the barrister

The largest independent magazine for Barristers practising in the UK

The importance of cyber response strategies in the legal sect

In January 2017, Lloyds Banking Group fell victim to a huge cyber-attack. Hackers operating overseas managed to get into the UK-based company's system and cripple it through several denial of service (DDoS) attacks, which prevented its customers from gaining full access to their accounts for more than two days.

No customers experienced any financial loss as a result of the attack, but the story resulted in a barrage of negative headlines aimed in Lloyds' direction that undoubtedly damaged its reputation. What's more, it proved that absolutely no business is safe when it comes to cyber-attacks; not even the systems of one of the biggest banking groups in the entire world could withstand the attack.

This is just one of many cyber-attack stories that have appeared in the news recently. The number of instances has been increasing steadily over the last few years — UK businesses suffered an average of 230,000 cyber-attacks in 2016 alone — which is in turn driven by an increase in the proliferation and sophistication of each one. With IT systems of all shapes and sizes coming under attack, no business can truly consider itself safe.

This is particularly true of those within the legal sector. Whether a barrister or solicitor, the confidential and high-profile nature of the work means that they are particularly desirable targets for hackers and cyber-attackers.

It used to be the case that businesses took a more relaxed approach to cyber-security. The issue would rarely cross the mind of a typical IT manager until a cyber-attack actually presented itself, at which point it's usually too late to do anything about it. However, with the frequency and severity of cyber-attacks continuing to increase, it's imperative that all barristers and legal companies ensure that their approach to cyber-security is proactive instead of reactive.

On a wider scale, businesses have already started taking heed of this warning. In 2015, companies across the UK doubled their cyber-security budgets, while the IDC anticipates that by 2020 organisations globally will be investing an astronomical £101.2 billion in order to keep themselves protected.

With so much at stake, it's essential that businesses respond to cyber-attacks in the appropriate way. This is why every business needs a **cyber response strategy** — a pre-determined plan that all employees are required to follow in the event of a cyber-attack.

What should a cyber response strategy include?

Importantly, cyber response strategies should not be a matter of 'copy and paste': each one needs to be tailor-made according to the specific working nature of the business. Therefore, for barrister chambers and other areas of the legal sector, these strategies need to be well planned.

The first step when developing a cyber response plan is to map out every likely cyber-threat that your business could be faced with, whether it's a DDoS attack, ransomware, theft or a data breach. You then need to consider working styles. From a barrister's perspective, take into account the fact that the job involves regular travel to various courts and offices across the UK and beyond, the transport of sensitive data using a range of devices from laptops to USB keys, and the frequent need to exchange information with their clerk. This expands the geographical range in which an attack could be experienced.

Once this has been laid out, businesses need to identify their most critical assets and make sure it's clear where they are all located. They then need to look at each of those assets and outline exactly what risks would be posed if those assets were to be seized or leaked during a cyber-attack. This is another process that can be extremely time-consuming for those who have high quantities or valuable or confidential assets, but it's a process that must be carried out properly if the cyber response strategy is to prove effective when it matters most.

How is the plan put into practice?

Once you've identified all the risks, outlined potential situations where a cyber-attack could occur and translated it into a cyber response strategy, it can be easy to put it to one side and forget about it. As soon as a cyber-attack occurs, however, the business will need to refer to the strategy immediately, and so it needs to be easily accessible to the right people.

As soon as a cyber-attack hits, barristers need to consult the strategy and follow these four useful steps:

- **Identify the incident** — the first step is always to identify the nature of the attack, and this can usually be achieved through monitoring, cyber intelligence, looking through log alerts and evaluating any threat analytics. For barristers, the threat is more likely to come in the form of an attempted data breach than, say, a DDoS attack, due to the confidential nature of their assets.
- **Define the impact** —It's also important at this stage to identify what aspects of the business have been affected, what assets have been stolen and the timescale of the attack itself.
- **Communications** – keeping all staff in the chambers coordinated during a cyber-attack is critical. The remedial work undertaken by individuals often complicates the overall efforts to address the problem. A clear communication plan using various mediums (SMS, email, voice) is critical. The instructions provided will be strongly influenced by the nature of the attack.
- **Gather the data** — once the business has an understanding of the incident, it's essential to collate all of this information for reference. Contacting the relevant authorities and gathering any evidence that could prove useful further down the line is vital.
- **Commence recovery** — this is the stage at which remediation must be carried out appropriately, and it can take some time depending on the severity of the attack. This could involve anything from resetting passwords on employees' systems to enhancing and improving the entire security infrastructure of the business.
- **Review** – once the immediate thread is addressed, look back at your process to see if improvements could be made. What parts of the process didn't not work as expected? How could subsequent risks be reduced?

Conclusion

Due to the work it deals with on a regular basis and the desirability of hackers getting their hands on it, the legal fraternity may be at a higher risk. No chambers can afford to be complacent, and each must have a pre-determined cyber response strategy that covers any and every possible eventuality. Whether they draft this up independently or collaboratively with a team of cyber-security experts, it's essential aspect of business in the 21st century.

Link to the original article:
http://www.barristermagazine.com/the-importance-of-cyber-response-strategies-in-the-legal-sector/