JULY 2018

PARLIAMENT STREET

*partnership in policy*

# IDENTITY CRISIS

## THE RISKS OF PERSONAL DEVICE SECURITY

# INTRODUCTION

## Who do you think you are?

The explosion of personal devices and proliferation of social media accounts means that never before in our history have human beings had so many online identities. As technology has progressed, this problem has increased as dormant identities lie online, often with outdated information and email accounts remaining inactive, despite often containing a wealth of highly personal information.

This environment is irresistible to fraudsters, seeking any method necessary to make money and exploit loopholes in our personal security. Once upon a time ID fraud was conducted by rustling through dustbins, now it can easily be initiated through gaining access to an individual profile online.

Recent research from Cifas suggested that there were a record 89,000 cases of identity theft in the first half of last year. Identity theft has reached epidemic levels in the UK, with incidents of this type of fraud running at almost 500 a day, according to the latest figures.

Whilst much attention has been given to the impact personal device losses and identity breaches have on individuals, little attention has been given to the potentially catastrophic consequences these malicious acts will have on businesses.

Official data from the UK government, published this year suggests that over four in ten businesses and two in ten charities have experienced a cyber security breach or attack in the last 12 months alone. Additionally it has been suggested in the report that Three-quarters of businesses (74%) and over half of all charities (53%) say that cyber security is a high priority for their organisation's senior management.

The problem is made worse when you consider that companies are grossly underprepared to deal with the threat. Three in ten businesses (27%, versus 33% in the previous 2017 survey), and two in ten charities (21%) have a formal cyber security policy or policies

To explore the problem of mobile device losses and the challenge of identity access management, the Parliament Street think tank research team communicated with Transport for London to gage the volume of lost personal devices in the capital and liaised with leading experts in this area. Our findings make fascinating reading, revealing a high volume of personal device losses, which could expose businesses to severe security risks for the long term.

# METHODOLOGY

An overview of our research approach

The Parliament Street research team liaised with Transport for London (TFL) to obtain data on the volume and diversity of personal electronic devices which were discovered as 'lost property' over the last financial year. TFL kindly provided us with a complete breakdown of the numbers of devices lost along with specific details around the make and model of devices involved.

The team them presented the findings to a series of key security experts who helped us shape our thesis that lost devices can cause significant issues for identity security and potentially give fraudsters access to the wider corporate network.
The data has been analysed and brought to life in a series of graphs and charts contained within this industry report.

All information was sourced under Freedom of Information (FOI) legislation and returned in June 2018.

# SECURITY FEARS

## A rising tide of personal device threats

Businesses leaders are spending millions on firewalls and anti-virus protect measures as part of their wider cyber security, but other threats remain. In the current climate of fear, fuelled by large scale, headline generating data breaches, there are many reasons why this approach is the right one.

It's not just the corporate enterprises that come under attack, data has suggested that the UK's 5.4 million small businesses are collectively attacked more than seven million times a year, with Bring Your Own Device (BYOD) policies being a particular concern.

Research published by Zurich has revealed that as many as 875,000 UK small and medium sized enterprises have suffered a cyber security breach within the last 12 months alone. Intriguingly, despite the risks, nearly half (49%) of SMEs plan to spend less than £1,000 on cyber security in the next 12 months, leaving them vulnerable to substantial losses.

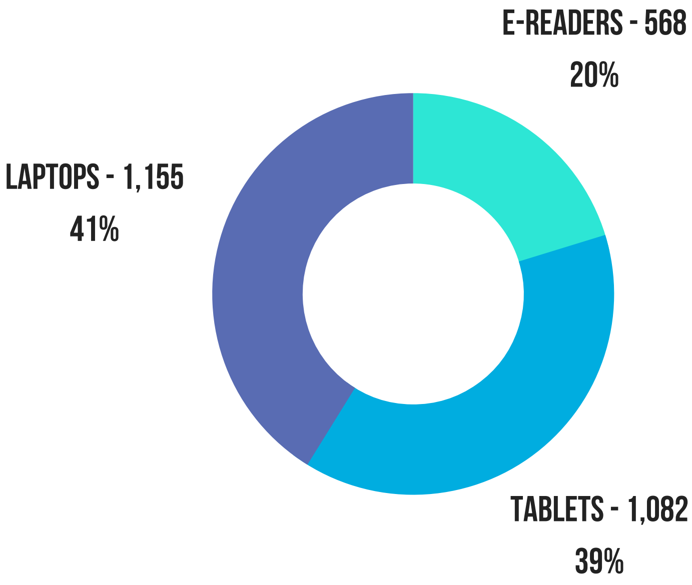
Data breaches have impacted companies large and small. Uber has revealed that 2.7m UK users of its app were affected by a mass data breach in 2016, which the company disclosed last week.

Meanwhile the Equifax breach meant that around 400,000 people in the UK may have had their information stolen following a cybersecurity attack. Worryingly, the data included names, dates of birth, email addresses and telephone numbers, but does not contain postal addresses, passwords or financial information.

It is clear that businesses are coming under attack and they need more help than ever before to verify and secure the identities of their employees.

# DATA ANALYSIS

Overview of lost devices in London in the last financial year



23,453

MOBILES

7,394

APPLE

MOBILES

6,091

SAMSUNG

MOBILES

We obtained the data around personal device losses from Transport for London's lost property office. The information we have analysed was sourced from the organisation's most recent financial year, 2017-2018.

The information obtained raises serious questions about threats individual devices pose to company data security and the need for improved identity access management.

We discovered that 26,272 devices were lost on the network between April 2017 and April 2018 and handed into TFL lost property. Breaking down the data into specific devices, mobile phones topped the list with a staggering 23,453 devices lost last year.

The second largest is laptops with a total of 1,155 lost, after that it is tablet computers at 1,082 devices lost. 568 eReaders were reported to be lost, 10 drones and four Amazon Echo's.

Under the mobile phone category, Apple iPhones were found to be the most lost device at 7,394 followed closely by Samsung devices at 6,091. Nokia devices placed third with 3,012 devices lost, followed by Alcatel with 1,515 of their mobile phones reported lost. The risks of identity theft to individuals and important data loss to businesses is prominent in mobile phone devices.

For laptops, the largest brand lost on the network was Apple products at 337 devices reported. Second to this was Lenovo laptops with 201 devices reported lost.

# RISKS TO BUSINESSES

Our research has proven that there is currently an extraordinarily high number of electronic device losses on London's transport network and that this trend is set to continue indefinitely. These losses in turn provide major challenges for the personal security and safety of businesses and their respective employers.

An independent study from identity access firm Centrify has suggested that in the UK, younger employees are the "main culprits" for data security breaches in the workplace.

The research also revealed that decision makers are doing very little to allay their own fears, with over a third of 18-24-year olds able to access any files on their company network and only one in five having to request permission to access specific files. The issue is compounded by the fact that less than half (43%) have access only to the files that are relevant to their work.

With these facts in mind, it is important that businesses take the threat posed by employee device breaches seriously and develop a long-term strategy to verify and protect the identity of individuals with access to confidential information in the corporate enterprise.

Responding to the research, industry experts point to the risks associated with application vulnerabilities which are a major target for cyber criminals. Robert Coleman, UKI CTO, CA Technologies says, "With businesses investing heavily in purchasing and developing growing volumes of applications to improve employee productivity, the security threat posed by lost and stolen devices has increased dramatically. Apps without strong security protection can be an easy route into a goldmine of corporate data.

Nobody can prevent mobiles and tablets from being misplaced, but companies can ensure that the applications which reside on these devices are only accessible by the correct privileged users, so that fraudsters cannot exploit them as a backdoor into the business," concluded Coleman.

# RECOMMENDATIONS

## 1. Implement an identity verification strategy for every employee

Companies can no longer naturally assume that an employee accessing the company network is a legitimate member of staff, particularly with so many devices being lost on public transport systems.

To overcome these challenges, businesses need to ensure systems are in place to validate the device, the employee identity and where appropriate to restrict access to confidential data that could put the security of the organisation at risk.

## 2. Increase security verification training for all members of staff

All too often, devices go missing and employees may be cautious of reporting the incident to their employers. With so many mobiles, tablets and laptops going missing on trains, every device is potentially a security breach, so employers need to know about it.

It's worth bearing in mind that our research only lists devices handed in as lost property, the true number of devices stolen will likely be much higher. Staff need to be made aware of the risks and the necessary processes for protecting themselves and their company.

## 3. Scrap trust as a strategy

With cyber-attacks rapidly on the rise, a healthy paranoia is a positive force for change within the organisation. The truth is that companies can no longer risk the assumption that staff are valid employees, and thus should implement electronic verification and restricted access to information to protect company IP and data assets.