MAY 2017

LPM

LEGAL PRACTICE MANAGEMENT

THE ONLY MAGAZINE FOR LAW FIRM MANAGERS

Sodium Chlorid
Injection USP
500 mL
EACH 100 mL
pH 5.0 (4.5 TO 7.0) mEq/L SODIUM 154 CHLORIDE
OSMOLARITY 308 mOsmol/L (CALC) STERILE
NONPYROGENIC SINGLE DOSE CONTAINER ADDITIVES MAY BE
INCOMPATIBLE CONSULT WITH PHARMACIST IF AVAILABLE
WHEN INTRODUCING ADDITIVES USE ASEPTIC TECHNIQUE
THOROUGHLY DO NOT STORE DOSAGE INTRAVENOUS
DIRECTED BY A PHYSICIAN SEE DIRECTIONS
SQUEEZE AND INSPECT INNER BAG WHICH MAINTAINS
STERILITY DISCARD IF LEAKS ARE FOUND MUST NOT BE
IN SERIES CONNECTIONS DO NOT USE UNLESS SOLUTION
CLEAR Rx ONLY STORE UNIT IN MOISTURE BARRIER
OVERWRAP AT ROOM TEMPERATURE (25°C/77°F)
TO USE AVOID EXCESSIVE HEAT SEE INSERT

LAW FIRM PROFILE

How MLP Law boosted business support to aid growth

BOOK REVIEW

Stepien Lake's practice director delves into Robots in Law

Can PI survive?

Will the government's personal injury reforms kill road traffic accident firms?

BUSINESS INFORMATION FOR EVERYONE IN PRACTICE MANAGEMENT

CLOUD NINE SECURITY

Nigel Redwood, CEO at Nasstar, on the changing cybersecurity landscape and how firms can prepare

Law firms are embracing a tech-led world and becoming more efficient, cost-effective and competitive in the process – but there's a dark side to digital advantage. Cybercriminals are lurking at firms' digital gates and finding ever more sophisticated ways of breaking through.

Nigel Redwood, CEO at Nasstar, says law firms are particularly attractive targets to cybercriminals because they hold large amounts of money and, perhaps more importantly, a cornucopia of valuable sensitive data.

The big problem, he says, is that SME law firm managers often don't think their firms are targets because of their size.

"LPM's 2017 Legal IT landscapes report showed that on a 'threat scale' of zero to 10, SME firms ranked cyberattack at 5.2. But they need to realise that the threat is much greater and should be ranked at least nine."

Redwood says that SME firms can make themselves more secure by acknowledging the threat, building up their security resource and outsourcing IT to a provider with a high-quality security service.

"Nasstar, for example, employs 190 technical engineers who work constantly to adapt to an ever-changing technical landscape. A firm's IT department juggles multiple responsibilities – such as keeping the lights on and finding ways to make the firm more agile – and don't necessarily have the technical resource or know-how to keep their environment safe."

But just because a firm's IT infrastructure is managed, he adds, doesn't mean it's completely protected against attack. If firms want the best possible chance against cyberattackers, they need the right procedures in place and a certain standard of staff training.

"Technology is important but so is awareness. GCHQ says technology can prevent 20% of breaches but it's people that stop the other 80%. That's why firms should be investing in a cybersecurity certification that gives them an understanding of how to buttress information security."

SERVICED CERTIFICATION

The problem with managed IT infrastructures, says Redwood, is they can give firms a false sense of total security.

"Managed IT providers invest heavily in security but tech can only protect businesses to a certain extent. Cybercriminals see staff as the soft underbelly of a business – they're your digital gatekeepers and need to be trained to recognise friend from foe."

He adds that as law firms' staff become increasingly mobile, firms also need to prepare for threats outside the office.

"One of our clients recently suffered a man-in-the-middle attack – where a criminal sets up a wireless network with the same name as a nearby coffee shop, waits for someone to connect and intercepts their data."

But firms can equip their staff with the basic tools to question their environment and keep the business safe by becoming certified in the government's Cyber Essentials scheme or the international IT security standard ISO27001.

"The route to these certifications, however, can be long, complex and expensive – which is why Nasstar has developed its certification-as-a-service solution."

This solution, he says, helps firm adopt the critical criteria and compliance requirements to pass the ISO27001 and Cyber Essentials life cycle. When a firm isn't compliant, Nasstar sends certification specialists to recommend solutions to help it demonstrate advanced security.

"These certifications will help the business become cyber-ready, but they also show clients that the firm meets a certain standard of security," says Redwood.

He adds that cyber certification is an excellent step in the right direction, but there are lots of exercises firms can undertake to keep their staff on their toes.

"Once staff have been trained it's important to not let them become complacent and keep them aware that the criminals are still out there. Firms could, for example, send out white-hat attacks to see who falls for them and then inform them of their mistake." If firms are to test their defences, managed IT providers such as Nasstar are on hand to give advice and help keep staff up to date with their cyber training.

> *"Cybercriminals see staff as the soft underbelly of a business – they're your digital gatekeepers and need to be trained to recognise friend from foe."*

CLOUD FORTRESS

Redwood says that as well as having knowledgeable and cautious gatekeepers, firms should make sure their digital walls are thick, tough and regularly renovated to keep up with constantly evolving digital threats.

"But keeping up to date with the cybercrime landscape and preparing appropriately can put a significant strain on firms that want to focus on clients and cases. Fortunately, managed IT providers can help firms adapt, but they need to choose one that has information security at the top of its agenda."

According to Redwood, the technical side of information security is changing so rapidly that even a managed IT provider with a state-of-the-art data centre would find it difficult to keep up – which is why Nasstar teamed up with cyberdefence company Falanx Cyber Defence to stay on top of cybercrime.

"Falanx works hand in hand with our technical teams and deploys agents to every single server in our seven datacentres. These agents log events which are then analysed by a machine-learning system to identify trends. By doing that we can identify that a client has logged a meeting with someone in Telford, and if they suddenly log into a PC in France then the alarm is raised."

Nasstar also has a professional services team that works with clients to ensure their own systems are secure.

"In that team, we've got what we call an ethical hacker, who will try and hack our customer systems. Wherever there's a web-facing environment for clients, for example, they will try to enter the business there. That way we can go back to the client and tell them where their weaknesses are and what we can do to fix them."

Though cybercriminals pose more of a threat to the legal industry than ever, SME firms can prepare and protect themselves. By testing systems and becoming cyber certified, firms can give their staff the tools and knowledge they need to protect the business. But the time and resources required to constantly buttress the business's information security can bring significant strain – so fortunately, managed IT providers, such as Nasstar, can provide the expertise firms need to make the process as easy as possible. LPM