PHILIPS

Dictation

Cyber-security tips **for legal professionals**

eBook

www.philips.com/speech
info.apac@speech.com

Legal industry is one of the most vulnerable industries in Australia when it comes to cyber risk. In the Decoding Cybersecurity: Cause and Effect Survey conducted by LexisNexis in 2019, among the 60% of legal practitioners surveyed, more than 85% confirmed the need to update their cyber security measures.

In the modern technological era, it becomes challenging to stay from internet of things and the worldwide web due to ease of connectivity and the information hub it has become. Like many other industries; lawyers, practice managers, administrators and others in the legal sector is reliant on technology as it provides easy file access across multiple platforms, better connectivity among peers and professionals, freeing up time from repetitive tasks and facilitate workflow efficiency. On the flipside, in an increasingly digitized world cybersecurity attacks and security breaches are always causes of concerns.

Here are 4 ways legal firms can take appropriate measures to protect themselves from these threats.

Software as a service (Saas) option

SaaS is trending more these days, and while it might sound like a new revolutionary concept it has been around for some time now. The idea behind this concept is that firms don't have to purchase servers and applications software in-house but rather create a sophisticated virtual workflow environment between their authors and transcriptionists. On the SaaS model, firms benefit from a robust workflow software without incurring large investments. Instead of a large upfront cost the payment is made monthly. It allows firms to have full control of their budget and the number of employees with access to confidential information.

Cost and control aside, SaaS model also provide other benefits. As operating systems evolve, it ensures that the workflow software remains compatible without disrupting work leading to unbillable hours. There's nothing worse than dictations piling up because the computer's operating system is not supporting the software. Software upgrades are necessary to protect data from unknown threats and help safeguard valuable information. An upgrade is also a medium for the content creators to fix security loopholes, offer new features, incorporate latest technology trends and make improvements to performance issues.

There's nothing worse than dictations piling up because the computer's operating system is not supporting the software.

Encryption function for highest security

Most cloud based systems do not provide the additional layer of security unlike a computer which is protected by a firewall, when connected to a local network. It only requires the username and password to access the cloud system. Multi-factor authentication provides another a layer of security to reduce the security risk. However, it's also possible to go one step ahead to restrict unauthorized access by encrypting data.

While choosing a speech-to-text software solution, it's important to take security into consideration. To guarantee the maximum protection of files in the cloud, real-time encryption is the highest security standard available. End-to-end double encryption which involves encrypting dictations during recording, while sending and saving those safely in the cloud, ensures against unauthorised intrusion. Some cloud services even provide optional data storage plans for back-up, in case of loss of data.

Bring your own device policy

For busy professionals like lawyers, they are given the freedom to use their own devices like a smartphone, tablet and other smaller connected devices while being out and about. This allows them to be on top of their game, either dictating their cases on a smartphone app, managing their correspondences or taking notes, no matter where they are working from. It's not uncommon to have variety of apps in the devices, paid or unpaid. When apps are downloaded from unrecognized sources, information stored in the app or any other devices connected through the cloud becomes susceptible to security breaches. It's not just exposure of photos and emails, but sensitive information like bank details or client information.

Bring your own device policy can be an outstanding way to be mobile, facilitating convenience by working anytime from anywhere and quite often allowing a smooth integration into existing workflow; but it's important to maintain the same security protocol as one breech can cause exponential damage to intellectual assets.

One device at-a-time plan

It might sound unreasonable, but cyber-attacks can take place due to human negligence. A lost or unattended device without proper protection measure or multiple users' usage on one device or license can be a realistic threat to security. To protect against all internal and external threats, it's better to extend the reach of data security and confidentiality to individual user level. This will also allow data tracing and user accountability for data safety. But to err is human nature so it's unequivocal to have measures in the software solution that will lockout the device after a certain time to avoid unwarranted access.

Data leakage or cyber-attack is any firm's worst nightmares come true but in this time and age of digital innovations and technology, it's also essential to make the right use of automation to facilitate growth and productivity by increasing accuracy and driving efficiencies. Given the sensitivity of data and high risk of cyber-attacks in legal industry, it is vital to have proper security policies in place and selecting the right solution provider that supports the safety policies.

To learn more on advanced and secured speech-to-text solutions, visit our website or email us at info.apac@speech.com.