bsi.

Insights paper

Trust Series – Healthcare

Now is not the time for complacency on cybersecurity

How can the cost of a cyberattack be quantified during the Covid-19 Crisis?

The Covid-19 crisis has affected so many globally. It has put our healthcare services on the front line and stretched them to the limit. Maintaining capacity within these services to cope with the sheer volume of patients affected by the virus, is of critical importance and a matter of daily reporting across all media from top government officials.

Our hospitals, doctors' surgeries and all the organizations involved in their procurement and support are heavily dependent on technology. The security and resilience of that technology is critical to their ability to continue providing those services.

Serious ransomware-based outages typically take weeks to resolve and restore services. The consequences of such an attack at this time could be devastating

Attacks are on the increase

This crisis has brought out the best in so many and the positive power of the Internet to connect people when they cannot be together has been highlighted in ways never seen before. Unfortunately, malicious cyber actors seek to exploit the increased reliance associated with Covid-19 with related malware and phishing attacks increasing hugely in recent weeks.

Even more worryingly, hospitals in Spain have been targeted with coronavirus-themed phishing lures by attackers looking to disable their systems with Netwalker ransomware.

Ransomware

The type of malware that encrypts files on systems, add extensions to the attacked data and hold it "hostage" until the demanded ransom is paid – is also on the rise.

Phishing

The fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details – has also seen an exponential leap since the pandemic first appeared at the turn of the year. According to the NCSC[1] Advanced Persistent Threat (APT) groups and cybercriminals are targeting individuals, small and medium businesses and large organizations with Covid-19 related scams and phishing emails. Victims of the scams are directed to apparently legitimate web sites from which malicious software or viruses. This can be inadvertently downloaded by the user, infecting their machine and enabling the attackers to access or disrupt the systems and networks to which they are connected.

[1] National Cyber Security Centre (NCSC): Joint Advisory Covid-19 exploited by malicious cyber actors V1.pdf

Act now and be prepared

As always, preparedness and prevention are far better than remediation. Good cybersecurity practices could mean the difference between maximizing the healthcare resources we have to deal with the crisis or needlessly losing critical capacity through criminal activity.

Be aware – awareness at all levels of the organization is paramount for effective mitigation

The UK and US Security Agencies have issued guidance and advisories for individuals and organizations on Covid-19 related malicious cyber activity and urged the public to report related scams.

User awareness

Targeted and effective communication for staff and users at all levels is a key preventative measure. Ensure that your users are aware of the increase in Covid-19 based scams and they know what to do in the event of a breach or suspected breach.

Board level awareness

This is not a problem for the IT department. Ensure that key business stakeholders are aware of the cyber threats and involved in critical decisions.

Highly Reactive Environment

Healthcare IT professionals are under huge pressure to ensure that remote working can be supported

Normal processes and due diligence bypassed or ignored

- Downloading untrusted applications
- Procurement of services from untrusted sources
- Proliferation of Covid-19 based communications
  - News Updates | Announcements | Warnings | Memes
- Users not trained or accustomed to installing or using communication tech
- Proliferation of shadow IT
- Layoffs including IT Staff and freelancers with privileged access
  - JML processes not followed
  - Laid off staff disgruntlement
- Malicious cyber actors seeking to exploit situation
  - Phishing | Online Scams | Malware

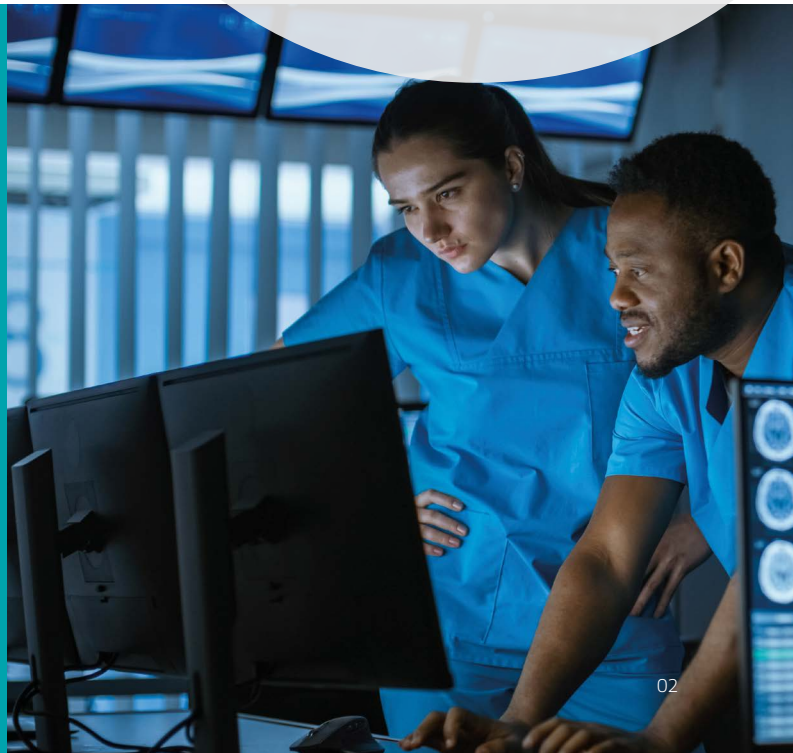
Practical Steps to Mitigate Threat

- ✓ Ensure that only trusted services and applications are used to support mobile communication and conferencing
- ✓ Ensure that they are securely deployed and configured
- ✓ Understand your key risks and use this understanding to set tactical priorities
- ✓ Targeted penetration testing of key systems including intelligence lead penetration testing can quickly identify key priorities
- ✓ Ensure that policies, processes and guidance are updated to support people working in new circumstances
- ✓ Ask for help. Resources are stretched and skills are in short supply.
- ✓ Incident readiness assessment to ensure that you are prepared to deal with an incident should it occur

Our trusted advisors are ready to support your cybersecurity challenges in the short, medium and long term. Call us now to discuss your cybersecurity needs with one of our experts:

Call: +1 800 862 4977 (US)
+44 345 222 1711 (UK)
+353 1 210 1711 (IE)

Email: cyber@bsigroup.com



Act now and be prepared

BSI consultants will work directly with your IT teams to share their findings immediately helping and supporting quick and effective mitigation

Many organizations have some expertise in a number of cybersecurity domains

BSI's teams of dedicated specialist cybersecurity experts ensure that our customers have the support they need when they need it across all cybersecurity domains

No organization is exempt from the threat. Not even the World Health Organization (WHO). According to Flavio Aggio, Chief Information Security Officer, reports that cyberattacks on it have doubled in recent weeks including an attempt to steal passwords belonging to WHO agency staff. (source: Reuters[2])

[2] Reuters.com (date accessed: 15/04/2020)

How do we help customers achieve trust

Trust is critical for all aspects of healthcare services. These services are increasingly provided on digital platforms making the cyber resilience of these services more important than ever.

BSI cybersecurity services support healthcare providers and their delivery partners by helping to address all cybersecurity challenges from the board level to supply chain. This also extends to system architecture design and penetration testing through to incident response and governance risk and compliance, our teams are highly qualified and experienced.

By providing flexible and pragmatic support, BSI's trusted advisors enable organizations, assuring their information resilience and building trust in the long term.

Trust Type

Intrinsic – an activity which provides confidence in the process applied by the supplier during the development of the product, service or system. **BSI's trusted advisors work with you to define and implement processes which are demonstrably and measurably secure.**

Extrinsic – an activity independent of the development environment which provides a level of trust in the product, service or system. **BSI can independently assess products and systems in a formal test lab environment to achieve information resilience under a number of schemes including the BSI kitemark and National Cyber Security Centre (NCSC) schemes.**

Implementation – any activity which provides confidence that the product, system or service has been correctly implemented. **We carry out in depth technical penetration testing of a wide range of technology implementations. Our Testing team is qualified to the highest industry standards including CREST and NCSC CHECK.**

Operational - the activities necessary to maintain the product, system or service's security functionality once it has entered operational use. **BSI's trusted advisors carry out cybersecurity assessments and audits of operational systems to identify cybersecurity weaknesses and offer pragmatic solutions.**

This level of trust instilled in our clients ensures that they can achieve the desired state of information resilience, meaning this can keep them, their business, people and reputation safe and secure for the long term, withstanding the test of time.

Cybersecurity Services

Robust, industry leading processes developed through expert engagement and training

Certification and validation by trusted body

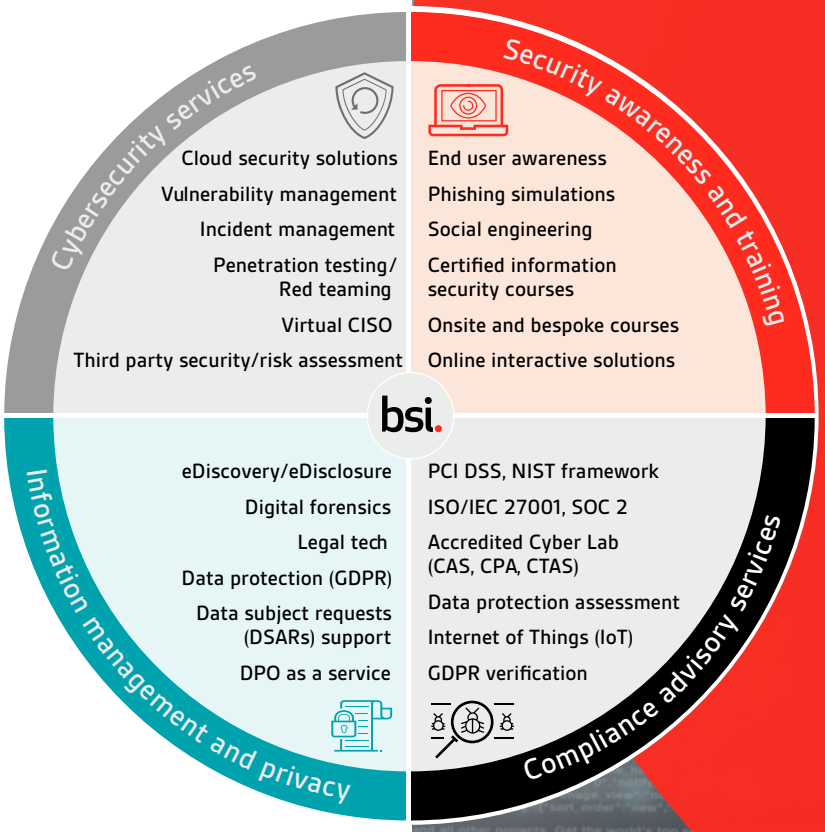
Systematic security management processes with surveillance and validation

Penetration testing and technical validation of effectiveness of security controls implemented

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 Digital Trust Services include:



Our expertise is accredited by:

Find out more

EMEA	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: digitaltrust.consulting.IE@bsigroup.com	digitaltrust.consulting@bsigroup.com	digitaltrust.consulting.US@bsigroup.com
Visit: bsigroup.com/digital-trust	bsigroup.com/digital-trust	bsigroup.com/digital-trust

bsi.

Subscribe to our newsletter

Follow us on