We spoke to over 600 senior business decision makers and 1,200 employees in the UK, US, Germany and Australia after the attack. Here’s what we found:

- 58% of UK organizations now feel another attack is imminent.
- 77% of people surveyed were aware the attack had happened.
- 33% have changed their passwords.
- 24% have enrolled in formal courses.
- 26% are taking steps to make sure their companies raise their game in cyber security in the aftermath of the events.

Private sector is more concerned about how their data is held:
- 83% are worried.
- 72% in public sector vs 55%.

Of those aged 18-24 are more likely to take action following the attack.

Over three quarters in the UK:
- 88% either their company, them personally or a service they use were affected by the attack – either their company, them personally or a service they use.

The WannaCry attack on May 12 was a Ransomware attack that struck...

- 230,000 computers
- 150 countries

WannaCry attacked 8,078 organizations and pharmaceutical and medical operations were cancelled along with 150 operations.

Demands of approximately £300 were made per device to unlock encrypted files. Since then £188,000 in bitcoin paid by victims has been withdrawn.

29% of UK firms will add cyber security to the boardroom agenda following WannaCry attack.

29% of firms worldwide have pledged to implement stronger cyber security measures.

38% of employees are now reading more about cyber security.

33% of people we spoke to about their password security.

24% of people we spoke to about their overall data and file security.

80% of people we spoke to about their password security.

83% vs 72%.

55% of people we spoke to about their overall data and file security.

77% of people we spoke to about their overall data and file security.

88% of people we spoke to about their overall data and file security.

TAKE ACTION TO PREVENT RANSOMWARE ATTACKS

AUGMENT YOUR EXISTING SECURITY INFRASTRUCTURE TO COMBAT TODAY’S INFORMATION BORNE THREATS.

DISCOVER CLEARSWIFT SECURITY+