Reopening the office

Implications for cybersecurity and data governance

Five steps that organizations need to consider when opening their offices again

01 Physical Security

Account for new norms where there are fully remote and office workers along with the hybrid model of workers who split their workweek onsite and remote with a security perspective. Identify new technology, policies and actions around data protection, employee safety and access to facilities and data

02 Data Protection and Privacy

Employers must guarantee that the health and wellbeing of staff is prioritised, managed whether as a collective or individually. Contact tracing systems, onsite health check and employee data health are only a few examples of new requirements the 'new normal' has requested by organizations. Ensuring transparency and efficient storage of this data, in line with GDPR and other privacy law is critical

03 Asset Management

Organizations need to ensure that not only people, but data and systems are kept safe. Revisiting, updating or even implementing new policies and procedures that reflect the new guidelines is critical. BSI also recommends that organizations revisit their policies with their employees ensuring that staff is aware of business security needs avoids unintentionally placing the organization at risk through Bring Your Own Device (BYOD), unauthorized or unsecure applications and/or use of external USB's and peripheral devices

04 Business Continuity and Incident Management

BSI suggests that organizations review and improve business continuity management (BCM) strategies, refining the plans ensure that their initiation will be even more effective when called upon again. Patching is a challenge even for an information resilient organization. In returning to the office, organizations must evaluate their patch posture, and where found wanting prioritization patching

05 Governance of Management and Operations

BSI recommends that organizations re-evaluate temporary measures and licence systems used while working from home. Organizations should look to update employee antivirus and network security protocols and ensure systems are running with the latest definitions. Also, organizations 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

bsi.

Subscribe to our newsletter

Follow us on

Find out more

EMEA
Call: +353 1 210 1711
Email: digitaltrust.consulting.IE@bsigroup.com
Visit: bsigroup.com/digital-trust

UK
+44 345 222 1711
digitaltrust.consulting@bsigroup.com
bsigroup.com/digital-trust

US
+1 800 862 4977
digitaltrust.consulting.US@bsigroup.com
bsigroup.com/digital-trust