Source: **Les Fraser** **Version** **V0.1**

Document for:

Decision	
Discussion	x
Information	

Social Networks – Problems of Security and Data Privacy
Statement

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS –which represents 37 Member Societies in 33 countries across greater Europe – has agreed on the following statement:

1. Introduction

The use of the Internet is changing as new ways of exploiting it are found – social software / social networking services move the focus of the web away from the content suppliers and give more control to the user. This is, in general, a good thing but brings security and privacy problems.

From a personal perspective, there is a huge growth in the volume of personal information being shared on the web and often those sharing their information do not think carefully enough about how this information may be used. Both the individuals and the companies providing the services need to be more security aware and to take greater responsibility for their actions.

From a commercial/business perspective, there is an overwhelming business case for exploiting the opportunity to interact with customers through the these sites, but the benefits also bring new risks to the business, as social software sites become integrated into the business computing strategy yet are not controlled by the business. The level of security offered on these sites is not robust.

2. Issues

Personal information may be uploaded by an individual to be made available to their friends, or company information may be supplied by an organization to communicate with staff or customers, but the information may be placed on a server which is located anywhere in the world and viewed globally. Those providing the information need to be more aware of the potential consequences.

Companies offering the services people use need to be security-aware and to be more open about the level of security offered.

National initiatives are usually ineffective in cases where information is stored in a foreign server farm which is owned by a foreign company and is then exploited by hostile foreign individuals, and wider international agreements need to be put in place.

Virtual reality sites such as 'Second Life' have additional issues which are not yet fully recognized. These sites offer opportunities for individuals to interact in various ways, by use of 'avatars' or virtual people which the participants can control. This may expose not only personal information, but attributes of behaviour which may be analysed. The exploitation of the facilities on offer for illegal purposes is not well understood, but where the virtual world environment has an economy based upon real money, and allows people unlimited scope to work through their avatars to interact with others, exploitation is inevitable. It may be a game, but the consequences can be real, and the internationally based virtual world needs to be policed.

For a more detailed analysis of the issues described here, please refer to the CEPIS Background paper on Social Networks – Problems of Security and Data Privacy.

3. Recommendation

CEPIS sees extreme importance in ENISA and national authorities taking the following actions:

(a) Encourage the citizen to gain a better awareness of the issues involved, to protect the citizen from the consequences of their actions;
(b) Encourage international agreements on security and privacy protection responsibilities of the service supplier, and on the standards to be adopted;
(c) Initiate a debate on the need for new standards and a new approach to security and privacy protection for organizations wishing to use these sites for commercial purposes;
(d) Initiate debate on the legal and social implications of virtual world 'crime', including the extent to which the actions of avatars may be legally attributable to the avatar 'owner' and an agreed way of defining the jurisdiction under which this may fall;
(e) Promote 'Safer Social Networking' for all.