



## ISSA 5173: Update

### **Feedback**

Many thanks to all of you who have taken the time to download and review ISSA 5173: a new information security standard specifically for the Small to Medium Enterprise (SME) community, developed by the UK chapter of the ISSA.

The feedback has been overwhelmingly positive, with many feeling ISSA UK have addressed an issue which has been overlooked, despite the huge contribution of the SME community to the UK and global economies.

The standard was published by ISSA UK in March 2011 with much uptake by the IT press. ISSA UK has calculated that the standard readership had been around 30,000 worldwide and the ISSA have had offers of help with the standard from as far afield as New Zealand for the APAC region and the articles translated into Spanish for the Central & South American market.

*Here are the responses to the most popular questions you have been asking:*

### **What is the background & business case for this standard?**

David Lacey, ISSA UK's Director of Research, published a study *Review of Availability for Small/Medium Sized Organisations* via the Information Commissioner's Office in March 2010 and presented his findings to the ISSA later that month. Key research from that study discovered:

- SMEs provide 65m jobs in the EU
- SMEs account for 99% of the number of enterprises in the UK and EU
- In the UK alone there 4m micro businesses (10 headcount or less)
- SMEs rely heavily on the processing of information for their business
- SMEs' current weak security posture is the soft "underbelly" for industry and government, and often the weak line in the supply chain
- SMEs typically do not have in-house IT or legal expertise as do large companies.
- Current advice for SMEs online is disparate, with different websites excelling in different areas, and often not kept up to date.
- Existing approaches to information security do not sit well with the mindset of the small business owner, and do not encourage them to take action



### What makes ISSA 5173 different to existing information security standards?

- A free and open standard : cost is often an inhibitor to action in the SME space
- Drafted in language that is relevant and applicable to the small business owner.
- To provide a central source of practical guidance for SMEs that addresses current threats that are directly applicable to their lines of business
- To appreciate that different sizes of SMEs require a different approach and therefore tailor the approach to suit the SME. In all cases, the approach is to ensure board buy-in and end user awareness, but the delivery approach is more detailed the larger the SME.

### Are there any case further case studies or statistics that cover the SME sector?

This was addressed by Phil Stewart, ISSA secretary & Comms. Chapter Officer in his presentation to RSA Europe: [ISSA 5173: A New Approach to Information Security](#) . Case studies which either wholly or fully address this question include:

- Verizon Breach Report 2011
- Information Security Breaches Survey 2010 (*PWC*)
- SME Statistics for the UK & Regions 2010 (*BIS, May 2011*)
- Payment Card Trends & Risks for Small Merchants (*TrustWave*)

### What are the next steps?

- Currently the ISSA 5173 workgroup has defined 12 areas of key concern to the SME owner. These will form the basis for a series of – initially 12- guidance documents, to be published over the coming year
- Guidance will be localised to geographies to accommodate local legislation and working practices
- Guidance will be published, and also targeted to organisations to which most SMEs have access to (accountants & solicitors/ lawyers)

### Contacts & More Information

- The standard can be downloaded from the [ISSA](#)
- Feedback on the standard can be given to [SMESecurity@issa-uk.org](mailto:SMESecurity@issa-uk.org)
- Further updates will be announced on the [ISSA website](#) and also via [Twitter](#)