# Management Clueless on 'Bring Your Own' Vulnerabilities

Submitted by: ECSC Ltd
Monday, 19 November 2012

The rise of employees being allowed to 'Bring Your Own' (BYO) device into the workplace is a major set-back for information security.  However, this development is being led by senior managers who are largely ignorant to the risks.

Who is to blame, and how bad is this situation?

A couple of years ago, the idea that employees might be encouraged to bring their own computing devices into the organisation, and use them for work, would have been considered a crazy idea - and a big backward step for information security.

However, a recent study by ISACA members shows that 23% of UK businesses are already allowing this.  The industry even has a catchy name for it 'Bring Your Own' (BYO).

Why is BYO being pushed so strongly.  Clearly, the rise of the iPad has played a big role.  You only have to walk down a first class rail carriage to see more of these in use by high salary individuals than traditional laptops.  Clearly, device manufactures are all for it - giving them a convenient entry into the business market with what was only ever designed as a consumer product.  Their concern is sales, not ensuring that security is maintained.

Ian Mann, founder of ECSC, says “Information security professionals all recognise the risks.  Devices outside of organisational control are a source of vulnerabilities.  They create a route for hackers to obtain confidential information, and this area is likely to be the next big cause of security breaches”.

So, is the answer to ban all employee owned devices?  Perhaps not, according to Lucy Sharp of ECSC, “Rather, you need to assess the risks.  What access are you giving them, what data may be accessed from (or stored on) these devices.”

As with all technology developments, you need to understand the risks, and develop appropriate controls to allow you to exploit new opportunities without compromising your information security.

Ian Mann, commenting on senior managers says, “The big problem here is one of communication.  Security and IT teams find it difficult to challenge the CEO who wants to use their iPad.  However, in our experience, if you effectively communicate the risks to management, they make more sensible decisions.”

Paul Lambsdown, Sales Director with ECSC adds, “As with all technology developments, there are potential business benefits - and these cannot be ignored.  It is the role of information security to facilitate new developments, whilst protecting critical information.”

ECSC has produced a Management Briefing 'Bring Your Own... Vulnerabilities', to help you understand the risks of BYO, and explain them to senior managers.  This can be downloaded from the ECSC web-site

homepage at
www.ecsc.co.uk

ECSC

Established in 2000, as vendor independent information security specialists, ECSC has grown rapidly to be the UK's leading service provider.  ECSC is a Level-1 Certified PCI DSS Service Provider for managed IT services, CREST accredited for penetration testing, and holds ISO 27001 (security), 9001 (quality) and 2000 (service management) certifications.

Covering managed services, consultancy and testing, it services all sectors, including financial, retail, transport, telecommunications, government and military.

Ian Mann is a Senior Consultant, and founder of ECSC.  He is best known as the author of Hacking The Human – the definitive book on social engineering, having previously been a consultant with GCHQ.
Paul Lambsdown is Sales Director, with oversight of all sales and marketing activities.
Lucy Sharp is Operations Director, with oversight of all ECSC service delivery.  She was previously a lead ISO 27001 consultant.

Call +44 (0) 1274 736223 and ask for Paul Lambsdown, or email paul.lambsdown@ecsc.co.uk for more information.

ECSC Ltd
London Office
Tower 42, 25 Old Broad St, London, EC2N 1HN, United Kingdom

Edinburgh Office
10 Lochside Place, Edinburgh, EH12 9RG, United Kingdom

Security Operations Centre
1 Valley Court, Bradford, BD1 4SP, United Kingdom

Tel: +44 (0) 1274 736 223
Fax: +44 (0) 1274 736 761
www.ecsc.co.uk

If you effectively communicate the risks to management, they make more sensible decisions.

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of ECSC Ltd

Copyright © 1999-2022 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051  f: 0345 370 7776 w: https://www.responsesource.com

responsesource