Keep calm and carry on? Not an option

Too many businesses are acting as if the data revolution hadn't happened, argues **Colin Tankard**

The headlines may be about cyber war and digital Armageddon, but cyber attacks affecting businesses of all sizes and are on the increase. Criminals are fast realising that electronic crime offers fast returns, with a much-reduced chance of being caught.

The growth in cyber crime coincides with the explosion in the number of digital devices such as smartphones, laptops and tablets. Meanwhile, social media and the web have become integral parts of life.

Yet many businesses are operating as if this data revolution hasn't happened. They face two challenges: their conventional defences against cyber attack are likely to be inadequate and their employees are often unaware of the tricks that cyber criminals will use to get information.

Basic technical precautions are still important. Anti-virus software and server security patches should be applied and email systems, as a minimum, should have spam filters.

A firewall acting as a barrier between the outside world and the company is still a requirement. Important data or devices must be protected by strong passwords and subject to access controls to prevent accidental or deliberate leakage.

The problem is that such basics were designed for a different, more static, business environment. The world has gone mobile and the data along with it. Attackers know that many employees use their personal devices for business use as well. They share emails across web-based email, and download office documents to unprotected devices or cloud-based storage.

This means that increasing amounts of company data and access points exist outside the traditional company perimeter, way beyond the protection of the firewall.

Criminals are also adept at exploiting the vulnerability of employees through social engineering techniques. They send fake emails that look like they originate from official bodies. These contain web links that, once clicked, may download malware designed to steal company data or steal passwords and login details from unsuspecting employees.

Hackers will obviously go after data that they can see on company servers, but what if it was hidden from prying eyes? After all you can't hack what you can't see. Technology exists that can do just that and make data servers go dark.

Such stealth technology puts a virtual cloak around servers so only the rightful owners and those users, devices and applications that are authorised to access the data can see it.

Businesses should also consider two-factor authentication where users need more than a password to access data that is essential. This can be in the form of a randomly-generated pin or biometrics such as a fingerprint scan. And, of course, passwords should also be as strong as possible.

Encryption is great but not enough on its own. Again only those authorised to read the data should be able to fully decrypt the data – for example, system administrators should be able to know that the data exists but cannot read it.

Effective business security is more than just a one-time fix. Protecting the company's "crown jewels" is an on-going process and needs regular checks to ensure that the processes put in place are good enough to keep cyber attackers at bay.

According to research by Kaspersky Lab, a security firm, one third of UK small businesses wouldn't know what to do if they suffered a security breach, while a quarter admit they wouldn't be able to recover any lost data.

All businesses need to get wiser about cyber security and think beyond simply spending more on an ad hoc basis. Cyber defences need to be planned and technology choices made carefully.

With the sophistication of cyber criminal gangs increasing all the time, the option for "keeping calm and carrying on" is not on the table.

Colin Tankard is managing director of Digital Pathways

For more from Digital Pathways visit: digpath.co.uk