

## Raising awareness of the 12 main threats to online security

### Monthly Information Risk Themes

Press Release – 17<sup>th</sup> February 2010 - The Information Security Awareness Forum (ISAF) has produced a rolling calendar of themes for the 2010 where each month sees a focus on a main threat to information security. Many of the member organisations will be working on awareness activities to this schedule, magnifying the message. The information security world has never been very good at delivering bite-sized and interesting nuggets of knowledge to the General Public, even though the threats to those people are ever increasing<sup>i</sup>, with the digital netherworld of criminality costing the UK “billions”<sup>ii</sup>. Formed in 2008, the ISAF was created to co-ordinate the awareness activities of its 23+ member organisations and to improve the communication of information risk issues to industry and the General Public.

Like insurance, information security tends to be interesting only to people when something bad happens. It is quite easy to take simple steps to reduce the likelihood of the victim being you.

“The ISAF calendar will help the member organisations and others in the industry co-ordinate their awareness activities around specific themes. This increased focus will help create opportunities for partnership and assist in planning and collaboration to raise awareness of good security practices.” Dr David King, Chair of the ISAF

Professor Jim Norton, Chair of the IET IT Policy Panel welcomed the initiative saying: “Creative use of ICT continues to bring great benefits to our Society, but every silver lining has a dark cloud. It is vital that we continue to raise awareness of the risks involved and I commend ISAF’s comprehensive approach to this.”

Tony Neate, managing director of Get Safe Online the UK's national internet security initiative, commented: "Get Safe Online very much welcomes the work that the ISAF is doing in collating the activities of its member organisations through its new monthly themed calendar. The calendar will be an essential tool in the co-ordinating security events that the ISAF does so well. This initiative will help to harness the skills and experience of a wide variety of experts to raise awareness and get the message of good security to all."

John Colley, Managing director of (ISC)<sup>2</sup> EMEA, “As founding members of the ISAF, (ISC)<sup>2</sup> welcomes this initiative. Too often awareness is ineffective due to the fact that too many messages are being communicated to too many people. By focussing on specific issues each month, the calendar provides a means to deliver these important messages to the people that really need to understand them”

### **The Calendar**

#### **January – Social Engineering/Phishing**

Confidence tricksters will try any method to extract information or money from victims and are surprisingly successful. Social Engineering is the general term for the process of gaining a person’s trust to the point where they part with valuable information that they would otherwise keep private. In a business, this might involve someone pretending to be from the IT department and asking for a username and password: most people are conditioned to be helpful and will provide this information. In a home context, this might manifest itself as a phishing scam, where a user is fooled into logging on to a page that looks like their bank, but it isn’t.

#### **February – Mobile devices**

Mobile phones, laptops and PDAs are increasingly holding vast amounts of information. Aside from the resale value, devices synchronised with email, either personal or through work, are useful to identity thieves. Many people use their devices to carry contact details, birthdays and files around with them, but apply less security than where this data normally lives, i.e. on their computer. Every device has the facility to PIN or password protect it, but most people don’t use this functionality.

#### **March– Child Protection/Online identities**

“On the Internet, nobody knows you’re a dog” – New Yorker cartoon, 1993  
([http://en.wikipedia.org/wiki/On\\_the\\_Internet,\\_nobody\\_knows\\_you%27re\\_a\\_dog](http://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog))

<sup>i</sup> <http://www.ft.com/cms/s/0/e160f504-1d76-11de-9eb3-00144feabdc0.html>

<sup>ii</sup> <http://www.ft.com/cms/s/0/5ea68e12-61eb-11de-9e03-00144feabdc0.html>

It is very hard for people to really know who they are talking to online. Children find this especially hard, as they have not had the life experiences that make most older people cautious. Predatory paedophiles take advantage of this trait to trick children into believing they are talking to a person of their own age.

#### **April – Awareness – Infosecurity Europe**

Part of any drive to improve information security must include raising awareness of staff and customers of the risks of using the Internet and computers in general. The most important element in this piece is to identify the audience, bearing in mind that many people wear multiple hats (employee in a large corporate and a home user) and what is relevant, specifically, to them. It is important that awareness is not restricted to campaigns in big business, or the Government, but is promoted by everyone with the capability to provide advice.

#### **May – Compliance/The law**

While the Internet does seem to be very open and borderless, this isn't actually the case. Geographic laws apply equally online as in the real world. The Internet reduces the distance between them. Companies and individuals should be aware of where their data is being stored and what laws apply to it. For example, two people in the UK communicating using Hotmail are actually exporting their data to the US. Different countries have different laws on encryption, and international travellers should be aware of these. There are also a series of conditions for trading that many companies need to adhere to, for example relating to credit card processing, that sit over and above the laws of the land, like PCI DSS.

#### **June – Identity Protection**

Identity theft is an increasing problem and criminals are getting more inventive. There are a number of simple ways to protect yourself from falling victim to these sorts of scams, including reviewing what information you post on social networking sites, shredding important documentation before it goes into the bin and regularly reviewing your credit rating.

#### **July – Convergence/Physical protection relating to InfoSec**

Many of the concepts in physical security are just as applicable to electronic security. The two disciplines complement each other and, yet, few organisations take a holistic approach to both. Often, the responsibilities lie with different parts of the business and opportunities are missed. Major benefits can be realised through the bringing together of physical and information security.

#### **August – Risk Management/How to assess dangers online**

The basis for implementing any sort of information security programme must be based on an understanding of the risk being faced. Similarly, home users should be aware that some of the people connected to the Internet do want to do them harm. Most unprotected PCs on the Internet will be infected with malicious software within minutes.

#### **September – Business Continuity/Backups**

It is important when planning to protect yourself that you consider the worst case scenario. If your data is lost, what is its value to you and what do you put in place to protect it. In many cases, the information that a company holds is its most valuable asset. At home, many families prize their digital photo albums. By keeping backups and recovery strategies, you will ensure that your information remains available even after the worst case.

#### **October – Corporate Governance**

Companies that want to reduce their risks associated with information security should undertake a strategically-focused programme of works, centred on a formal methodology for information security management. A number of sets of standards exist to help with this, the best known of which is the ISO27000 suite. By creating a framework within which to operate, companies can ensure that they cover all aspects of the discipline and reduce their risks in a controlled manner.

#### **November – Crime**

Due to the Internet's nature of removing distance as a barrier between people and the ease of interacting with large numbers of people simultaneously, criminals are exploiting the Internet in a similar way to business. All users of the Internet must be made aware that the scale of the criminal activity on the Internet is enormous, running into billions of pounds each year and comprising multiple layers, from money mules to organised crime bosses. However, the frontier-nature of the Internet is coming to an end. The same sorts of crimes can be committed online as in the real world, by and large, and the Police are increasingly dealing with online crimes in the same way as those committed offline.

#### **December – Malware**

Malicious software is a constant threat on the Internet. It installs itself on a victim's computer and then undertakes some unwanted action, without the victim's consent. Much of it has links back to organised crime and the effects on infected machines vary. Bot nets are virtual networks of infected machines that are rented out to other criminals to do a variety of things, including send spam, take down established businesses if they don't pay protection money and more. It is imperative that everyone uses anti-virus software and keeps their machines patched.

### **About 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 (ISAF) [www.theisaf.org](http://www.theisaf.org) 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 forum was launched on the 13th February 2008. The member representatives meet monthly to progress the agenda and actions of the forum.

Founding members of the forum include ASIS International, the BCS, CMA, the Cybersecurity Knowledge Transfer Network, eema, EURIM, Get Safe Online, IAAC, the Information Technologists' Company, Infosecurity Europe, the Institute for the Management of Information Systems (IMIS), the Institution of Engineering and Technology, the International Underwriting Association of London (IUA), ISACA, (ISC)<sup>2</sup>, ISF, ISSA, the Institute of Information Security Professionals, the Jericho Forum, the National Computing Centre, the National e-Crime Prevention Centre (NeCPC), the Police Central e-Crime Unit, SANS and SASIG.

The forum is chaired by Dr David King and its secretary is Stephan Freeman.