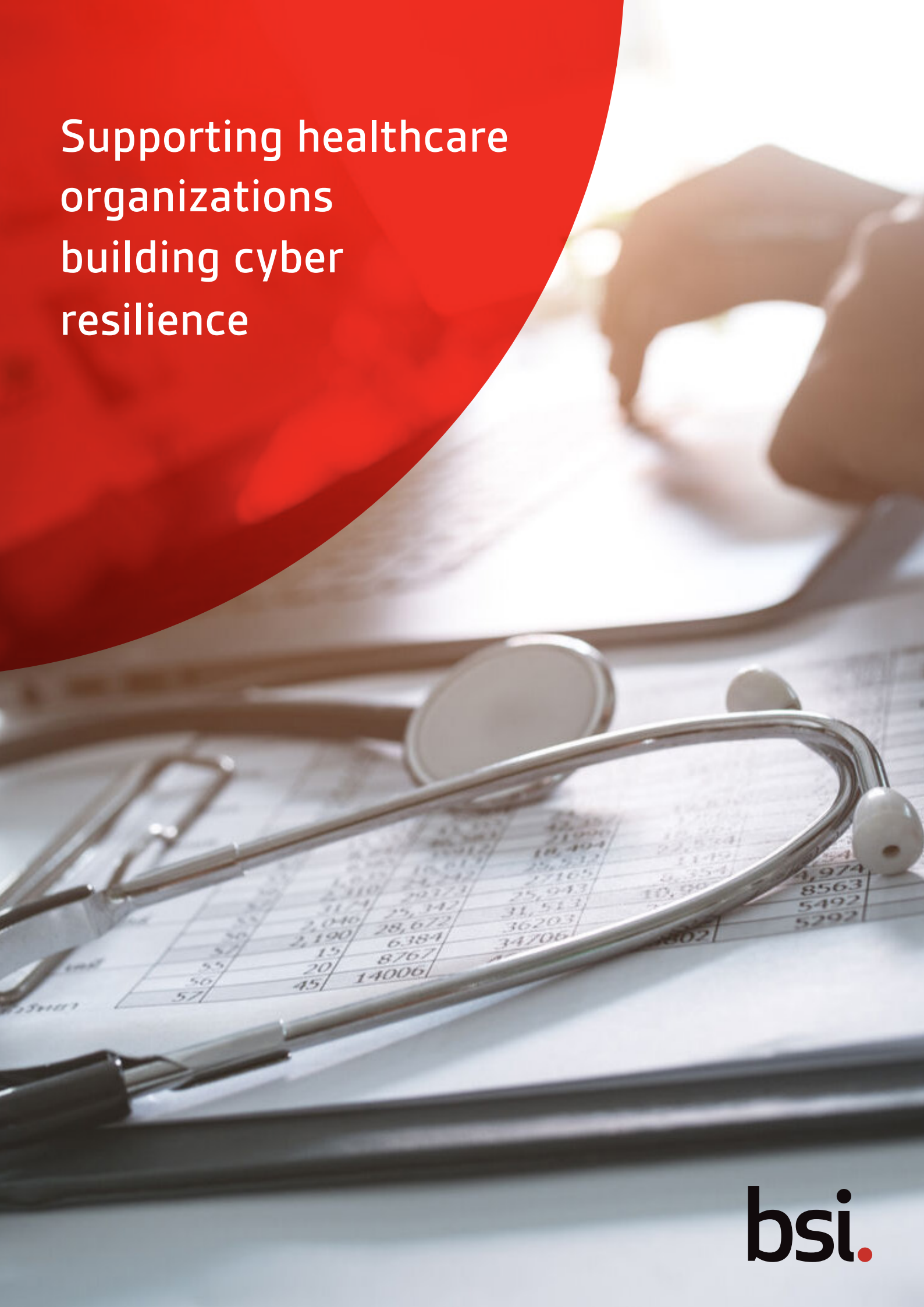
Supporting healthcare organizations building cyber resilience



bsi.

Protect your information, people and reputation

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 only 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 taking quick steps to thwart countermeasures.[i]

The global healthcare sector has long been hard-pressed to implement more penetrating means to counter this trend of data attackers outpacing medical enterprises.[ii] But with these changes happening so slowly, organizations are more vulnerable to attack by the day.[iii]

In recent years, South Africa has experienced an acceleration of attacks.[iv] Local hospitals and other medical facilities have been exposed as amongst the most vulnerable in the world.[v]

Fundamentally, healthcare in South Africa has the opportunity to embrace a complete rethink 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 rather than on cyber resilience.[vi] The same applies when considering the increased adoption of innovative technologies to expedite organizational objectives: to date, cyber security has mostly taken a back seat to improving quality and performance through digital transformation.[vii]

It's speculated 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, organizations 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, organizations 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-ever human 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 the hospital'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 also only treat half the number of daily patients, and it simply couldn't take any new admissions. Eventually, it took the hospital about two weeks to restore essential services and reopen its emergency rooms. It took even longer to become fully operational again.[x]

This incident demonstrates the potential impact of a sophisticated cyber-attack by criminals who have little regard for human life.

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.[xi] Targeted data can include patients' protected health information (PHI)and financial information as well as personal identification information. [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.

The cost to remediate a breach is also three times higher than the cross-industry average. What's more, in 2020 the time it took to identify a breach averaged at 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 South Africa's healthcare sector having become such a prime target, it is listed as one of the top countries in the world for the highest quantity of system breaches.[xvii]

Ransomware

Ransomware attacks globally 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. 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).

Implantable IoT healthcare device

Implantable medical devices such as cardiac implants and deep-brain neurostimulators, radio frequency identification tags, and pacemakers are prone to severe security vulnerability. The rapid growth of these connected devices is redefining patient care processes, as doctors and patients are now using their smart-phones to control and monitor ailments. Imagine the risk when there's a zero-day exploit – patient injury or death can result and without the cause being detected.[xix]

Insider threats

Not all threats are external; often the most common threat actors 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).[xx]

There are of course many other major cyber threats, 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 organization. Such a framework should be able to quickly detect a cyber disruption, minimise its impact, and ensure that operational continuity is maintained.

We at BSI, the world leader in standardisation frameworks, can help healthcare facilities and companies. Our comprehensive information security solutions have been at the forefront of driving resilience in industries across the globe.

A holistic information security approach

Establishing your journey towards cyber resilience is dependent on a strong foundation. And that's where ISO/IEC 27001 – the international standard for Information Security Management Systems (ISMS) provides a holistic approach to embed an information security culture that helps prioritize addressing both physical security threats as well as the increasing number of cyber-threats.

ISO/IEC 27001 is internationally recognized and represents an ideal first step for healthcare organizations in South Africa to 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 organization.

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

- Provides best practice information security requirements to embed as part of your organization's governance framework, supporting business objectives
- Requires you to continually detect and evaluate information security risks and breaches and to ensure the procedures and controls you activate are sufficient
- 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 organization
- Helps inspire trust that data is protected, which in turn will strengthen your reputation and help cultivate patient and workforce confidence

Enhance your resilience with ISO/IEC 27701 Privacy Information Management

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

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. So, your healthcare organization can take a holistic approach, enhancing your ISMS to address specific privacy and data protection obligations with a Privacy Information Management System (PIMS) based on international best practice.

Reference: Voice of the customer survey 2020

Benefits of ISO/IEC 27701:

- Builds trust in managing personal information
- Provides transparency between stakeholders
- Facilitates effective business agreements
- Clarifies roles and responsibilities
- Supports compliance with privacy regulations
- Reduces complexity by integrating with the leading information security standard ISO/IEC 27001

Why BSI?

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 organization.

Next steps

We are aware that achieving resilience around cyber and information security is not going to happen overnight. But by complementing your organization's existing culture of patient care with an entrenched culture of information security – 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.

Bibliography/References

[i]<https://healthcareglobal.com/technology-and-ai-3/ounce-prevention-how-healthcare-industry-can-fight-cybercrime>
[ii] <https://www.hcinnovationgroup.com/cybersecurity/data-breaches/article/21209658/with-new-attack-vectors-healthcare-data-breaches-continued-to-soar-in-2020>
[iii]<https://ssrn.com/abstract=3688885 or http://dx.doi.org/10.2139/ssrn.3688885October 20, 2020,
[iv]<https://www.itweb.co.za/content/JN1gPvOYBWPMjL6m>
[v] <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] <https://www.fiercehealthcare.com/tech/could-patients-be-at-risk-during-a-hospital-cyber-attack-it-depends-how-far-hackers-are>
[vii]<https://digitalguardian.com/blog/healthcare-information-security-top-infosec-considerations-healthcare-organizations-today
[viii]<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]<https://www.uniklinik-duesseldorf.de/ueber-uns/pressemitteilungen/detail/krankenhaus-derzeit-nur-sehr-eingeschraenkt-erreichbar-patientenversorgung-eingeschraenkt>
[x]<https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html>
[xi] <https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety>
[xii]<https://www.draeger.com/en_uk/Hospital/Cybersecurity-In-Healthcare>
<https://www.youtube.com/watch?v=7z0Pri_H09U>
[xiii]<https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web>
[xiv]<https://www.totalprocessing.com/totalprocessing.com/public/blog/how-much-is-your-data-worth-on-the-dark-web>
[xv]<https://www.ironmountain.ie/resources/general-articles/a/avoid-the-costs-of-a-healthcare-data-breach>
[xvi] <https://www.varonis.com/blog/data-breach-statistics/#:~:text=Average%20Response%20Time%20and%20Lifecycle,days%2C%20respectively%20(IBM)>
[xvii] <https://www.safetydetectives.com/blog/ransomware-statistics/>
[xviii]<https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware>
[xix] <https://arxiv.org/ftp/arxiv/papers/1908/1908.00666.pdf>
[xx] <https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf>

bsi.za@bsigroup.com
bsigroup.com/en-ZA
+27 (0) 12 004 0279