NHS cyber-attack: lessons for other companies

The NHS's cyber security chaos provides vital lessons for other UK companies.

The actual cyber-attack was fairly simple and could happen to any company that uses an email system.

Many NHS hospitals had **not updated their Windows operating system** to include a recently released security patch. This meant that NHS workers unwittingly spread a malware when they opened attachments in emails. The impact was magnified because many NHS Trusts were running outdated and unsupported Microsoft operating systems, such as Windows XP.

The **ransomware** used was not particularly sophisticated – in fact it emerged three months ago – and it wasn't even specifically aimed at the NHS.

In essence, the huge disruption experienced by the NHS resulted from 1) inadequate computer systems maintenance and 2) human error.

Below are five general lessons that companies (from any industry) can take from this incident.

Lessons to learn:

1. Ensure your operating systems are supported and up to date. Apply patches as soon as they become available (for **WannaCry ransomware** specifically ensure MS17-010 has been deployed).
2. Ensure you are using antivirus solutions. (It's debatable whether this would have stopped this particular incident, but it is good practice and could help to prevent similar incidents.)
3. Ensure you have current back-up. This back-up should not be on the same network – what IT practitioners term 'out-of-band' – for example, on the cloud.
4. Ensure staff are trained not to open suspicious emails. More generally, ensure that staff are trained to understand and be vigilant against different types of cyber-attack/incident. Many successful cyber-attacks occur because of **common mistakes made by employees**.
5. Evaluate your cyber insurance options. Insurance, while not designed to replace your organisation's IT security, can assist in your risk mitigation. A specialist cyber insurance policy should pay the ransom, if deemed appropriate, and the associated costs incurred by you or the insurer's breach response to remediate the ransomware attack.

Ransomware attacks of this kind are not new – **almost half of NHS trusts in England had been hit by ransomware in 2015.** They are becoming seen, however, as a relatively easy way for cyber criminals to make money.

All companies are potential targets. Technology alone will not protect you – unless it is married to the right culture and company-wide vigilance.

If you would like to discuss any of these matters in more detail, please speak to your Lockton contact.

Peter Erceg
Senior Vice-President, Global Cyber and Technology
0207 933 2608
Peter.Erceg@uk.lockton.com

Lockton Companies LLP.
Authorised and regulated by the Financial Conduct Authority.
A Lloyd's broker. www.lockton.com

LOCKTON®