Reopening the office

Implications for cybersecurity and data governance

Insights paper

Reopening the office

Given the novel COVID-19 pandemic, organizations needed to act to ensure their operability in line with government lock down mandates and directives. This happened with relatively short notice, where they needed to mobilize – a paradigm shift – and enable effective working from home (WFH) solutions. Achieving effectiveness involved some of the basics like travel plans, ensuring a good wi-fi connection and managing confidential business information up to more advanced security measures like VPN connectivity, back-ups, and mobile device security.

In a matter of months, after starting to become accustomed to their "new normal" – constituted as a new way of working though many organizations had already robust WFH policies – we are seeing phased plans for the reopening of premises and the rebuilding of economies. There is a need for mindful action to ensure cybersecurity risks are managed and data privacy regulations are not violated.

Going forward, WFH and working from office (WFO) scenarios will need to be applied by organizations interchangeably, combining both forms will allow transparent transitions as local situations develop and national loosening of lockdown plans unravel.

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. The demand and requirements the situation has put on these business continuity planning strategies has provided the opportunity to customize, review, update and improve our response plans, ready for the next call to action.

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

BSI's consultants are helping organizations plan and prepare for reopening and develop a sustainable methodology to working. Here we share ten key areas that need to be considered when reacting to national and regional plans to reopen society and business.

01
Physical security

All organisations will be making modifications to business premises to enable the recommended standards for hygiene, sanitization and social distancing. In doing this, the impacts upon the security of information and data must be reviewed.

Physical access controls

Controls such as pin pads or biometrics should be assessed especially where direct contact is concerned. For organizations at higher risk e.g. larger footfalls where there is increased difficulty to manage end-to-end security, the implementation of non-contact inspectors might work in the short term with a view to more advanced contactless systems (automated turnstiles / doors) in the long term.

Employees identity

Unlike the work environment prior to COVID-19, organizations may need to collate data to enable contact tracing by authorities should this be required. This may involve recording of identities, movements, times and durations. Similarly. it will be important to consider local privacy legislation and to prepare an appropriate policy, declaring how this information will be managed.

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 media storage devices that may have been in use during the work from home period.

"Whilst introducing sanitization requirements and social distancing arrangements, consider impacts upon physical security of the premises."

02
Data protection and privacy

At the outset, organizations should seek the advice of their data protection officer / privacy officer (DPO) or a data protection consultant in relation to the impact of the COVID-19 pandemic and any changes in working practices. Some important highlights that will require the DPO's advice are considered below.

Desk/workstation changes

To ensure social distancing rules, some organizations will need to rethink desk positioning. During this activity, it is important to ensure that employees personal data are protected and that they are aware that any personal belongings left in the office prior to lockdown could be moved to a different location. This will help to demonstrate an organizations compliance with its transparency obligations under GDPR and / or CCPA.

Onsite health or temperature checks

Public health guidance and organizations will not want people to present for work if they are symptomatic of COVID-19. We may see employers choosing to take and record the temperature of employees before entering the work premises. Employers should consider whether there is a legal basis under the relevant jurisdictions law to process this data. Again, it is important to note that a person's temperature will be considered as a special category of data under the GDPR and can only be processed in compliance with Article 9, GDPR.

Contract tracing

Recent guidance issued by the Health Protection Surveillance Centre (HPSC)* stated for those contacts who have shared a closed space with a case for longer than two hours, a risk assessment should be undertaken taking into consideration the size of the room, ventilation and the distance from the case. This may include office and school settings and any sort of large conveyance. Accordingly, should a person become infected with the COVID-19, then these close contacts will be required to self-isolate, even if asymptomatic. Ergo, employers will be required to have a register on who is in the work premises at any given day to comply with guidance. However, employers should consider GDPR requirements before sharing this personal data with any third parties.

Employee health data

During COVID-19 it may be the case that your organization has come into possession of medical information which 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. Should this be the case, you must ensure that the confidentiality and security of this personal data is ensured, and that it is handled in line with privacy regulations. Health data under the GDPR is considered as a special category of personal data and has special status. Particularly, it should be noted that absences and sickness should be handled in compliance with Article 9, GDPR, whereby in the absence of a clear legal basis under legislation to process this data, it can only be processed with the explicit consent of the employee. If consent is the only legal basis that an employer can use it is important that they have a compliant consent management process and also that there are no negative impacts for the employee if they do not provide consent.

Data Protection Impact Assessments (DPIAs)

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. Prior to engaging in any new processing of personal data because of the pandemic, employers are required to conduct DPIAs as such processing will be likely to result in a high risk to the individuals.

Data Subject Requests

The General Data Protection Regulation (GDPR), under Article 15, gives individuals the right to request a copy of any of their personal data which are being 'processed' (i.e. used in any way) by 'controllers' (i.e. those who decide how and why data are processed), as well as other relevant information. These requests are often referred to as 'data subject access requests', or 'access requests'. 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) are still expected to be met.

Transparency

Transparency is a fundamental tenet of any organisation when demonstrating accountability and compliance with GDPR. i.e. the right to information in relation to processing of personal data. Accordingly, 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. Transparency requirements are detailed in Article 13 & 14, GDPR.

* www.hpsc.ie/a-z/respiratory/coronavirus/novelcoronavirus/guidance/contacttracingguidance

03
Asset management

Asset management

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

- **Data** – knowing all 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, need to be 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** – don't forget your people, your staff. 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

Device management and Bring Your Own Device (BYOD)

Organizations often turn to Bring Your Own Device policies (BYOD) 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. Organizations must ensure that all non-inventoried assets are correctly logged and that Bring Your Own Devices (BOYD) positions are re-evaluated.

04
Access control

Credentials

Multi-factor Authentication (MFA)

MFA is one of the most effective mechanisms for preventing a cyber-attack, many organizations enabled this feature during the move to home phase, and BSI suggest that this control is left in place and tuned appropriately if needs be.

Password expiry

To facilitate user remote working, many organizations also extended their password policy expirations rules. This temporary measure should be adequately risk assessed and evaluated to determine if it is still required or could be improved. Industry guidance is to use long passwords, which do not expire often. This approach is valid where an organization has the capability to monitor for indicators of a compromised account, where this is not the case, password expiry still holds some value.

Access to resources

To allow continuity of IT operations, companies may have exposed systems to the internet which were not published online previously. If the requirement remains in place to have remote access to these systems, those newly provisioned configurations should be risk assessed and their security posture should be verified through configuration review, scanning and penetration testing.

"Multi-factor Authentication (MFA) is one of the most effective mechanisms for preventing a cyber-attack, many organizations enabled this feature during the move to home phase, and BSI suggest that this control is left in place and tuned appropriately if needs be."

05
Network security

Remote access

Remote access capabilities are still relevant and will be required to ensure that remote staff are able to manage their operations. Remote access solutions should be configured to determine that they are secure and that appropriate bandwidth is provisioned. Ensure that the remote working and business continuity plans learnings are applied in case lock down national plans need to be altered and restrictions are re-established, should another spike in COVID-19 infections present itself.

Network services

Remote Desktop Protocol (RDP)

RDP is used to simplify IT maintenance tasks and allow staff access to their desktops over the internet. RDP is one of the protocols targeted by nefarious actors. Interfaces accessible through RDP are often exposed to systems where passwords can be easily deciphered or the server in question is unpatched and exploitable.

Exposed RDP numbers have increased exponentially since the beginning of the pandemic and companies were forced to deploy more RDP systems online, increasing the attack surface for hackers.

Virtual Private Network (VPN)

The mass adoption of video conferencing has meant that organizations have suffered bandwidth constraints in "backhauling" web traffic to their datacentres to be proxied. To combat this, 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.

06
Operations security

Configuration management

Organizations need to review any bespoke IT configurations necessitated during the work from home period and whether they are still required and/or impact negatively on the return to the office environment.

For example, a configuration change may have required anti-malware updates to be made directly to an employee's device from the provider as opposed to from a centrally managed in-house server. Organisations should make a determination whether this is still optimal for the return to the office. The same considerations and determination should be made for patching, WSUS, SCCM etc.

Capacity management

Allowing adequate bandwidth and remote capabilities licensing was at the core of the COVID-19 response. Organizations should verify if the newly required capacities are in line with their demands. Revaluating the organization's capacity demand, in a self-provisioning cloud ecosystem, could support cost saving efforts that are now at the core of COVID-19 response strategies.

"Organizations need to re-evaluate any configurations they made during the work from home period to ensure that they are still the most effective."

07
Vulnerability management

Patching

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. Microsoft had several significant vulnerability remediation cycles, which certainly should not be overlooked. These included remediations for Remote Code Execution vulnerabilities being actively exploited in the wild.

Legacy systems

It is also likely the case that given Microsoft's recent sunsetting of Windows 7 and Server 2008, many organizations who had been prioritising their removal may have been side-lined, and indeed forced to use these devices to facilitate remote working. Efforts to deprecate Windows 7 and Server 2008 should recommence immediately to ensure that organizations are not facing ongoing exposure to threats resulting from *unsupported vendor operating systems.

Vulnerability scanning and pen testing

Organization should 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.

08
Business continuity

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. The need to evacuate offices and work from home at relatively short notice, enabled live testing of business continuity plans (BCPs) for organizations fortunate to have them.

Moreover, now is the time to sit, review and improve business continuity management (BCM) strategies, refining the plans ensure that their initiation will be even more effective when called upon again.

"Organizations should ensure that where new systems have been added to the network, that these are added to the vulnerability scanning schedule and security tested where they are to remain in place."

*It is acknowledged that ESU Extended Security Updates are available for some varieties of Server 2008 and Windows 7 so this risk may not apply equally to all.

09
Incident management

Incident response readiness

Incident response management services can equip you 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 implement 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 – in addition to developing an incident response policy in an organization, providing real-time first responder services are need 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.

10
Security governance

As offices reopen, security governance is as important as ever.

Security governance is the set of responsibilities and practices exercised by information and cybersecurity 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.

Given the recent developments, many organizations should be taking proactive steps to ensure that their security controls directly support their objectives for the business. Integrating both the physical security, as expressed earlier in this paper, combined with cybersecurity is an essential element of a return to work strategy. By the combination of security governance and risk management, in line with physical security, this can give organization an advantage and better protection for their cybersecurity, data governance, privacy management and staff and stakeholders

Risk management, policy and procedures update

Establishing a robust information risk management framework allows you to prioritize resources to address the issues which present a significant risk to your organization. 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.

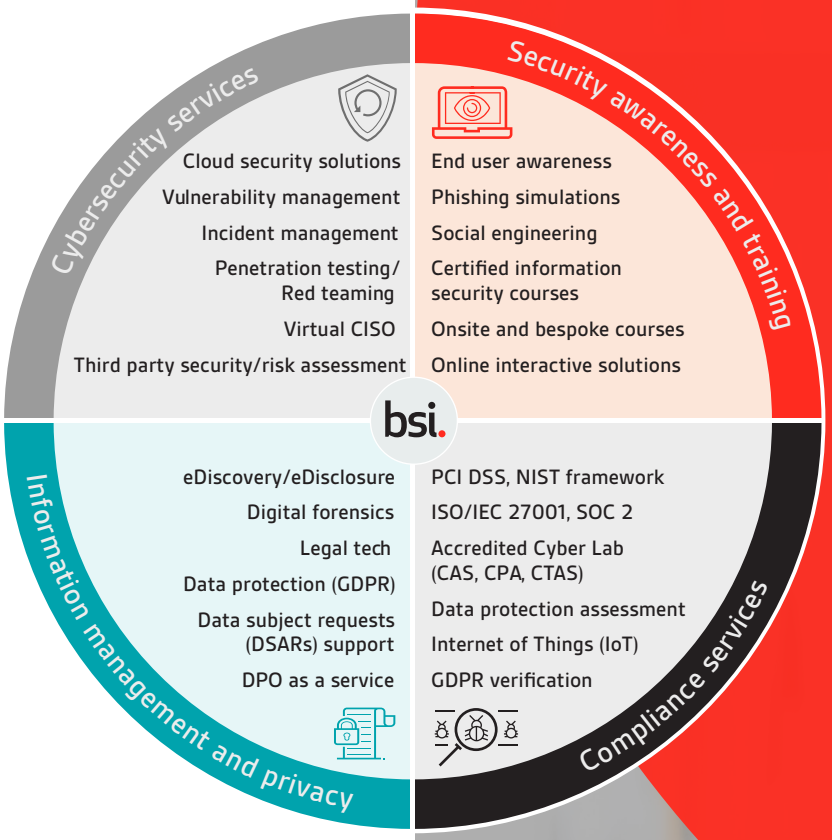
Risk registers should all be reassessed given the newly restructured threat and regulated landscape. Updating the risk register is an ongoing process and updates can occur at any time.

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.

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, and consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Consultancy Services include:



Our expertise is accredited by:

CREST · PCI Security Standards Council QUALIFIED SECURITY ASSESSOR · CYBER ESSENTIALS · CREST STAR · CHECK IT Health Check Service

Find out more

IE/International	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: cyber.ie@bsigroup.com	cyber@bsigroup.com	cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-ie	bsigroup.com/cyber-uk	bsigroup.com/cyber-us

bsi.