CEP Magazine - October 2020

Compliance in a work-from-home environment

By Robert Bond

Robert Bond (robert.bond@bristows.com) is Partner & Notary Public at Bristows LLP in London, UK.

The lockdown that was imposed during the COVID-19 pandemic has changed forever the way in which many of us work, and remote access to the office infrastructure and working from home may well be the new normal. However, in the first few weeks of lockdown, many of us were working from home in circumstances that were never anticipated by management—and also without the appropriate technical and organizational structures to manage the information and personal data that we were processing. Now we need to ensure that we manage our obligations regarding data protection, confidentiality, and information security if working from home and from the office have to sit side by side.

Regulatory compliance

Many regulated organizations in the financial and insurance sectors have had difficulty adjusting to working from home, as it makes it harder to supervise traders and staff, monitor for market abuse, and protect client confidentiality. Professions where transactions require identity and authentication to be face-to-face have struggled to adapt to "self-distancing" and also to comply with laws that were created in an age of paper, pen, and ink.

Technology may provide some of the solutions, such as remote monitoring of the use by staff of devices and communication channels, as well as electronic signatures and virtual meetings for documents and authorizations, but these require a reassessment of regulation, risk, and trust.

Information security

In the US, research suggests that successfully changing the culture or attitudes of staff is influenced by the behaviors and communications of senior management.[1] When leaders make cybersecurity a priority and firmly instill it in messages to employees, it sends a very strong signal to the team and also makes it a priority for staff.

The report says, "Here are three things executives can do today to build and reinforce a culture of cybersecurity in their organizations:

1. "**Make cybersecurity a personal priority and 'walk the talk'**: Simple actions like making sure to not click on emails or open links without checking if they are real are examples of cybersecurity hygiene everyone needs to follow."
2. "**Bring cybersecurity into the light**: It's important for leaders to make cybersecurity a personal priority, but it's also important to talk about it often with the organization. To establish a culture of cybersecurity for the whole organization, senior leaders must let everyone know that they are making cybersecurity a personal priority."
3. "**Give extra support to your digital colleagues**: Meet with security and technology teams regularly to learn

> and participate in business impact discussions. Listen to their immediate concerns and needs and provide a way to increase support....Perhaps create cross-functional task forces to address these issues immediately so the business impact is minimized."

In the UK, the National Cyber Security Centre (NCSC) has produced guidance[2] for businesses on how to prepare the organization and staff for working from home, including the use of two-factor authentication for login and the requirement for businesses to produce how-to guidance and webinars to help staff with issues of remote access and the use of conferencing and video services. The NCSC guidance also addresses the need to alert staff to email scams and social engineering as more access is made to online services across a number of devices.

From an information security and cybersecurity point of view, the increased use of social media and the internet give rise to risks surrounding social engineering, phishing, ransomware attacks, and the like; again, guidance needs to be given to staff around awareness of these issues.

Finally, the business needs to consider how it can improve physical and technical security at home for its staff as well as the management of confidential information, including, in particular, manual records and print. While in the office environment, there is usually a control around the disposal of paper and confidential documents, and while it may be harder to manage this within the home environment, the liability still remains.