SPONSORED EDITORIAL

HEED THE WANNACRY WARNING

NATASHA RAWLEY, THE FILE QUEEN

> *One of the biggest issues with cybercrime is how vulnerable smaller businesses are. It can have a devastating impact on turnover and reputation.*

As I sit down on a train to write this column, the world has woken to one of the biggest IT nightmares ever experienced. The NHS was struck by a hugely destructive ransomware attack, 'WannCry', and over 300,000 computers across 150 countries were affected by the malware strike (although these are just the reported ones).

This has been devastating to organisations throughout the world. I recall two years ago that I attended a data protection conference hosted by some awesome American IT wizards. The warning on that day to attendees was: "Malware can and will get you."

At the time, I found this strapline very threatening and thought it was a tad dramatic in my British v US manner. But reflecting over the last two years, I know people who have been personally impacted by ransomware, and have seen the threat grow at an astonishing rate. Businesses now face the prospect of cyberattack every day – and whether we like it or not, ransomware is now one of every single company's daily operational threats.

But one of the biggest issues with cybercrime is how vulnerable smaller businesses are. It can have a devastating impact on turnover while they're frozen out of data, and also on their reputation. In one of the companies I know, ransomware had been sitting on their systems for eight weeks before it was activated. This meant that not only was their network infected, but eight weeks of backups were also infected. I'm happy to say they did start trading again, but the loss to turnover was catastrophic.

So, what can small businesses do? I'm not an IT expert, but I am a believer in learning from experiences so we can make better decisions in the future.

These attacks are all about vulnerabilities, and here are the hot tips I learned at my data protection conference:

First, backup, backup and backup – yes, that's three times. Never rely on a single form of backup. Many of our clients back up to the cloud but then also employ document and data storage companies like us to rotate data tapes/portable hard drives daily, weekly or monthly. This acts as another safety net and also a great disaster recovery tool.

Then, make sure all your IT updates are done. The NHS cyberattack reportedly happened because of security flaws in an old Microsoft OS version. Microsoft released an update yet PCs had not been updated – leaving them vulnerable.

Use virus protection software. Many people use virus protection solutions, but one of the biggest issues is making sure scans are regularly run on each PC and that the software itself is consistently updated. Automate this.

And finally, test your vulnerabilities. One of our clients hires a specialist company to attack their network and test it. Many companies do this, but the great thing about this company is they send test emails to all members of the team that contain fake viruses and worms. The team members who open them are then placed onto cybersecurity awareness courses – as staff are a business's key weak point. This is a great tool.

Bye for now, LPM readers – in my next column we will be looking at steps to tackling the EU's GDPR, which is less than a year away. LPM

ABOUT

ADDS
Saving firms from paper hell
Contact Natasha on:
0800 328 0272
www.archivestorage.net
@Thefilequeen

Archive
Document
Data
Storage