What HR should tell staff after a major hacking incident

Developers of Activ People HR, Codel Software offer helpful advice for HR Managers in the wake of the NHS hack.

The Wannacry ransomware attack which attacked workplaces worldwide and affected much of the UK's NHS network was stopped in its tracks accidentally by registering a new domain, which acted as a 'kill switch' – but not before many huge organisations had been massively impacted.

Having happened on a Friday, workplaces were worried as many of the Nation's computers have been turned off all weekend – there are of course fears that when users return to work on Monday, the virus could again be spread by unsuspecting users.

Hackers don't take weekends off. New variants of the virus were already available by Monday, responding to the 'kill switch'. Thankfully IT teams had been on the case all weekend, too, updating systems and making sure that networks were protected.

However, it's vital that HR gets on board, too. Every single person in the office is responsible for safeguarding your systems – and that means HR support is critical.

Richard Hocking, Technical Director for Welsh software developer Codel Software explains why cybersecurity is a problem for EVERY member of staff and why HR should stress basic precautions at work:

What HR should tell staff after a major hacking incident

"We've worked hard to get ISO27001 certification as a developer, and cyber security precautions are vital.

"It is important to consider security when making new software purchases, only use trusted suppliers, ideally with ISO27001 certification – these providers will have been externally assessed and will protect critical data by having high security standards. However, it isn't all about external protection.

"Failing to take basic cyber precautions is the equivalent of leaving a purse on the seat of your unlocked car and as we have seen this weekend, the impact of a virus, ransomware or data hack can be huge.

"Workplace networks are only as secure as their weakest user, so it's really important that HR are reinforcing any IT messages. Make sure staff are advised of good practice, such as only opening emails from trusted sources. While Windows Updates can seem annoying, it is really important that users let them run, they can't just assume that 'IT will sort it'.

"Even if a source is trusted, be careful when opening attachments, if something looks suspicious, it's definitely worth a quick call to it rather than taking the risk. It's also important to remember to continue doing this after the news goes quiet – the threat of a cyber attack won't always make headlines."

"It's not just tech. Every single staff member has a role to play in cyber security – both by taking the precautions above, and by choosing secure passwords and being careful who they share information with. Physical security is important too – if someone says they need to access your computer, on the phone or at your desk, check whether they are who they say they are! Security definitely isn't just an 'IT' problem. Nobody can afford to allow staff complacency – the risks are too great."