

Industry Cooperates to Address Information Security Awareness in the UK

The text below is the basis of a talk given by Dr David King, Chair of the Information Security Awareness Forum to the Parliamentary IT committee and the All Party Policing Group on the 18th March 2008.

Recent incidents of data leakage over the past 6 months have raised public awareness of the potential consequences of security breaches. In addition, there is an increasing awareness of the risk of “identity theft”, or “impersonation” as it has been more commonly called in the past. What can we do to mitigate the risk to individuals? And what should individuals do in the event that they are the victim of a “theft”.

Information security awareness continues to be a major concern to organisations. A survey by Infosecurity Europe on behalf of the Information Security Awareness forum of 1,311 companies has found that for 79% of organisations the single greatest security weakness that their organisations face is lack of awareness, with people not knowing about, ignoring or circumventing security processes and technical countermeasures.

In the UK, there is a question of who to listen to. Each of us has a different and several-fold role in society as an individual, employer, “Who do we listen to?” employee, consumer, seller and so on. There are several suppliers of advice on information security coming with a variety of different slants and agendas. But how can we pick apart these messages and get clarity. Who do we listen to?

There are several challenges that we face. At one level this challenge is apparently simple - what are the key messages for the audiences we are trying to address, and second, what channels and delivery mechanisms should be used. All of us are end-users and consumers of IT, many of us are employees of an organisation, large or small, some of us are directors or owners, than then are those of us who are in a position of influence to make a difference. It seems that we need to tackle awareness from many angles, and use a variety of approaches to deliver the message. No single delivery mechanism is likely to be sufficient to get the message across.

“need to use a variety of approaches to deliver the message”

The Information Security Awareness Forum

A number of professional bodies and organisations involved in information security have come together to form the Information Security Awareness forum to coordinate and build on existing work and initiatives, to improve their overall effectiveness, and ultimately to increase the level of security awareness in the UK that will help protect us all. We are a group whose aim is to deliver rather than to merely talk about awareness.

“...the aim is to deliver...”

A dilemma in creating a new forum is that it creates yet another organisation in what is already a very crowded security industry. However, we recognise that it is only by working together can we remove some of the duplication and overlap that exists, and to do this requires a mechanism that is recognised by the players in this space and with whom they can engage. There are many awareness initiatives, but there are overlaps in what is delivered and there also gaps.

The forum has no constitution or statute. The operation is based on trust, which we have established through a “neutral ground”, with no one member dominating the agenda. The representatives that sit on the forum are volunteers, and so resource and time is limited. The choice has therefore

been made not do develop a constitution or a statute. The focus of its members is on getting things done, and this is being achieved on the basis of trust and partnership.

One of the first deliverables of the forum will be a Guide for Directors. This will be a set of short guides covering different aspects of information security which directors of organisations need to be aware of. The guide is being developed in conjunction with BT and the Information Assurance Advisory Council, and is an example of how we will engage with industry players through our support of projects focused around specific deliverables and outcomes.

The forum is developing a register of activities and events for its members which will assist in identifying overlaps and gaps. Other activities will be the preparation of messages in response to incidents and issues in the public domain, development of a web-site for the forum to endorse and link to awareness resources, and providing content review and input to major initiatives such as GetSafeOnline and the BERR Information Security Breaches Survey for example.

The Information Security Awareness Forum is also organising a Security Awareness Week which will take place between the 21st and the 25th April this year. Many members of the forum are engaged in awareness activities during the week. The week will see the launch of the BERR Information Security Breaches Survey. (ISC)² will be issuing the results of the Global Information Security Workforce Study 2008. The week also features the InfoSecurity Europe 2008 show at Olympia, and the Jericho Forum conference.

Linking up with eCrime

The awareness work that our members are engaged in needs to be complimented by an effective mechanism for reporting and handling

investigations into eCrime. There needs to be an effective reactive mechanism to compliment the proactive awareness activities, and the forum is not in a position to deliver this part of the equation. However, I believe that it is essential that the forum engages with an effective eCrime policing function to ensure a joined-up approach to reducing eCrime and protecting the interests of all of us. We very much welcome the current debate and look forward to exploring opportunities to work together.

[wc:937]