian Grunow, July 9, 2019 <https://www.youtube.com/watch?v=7z0Pri_H09U>

[xiii] Fierce Healthcare, Paul Nadrag (Capsule Technologies), Jan 26, 2021, “Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web” <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>
CyberPolicy, “Why Medical Records are 10 Times More Valuable Than Credit Card Info” <https://www.cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info>

Aatif Sulleyman, The Independent, May 12, 2017 "NHS Cyber Attack: Why Stolen Medical Information is so much more valuable than Financial Data" <https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-sell-financial-a7733171.html>
Juliann Schaeffer, For The Record, March 2016, "PHI: Valuable and Vulnerable", <https://www.fortherecordmag.com/archives/0316p18.shtml>

[xiv] Total Processing, Rebekah Moss, September 17, 2019, "How Much is your Data Worth on the Dark Web?" <https://www.totalprocessing.com/totalprocessing.com/public/blog/how-much-is-your-data-worth-on-the-dark-web>
Fierce Healthcare, Paul Nadrag (Capsule Technologies), Jan 26, 2021, "Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web" <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>

[xv] Iron Mountain, "Avoid the costs of a healthcare data breach" <https://www.ironmountain.ie/resources/general-articles/a/avoid-the-costs-of-a-healthcare-data-breach>

[xvi] Varonis, Rob Sobers, updated April 16, 2021 "98 Must-Know Data Breach Statistics for 2021" <https://www.varonis.com/blog/data-breach-statistics/#:~:text=Average%20Response%20Time%20and%20Lifecycle,days%2C%20respectively%20(IBM)>
"How much would a data breach cost your business?" -IBM's 2020 Cost of a Data Breach Report- <https://www.ibm.com/security/data-breach>

[xvii] Safety Detectives, "Ransomware Facts, Trends & Statistics for 2021" -How many organizations reported ransom attacks in the last year- <https://www.safetydetectives.com/blog/ransomware-statistics/>
Desmond Latham, Health-E News, January 9, 2020, "Cyberattackers increasingly target healthcare and South Africa is not immune" <https://health-e.org.za/2021/01/09/cyberattackers-increasingly-target-healthcare-and-south-africa-is-not-immune/>

[xviii] Jessica Davis, Health IT Security, xtelligent Healthcare Media, "Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware" <https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware>
Netwrix, "2021 Cloud Data Security Report" <https://www.netwrix.com/2021_cloud_data_security_report.html>
CISION, PR Newswire, "39% of Healthcare Organizations Suffered Ransomware Attacks in the Cloud in 2020" <https://www.prnewswire.com/news-releases/39-of-healthcare-organizations-suffered-ransomware-attacks-in-the-cloud-in-2020-301234204.html#:~:text=All%20Products-,39%25%20of%20Healthcare%20Organizations%20Suffered%20Ransomware%20Attacks%20in%20the%20Cloud,was%20sued%2C%20Netwrix%20study%20finds>

[xix] HIPAA Journal, "Protect Healthcare Data from Phishing" <https://www.hipaajournal.com/protect-healthcare-data-from-phishing/>

[xx] Mary Lee, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, Bryce Downing, Rand Corporation, 2020, "The Internet of Bodies – Opportunities, Risks, and Governance" <https://www.rand.org/content/dam/rand/pubs/research_reports/RR3200/RR3226/RAND_RR3226.pdf>

[xxi] George W. Jackson, Jr. and Shawon S. M. Rahman, International Journal of Network Security & Its Applications (IJNSA) Vol. 11, No.4, July 2019, "Exploring Challenges and Opportunities in Cybersecurity Risk and

Threat Communications Related To The Medical Internet of Things”
<https://arxiv.org/ftp/arxiv/papers/1908/1908.00666.pdf>
Marianne Kolbasuk McGee, Healthcare Info Security, June 24, 2015, “Wearable Devices: Security Risks”
<https://www.healthcareinfosecurity.com/interviews/wearable-devices-security-risks-i-2764>
Anil Chacko, ResearchGate, July 2018, “Security and Privacy Issues with IoT in Healthcare”
<https://www.researchgate.net/publication/326568227_Security_and_Privacy_Issues_with_IoT_in_Healthcare>

[xxii] Verizon, “2020 Data Breach Investigations Report”
<https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf>