



Spotlight on data security:

Seven tactics to prepare your firm for hybrid office and home working

The scale of the global health emergency forced legal firms to implement remote working almost overnight. Many businesses had no alternative but to take security risks that were undesirable in other circumstances. Now is the time to devise a stable model for the future. Part of that means updating data security practices and re-establishing effective control over company data, cyber threat and fraud detection.

To help you on this journey, we have delved into the experiences of our customers in the legal sector and devised seven data security tactics for a successful transition to the new reality of a hybrid home and office workforce.

1 | **The basics**
Encryption protects endpoints such as laptops, tablets, smartphones, and digital voice recorders, as well as data during transmission. It's an essential element to conceal identifiable information from cybercriminals. When searching for a management tool that supports document creation and billing hours, for example, consider the combination of hardware devices and business applications that feature multiple layers of encryption to create a secure end-to-end path for safe transfer and sharing of data. This will give you a secure central workflow to handle back-office admin task delegation that supports remote team working and virtual collaboration between lawyers and support staff.

2 | **Agile workforce**
The rise of today's agile workforce, with staff using company-issued or BYOD smartphones and tablets, only stresses the importance of encryption. A firm's data protection policy must cover mobile-specific security features such as real-time data encryption and using virtual private networks (VPN) for Wi-Fi connection to prevent these devices from becoming points of failure. PIN or biometric-protected devices, role-based permissions for business applications, and password complexity requirements should also be used to maintain data security. The best remote working devices and applications are the ones that not only allow the staff to remain productive from anywhere but also integrate or are compatible with these types of security functionalities.

3

Innovation and security

Artificial intelligence is changing the way people produce and access information. Speech recognition and the understanding of language by software are key to the future of information management. Modern document creation platforms integrate speech recognition to proactively maximise team capacity. They provide access to a centralised view of all admin tasks via desktop or mobile. This means that a team of lawyers, for instance, can send tasks to a secure workflow system and check the status of work at any time, allowing them to better communicate with their clients; while office administrators make use of speech recognition to accelerate work completion and make the most of resource capacity. These systems can be on premises or through the Cloud and have built-in strong security functionalities that protect data at rest and in transit.

4

Cloud enablement

Superior security is one of the major reasons for the growth in cloud-stored data. Because cloud services typically employ more complex security methods than local servers, they provide an added level of protection. Updates to improve security and performance of business applications are executed regularly so there is no need to dedicate staff to track system maintenance, since upgrades happen automatically. Files are backed up and can be accessed by the firm's personnel from anywhere on any device. The cloud has also proven to be an affordable route for smaller legal firms to access disaster recovery without a large up-front investment. The model offers a predictable payment schedule, becoming part of operational expenditure.

5

Security standardization

Consistency in security procedures and requirements complements the technological aspects of any organisation's security posture. Without formalized standards and consistent adherence enforcement of those standards, your firm may be left vulnerable by ad-hoc processes or practices that are not robust enough to shield against cyber-attacks. Consistency must also extend to regular updates of hardware and business applications latest versions. These products evolve to support high standards, regulatory requirements and enhanced security systems and protocols in order to improve threat detection and better protect your data.

6

Workaround vs. designed for purpose

The rush to turn entire workforces to remote working may have driven many firms to adopt workarounds due to a lack of time or knowledge. Sending confidential work to a free file hosting service might address a need to transfer data between staff in different locations, but it can cause a mammoth headache for someone else in the firm who has to deal with a potential fallout of a data breach caused by information being exposed to cyber-attacks. Design for purpose systems better protect your data and are more efficient and cost effective in the long run. Voice-controlled document creation platforms cater for remote working by allowing lawyers to send work to a central flow, where they are automatically routed to the right admin staff and can be tracked through to completion, while adhering to confidentiality requirements.

7

Employee empowerment

Finally, risk can never be eliminated, only mitigated; and there isn't a silver bullet solution that will make an organisation compliant with regulations. That's because regulations have technical, administrative, management and human components. No matter how secure technologies are, employees are still the key to maintaining data privacy and confidentiality. Due to the Coronavirus pandemic, many firms – which once had a clear-desk office policy – were faced with staff handling confidential data while working from home. The pandemic, however, has also shown that staff are agile, pragmatic, and have adapted. Equipping teams with regularly updated training and education tools, along with adherence requirements, gives them ownership in safeguarding sensitive information.

Philips Dictation is the global driving force in speech technology innovations for over 60 years. Our products enable busy professionals to work more productively by creating and sharing documents from anywhere. Our speech-to-text solutions deliver dictation and transcription flow management, automated document generation through speech recognition, mobility via smartphone applications, and data security through encrypted solutions. For more information please visit www.philips.com/speech.