Staying ahead of the data security challenge

Despite increased awareness and more sophisticated security measures, the numbers of reported data breaches continue to grow, with high profile incidents frequently gracing the headlines. The legal sector is not sheltered from these risks. In fact, the confidential nature of data held by law firms makes the legal sector a natural target. The immense financial and reputational impact is clear. In 2012 the estimated cost per company reporting a data breach stood at £3.5 million.

The modern law firm wants to embrace advanced technologies, utilise cloud services and enable flexible working practices through remote document management systems. However, these pressures have multiplied the type and complexity of possible data loss routes making countermeasures difficult to develop.

With this in mind, law firms need to be prepared to defend themselves on a variety of different fronts. A data loss incident may be the result of malicious activities originating from an external or internal source; or occur accidentally as a result of an employee security breach. Furthermore, popular mediums, such as social networking sites and instant messenger, provide new channels for data loss, whilst the increased use of corporate and BYOD smartphones and tablets capable of storing and accessing large volumes of data remotely have further altered the threat landscape.

In this context, the adoption of new technologies and work practices require organisations to re-think the data security controls required to minimise risk and exposure. Add to these considerations the additional dimension of increasing pressures on law firms to comply with national and international regulations, including DPA, SRA and EU data protection directive, these challenges are surely enough to put any DLP strategy to the test.

Data loss prevention (DLP) solutions have evolved over time in response to these changing circumstances. In the early stages, network security technologies were deployed to protect data from external threats, such as viruses and unauthorised access. Following this, there was a drive towards end-point security technologies to protect the data stored on PCs, laptops and mobile devices by deploying data encryption techniques.

However, individual end-point measures alone have become limited and there is a need for information-centric security technologies. The aim of the latest DLP solutions is to protect an organisation's critical data wherever it exists by identifying sensitive data at rest (in storage), in use (during an operation) or in motion (transmission across a network). Law firms' intent on staying ahead of the curve and maintaining their competitive edge, must embrace the new data security reality and diverge from traditional data protection measures.

Gartner recently coined the phrase “content aware DLP” to describe a set of technologies able to classify information content within an object, such as a file, email, data packet or application; and dynamically apply a policy, for example, reporting, logging, classifying, relocating, tagging and encrypting data throughout the entire data life cycle.

Whilst DLP solutions can be a powerful tool in preventing data loss incidents and aiding in an organisations desire to be compliant with regulation and legislation, many businesses are struggling to effectively implement these sophisticated solution. Comsec has designed a methodology for assisting law firms implement DLP strategies based on best practices and international standards.

With Comsec’s exclusive access to cutting edge technology and our world class consulting services, we can effectively manage the risks associated with data loss through file-centric data security, comprehensive access management processes and intelligence-led cyber solutions providing pre-emptive threat analysis.