bsi.

Returning to work – post pandemic

Implications for cybersecurity and data governance

An insights paper

April 2021

Reopening the office
Implications for cybersecurity and data governance

One year on into the COVID-19 pandemic, most organizations have now adapted to the work from home (WFH) reality. Whilst many organizations are exploring new hybrid ways of working moving into the future, many others are beginning to encourage their employees to return to the office in some capacity.

Although the lure of getting back to what was familiar for so long may be enticing, the hybrid working set up of the last year has introduced new health and security challenges far beyond the use of face masks and the implementation of social distancing. In an increasingly connected world, the simple act of employees returning to their desks and reconnecting their machines to the office network may result in the creation of a wide range of security issues that can place your business at risk of a cyber-attack.

On the other hand, many organizations have now adopted a hybrid workplace where employees can work from home or from the office as suited to them. This increases the challenge of ensuring data is protected and information issecured.

As lockdowns globally ease and life begins to resemble what we once knew as normal working life, organizations need to ensure that these changes do not introduce more security risks. Human ingenuity and technology-based solutions can be used to support this change ensuring a safe and productive environment, regardless of the newfound set up.

Business continuity has been at the forefront of the pandemic, testing many organizations of all shapes and sizes, across all verticals, in most regions globally. However, the unforeseen demands put on employers' business continuity planning strategies has also provided organizations with the opportunity to customize, review, update and improve our response plans, ready for this next call to action.

As a key part of any organizations' reopening plans, it is vital that those responsible for cybersecurity and data governance within the company are involved from the outset to ensure that the correct protocols are adhered too and implemented to enable them to operate in a secure, safe, sustainable, trusted and resilient manner.

BSI is actively supporting organizations to plan and prepare employees to return to work post pandemic and to develop a sustainable methodology to working moving into the future. In this paper, we share five key areas that organizations need to consider when opening their offices again.

> "With offices reopening, organizations globally will need to introduce and implement new safety procedures, security technologies and data handling processes to ensure a safe, productive and cost-effective approach to the new hybrid work model."
>
> **Mark Brown, Global MD, Cybersecurity & Information Resilience, Consulting Services, BSI**

01
Physical security

The advent of widespread vaccinations globally has significantly reduced risk in many countries and therefore allowed society and business to reopen to a certain extent. However, organizations are now facing new challenges in relation to reopening their offices. Besides simple sanitation and one-way system changes, employers now also need to account for new norms when it comes to physical security practices. This is especially true where full-time workers are now working alongside 'hybrid' workers who split their working week both onsite and remotely.

Full time office workers

To ensure the safety of employees returning to the office at full or part-time capacities, organizations will have to monitor employee health and their movements effectively for contact tracing purposes. This may involve recording identities, activities, access times and durations, and health and personal data recording in order to provide them with physical access. Employers will now be responsible in managing new technologies including the introduction of more advanced contactless entry and exit systems (automated turnstiles/doors) and the use of mobile applications and QR codes to record testing information. BSI advises organizations to comprehensively test, analyse and secure any new technologies or systems put in place while concurrently ensuring that they are preserving individual privacy and minimizing risks to the business.

Remote workers

Physical access may not be a problem for the employees working remotely amidst the COVID-19 pandemic. However, employee identity must be taken into account considering vulnerable Virtual Private Networks (VPN), cloud adoption and a spike in hacking instances in work from home conditions. Since home networks are never going to be as secure as corporate networks, employers must support staff in strengthening boundaries. BSI encourages organizations to consider the implementation of security and phishing awareness training amongst all staff working remotely as a preventive measure to the currently exposed weaknesses of security infrastructures. Moreover, educating staff on how to effectively secure devices at home becomes an extra layer of defence and acts as an imitation of the corporate firewall.

Hybrid working model

The hybrid model will provide flexibility to the staggered return to the office. However, this will call for CIOs to revisit their practices scheduling and tracking employees' access to physical spaces in the office. On the other hand, controls such as pin pads or biometrics should be assessed, especially where direct contact is concerned.

Physical media

In returning to the office, organizations should ensure that a facility is provided for staff to either return or securely destroy any physical hard copy media or electronic storage devices that may have been in use during the work from home period. Also, to ensure a safe return, employees should ensure physical devices are clean and disinfected before introducing them to the office environment.

> "To ensure the safety of employees returning to the office at full or part-time capacities, organizations will have to monitor employee health and their movements effectively for contact tracing purposes."

Mark Brown, Global MD, Cybersecurity & Information Resilience, Consulting Services, BSI

02
Data protection and privacy

As employees who have been working from home begin returning to the office, employers must guarantee that the health and wellbeing of staff is prioritized, managed and monitored. Simultaneously, employers need to ensure that as they begin to collect personal data in this endeavour, they are respecting their obligations as data controllers, as well as the privacy rights of their employees.

Contact tracing

Recent guidance issued by the Data Protection Commission (DPC)[1], the Information Commissioner's Office (ICO)[2] in the UK and the Office of the Data Protection Commissioner (ODPC) in Ireland, states that personal data held in a contact log should generally not be processed by an employer for any other purpose besides facilitating the health service's official contact-tracing procedures and employers should avoid disclosing information relating to a particular employee's COVID-19 diagnosis to other employees. BSI recommends that from the outset, organizations should seek the advice of their Data Protection Officer (DPO) or a data protection consultant in relation to any changes in working practices and that any personal data should be retained only for as long as considered necessary for this purpose.

Onsite health check and employee health data

As employees return to the office, organizations will come into possession of medical information it may not have necessarily processed previously. This might include health check data, temperature check data, sanitization related records, sickness certificates and other COVID-19 related data. BSI recommends that employers conduct a Data Protection Impact Assessment (DPIA) in order to guarantee that the confidentiality and security of this personal data is ensured and that it is handled in line with privacy regulations.

Transparency

Transparency is a fundamental tenet of the GDPR and most country data protection regulation and organizations when demonstrating accountability and compliance with privacy regulations. BSI advises that employers explain the purpose, methodology and handling procedures related to the collection of any employee personal data. Any impacts that the pandemic may have concerning the processing of personal data will need to be notified to employees in compliance with GDPR and other legal transparency requirements and employers should look to gain explicit employee permission to gather specific data. GDPR and other privacy laws are not suspended as a result of COVID-19 and therefore if an organization receives a relevant request to access or erase their data, then they will need to comply and timeframes (e.g. 30 days). BSI can help organizations to simplify, automate and reduce response times to such requests through our Data Subject Access Report (DSAR) support services.

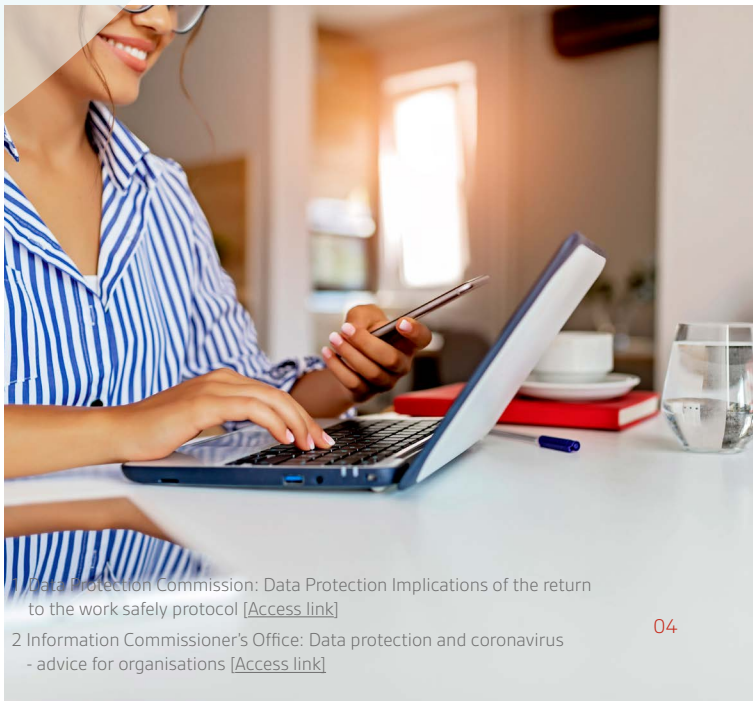
03
Asset management

When it comes to asset management, there are four primary areas organizations need to review when reopening premises. These include:

- **Data** – having a view of all of the data moving in and out of your organization, where it is stored, and how important it is
- **Hardware and software** – identifying all the hardware devices and software applications that are processing the data and ensuring that they are checked and reassessed
- **Facilities management** – extending beyond the hardware and software is critical, ensuring you have the appropriate security processes in place to protect the physical assets is essential
- **Your people** – ensuring that staff understand their roles in keeping the organization safe, you may need to invest in an updated end-user security awareness programme and test their vigilance

Organizations often turn to Bring Your Own Device (BYOD) policies for their mobile device capabilities. However, data breaches and other incidents can happen and can be expensive for the companies to remediate and recover from.

In the first phase of the COVID-19 response, organizations allowed many exceptions to asset management. However, organizations must now ensure that all non-inventoried assets are correctly logged and that BYOD positions are re-evaluated.



1 Data Protection Commission: Data Protection Implications of the return to the work safely protocol [Access link]

2 Information Commissioner's Office: Data protection and coronavirus - advice for organisations [Access link]

04
Business continuity and incident management

Business continuity readiness

Business continuity management and planning is the holistic process of identifying potential threats and impacts to an organization and building resilience through effective response plans.

The COVID-19 pandemic and crisis response allowed organizations to test their business continuity plan outside the controlled annual tabletop exercise, in potentially, the largest proof of concept of WFH initiation ever seen.

With organizations and staff slowly returning to the office, now is the ideal time to sit, review and improve your organization's business continuity management (BCM) strategies to ensure organizational resilience moving forward into the future.

Incident response readiness

Incident response management services can equip your organization with the necessary skills to proactively act or reactively respond in the event of a data breach, ransomware or some other form of attack or outage. Planning and implementing policies and procedures needed to respond to a data breach instantly are necessary to minimize business impact.

Specific industry sectors are being targeted by malicious actors. Advanced persistent threat (APT) groups are focusing on pharma and healthcare to steal intelligence, and organized crime is shifting to COVID-19 based "lures" to conduct phishing and malware based attacked.

Incident response represents the last line of defence should a successful attack materialize. Where incident response playbooks already exist, these should be reviewed to account for the likely scenario where staff may be returning on a phased basis to the office, meaning some are working from home and some may be in the office.

Steps in managing your incident management strategy should include:

- **Prepare** – planning and implementing disaster and incident dry-runs to give assurance that your systems work. Implementing a robust incident response programme means you can quickly react to a security incident, limiting the amount of damage an incident may have
- **Respond to** – providing real-time first responder services to respond when an attack has been identified
- **Follow up** – forensics and information management can help identify the extent of Personal Identifiable Information (PII) exposed in a breach. Investing in forensics and discovery software to analyse where the breach happened, when the breach happened and was data compromised is essential in line with data protection and privacy regulations

"Business continuity management and planning is the holistic process of identifying potential threats and impacts to an organization and building resilience through effective response plans."

Mark Brown, Global MD, Cybersecurity & Information Resilience, Consulting Services, BSI

05
Governance of management and operations

Security governance is the set of responsibilities and practices usually exercised by the Chief Information Security Officer (CISO) and information/cyber security teams with the aim of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Seven security governance essentials considerations are listed below:

- **Re-evaluate temporary measures**: With the need to work remotely some organizations have set up temporary measures such as Multi-factor Authentication (MFA) or temporary password expiry policies. These should be reassessed to determine if these are still required and/or could be improved
- **Revoke unnecessary licences systems**: With blurred lines between the home office and company office, new licences may have been downloaded and/or installed that may no longer be necessary in an office setting. Revisiting all applications and assessing their necessary as well as revoking any non-essential licences will not only save storage space but keep your systems secure.
- **Update antivirus**: Many antivirus programs may block certain actions and therefore may have been disabled. This can endanger the antivirus efficiency to stay updated. Scan your network for antivirus settings and ensure all users are running enterprise-grade antivirus with the latest definitions
- **Network security**: Remote access solutions should be configured to determine that they are secure, and that appropriate bandwidth is provisioned. Also, Remote Desktop Protocol (RDP) should be used to simplify IT maintenance tasks and allow staff access to their desktops over the internet, ensure that protocols are up to date and effectively working for all users.
- **Virtual Private Network (VPN)**: Many organizations have implemented "split tunnel" VPN, which allows certain sites to avoid centralized proxy inspection to save bandwidth. As many organizations likely made this decision during increased pressure scenarios, now is the time to re-evaluate whether this is the right approach, particularly if all web traffic was sent to a local internet break out, as opposed to being proxied. Options other than increasing network bandwidth are to use host-based proxy solutions, or to use a cloud-based solution such as Zscaler
- **Vulnerability management**: Many organizations struggle with patch management in a regular environment. In returning to the office, organizations should evaluate their patch posture, and where found wanting prioritisation patching. Organizations should also ensure that where new systems have been added to the network, that these are added to vulnerability scanning schedule and penetration tested by cybersecurity experts where they are to remain in place.
- **Risk management, policy and procedures update**: With returning to work, the information risk management strategy and methodology should be addressed at a strategic, tactical and operational level in order for the process to be effective and consistent across an organization. Risk registers should all be reassessed given the newly restructured threat and regulated landscape. So too, policies and procedures. An effective policy management system can mitigate risk by making policies more quickly accessible to staff and guiding decisions. During the reopening of offices and in line with national returning to work plans, keeping policy and procedures up to date will be essential.

"Security governance is the set of responsibilities and practices usually exercised by the Chief Information Security Officer (CISO) and information/cyber security teams with the aim of providing strategic direction"

Mark Brown, Global MD, Cybersecurity & Information Resilience, Consulting Services, BSI

How can BSI help?

At BSI, we have a large team of highly experienced, industry-leading consultants that will help to ensure that you and your business can welcome your employees and clients back onto your premises in a secure and sustainable manner.

With services ranging across the areas of security testing, security technologies, risk and compliance and data protection, our team possesses years of industry-relevant experience and expansive multiple sector expertise.
We provide you with cutting edge and leading insights to guarantee your organization's information resilience moving forward into the future.

Additional services

- Business continuity management
- Incident management
- End user awareness and phishing simulations
- Virtual Chief Information Office (vCISO)
- Certified cybersecurity courses

Author:

Mark Brown

Global MD, Cybersecurity & Information Resilience, Consulting Services, BSI

Mark joined BSI in February 2021 and is responsible for overall 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 more than 25 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

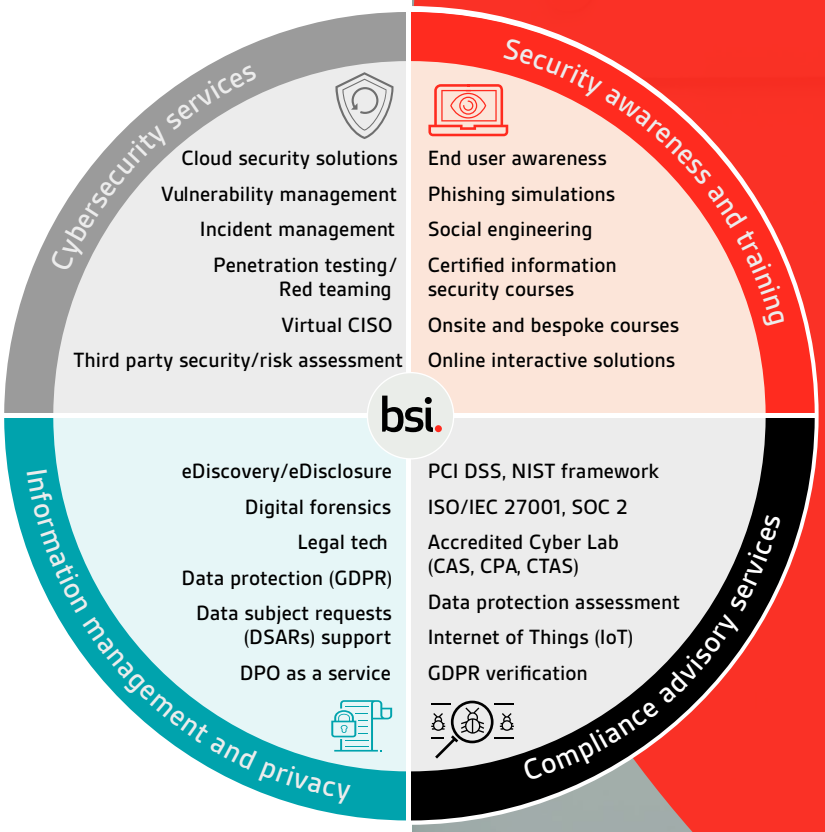
linkedin.com/in/markofsecurity

twitter.com/@markofsecurity

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