NHS DATA SECURITY DEVICE LOSS

AN ANALYSIS OF HOW DEVICE THEFT IS PUTTING NHS DATA SECURITY AT RISK

PARLIAMENT STREET

partnership in policy

JUNE 2019

INTRODUCTION

The National Health Service (NHS) is one of the most respected systems in the world, relied upon and revered by millions.

The organisation's ability to offer high quality, free care to the nation is something treasured by the public and supported by politicians. However, in recent years debates around how best to fund, support and improve the NHS have increased. These discussions have been inflamed by issues such as austerity and an alleged financial blackhole along with a series of high-profile cyber-attacks.

As the custodian of millions of private patient records, containing confidential personal information on treatments, conditions as well as bank accounts, home and email addresses, data security is a serious issue for the NHS. It is no surprise that with cyber criminals targeting charities and critical national infrastructure, the NHS has become a top target for those wishing to steal data and wreak havoc.

The largest security crisis that the NHS faced was the WannaCry attack which took place exactly two years ago. Coined as the 'biggest ransomware' offensive in history, the global attack infected more than 300,000 computers in 150 countries and meant that 6,900 appointments had to be cancelled. Whilst this scale of this issue was huge, it later came out that the attack on the NHS could have been prevented if the correct security advice had been followed. After the WannaCry attack, the NHS pledged £150m to bolster its defences against the growing threat of cyberattacks.

Almost directly after this attack, the NHS communicated that it had suddenly lost a total of 864,000 documents, 702,000 of which were pieces of paperwork. This particular issue automatically questions why the use of paper documents is so high, particularly those that contain sensitive patient data.

This research paper aims to explore the state of device-loss reported within NHS hospitals, looking at tablet computers, mobile phones and laptops specifically. We aim to illustrate that device loss remains a major threat to the security of NHS Trusts and enhanced security plans should be put in place to tackle this growing threat.

METHODOLOGY

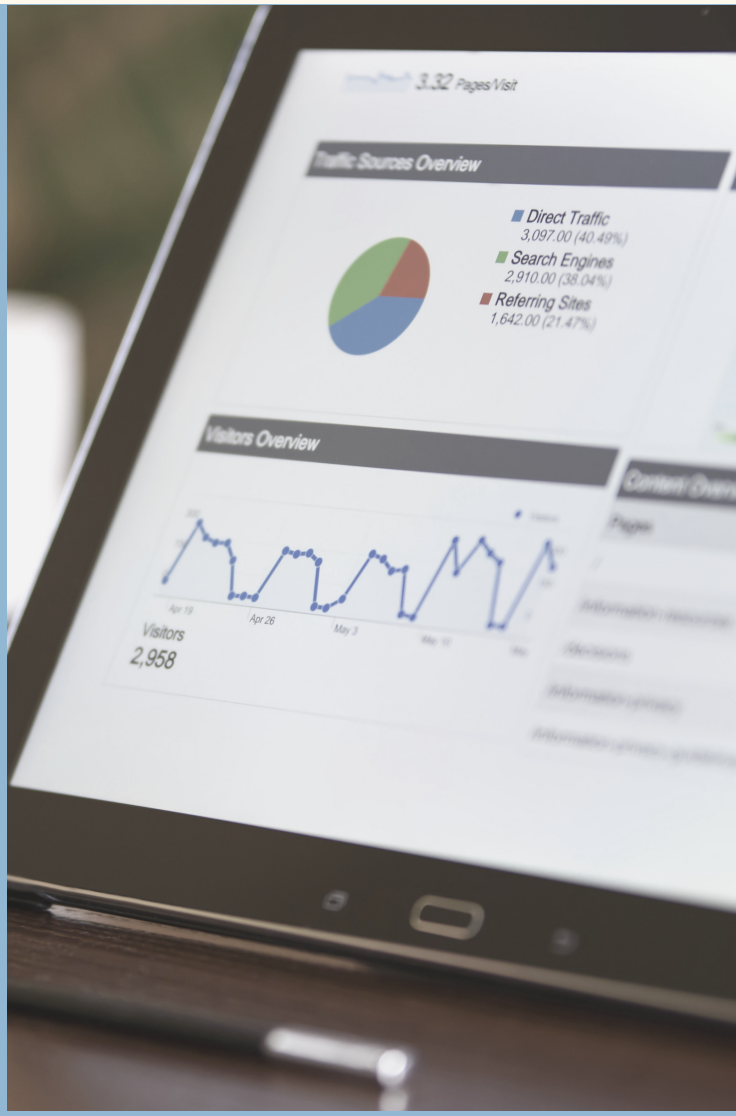
The Parliament Street health research team wanted to assess the security implications of lost or stolen devices within the NHS system over the last three calendar years.

A team of researchers issued a Freedom of Information Act (FOI) to all NHS trusts across the UK asking them to detail what devices they have had either lost or stolen over the last three full years, from 2016-2018.

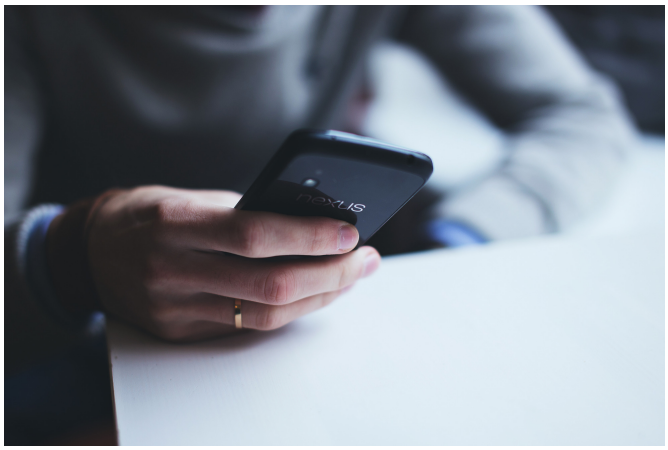
These included all devices reported missing onsite, comprising of NHS devices and some incidents of devices being reported stolen by the public.
In total, 58 hospital trusts responded to our request for information.

As well as asking for the figures of lost devices, we also asked for any detail they hold on the type of device stolen or lost and any corresponding information that matches the information held. Many trusts detailed that they had lost devices and provided extra information about those items missing and the scenario.

This report aims to analyse the figures of lost devices that hospitals across the country have had lost or stolen and the impact this has over security concerns, particularly when analysing the credibility of the NHS.



DEVICE LOSS: THE NUMBERS



NHS Device Theft Data

1,283

devices lost in the last three full years

33%

increase in reported losses over the period

29%

increase in theft of mobiles from hospitals

Overall, from the trusts that gave us full results, we have noticed a clear rise of lost or stolen devices over the past three years. The combined figure of lost devices over the last three full years reached a shocking 1,283 reported missing.

The results have been broken down into lost laptops, mobile phones and tablets. In 2016, the overall figure of lost devices was 383, rising to a staggering 511 in 2018 – an increase of 33%.

The device which saw the largest increase of loss or theft was the mobile phone, with 284 in 2016 and rising to 366 in 2018 – an increase of 29%. It is likely that this device had the highest figures because of their physical size and the number of mobile phones that will be held in a hospital at one single time.

The second largest increase of lost or stolen devices was from laptops with 55 reported missing in 2016, rising to 81 in 2018 – an increase of 47%. In 2016, 47 tablets were reporting missing which rose to 62 in 2018 making that an increase of 32%.

However, when analysing the results between 2016 – 2017, the responses show that the figures for lost or stolen tablets and laptops actually decreased, before rising again between 2017 – 2018. In 2017, it was reported that only 39 laptops were missing, down from 47 in 2016. As well as this, missing numbers of tablets declined to 43 in 2017 from 55 in 2016.

The overall figures of lost and stolen devices across NHS trusts are a real concern for security. On these personal and work-issued devices, there is often highly sensitive information that without having a copy, could affect future appointments and the overall service of the NHS.

If given into the wrong hands, hackers could cause some serious damage to the NHS's infrastructure, as previously seen with the WannaCry attack.

TRUSTS IN TROUBLE: LOSSES

Out of the results collated, some NHS trusts clearly topped the list of having the most recorded lost or stolen devices. Topping the list with the most recorded lost over the last three years is Eastbourne District General Hospital which lost a total of 110 devices over the last three full years. Despite this large figure, the reports declined from 42 in 2016 to 38 in 2018.

The second largest trust which had the highest number of lost devices was Bradford Teaching Hospital who had a combined total of 96 lost or stolen items, their largest issue being with mobile phone devices. The third largest was Salisbury NHS Foundation Trust which reported 81 lost or stolen devices over the last three years, with 2018 having the largest number of reports.

Northampton General Hospital reported 80 devices missing over the last three years, with 2017 being the worst year for reports. East Kent Hospitals University NHS Foundation Trust had reports of 61 missing devices, despite results declining from 25 in 2016 to 21 in 2018.

Despite these trusts having large numbers of devices reported missing, some of the trusts who responded to our request disclosed that they had no devices lost or stolen in the last three full years. These were James Paget University Hospital and Liverpool Heart and Chest Hospital.

As well as this, there were some hospitals who had very low numbers of devices missing – such as Wye Valley NHS Trust, The Queen Elizabeth Hospital Kings Lynn NHS Trust and Queens Victoria Hospital who all had one device reported missing respectively. Taunton & Somerset NHS Foundation Trust and George Eliot Hospital had both reported two missing devices over three years.

110

Devices lost

Eastbourne District General Hospital

96

Devices lost

Bradford Teaching Hospital

81

Devices lost

Salisbury Teaching Hospital

DEVICE THEFT: CASE FILES

As well as the data reported, we also asked for accompanying notes that the trusts may hold on file. The Royal Free London Hospital told us that they had a report of a camera mounted on a teaching slit lamp go missing from a secure, locked toom and that a report of an intruder breaking into a room and removing an old mobile phone.

The notes accompanying Kings College Hospital told us that in 2016 they had reports of two breast pumps being stolen and a microwave. As well as this, in the same year East Kent Hospital University Trust had a report of a computer going missing which included the screen, leads and the hard drive associated with it.

The hospital which had the most interesting corresponding notes was University Hospital Southampton which disclosed in 2016 they had observed on CCTV a male patients' friend take a laptop which belonged in the bay and left the department.

When confronted by two security officers, it was found that one of the males had an ambulance radio in his possession and managed to recover the stolen laptop off the male.

Another report highlighted an issue after a patient self-discharged themselves, they noticed that the ward TV that was in the patient's room had disappeared.

The registered mental health nurse said that the patient distracted him by vomiting on the floor and then asking for privacy so he could get changed, he then closed the curtain and came out a few minutes later with his bag packed. The nurse helped him carry his bags to the taxi rank, he reported that they felt quite heavy but that he didn't think anything of it at the time.

RECOMMENDATIONS

OUR FINAL THOUGHTS

From the data collected from Parliament Street researchers, it is obvious that security should be a real concern for the NHS. The data shows that as technical devices increase in popularity, so does the reports of theft or loss.

NHS-issued devices play an incredibly important role in keeping the NHS running and they often hold highly sensitive, confidential data that could cause severe issues if hackers were given access to them.

It is apparent that security standards must improve within the NHS if these numbers are to decrease. When patients are receiving treatment for an ailment, the last thing they want to be thinking about is whether their personal belongings are being kept safe and secure.

The NHS trusts must also begin to realise the implications that stolen electronic devices can have over the cybersecurity of the entire organisation and the scale of the problem one missing or stolen laptop could cause.

Key recommendations include:

1.) Create a central database of lost or stolen NHS devices
Ensure that all laptops, tablets and mobile phones suspected of containing confidential data are encrypted and risk-assessed. NHS departments should consider tracking devices and having a clear protocol in place for tackling these issues as and when they arrive.

2.) Improve employee awareness of security risks
Initiate full cyber training programme so that medical staff and support workers are fully aware of the importance of reporting incidents of device loss. This should include training around passwords, personal security and device management in the workplace.