Learn the Lessons of 2021

Factsheet 50

The past 22 months have proved to be very challenging for every firm with some coping better than others. Firms have had to learn fast what they need to do and what not to do. The trick now is to learn the lessons of 2021 to herald in a better and brighter future for 2022.

Business continuity plans have had to be re-worked and cyber security has needed more booster jabs to keep abreast, let alone ahead of the threats. Investment in stronger business continuity plans and cyber security awareness training is gathering momentum to become more the norm in future. By investing in these things now, firms can develop a stronger and more secure business platform, both in the office and for home workers, for the benefit of employees and customers alike. With vaccines in place firms can invest in their future with greater confidence.

Throughout the many lockdowns most firms have learned that whilst office-based security maybe solid, home working security needs tightening up along with investment in better laptops, microphones and webcams and other similar equipment that we now recognise as part of the essential home working kit. At the same time employees need smoother access to the firm's office software systems, whilst adhering to and practicing office-based password control regimes.

Cyber criminals took advantage of the lockdowns by increasing phishing and malware campaigns aimed squarely at the vulnerabilities of home workers' personal computers. Firms have learned a lot from this and are beefing-up security methods at home to ensure that office style security is also always in the home office.

Regulators such as the ICO (Information Commissioner's Office) that have in the past made some allowances for the consequences of Covid 19 are no longer making them.

Accreditations like the Cyber Essentials Certificate and ISO 27001 are more popular than ever and are helping firms make office style security work at home offices as well. Investment is also going into better and longer-term planning of home security with more firms now carrying out home risk assessments, where possible risks are identified and solved or mitigated.

Some firms are experimenting with internal evaluations where monthly meetings are arranged, on Zoom, Microsoft Teams, or in the office to discuss what might have changed and or needs changing. This and any other aspects concerning access to office software and systems and cyber and data security can each be reviewed. This is particularly relevant in regulated markets where strict compliance is essential.

It is even worth considering subscribing to CREST-accredited training to improve security awareness of employees working from home. The Bureau will be happy to introduce you to CREST-accredited trainers *(Council of Registered Ethical Security Testers*) for which we have many contacts.

For more information about home-worker security investment
Phone: 01342 301325
Email: thebureau@the-bureau.co.uk