Are public sector organisations more at risk from cyber-attacks on old computers?

May 17 2017, by Simon Parkinson

Credit: cottonbro studio from Pexels

Hospitals across Britain were crippled by the recent ransomware cyber-attack, making the country's National Health Service one of the most high-profile victims of the global incident.

The government has been criticised for cutting IT support for the health service and failing to replace old computer systems. Meanwhile, ministers hit out at NHS bosses for not improving cybersecurity, amid reports that an upgrade that could have prevented the attack was made available a month ago.

This story doesn't feel too surprising. Anyone who regularly deals with public services in person will probably have seen government employees struggling with outdated computer systems. Certainly, other major state-run organisations have also been hit by the ransomware, including German railway company Deutsche Bahn and the US Department of Homeland Security. But is the public sector really any worse than the private sector at keeping its IT security up to date and avoiding cybercrime?

The recent "WannaCry" attack was made possible by a flaw in the 15-year-old Windows XP operating system. Software manufacturers often provide updates or patches to their products after they discover such a flaw, to prevent cyber-criminals from exploiting it. However, Microsoft stopped routinely updating XP in 2014, and those still using it have to pay for custom support to receive any further patches.

Once the company became aware of the WannaCry flaw, it was quick to release a patch back in March. But because many customers were still using unsupported versions of XP, WannaCry rapidly infected a large number of systems when it emerged in May. Microsoft then made its patch available to all XP users but many of those who didn't update immediately were caught out. This is exactly what happened within the NHS.

The government has long acknowledged the need to update its old IT systems. When public XP support ended in 2014, the government said it expected the majority of its machines to be upgraded within a year. It then ended NHS funding for custom XP support, reportedly in an attempt to encourage health service bosses to upgrade their systems. But a report at the end of 2016 suggested that 90% of NHS trusts still had at least one XP system.

The most likely reason that out-of-date systems are still being used is the cost of upgrading them. In most cases, a new version of Windows or another operating system would also need a new computer that was powerful enough to run it, and potentially new bespoke hardware and software to enable the organisation to do its job. For example, a hospital X-ray department using an XP-based machine might need a new version of the software that controls its X-ray machines.

Public sector agencies also have a luxury in the form of highly-skilled government experts from the likes of the National Cyber Security Centre who are available to ensure that critical services, such as the NHS, are kept operational. So even if the recent ransomware attack acts as a necessary wake-up call, there's still a perceived safety net.

Private problem

However, WannaCry didn't just affect the public sector. Around 200,000 victims in 150 countries have been affected, according to EU police force Europol, many of them businesses including major corporations such as Nissan, FedEx and Hitachi. One source suggests that more than 10% of all desktop PCs run Windows XP, and a significant portion of those victims will likely be small businesses. In general, there is no specific evidence that public sector organisations suffer cyber-attacks disproportionately.

Although the NHS is clearly under tight financial constraints, governments have significant resources to mitigate cyber-threats and can raise large amounts of money if politicians choose to do so. In the UK, the National Cyber Security Centre alone has a £1.9 billion investment.

It is a completely different picture for small companies that don't have easy access to cash for upgrades or access to the highly-skilled resources of government experts or even IT departments. Often they don't even have the awareness that there's a problem to begin with. There are government-backed initiatives to help small companies with cybersecurity, such as the UK's Cyber Essentials, but these don't have the scale to reach everyone or even identify and help those most in need. We can certainly question whether they are having much impact given the scale of the recent Ransomware attack.

Cyber-attacks on the scale of WannaCry may remind organisations about the need to maintain their IT security. Getting people to understand how is still a serious challenge. Public sector organisations might too often rely on outdated computer systems but at least they're better placed than much of the private sector to do something about it.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Are public sector organisations more at risk from cyber-attacks on old computers? (2017, May 17) retrieved 25 April 2024 from https://phys.org/news/2017-05-sector-organisations-cyber-attacks.html