NEWS BRIEF
Presented by **Packetts**

Aftermath of WannaCry Ransomware Yet to Be Seen

WannaCry, a ransomware program that targets a vulnerability in outdated versions of Microsoft Windows, has spread across 150 countries and infected more than 230,000 computers since it was launched on 12th May. It disrupted many NHS hospitals in England and Scotland, infecting up to an estimated 70,000 devices including computers, MRI scanners, blood-storage refrigerators and theatre equipment.

Microsoft was aware of this cyber security gap and, as a precaution, released a Windows security update in March. However, many users have not yet run the update, which has allowed WannaCry to spread quickly.

As of 15th May, the spread of the ransomware program has appeared to slow down, but employers and their employees should be careful, as the effects in the United Kingdom have yet to be fully determined.

An Overview of WannaCry
After infecting just one computer, WannaCry can spread to every device in a network within seconds. It works by locking users out of their computers before demanding money in order to regain control of their data. Initially, WannaCry requests about £230, but, if no payment is made within three days, it then threatens to double the amount. If no payment is made within that time, the ransomware program then threatens to delete files after seven days.

According to Elliptic, a London start-up that helps law enforcement agencies track criminals, around £39,000 worth of bitcoin payments have been made to the hackers as of 15th May.

Response to the WannaCry Ransomware Attack
No one is certain about who is behind the attack, but Europol is working on a decrypting tool. Many firms hired experts over the weekend to prevent new infections, which seems to have worked in Europe, so far.

After the initial discovery of the WannaCry ransomware, Microsoft issued a warning to the US government concerning its data-storing practices. Microsoft claimed that the tool used in the WannaCry cyber attack was developed by the US National Security Agency and was stolen by hackers.

Cyber Security Precautions
Some experts recommend that you should not pay the ransomware if you've been hacked, as there is no guarantee that the hackers will return the files to you unharmed, if returned at all. Experts also recommend that you take the following precautions:

- Update your network security.
- Run the Windows update and turn on auto-updaters, if available.
- Install and update anti-virus as well as anti-malware software on all of your organisation's computers.
- Provide your employees with cyber security training. This should include valuable best practices, such as how to recognise a cyber attack and phishing email scams.
- Back up your documents regularly onto a separate drive.
- Purchase comprehensive cyber insurance to ensure that your organisation can sustain a cyber attack.

Contact Packetts if you have any further questions regarding how you can avoid disruptive business interruptions from cyber attacks.

Packetts