ALWAYS HAVE A BACKUP PLAN

An Uncomfortable Truth

Ransomware is a hot topic right now. The recent WannaCry malware attack shows just how vulnerable organisations are to cybercrime. Designed to take your corporate data hostage, ransomware is a growing problem, and no one is safe. Globally, it's estimated that ransomware affects another company every 40 seconds. Ransomware attacks doubled during 2016. Overall, cybercrime cost UK firms £34.1bn last year. The statistics are alarming, but also hide an uncomfortable truth. Many organisations fail to take the most basic precautions to protect themselves.

Upgrades, Patches and Version Control

The WannaCry attack revealed just how many firms are still running old, unpatched, unsupported versions of Microsoft Windows. In 2016, it was found over 60% of UK SMBs placed themselves at needless risk by continuing to use old, unsecured versions of Internet Explorer (IE). Certainly, there is no such thing as 100% security. However, you are not powerless. You can mitigate the risks of becoming a victim. You can also reduce the impact of an attack, should the worse happen. Of course, malware isn't the only threat you face. Security breaches and data

loss happen for a variety of reasons such as human error, accidental damage and theft. Nevertheless, the consequences can be just as catastrophic.

Human Error

While the multitude of threats from malware and hackers might cause sleepless nights, the real danger to your corporate data is probably closer to home. According to the Information Commissioner's Office (ICO), human error remains the main cause of data breaches in the UK. Staff need much better training and greater awareness of everything from opening suspicious emails to using unsecured file-sharing apps. We will take a closer look at user awareness and training in a later post.

Anti-Virus

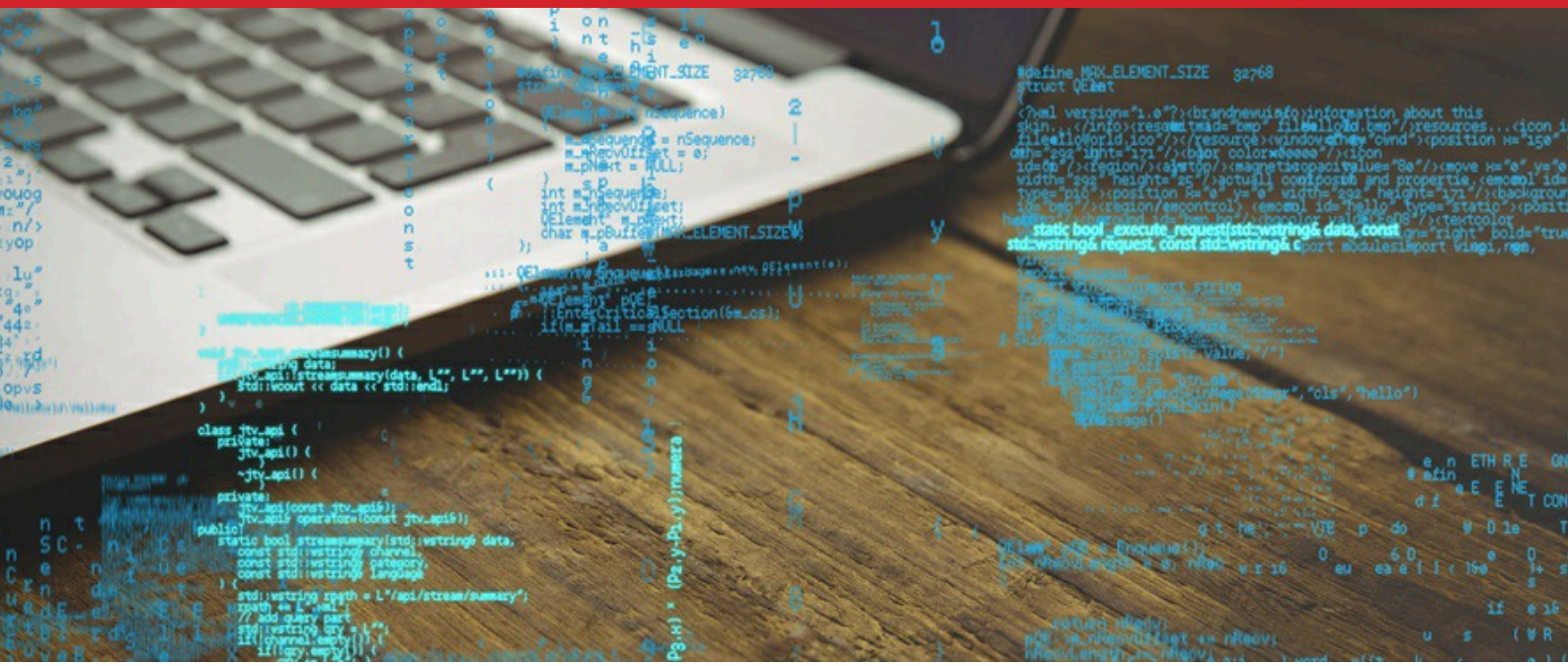
Although WannaCry caught many firms off guard and caused a nice media storm, the fact is that most enterprise-grade anti-virus applications, such as Webroot, can stop malware at the point of attack. The point here is having robust endpoint security policies and oversight of all the devices that connect to your network. How's your BYOD policies? Do you know which employees use personal devices on your network? Naturally, anti-virus is only as good as the latest update, the consistency of its deployment, and your firm having an integrated approach to network security.

Advanced Security

In the popular video game, Resident Evil the shadowy Umbrella Corporation creates a highly advanced, self-aware and homicidal security system called the Red Queen. The Red Queen adapts, evolves and anticipates new security threats, making her a formidable adversary. Today's advanced security systems might not be up to Red Queen standards yet, thank goodness, but they are evolving fast. Solutions such as Cisco's Umbrella gives organisations greater visibility and control of all Internet connected devices, over all ports, even when the users are off the corporate network. Umbrella does some clever stuff, learning from Internet activity to spot the telltale signs of a potential attack before it ever happens. Advanced network security is a big subject, which is why we have dedicated an entire post to the subject - see our blog/news pages.

Backup Plans

Regrettably, bad things happen, even to the most prepared organisations. Human error, hardware



failures, malware attacks, power outages and natural disasters. When the worst happens it pays to have a backup plan. That means multiple secure backups of all your company data, so everything is recoverable at a moment's notice.

Amazingly, over a third of organisations do not backup their valuable data*. Of the remainder, many firms have outdated or unreliable backup systems. The result being critical data is either corrupt, out of date or missing when it's needed most. Eliminating ransomware, for example, will require you wipe your systems. So, you'll need a company wide backup plan to quickly recover from the attack. The more frequent the backups, the less data is lost.

Strategy

Whatever your industry, data backup, archiving and recovery are critically important. You must develop a clear strategy. First, you will want to think about just how much data you're going to generate, it's probably a lot more than you would imagine. On the plus side, the costs of storage have fallen dramatically.

Redundancy

Next, you need to plan for redundancy. What happens if you backup fails? An on-premise server can instantly restore lost or corrupt data to the local network, but not if the building burns down, floods or collapses due to an earthquake. Then you will be glad of your Cloud backup. It means you can find a temporary office, recover your data and be back in business.

Compliance

You will certainly want to think about your legal and regulatory obligations around data storage, backup and recovery. Highly regulated industries, for example, have rules around data handling, retention, disposal and auditing. Not all data is created equal, so you might want to adopt different backup and retention policies for business critical and non-critical data.

Remote Workers

Over 30% of a company's data resides locally, on PCs, laptops and mobile devices. However, laptops are vulnerable to theft, damage, human error, mechanical failure and malware. Adopting an automated, secure Cloud backup ensures the integrity of your data, wherever it resides, even outside the corporate firewall, making it the perfect solution for remote workers.

Cloud-to-Cloud

Finally, some firms rely heavily on Cloud-based applications such as Office 365 and Salesforce. Certainly, these services are highly resilient and secure. However, many Cloud-based applications have limited data retention periods, which is no good if you are a regulated industry that must retain every email and document for 7 years. Some vendors offer very limited liability when it comes to compensating you for lost, stolen or corrupt data. Only you know the true value of your data to your business. Of course, having all your data reside with one vendor gives them a lot of power and makes it harder for you to go elsewhere. Having a backup gives you some leverage, and makes migrating to another service easier.

The reputational and financial cost of a high-profile cyber security or data breach can be immense. A study by the British Chambers of Commerce found that 93% of businesses that suffered a data loss for 10 days or more filed for bankruptcy within a year. Half of them went out of business almost immediately.

At Modern Networks, we understand the importance of having a secure, fully integrated data backup, storage and recovery strategy. We are always happy to discuss your business needs, provide expert advice and practical solutions.

About Us

Modern Networks provides IT and telecoms as a managed service to over 1600 commercial properties across the UK and hundreds of enterprise clients. We provide everything from computing and local area networks to VoIP, broadband and mobile solutions. All our services are fully managed, continually monitored and supported by our UK service desk.

Sources: Beaming report 2016, Manta report 2016, ICO 2016, Workspace.co.uk
Images courtesy of Freepik.com