BSI Digital trust:
Supporting the healthcare ecosystem

Author: Mark Brown, Global Managing Director, Digital Trust Consulting, BSI

Contents

Author: Mark Brown

Global Managing Director, Digital Trust Consulting Services, BSI

Mark Brown has over 30 years' experience in cybersecurity, data privacy and business resilience consultancy. He has previously held roles at Wipro Ltd. and Ernst & Young, among others. His wealth of knowledge includes extensive proficiency on the Internet of Things (IoT) and the expanding cybersecurity marketplace, always focusing on cybersecurity's strategic enablement and risk protection elements.

Abstract

The digital transformation of recent decades has highlighted the criticality of a fully functioning healthcare and pharmaceutical ecosystem, and the importance of employing accelerated technologies to manage and improve patient quality of care inside and outside the clinical setting.

In this insights paper, Mark Brown discusses:

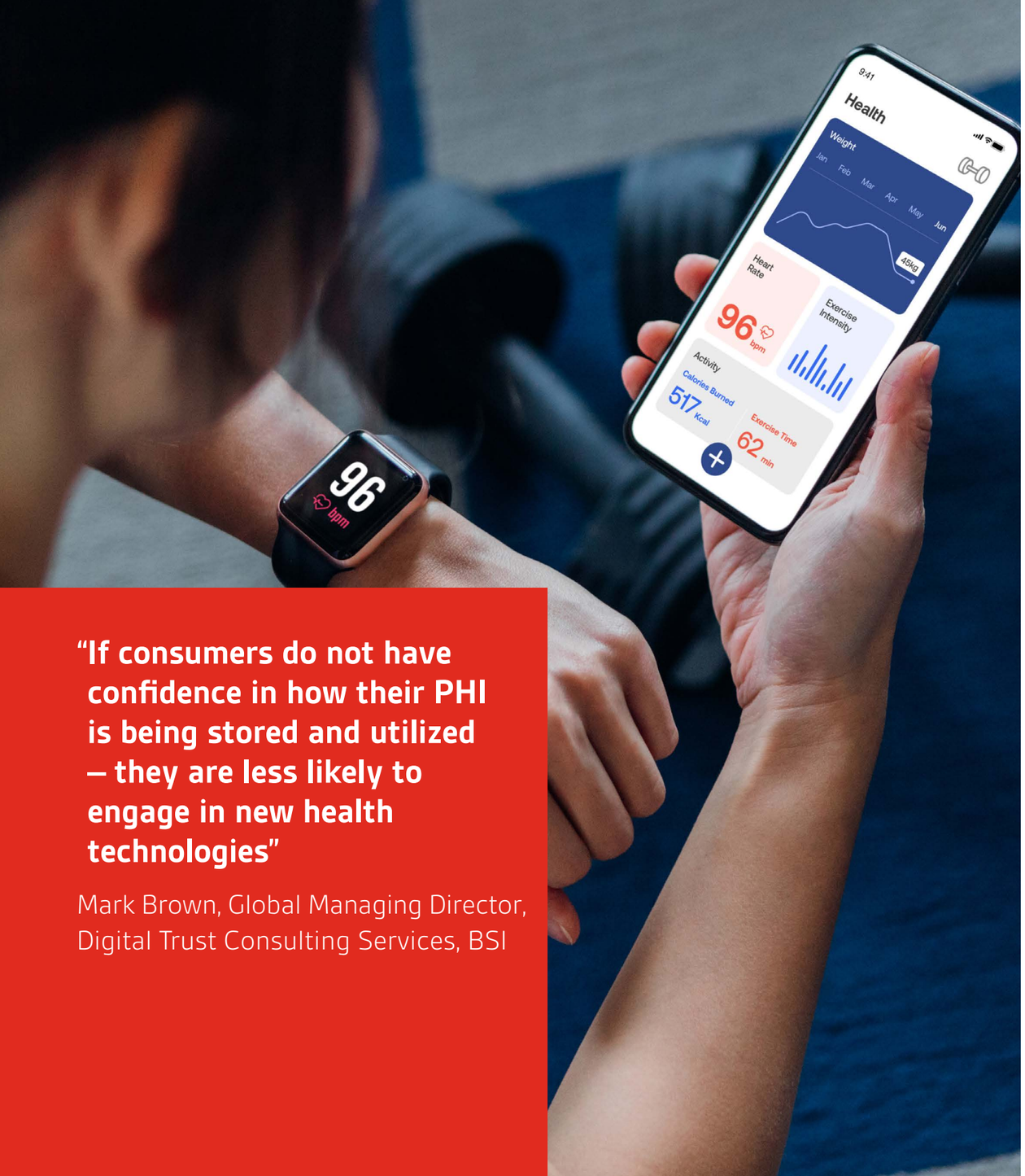
- How digital trust is changing in healthcare environments
- The global outlook for cybersecurity breaches
- What a breach looks like in a healthcare setting
- How BSI Digital trust can help you

This paper explores the changing landscape of digital trust in healthcare, why cyberattacks are still on the rise, and how BSI can help mitigate your risk of a security breach, and enhance the trust in new technologies creating a strategic enabler for expanded healthcare deliver.

22m

healthcare records have been breached in the US so far in 2022*

*https://www.medicaldevice-network.com/comment/cybersecurity-us-health-records



"If consumers do not have confidence in how their PHI is being stored and utilized – they are less likely to engage in new health technologies"

Mark Brown, Global Managing Director, Digital Trust Consulting Services, BSI

The changing landscape of digital trust in healthcare

Key trends in telehealth, wearables, Internet of Medical Things (IoMT) for remote monitoring, plus a rise in wellness apps, have drawn consumers into the convenience of managing their personal healthcare by digital means. With that, comes a heightened need for trust in the flow of consumers' personal patient health information (PHI) in the broader digital health ecosystem.

Increasing numbers of healthcare organizations are migrating from legacy systems to cloud computing, making it imperative to maintain security and privacy to anonymize PHI. Strict security requirements must be implemented to protect consumers' data; regardless of their size, location, or model of services.

Artificial intelligence (AI) and IoMT increase healthcare providers' ability to identify patterns in the patients they care for, allowing for earlier diagnosis, guidance, and feedback on remaining healthy. However, many patients and consumers lack trust and confidence in these modern technologies and are sceptical of them, which is the main barrier to adoption.

Protecting all aspects of healthcare information from theft, breaches, or corruption will ensure that healthcare services can continue to function and thrive.

While the societal and organizational risks are high, some mitigation techniques can be reassuringly simple. Ensuring staff know about and comply with the basics of cyber hygiene is one of the most important ways to reduce risk.

Cyberattacks in numbers: the global outlook

66%

of US healthcare organizations fell victim to a ransomware attack in 2021[1]

60%

of healthcare breaches in 2021 were reportedly caused by third party vendors[2]

47%

of executives revealed that their organization had been forced to shut down in the last six months due to a cyberattack[3]

4 in 5

NHS Trusts have faced record levels of cyberattacks following the Russian invasion of Ukraine[4]

785

cyberattacks are happening in the UK each week[5]

1 https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals#:~:text=More%20than%20two%2Dthirds%20of,US%2Dbased%20firms%20in%202021.

2 https://expertinsights.com/insights/healthcare-cyber-attack-statistics

3 https://expertinsights.com/insights/healthcare-cyber-attack-statistics/

4 https://www.telegraph.co.uk/news/2022/08/14/nhs-cyber-attacks-hit-record-levels-four-five-trusts-russian/

5 https://www.thebharatexpressnews.com/nhs-at-risk-of-further-major-cyber-attacks-this-year-experts-warn/

Did you know?

“Between 2021 – 2022, there was a 94% rise in ransomware attacks in the US, plus a steep rise in phishing and malware attacks across the globe”.[6]

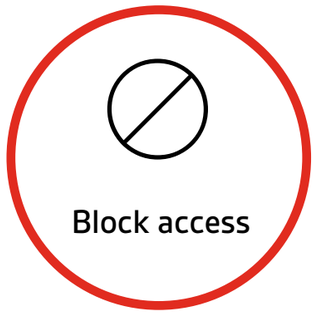
What could a cybersecurity breach mean for a healthcare provider?

Assuring consumers’ overall trust in innovative digital health technologies has raised the need for businesses and healthcare professionals to have well-developed security strategies and policies to mitigate cyber threats.

Cybersecurity threats in healthcare are growing in frequency and sophistication. New technologies, plus shifts to remote consultations, have contributed to numerous organizations experiencing the havoc a cyber attack can cause - consistently costing businesses around the world tens, hundreds, or millions of dollars.

For primary healthcare facilities experiencing a halt in services due to a malicious disruption, the inability to access services may be just the beginning. A breach means hackers can:

- **Block access** to email, online appointment booking and triage systems, patient records, staff rotas and contact details
- Manipulate or **corrupt data**, for example by removing ‘red flag’ alerts from clinical records, mixing up test results or even tampering with temperature controls for freezers storing life-saving vaccines
- Publish stolen, confidential **clinical records** relating to patient health



6 https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals#:~:text=The%20number%20of%20ransomware%20attacks%20on%20healthcare%20organizations%20increased%2094,up%20from%2034%25%20in%202020

Examples of recent targeted attacks on healthcare systems

These attacks highlight third-party vendors' financial and societal risks and raise the question: *are third-party vendors like Advanced liable for increasing cyber-attacks on our healthcare services?* The NHS has highlighted how critical it is to understand your third-party risk, with organizations relying so heavily on digital connectivity which are attractive targets for hackers.

Texas hospital

In October 2022, OakBend Medical Center reported a ransomware attack that caused system outage for over six weeks. The attack on IT systems resulted in hackers downloading medical records of around 500,000 patients.

Ransomware group, Daixin, came forward as responsible for the attack and demanded over $10m as ransom. The group has launched attacks on several healthcare providers in the last few months.

Advanced

In August 2022, Advanced – a software provider for the UK National Health Service (NHS) – was hit by ransomware attack. Though not a direct attack on the NHS, Advanced provides 85% of 111 services to the UK healthcare body.

111 is a free, 24-hour NHS phone line that people can call to get referred for medical attention with non-life-threatening issues. Ambulances are dispatched when required, appointments are made and emergency prescriptions are fulfilled, making it a critical system for society.

The attack led to 4 weeks of disruption to the 111 service; with longer wait times and NHS staff using pen and paper for processes while the issue was fixed. Advanced has not revealed if patient data was stolen in the attack, or if they paid a ransom, but the physical impact of the malicious attack is clear.

WannaCry

'Wannacry' was another third-party ransomware attack in 2017, which affected users in primary and secondary care, who were unable to access patient records, online diagnostics, appointment booking systems and emails. The attack exposed primary and secondary care as 'soft-targets' for such attacks. It was one of many organizations to fall victim to the attack, which exploited weaknesses in software operating systems, many of which were legacy and had not been adequately updated to provide security over time.

Even so, the attack caused widespread disruption. Some hospitals and practices had to temporarily close to admissions and cancel outpatient clinics while hundreds of machines were checked, disinfected and clean back-ups restored.
As Dr Ghafur points out: 'If you think about what happened in Wannacry, it would be very difficult now because everything, every bit of healthcare we are delivering has some digital element to it. Three years ago, some departments reverted to pen and paper to manage the inability to access patient records or diagnostics.
Now, with almost all records and imaging digitized, many staff working remotely and appointments and triage managed online, it is hard to see how that could happen.'

Mitigation of cybersecurity risks

Many of the risks outlined can be managed and substantially reduced by basic cyber hygiene.

By adopting a layered approach to security, organizations can make themselves less attractive targets to attackers and reduce the chances of successful attacks. Let's look at the various layers of security your organization should implement:

Physical security

Healthcare providers need to ensure the physical security of devices used to process or store sensitive information by following provided the guidance:

- Users must be educated to lock devices away securely when not in use and removable devices, such as USB memory drives, should never be used to store clinical information.
- Staff should be discouraged from lending their device to others, for example to their children to play computer games, due to the risk of loss or infection of the device with malware.

Education

Education is essential to help staff recognize phishing emails seeking access to information systems. Phishing is still an enticing way for cybercriminals to try to breach your organization. Therefore, it is vital to educate your users on what an attack that tries to get hold of their credentials looks like, by providing some training or simulation tools that can catch people out – then people can learn from their experiences.

Safe information storage

Healthcare providers should ensure the information stored on devices is protected, so if devices are lost or stolen, the information cannot be compromised. Organizations need to check their devices encrypt data while at rest, so that people who shouldn't have access to data, don't have access. Measures may need to include the ability to remotely 'wipe' data from devices, should they be lost or stolen. Protecting data is more manageable if all staff use devices purchased and provided by the healthcare organization, rather than using their personal devices.

Healthcare organizations should implement real-time visibility of the devices people are using, so they can spot anomalous activity early and respond to it remotely if necessary. In addition, providers need to ensure that devices are not compromised by installing and updating industry standard antivirus and anti-malware protection, plus ensuring patches and updates to software are installed promptly.

Safe use of information systems

Healthcare providers must ensure the systems used to access information remain secure. Effective access controls, such as requiring strong and regularly changed passwords and two-step authentication, are recommended.
In addition, we strongly recommend organizations use virtual private networks (VPNs) to allow remote users to securely access your organization's IT resources. If VPNs are already in use, then organizations should ensure they are fully patched.

Systems only work as well as the staff using them. It's important that users only log onto systems when they are needed, log out afterwards, and do not leave unlocked devices unattended. Organizations need to educate staff not to share login details or passwords or make them easy to find.

How we support healthcare organizations in building digital trust

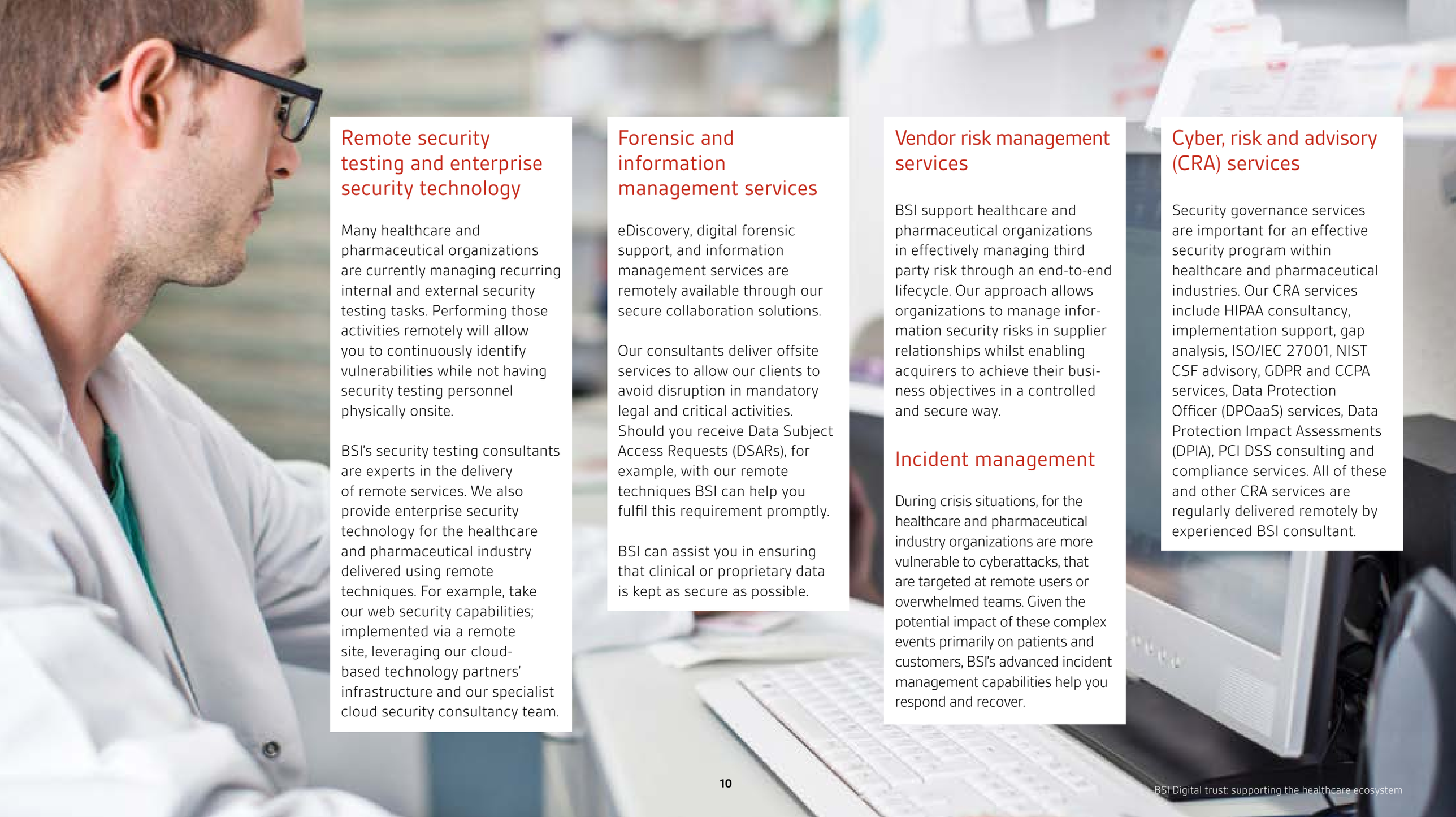
With the ever-changing landscape for the healthcare and pharmaceutical industries, from technological advancements, digitization and complex regulations, BSI can help organizations to adapt and embrace these changes.

As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions.

Whether it's certification, product testing, consultancy services or training and qualifying your people, we can help you achieve your goals of effective information security and data privacy resilience.

"Digital trust is about instilling confidence in an organization, that empowers the people, the systems and the technology to ensure their safety, security, compliance, privacy and ethical requirements."

Mark Brown, Global Managing Director, Digital Trust Consulting Services, BSI



Remote security testing and enterprise security technology

Many healthcare and pharmaceutical organizations are currently managing recurring internal and external security testing tasks. Performing those activities remotely will allow you to continuously identify vulnerabilities while not having security testing personnel physically onsite.

BSI's security testing consultants are experts in the delivery of remote services. We also provide enterprise security technology for the healthcare and pharmaceutical industry delivered using remote techniques. For example, take our web security capabilities; implemented via a remote site, leveraging our cloud-based technology partners' infrastructure and our specialist cloud security consultancy team.

Forensic and information management services

eDiscovery, digital forensic support, and information management services are remotely available through our secure collaboration solutions.

Our consultants deliver offsite services to allow our clients to avoid disruption in mandatory legal and critical activities. Should you receive Data Subject Access Requests (DSARs), for example, with our remote techniques BSI can help you fulfil this requirement promptly.

BSI can assist you in ensuring that clinical or proprietary data is kept as secure as possible.

Vendor risk management services

BSI support healthcare and pharmaceutical organizations in effectively managing third party risk through an end-to-end lifecycle. Our approach allows organizations to manage information security risks in supplier relationships whilst enabling acquirers to achieve their business objectives in a controlled and secure way.

Incident management

During crisis situations, for the healthcare and pharmaceutical industry organizations are more vulnerable to cyberattacks, that are targeted at remote users or overwhelmed teams. Given the potential impact of these complex events primarily on patients and customers, BSI's advanced incident management capabilities help you respond and recover.

Cyber, risk and advisory (CRA) services

Security governance services are important for an effective security program within healthcare and pharmaceutical industries. Our CRA services include HIPAA consultancy, implementation support, gap analysis, ISO/IEC 27001, NIST CSF advisory, GDPR and CCPA services, Data Protection Officer (DPOaaS) services, Data Protection Impact Assessments (DPIA), PCI DSS consulting and compliance services. All of these and other CRA services are regularly delivered remotely by experienced BSI consultant.

Conclusion

Healthcare and pharmaceutical providers are not technology companies – however, increasingly everything they do is underpinned by technology, and never more so than in today's digital world. Cybersecurity underpins safe patient care, the reputation of the healthcare organization, and the trust patients place in it. If the technology fails, the healthcare organization will fail too.

The vast strides made in recent times have allowed healthcare and pharmaceutical organizations globally to continue to operate. Protecting all aspects of healthcare information from theft, breaches or corruption will ensure that healthcare services can not only continue to function, but to thrive. Ensuring cybersecurity systems are in place, and staff are educated and supported to use them, is an essential part of healthcare management today.

Why BSI?

An independent body like BSI can provide a wide range of healthcare-focused cybersecurity support, from assessing your management systems to delivering certification or advisory support. We can assist with product and management systems certification across ISO 27799, ISO 13131 and ISO/IEC 27001 amongst other standards.

Learn more

We can test your IoMT device security. This testing involves penetrating and hacking into the device, as well as advice on operationalizing IoT security into managed services in conjunction with leading-edge, innovative technology alliance partners – **all to inspire trust in a more resilient world where we can resist threats.**

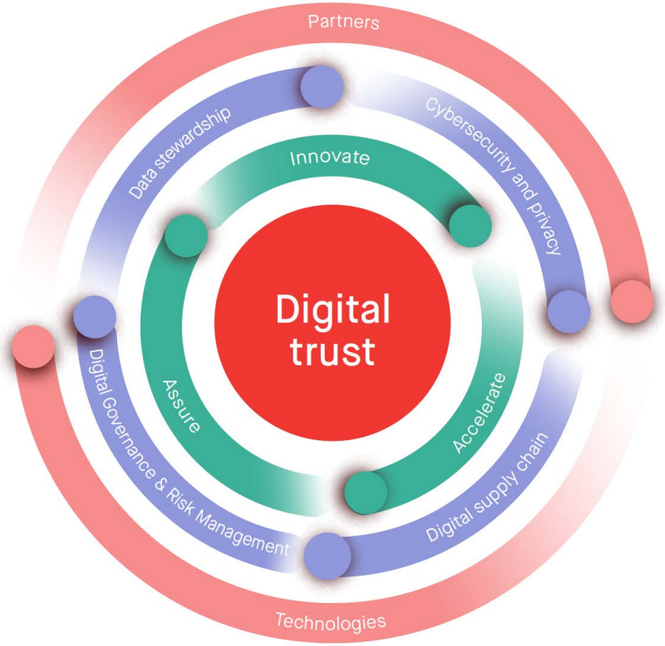
About BSI Digital trust

At BSI Digital trust, our global expertise enables our clients to better enhance their cyber resilience, protecting their critical information and IT infrastructure, people, and brand reputation.

We support organizations through our integrated portfolio of services including providing digital and cyber risk advisory, security testing services to clients, as well as looking at areas like data privacy, compliance and governance, as well as niche capabilities such as e-discovery and e-forensics.

Digital trust aggregates four subdomains with interlocking strategies, plans, and actions:

1. Cybersecurity and privacy
2. IT Governance and risk appetite
3. Data stewardship and AI ethics
4. Digital supply chain



"Digital trust is the confidence users have in the ability of people, technology and processes to create a secure digital world."

Mark Brown, Global Managing Director, Digital Trust Consulting Services, BSI

Get in touch

South Africa
Call: +27 0 12 004 0279
Email: bsi.za@bsigroup.com
Visit: bsigroup.com/en-ZA

Follow us on