bsi.

Supporting healthcare organizations in building cyber resilience

An insights paper

Introduction

The COVID-19 pandemic has evidenced the societal criticality of a fully functional healthcare and pharmaceutical ecosystem. Concurrently, it has also demonstrated the fragility of the healthcare network with the heavy reliance on digital healthcare. As many more staff are working from home, coupled with the rapid adoption of remote consultations evidencing a new era of telemedicine, numerous healthcare organizations around the world have experienced the havoc a cyber-attack can cause and the subsequent impact on wider society.

A prime recent example can be seen with Ireland's Health Service Executive (HSE), the country's public health and social services provider, where hackers brought parts of the health service to a halt through a targeted ransomware attack. This is not a standalone incident as Australia, New Zealand, Germany and the US in particular have seen a significant increase in attacks within public and private healthcare facilities. The very real threat of a cyber-attack leading to an organizational melt-down, and subsequently societal anarchy, in the middle of a pandemic now exists.

However, for many experiencing a halt in services due to malicious disruption, the inability to access services may only be the beginning. Hackers may also publish stolen sensitive mental health records online. There's the possibility of deliberate data corruption, for example by mixing up test results and even the temperature controls for freezers storing life-saving vaccines are susceptible to being hacked undermining confidence in the previously successful vaccination program.

Whilst the societal and organizational risks are high, some of the 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. Moreover, there is a wealth of advice and support to help organizations improve their cybersecurity posture which we will look at in more detail in this paper.

Author:

Mark Brown

Global Managing Director, Cybersecurity and Information Resilience, BSI

Mark joined BSI in February 2021 and is responsible for driving the growth of the Consulting Services business stream – Cybersecurity and Information Resilience – at a global level, harnessing a key focus on the Internet of Things (IoT) strategy and how BSI can help clients bridge their cybersecurity and data governance challenges.

Mark has over 20 years of expertise in cybersecurity, data privacy and business resilience consultancy. He has previously held leadership roles at Wipro Ltd., and Ernst & Young (EY), amongst others. He brings a wealth of knowledge including extensive proficiency on the Internet of Things (IoT) and the expanding cybersecurity marketplace having worked for Fortune 10 and Fortune 500 firms as Global CISO and Global CIO/CTO respectively. He has worked and provided services to clients across numerous sectors and industry verticals from Consumer Products, Retail/ eCommerce, Legal, Oil and Gas, Mining, Technology, Media, Manufacturing, IT and Real Estate.

mark.brown@bsigroup.com

bsigroup.com/cyber-uk

linkedin.com/in/markofsecurity

twitter.com/markofsecurity

Why the immediacy of cybersecurity in primary healthcare?

Cybersecurity, is defined by the UK's National Cyber Security Centre (NCSC) as 'how individuals and organizations reduce the risk of cyber-attack.' Cybersecurity should *'protect the devices we all use and the services we access from theft and damage' and 'prevent unauthorized access to the vast amounts of personal information we store on these devices and online'.*

For healthcare organizations, this means that all data stored digitally – everything from medical records to staff bank account details – is kept secure, so it can only be accessed, used or changed by those authorized to do so.

COVID-19 both raises the possible impact of a cyber-attack and increases the likelihood of it happening. With unprecedented demand on healthcare, the impact of service disruption caused by a cyber-attack is devastating. Acute medical services in particular are under strain, and there is no slack in the system to divert patients away from affected hospitals. In addition, the majority of healthcare is now reliant on digital technology. The cyber-criminal remains on the societal need for effective healthcare operations to prey on the sector through ransomware demands which are more often than not paid to resolve.

Cybercriminals have tried to take full advantage of the pandemic with Interpol reporting a significant uptick in phishing and ransomware attacks during the COVID-19 with many attacks focused on primary healthcare organizations.

Healthcare is particularly susceptible to phishing attacks with the aim of harvesting information, such as login details to systems holding valuable data, or bank details. This information is very often resold on the dark web for a fee.

An average stolen data set is worth about £20 (US$25) per record; clinical data can be worth up to £100 (US$140) per record. Healthcare data is more valuable to cybercriminals as unlike any other aspect of personal data, the healthcare records are permanent and not subject to easy change, whereas financial records once breached are terminated and replaced.

Adoption of remote and online working at speed significantly increases the risks by staff using their own devices (phones, tablets or laptops); working in new ways in potentially less secure environments; and using unfamiliar technologies such as teleconferencing for remote care provision.

In addition, moves beyond the clinical commissioning group structure of primary care towards new partnerships at local level will introduce new ways of working. Integrated care partnerships will bring together commissioner and provider bodies with local authorities and others to focus on population-level health – such as Infection Control during infectious disease outbreaks. This will inevitably mean more data sharing across organizations. While data sharing is vital to allow these partnerships to flourish, the sharing of unsecured data and reliance on potentially vulnerable information systems does expose gaps in cybersecurity which can be exploited by hostile actors or 'hackers', as they are more commonly referred to. Hackers can launch attacks by sending phishing emails or releasing code that exploits loopholes in software. The purpose is the same – to gain access to or disrupt data and systems.

"Healthcare data is more valuable to cybercriminals than ever. An average stolen data set is worth about £20 (US$25) per record; clinical data can be worth up to £100 (US$140) per record."

Reference - National Cyber Security Centre Annual Review 2020*

Supporting healthcare organizations in building cyber resilience
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email: cyber@bsigroup.com

*Available at: https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

What could a cybersecurity breach mean for healthcare providers?

A breach of cybersecurity means criminals can access, freeze, manipulate and publish data.

For a primary healthcare facility, this could include:

- blocking access to email, online appointment booking and triage systems, patient records, staff rotas and contact details
- manipulating or corrupting data, for example removing 'red flag' alerts from clinical records, changing test results
- publishing confidential clinical records

In 2017, the UK National Health Service (NHS) was infected by ransomware, malicious software which froze clinicians' access to the data, in the Wannacry attack. Affected users in Primary and Secondary care were unable to access patient records, online diagnostics, appointment booking systems and emails. The hackers issued a ransom demand, in an attempt to extort money to unlock the files. Since 2017, Wannacry type ransomware attacks have continued to evolve with Ryuk emerging as the most damaging in 2020.

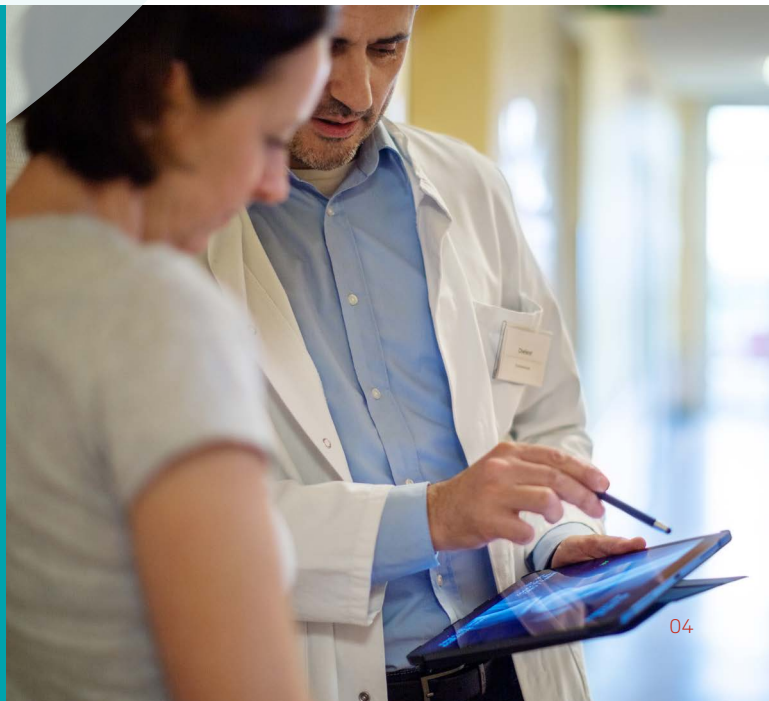
The NHS was not targeted specifically, this was a wholly opportunistic incident, but it did expose Primary and Secondary care as 'soft-targets' for such attacks. It was one of many organizations to fall victim of the attack, which exploited weaknesses in software operating systems, many of which were 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.

Dr Saira Ghafur, Digital Health Lead at the Institute of Global Health Innovation, Imperial College London, says: 'We've got a lot better [since 2017] in terms of phishing emails and educating staff and having systems in place to recognize them and filter them. But any cyber-attack in the middle of a pandemic would be absolutely catastrophic, if you had Wannacry hit a London trust or GP surgeries, when you are already struggling to provide good care [because of the impact of SARS-Cov-2].'

Healthcare industry reporting indicates that at least one death has already happened as a result of a ransomware attack as a German hospital recently had a ransomware attack and there was a patient on the way to the Emergency Department in an ambulance. This person was diverted to another hospital and they sadly died in the ambulance.

Today, the potential impact is even greater than 2017. 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.

> "...any cyber-attack in the middle of a pandemic would be absolutely catastrophic..."
>
> Dr Saira Ghafur, Digital Health Lead at the Institute of Global Health Innovation, Imperial College London



Targeted attacks

The UK NCSC reports an increasing trend for cybercriminals to target healthcare organizations specifically because they hold personally identifiable, sensitive information about patients. 'The NCSC has identified a new disturbing trend in ransomware attacks which sees attackers not only withholding access to the data but also threatening to publish it unless the ransom is paid,' said a NCSC spokesman.

In Finland in October 2020 an attack on a private company which runs psychotherapy services resulted in confidential treatment records of tens of thousands of patients being hacked. Patients were sent emails demanding money to prevent records of their confidential discussions with therapists being published online. Some records have been published, causing severe distress and a loss of trust. The incident has been blamed on lack of reliable encryption of data files stored by the company, evidencing the benefit of encryption of data at rest.

Increasing reliance on digital information increases the risk of data being corrupted for malicious purposes. 'It's all ways of hacking and attacking data,' says Dr Ghafur. 'If you rang up a hospital and said, 'every other blood result has been tampered with', what proof does the hospital have that it's not? And what is your back up, how would you test again, what does that mean for the samples you stored?' she asks. The possibility of tampering with test results underlines the potential harm that could be caused.

Furthermore, the integrity of data has become more and more important, and even more so for healthcare than the often-targeted financial services industry. If an adverse drug reaction for Penicillin is taken off the system, then the outcome for patients is much worse than not being able to access my bank account.

Dr Ghafur raises the possibility of other nightmare scenarios. Researchers in Israel last year demonstrated the ability to intercept digital images from medical scans and make changes which would change the diagnosis – for example adding or deleting signs of cancer by changing pixels on the scan. The researchers speculated that attackers could use this technology 'to sabotage research, commit insurance fraud, perform an act of terrorism, or even commit murder.'

It is estimated globally that circa three quarters 74% of the 2.6 million people who attend Emergency Departments each year require diagnostics, and that usually means digital imaging. 'When you consider that all imaging is digital in the NHS, if an organization loses its imaging department, it loses the ability to treat patients in the Emergency Department,' he says. He believes making clear the quantifiable impact of cybersecurity threats is important to ensure they are taken seriously.

This also introduces a new risk vector to healthcare, with the ever-increasing use of Internet of Things, which allows remote, digital control of systems such as fridges and freezers, could be another target. 'We've got these new vaccines coming on board, so how easy would it be if you had that dark mindset – which these people unfortunately do – to potentially hack into the thermometers for freezer or fridges that the vaccines are stored in?' asks Dr Ghafur. This is expanded further when considering the Internet of Medical Things (IoMT).

"The NCSC has identified a new disturbing trend in ransomware attacks which sees attackers not only withholding access to the data but also threatening to publish it unless the ransom is paid."

NCSC spokesman

The Internet of Medical Things (IoMT)

IoMT devices and data security

The Internet of Medical Devices (IoMT) is growing rapidly, so rapidly that it is being touted as the future of healthcare. The IoMT is an interconnected infrastructure of medical devices, software, monitoring devices, and data convergence systems and offers a variety of benefits, from remote monitoring to live time data feeds, to easing pressures on under-resourced hospitals and public health budgets, and potentially creating elastic capacity removing physical constraints. As technology pushes digital health in new directions, each new iteration brings both potential and challenges.

Growing IoMT connectivity presents a further nuance to the cybersecurity challenge. A major concern for the healthcare sector is the vulnerability of interconnected devices to external threats, usually in the form of viruses, hack-attacks, or denial of services ransomware. The stakes could scarcely be higher here – directly impacting patient health, safety or even mortality. Healthcare leaders must therefore ensure vital hospital facilities and power supplies can't fall into the wrong hands – not to mention control of smart medical devices and implants.

IoMT, Healthcare wearables and cybersecurity

Consumer wearables collect health related biometric and behavioural data:

- Exercise data
- Blood pressure
- Glucose levels
- Heart rate
- Sleep patterns
- Menstrual cycles

They also collect personal identifiable information:

- Date of birth
- Geolocation
- IP addresses
- Login details

These devices can expose users to privacy and security risks. Data is often synchronized to apps on other devices and is transmitted and stored in cloud-based platforms.

Risks

Malware
Activated by clicking fraudulent links triggering viruses, worms, trojans, spyware, etc. which can delete files and steal information.

Phishing
Deceptive emails or fake websites trick individuals into providing sensitive information, enabling access to personal and health-related data.

Ransomware
Software that encrypts data to prevent user access until a ransom is paid. Attackers can use blackmail – threatening to publish sensitive or valuable personal data.

Distributed Denial of Service attacks
Multiple computers or devices are compromised, then used to attack a target website, service, or app. The target system is bombarded with messages and connection

Manipulation of health data
Wearables are part of an ecosystem with health data being stored on devices, apps, linked phones and computers, and transmitted across Bluetooth and Wi-Fi to cloud-based platforms. Security weaknesses in any area can allow data to be accessed or stolen.

Measures to counteract threats

Secure the device and the digital infrastructure
Wearables must be secure by design and default. Default settings must be as secure as possible, and security or cryptographic primitives built into hardware and software. Manufacturers must manage device vulnerabilities throughout the product life and develop software patches to address them. Ecosystem and data chains must be secure and constantly monitored.

Clear and robust data privacy policies
Manufacturers need clear data privacy policies to ensure security and privacy of sensitive health data – not only to comply with data protection legislation but also to provide reassurance that user data are well-protected. The amount of personal identifiable information should be minimized by using unique account numbers and allowing pseudonyms.

Mitigation of cybersecurity risks

Many of the risks outlined above can be managed by basic cyber-hygiene. While nothing can guarantee that an attack won't happen, following the basics of cyber hygiene can substantially reduce the risk. Good cybersecurity means applying layers of security measures in case one fails. Indeed, by adopting a layered approach, organizations can make themselves a less attractive target to attackers and reduce the chances of an attack being successful.

Physical security

Healthcare providers need to ensure the physical security of devices used to process or store sensitive information, such as laptops, tablets and smartphones ensuring the following guidance is provided:

- Users need to be educated to lock devices away securely when not in use. 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.

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. It is vital for organizations 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. This is easier if all staff are using devices purchased and provided by the healthcare organization, rather than using their own 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 need be. In addition, providers need to ensure that devices themselves are not compromised, by installing and updating industry standard antivirus and anti-malware protection and ensuring patches and updates to software are installed promptly.

Safe use of information systems

Healthcare providers need to ensure the systems used to access information are kept secure. Effective access controls, such as requiring strong and regularly changed passwords and two-step authentication, are recommended. 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.

However, 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. Staff need to be educated not to share login details or passwords or make them easy to find.

Education is also important to help staff recognize phishing emails seeking access to information systems. Phishing is still a big way for cybercriminals to try to breach your organization and it is therefore important to educate your users in what an attack that tries to get hold of their credentials looks like, by providing some training or some sort of simulation tools that can catch people out – then people can learn from their experiences and that is really valuable.

"... by adopting a layered approach, organizations can make themselves a less attractive target to attackers and reduce the chances of an attack being successful."

Mark Brown, Global Managing Director, Cybersecurity and Information Resilience, BSI

Why BSI?

How BSI can help

An independent body like BSI can provide a wide range of support in Healthcare focused cybersecurity, ranging from assessing your management systems and providing either certification or advisory support. We can assist with product certification as well as management systems certification across ISO/IEC 27001, ISO/IEC 27701, and ISO 22301 standards.

We can test your IoMT device security, which involves penetrating and hacking into them, 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.

How we support healthcare organizations in building cyber resilience

With the ever-changing landscape for the healthcare industry, 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, and consultancy services or training and qualifying your people, we can help you achieve your goals of effective information security and data privacy resilience.

Remote security testing and enterprise security technology

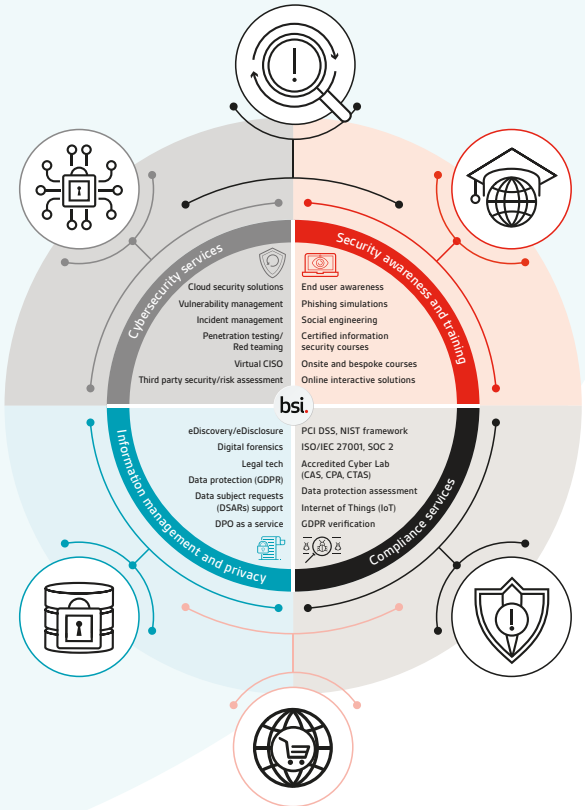
Many healthcare and pharmaceutical organizations are currently managing recurring internal and external security testing tasks. Performing those activities remotely will allow you to continuously identify vulnerabilities while not having security testing personnel physically onsite. BSI's security testing 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. Take our web security capabilities; implemented via a remote site, leveraging our cloud-based technology partners' infrastructure along with 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 a 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 cyber-attacks, 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.

Online training

Upskilling employees is a fundamental requirement in reducing the risks caused by human related cyberattacks such as phishing, which has seen a 400% increase within healthcare and pharmaceutical industry in the last year. Our SaaS based security awareness platform and virtual training courses can be designed and delivered remotely ensuring an enhanced client experience. Moreover, our tutor-led interactive learning courses can now bring the classroom to you.

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 consultants.

Supporting healthcare organizations in building cyber resilience
Call: +1 800 862 4977 (US) / +44 345 222 1711 (UK) / +353 1 210 1711 (EMEA)
Email: cyber@bsigroup.com

Disclaimer
BSI is an accredited Certification Body for Management System Certification and Product certification. No BSI Group company may provide management system consultancy or product consultancy that could be in breach of accreditation requirements. Clients who have received any form of management system consultancy or product consultancy from any BSI Group company are unable to have BSI certification services within a 2 year period following completion of consultancy.

Conclusion

Healthcare 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.

In the face of a global pandemic, the huge strides made in recent times have allowed healthcare organizations globally to continue to function. 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.

30,000

malicious emails were sent to the NHS in March and April 2020

6000%

increase in 'Phishing' attacks related to Covid in March and April 2020

51,910

signs of malicious activity were notified to the NHS by the end of August 2020

595

general practices were infected by the 2017 Wannacry attack

"Cybersecurity underpins safe patient care, the reputation of the healthcare organization, and the trust patients place in it."

Mark Brown, Global Managing Director, Cybersecurity and Information Resilience, BSI

References

National Cyber Security Centre Annual Review 2020. Available at: https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

NHS Improvement, Lessons learned review of the WannaCry Ransomware Cyber Attack, published February 2018.

Available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyberattack-

cio-review.pdf

National Cyber Security Centre What is Cyber Security?

Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

The Guardian, 'Shocking' hack of psychotherapy records in Finland affects thousands.

Available at: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

Y Mirsky et al, CT-GAN: Malicious tampering of 3D Medical Imagery using Deep Learning. Published in the 28th USENIX Security

Symposium (USENIX Security 2019). Available at: https://arxiv.org/pdf/1901.03597.pdf

Is primary care ready to switch to Telemedicine? Medscape UK, March 2020. Available at: https://www.medscape.com/viewarticle/927631

NHS Digital, Advice on using video consultation systems.

Available at: https://digital.nhs.uk/services/gp-it-futures-systems/approved-econsultation-systems

NHS England, Securing Excellence in Primary Care Digital Services.https://www.england.nhs.uk/wp-content/uploads/2019/10/gp-it-operating-model-v4-sept-2019.pdf

NCSC, About Cyber Essentials. Available at: https://www.ncsc.gov.uk/cyberessentials/overview

NCSC, Exercise in a Box toolkit. Available at: https://www.ncsc.gov.uk/information/exercise-in-a-box

NHS Digital, Data security and protection toolkit. Available at: https://www.dsptoolkit.nhs.uk/

Department for Health and Social Care, 10 Data Security Standards.
Available at: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-policy/

NHS X, Remote Working in Primary Care Guidance for GP Practices during COVID-19 Emergency Response. Available at: https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/C0165-remote-working-in-primarycare-

gp-practices-during-covid-19-v1.2.pdf

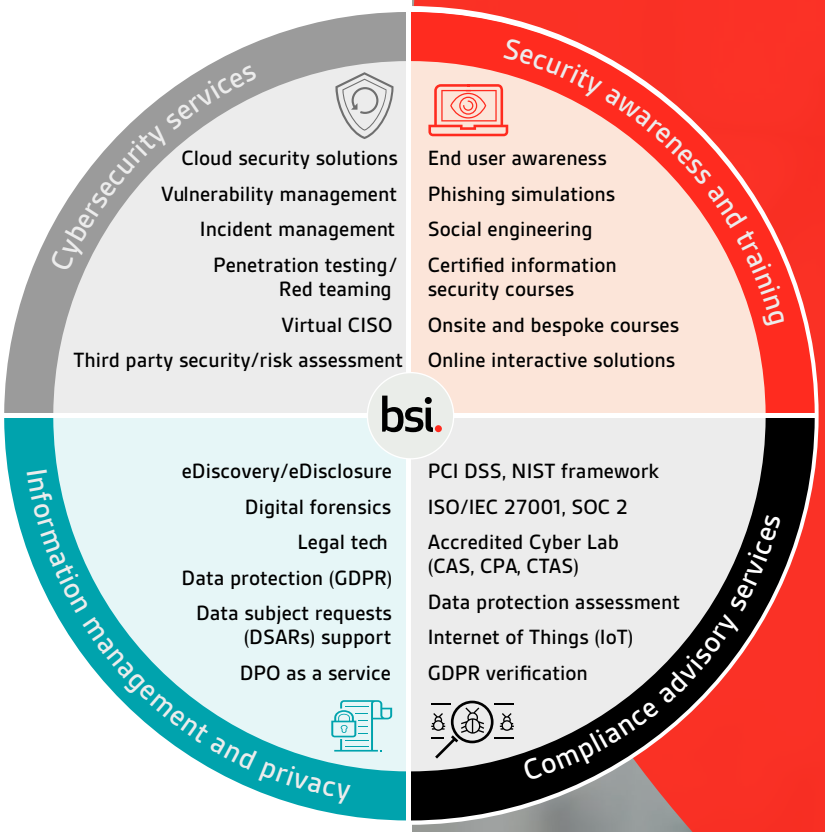
NHS X, Bring your own device policy. Available at: https://www.nhsx.nhs.uk/key-tools-and-info/procurement-frameworks/clinicalcommunications-procurement-framework/bring-your-own-device-policy/

International Standards Organisation, Information security management ISO/IEC 27001. Available at: https://www.iso.org/isoiec-27001-information-security.html

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. 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, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Services include:



Our expertise is accredited by:

Find out more

EMEA
Call: +353 1 210 1711
Email: cyber.ie@bsigroup.com
Visit: bsigroup.com/cyber-ie

UK
+44 345 222 1711
cyber@bsigroup.com
bsigroup.com/cyber-uk

US
+1 800 862 4977
cyber.us@bsigroup.com
bsigroup.com/cyber-us

bsi.

Subscribe to our newsletter

Follow us on