Kennett insurance
Keeping Yorkshire covered since 1972

In May 2017, “WannaCry” ransomware reportedly hit over 200,000 computers in 150 countries, affecting many NHS Trusts in the UK.

Operations and appointments were cancelled and ambulances diverted as up to 40 hospital trusts became infected by a ‘ransomware’ attack demanding payment to regain access to vital medical records. So what is the reality of a cyber-attack and how can you protect yourself against this growing threat?

It happened because the ransomware was able to exploit a weakness in the Microsoft Windows operating system. Back in March, Microsoft released a patch to protect against this vulnerability, but not all users updated their computers.

Users opened infected email messages, enabling “WannaCry” to encrypt files on the target computer.
A ransom, payable in Bitcoin, was demanded to unlock the files. Typically, this was around £230, with three days to pay, before the ransom doubled. If not paid within seven days, the files were unrecoverable.

Although ransom demands are often small, the interruption to business can produce sizeable losses, especially if occurring during peak trading periods. For hackers, it can be very lucrative given the high frequency of attacks.

Demonstrating the increasing frequency of cyber-attacks, “NotPetya” was released at the end of June, seemingly from the Ukraine. This virus quickly spread across the world in a similar fashion to “WannaCry”, locking infected systems with a ransomware demand to be paid in Bitcoin.

Anyone who uses a computer, the Internet, and/or processes payment card information is under threat from cyber-attack.

The following basic safeguards will help minimise the risk:
ensure your IT operating system is up to date, and any new patches fully installed
use commercially licensed anti-virus software and firewalls
do not open unexpected emails or attachments
back up files regularly
train staff in cyber safety – you’re only as strong as your weakest link.
You may also want to consider Cyber Essentials, a Government backed scheme aimed at enabling companies to demonstrate their commitment to cyber security via a verified self-assessment process. The certification is widely recognized in the UK and has been designed in consultation with the SME business sector. The Federation of Small Business says that two-thirds of small firms have been victim of a cyber-attack in the last two years with the average cost of an attack being £3,000. Cyber Essentials may help you ensure your business is not one of them.

As a member of Willis Towers Watson Networks, we have access to AIG’s “CyberEdge” insurance, one of the most comprehensive cyber risk policies available. If your first line of defence is breached, “CyberEdge” is designed to help you manage and control the impact and get “back to business” as usual.

Designed to help safeguard your business, “CyberEdge” provides access to independent experts, including forensic, legal and communications specialists, and covers you against sensitive data breaches, computer hacking, dumpster diving, computer viruses, employee sabotage or error, pilferage of information and identity theft. Cover also includes ransom negotiation, data restoration, reimbursement of ransom and advice on mitigating reputational damage.

In a changing world where cyber criminals can affect your business we can provide you with appropriate Cyber Insurance and advice. To learn more about how to protect to your business, contact us today.

Sources:
RSA,
AIG
AIG
The Telegraph