# SAFE & SECURE

## PROTECTING LONDON'S DATA

GARETH BACON
GLA CONSERVATIVES
GREATER LONDON AUTHORITY

2016

# CONTENTS

*Issue Date:31/08/2016*

# INTRODUCTION

Cybercrime is no longer the preserve of the perceived lone wolf bedroom hacker, and nor is cyber security the preserve of just large multinational companies' IT Departments. The inherent and simultaneous benefits and risks of modern digital networks mean that the ability to protect data should be at the heart of all organisations.

More than ever, individuals are willingly providing their personal data to organisations in order to access services[1].

This places the organisations which hold this information at a constantly increasing risk of online security breaches, and the individuals who provide their data at an ever increasing risk of their personal information ending up in the wrong hands.

Information held on computer systems can be breached or compromised in a variety of different ways – via malicious attacks, accidental human error, or simply because of software failures.

Security breaches take a variety of different forms, such as infiltration by hackers, infections from viruses, or the use of denial of service attacks. In fact, even the Greater London Authority itself experienced a Denial of Service attack in August 2012[2].

While it remains important that all potential risks are considered and mitigated against, the protection of data from malicious attacks is rapidly growing in importance.

Security breaches of large organisations increased by nine per cent between 2014 and 2015; and security breaches of small companies increased by 14 per cent over the same period[3].

While schemes exist, such as the Government's 'Cyber Essentials'[4], to help businesses secure their systems and protect their data – it is clear more needs to be done.

The Mayor of London, and the Greater London Authority as a whole, is in a unique position where they can influence the decision making of businesses across London.

This influence, if wielded effectively, could encourage better data security standards which will not only be beneficial for London's businesses, but anyone who provides their personal data to an organisation based in London.

London has the opportunity to lead the way in improving data security, setting standards that the rest of the country aspires to match.

[1] Consumers worldwide will allow access to personal data for clear benefits, Infosys, June 2013: https://www.infosys.com/newsroom/press-releases/Pages/digital-consumer-study.aspx

[2] Denial of service attacks on GLA websites, London Assembly, September 2015: http://questions.london.gov.uk/QuestionSearch/searchclient/questions/question_283456?facet=true&q=*%3A*&facet.field=question_questionby_s&facet.field=question_questionbyparty_s&facet.field=question_answerby_s&facet.field=question_meetingtype_s&facet.field=question_year_i&facet.field=question_theme_s&facet.field=question_answered_s&facet.limit=-1&facet.mincount=1&facet.date=question_meetingdate_dt&facet.date.start=2000-05-01T00%3A00%3A00.000Z%2FDAY&facet.date.end=2016-08-14T00%3A00%3A00.000Z%2FDAY%2B1DAY&facet.date.gap=%2B1DAY&json.nl=map&start=750&fq=question_questionbyparty_s%3A%22GLA%20Conservatives%22&sort=question_meetingdate_dt%20desc

[3] 2015 Information Breaches Survey, PwC, June 2015: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

[4] Cyber Essentials Scheme, HM Government, June 2014: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

# SCALE OF THE PROBLEM

As technology becomes more widely available and readily affordable, it increases the wide range of potential threats to data security. Suffering a security breach has become worryingly commonplace in the UK, with a huge number of potential perpetrators across the globe engaging in such attacks.

In 2014, 81 per cent of large organisations[5*] experienced a security breach, and 60 per cent of small organisations[6**] also experienced a breach.

These security breaches came in a variety of forms, but specifically 55 per cent of large organisations were attacked by an unauthorised outsider, and 73 per cent of these organisations also said they'd suffered from infection by viruses or malicious software. Denial of service attacks were also reported by 38 per cent of large organisations.

In small organisations, 33 per cent of them had been attacked by an unauthorised outsider, with 45 per cent of them suffering from infection by viruses or malicious software. Denial of service attacks were reported by 16 per cent of small companies[7].

Overall in 2015, 90 per cent of large organisations experienced a security breach, and 74 per cent of small organisations also experienced a breach.

Specifically, 69 per cent of large organisations were attacked by an unauthorised outsider, and 84 per cent of these organisations said they had suffered from infection by viruses or malicious software. Denial of service attacks were also reported by 30 per cent of large organisations.

In small organisations, 38 per cent of them reported being attacked by an unauthorised outsider, with 63 per cent of them suffering from infection by viruses or malicious software. Denial of service attacks were reported by 16 per cent of small companies[8].

As is clear, there is an upward trend in the number of security breaches experienced by organisations in the UK – with large companies experiencing a 9 per cent increase, and small companies experiencing a 14 per cent increase between 2014 and 2015.

# THE FINANCIAL IMPACT

Year on year, the cost of security breaches to large and small organisations has increased.

In 2014 the cost of a security breach to a large organisation was estimated to be between £600,000 and £1,500,000; in a small organisation the sum was estimated to be between £65,000 and £115,000.

However in 2015, the estimated cost to a large organisation had risen to between £1,460,000 and £3,140,000; in a small organisation the estimated cost has risen to

[5] * A large organisation is defined as one employing 250 people or more.

[6] ** A small organisation is defined as one employing 249 people or fewer.

[7] 2014 Information Security Breaches Survey, PwC, May 2015: http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

[8] 2015 Information Breaches Survey, PwC, June 2015: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

between £75,000 and £311,000[9].

As of 2015 in the UK there were 2,440,065 small organisations with up to 249 employees, and 9,350 large organisations employing 250 or more people. In London specifically, there were 442,980 small organisations and 1,900 large organisations[10].

Given it is estimated 90 per cent of large organisations and 74 per cent of small organisations experienced security breaches in 2015, it is possible to say that in total across the UK 1,814,063 organisations could have experienced some form of security breach.

This is broken down as of 8,415 large organisations and 1,805,648 small organisations across the UK experiencing a security breach.

In London specifically, it is estimated in 2015 that 329,515 organisations experienced some form of security breach.

This is broken down as 1,170 large organisations and 327,805 small organisations experiencing a security breach.

The potential financial implications of a security breach to organisations are endless, and some elements – such as reputational damage, almost impossible to estimate.

However, using the lower-end of the estimated costs to organisations of security breaches, it is possible to suggest that there is a potential cost to the UK economy of around £147,709,500,000 per year.

This is broken down as a cost to large organisations of £12,285,900,000 and a cost to small organisations of £135,423,600,000.

In London specifically, it is possible to estimate conservatively that the cost to the economy from security breaches could be in the region of £35,997,500,000 per year.

This is broken down as a cost to large organisations of £2,774,000,000 and a cost to small organisations of £33,223,500,000.

## PROTECTING AGAINST SECURITY BREACHES

There has been relatively little consensus on how best to secure systems, and prevent security breaches.

A Government consultation in 2013 found that no existing standard or approach fully met the needed requirements. However, it also suggested that the tech industry was keen to help in the development of a definitive standard[11].

[9] 2015 Information Breaches Survey, PwC, June 2015: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

[10] UK Business Counts – Enterprises, NOMIS, October 2015: https://www.nomisweb.co.uk/query/construct/summary.asp?mode=construct&version=0&dataset=142

[11] Call for evidence on a preferred standard in cyber security, Department for Business Innovation & Skills, November 2013: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf

The International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) currently produce the most globally recognised framework for best-practice information security management – they are known as the ISO/IEC 2700 Family of Information Security Standards[12].

It is possible for organisations to receive certification that they adhere to the ISO/IEC 2700 series. However, this is voluntary – there is no requirement to seek formal certification[13].

The same Government consultation from 2013 suggested that while the ISO/IEC 2700 series had the greatest level of support from industry, there were still concerns.

These concerns mainly related to the fact that implementation costs for small and medium sized organisations were high; and also the standards are relatively complex which can lead to difficulties with implementation. Another weakness highlighted was that in previous versions those who signed up to the standards were free to define their own scope for which area of their organisation was covered. This made the potential for comparison and audits ineffective and inconsistent.

More recently, the Government has launched a scheme known as Cyber Essentials, in order to promote cyber security in UK organisations. The intention was to provide a scheme which was far simpler for organisations to implement.

The scheme was designed to fulfil two functions: firstly it provides clear information which all organisations should implement to mitigate the risks from internet based threats, and secondly it offers a way for organisations to demonstrate that they have taken such precautions[14].

However, as of March 2016, only 2,181 Cyber Essentials and Cyber Essentials Plus certifications had been issued[15], which equates to approximately less than one per cent of organisations operating in the UK.

## LONDON'S RESPONSE TO DATA SECURITY

London, as the home of nearly 20 per cent of the UK's organisations, and a place which generates over 22 per cent of the UK's GVA[16], is at a significant risk of security breaches.

However, a large number of these security breaches often go unreported – with estimates suggesting around 88 per cent of organisations fail to report cyber-attacks[17] due to concerns over losses of reputation or a fall in share prices.

In October 2015, the then Mayor of London, Boris Johnson, launched the London Digital

[12] The ISO/IEC 2700 Family of Information Security Standards, IT Governance, July 2016: http://www.itgovernance.co.uk/iso27000-family.aspx

[13] ISO/IEC 2700 – Information Security Management, ISO, July 2016: http://www.iso.org/iso/iso27001

[14] Cyber Essentials Scheme, HM Government, June 2014: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

[15] Small Businesses: Cybercrime, House of Commons Hansard, April 2016: http://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-12-08/19259/

[16] Regional Gross Value Added (Income Approach), Office for National Statistics, December 2015: http://www.ons.gov.uk/economy/grossvalueaddedgva/bulletins/regionalgrossvalueaddedincomeapproach/december2015

[17] Met Chief: Police must do more to beat hidden threat of cyber-crime, Evening Standard, July 2015: http://www.standard.co.uk/news/crime/met-chief-police-must-do-more-to-beat-hidden-threat-of-cyber-crime-10406799.html

Security Centre. The centre was England's first organisation dedicated to helping small and medium sized organisations protect themselves from security breaches[18].

The London Digital Security Centre was a central recommendation in the former Mayor's July 2014 Business Crime Strategy, which sought to protect and increase threat awareness amongst businesses in London[19].

The London Digital Security Centre provides a shared service which involves the Metropolitan Police Service, the National Crime Agency, and the City of London Police working alongside academics, major businesses and technology organisations.

The Mayor's Office for Policing and Crime provided the initial funding for the London Digital Security Centre, and after two years it is expected to become self-sufficient – paid for by revenues generated from selling its services, and from donations.

As part of his election manifesto, the current Mayor for London, Sadiq Khan, indicated that he would "ensure Londoners and businesses have the information and resources they need to stay safe online"[20]. However he is yet to expand on how his commitment will work in reality, other than suggesting he will appoint a Chief Digital Officer at the Greater London Authority.

Therefore, the new Mayor has an opportunity to shape the way in London seeks to protect organisations from security breaches.

There is an opportunity to use the expertise developed by the London Digital Security Centre to develop proposals which will further help secure the data of all the organisations based in London.

While the London Digital Security Centre already offers organisations in London a security assessment, conducted by leading universities specialising  in ethical hacking, technology and businesses courses[21], it has not developed its own data security standard.

The establishment of a 'Mayoral Standard' for data security, developed by the London Digital Security Centre, has the opportunity to drastically improve the effectiveness of data protection in London.

Through the use of the Mayor of London's powers of convening, the development of a 'Mayoral Standard' could potentially enable all organisations in London the opportunity to introduce and adhere to a simplistic and cost-effective data security strategy.

The Mayor of London branding is well respected and instantly recognisable – it gives anything which contains it credibility.

Should a 'Mayoral Standard' include such branding, and those adhering to it be given an opportunity to display their certification containing the logo – this would boost the confidence Londoners would have in how their data was being handled by organisations

[18] Mayor brings in London Digital Security Centre to tackle cyber-crime, Mayor of London, October 2015: https://www.london.gov.uk/press-releases/mayor-tackles-cyber-crime

[19] Business Crime Strategy 2014-2016, Mayor of London, July 2014: https://www.london.gov.uk/sites/default/files/gla_migrate_files_destination/Business%20Crime%20Strategy%202014-16.pdf

[20] A safer and more secure London, Sadiq Khan for London, May 2016: http://www.sadiq.london/a_safer_and_more_secure_london

[21] Security Assessment, London Digital Security Centre, July 2016: https://londondsc.co.uk/services/security-assessment

they engage with.

The most important aspect of any 'Mayoral Standard' should be that it is both simple and cost effective – as this would encourage organisations to engage with it. This is often where existing attempts at standards have failed.

**RECOMMENDATION 1:** The Mayor of London should introduce a 'Mayoral Standard' for data security in organisations in London.

Another area where existing standards have struggled is in their market share. While the ISO/IEC 2700 series are widely recognised by professionals, the awareness of them generally is not particularly high[22], particularly within small and medium-sized organisations.

The Mayor of London, as a brand, has a significant level of recognition across London[23].

Should such a 'Mayoral Standard' include the opportunity to display Mayor of London branding[24], which would identify that an organisation has confirmed to it – it is highly likely that the confidence generated by the Mayor of London branding would be passed onto that particular organisation.

Therefore, in order to encourage awareness of any 'Mayoral Standard' it should include the opportunity to display an image prominently, indicating that an organisation conforms to it.

**RECOMMENDATION 2:** Organisations who sign up to the 'Mayoral Standard' should be provided with a Mayor of London branded image to display, thereby publicising that they conform to the standard.

The Mayor of London also has another valuable role in increasing the number of organisations who sign-up to a 'Mayoral Standard'. This role relates to those organisations that work with and supply the Greater London Authority and its associated organisations.

Should the Mayor of London actively encourage those organisations, who directly supply the Greater London Authority or its associated organisations, to adhere to the 'Mayoral Standard', it would generate awareness of the scheme.

Also, as the larger organisations working directly with the Greater London Authority and its associated organisations began to implement the 'Mayoral Standard', there would be a trickle down towards smaller organisations further down the supply chain.

While it remains important that the Mayor of London does not seek to heap extra regulation on businesses operating in London, his support for a 'Mayoral Standard' would be encouraging to those organisations who wish to work with the Greater London Authority and its associated organisations.

As organisations adopted the 'Mayoral Standard', they would begin to expect those

[22] Measuring effectiveness in information security controls, SANS Institute, April 2010: https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398

[23] The London Brand: 2000 years young, City Mayors, October 2012: http://www.citymayors.com/marketing/london-brand.html

[24] Look Book – Mayor of London Brand Guidelines, Mayor of London, July 2016: https://www.london.gov.uk/sites/default/files/2015_guideline_design_v2_fa.pdf

organisations they traded with to also adopt the 'Mayoral Standard' to ensure there were no weak links.  This would gradually lead to more and more organisations adopting the 'Mayoral Standard'.

**RECOMMENDATION 3:** The Mayor of London should work with organisations already supplying services to the Greater London Authority and its associated organisations and encourage them to adopt his 'Mayoral Standard' for data security.

# CONCLUSION

With a potential estimated cost of over £147 billion across the UK, and specifically over £35 billion from security breaches - it is clear that security breaches pose a significant risk to organisations.

While protections and schemes already exist, none of them have achieved the level of success they have predicted.  This has often been because of the complex nature of such schemes, or the costs involved in implementing them.

London is in a unique position – it can act as a market leader in data security, and encourage other parts of the country to follow its lead.

The introduction of a Mayor of London's 'Mayoral Standard' for data security would help protect London's data, and drastically reduce the number of security breaches which occur.

# LIST OF RECOMMENDATIONS

**RECOMMENDATION 1:** The Mayor of London should introduce a 'Mayoral Standard' for data security in organisations in London.

**RECOMMENDATION 2:** Organisations who sign up to the 'Mayoral Standard' should be provided with a Mayor of London branded image to display and therefore publicise that they conform to the standard.

**RECOMMENDATION 3:** The Mayor of London should work with organisations already supplying services to the Greater London Authority and its associated organisations and encourage them to adopt his 'Mayoral Standard' for data security.

## FEEDBACK

Connect with us online and tell us what you thought about this paper.

Twitter: @assembly_tories
Facebook: facebook.com/glaconservatives
Email: assembly.tories@gmail.com

GARETH BACON
LONDON ASSEMBLY
Greater London Authority
City Hall, The
Queen’s Walk
London SE1 2AA