Social Networking – General Risk Assessment

Scottish Information Assurance Forum
Best Practice Working Group

Social networks may be described as internet-based applications that allow users to create profiles and share content easily with other users. A huge variety of these applications are readily available and users can interact from a large range of devices, including mobile phones. Many organisations have embraced Social Networking as a cost-effective and quick way to engage their clients or promote their brand to new and existing markets.

As with other internet-based systems, there are a number of risks that should be fully managed and understood before organisations adopt social networking too widely. A range of controls will usually be required in order to balance these risks with the business needs.

This document is presented in an effort to describe some of the main risks in a non-technical way, to aid the debate within organisations around social networking. The risks detailed in the table below are based on the assumption of relatively open access to social networking for staff in a business environment.

Actual measures of risk are not given as these can vary between organisations and sectors. For example, a bank may be more risk-averse than a marketing organisation. Similarly, risk mitigation strategies are not discussed here as without an understanding of the exposure to a risk it is difficult to generalise as to what would constitute an acceptable mitigation strategy.

Some of the risks described in the table below are associated with the behaviour of staff. Governance must take into account technical capabilities and relative tendency of staff to engage in risky behaviour on these sites. It may be easier to anticipate bad behaviour and reputation damage so that these risks can be mitigated prior to adoption.

It should also be noted that some of the risks are not related to the actual technology used, or to the security of information. For example, the risk of 'loss of productivity' or 'time-wasting' is often cited as the primary reason why some organisations choose to block access to social networking sites. Similarly, when it comes to the risk of 'reputational damage', the reaction to a incident needs to be very carefully managed, usually with input from 'communications' or 'public relations' staff.

As social networking risks and benefits may be shared across different business units, it is recommended that an organisational-wide strategy is developed which engages risk owners and stakeholders.

It is also worth noting that some of the risks below are already established risks, for which some mitigating actions may already be in place. An example might be the risks associated with 'virus infection' or 'malware'.

In reading the table below please bear in mind that these risks are being presented to help stimulate informed debate around the issue of social networking, and to help the business understand some of the risks that may need to be considered in your organisation.

No	Risk	Detail	Symptom	Area of Responsibility	Category
1	Disclosure of Personal Data	Social networking sites allow people to share personal information about themselves. This might include their name, age, gender, location, workplace, family members, interests, and so on. Photos can also contain information such as car registration plates in the background. Photos taken on certain devices (such as mobile phones) may also be tagged with location information as part of the photograph properties. Personal information posted in a user's online profile may be mis-used, potentially leading to 'identity theft' or 'social engineering attacks' (see below).	Identity theft / account hi-jacking Social engineering attacks	Information Security	People
2	Identity Theft	Some of the personal data sometimes posted on social networking sites may also be used for identity verification (e.g. birthday). This data may be used by criminals to impersonate an individual, usually in order to gain access to resources such as a bank account, or to obtain credit or other benefits in their name.	Fraudulent activity, usually financial, which can adversely affect the victim of identity theft	Information Security	People
3	Social Engineering Attacks	Social engineering attacks can occur when personal information available online is used to help trick people into releasing confidential, sensitive or otherwise useful information, either about themselves, or their organisation. The personal information available online might make it easier to successfully target an individual. For example, 'LinkedIn' often contains organisational information.	Information wrongly provided to a third party, which is subsequently used for malicious purposes	Information Security	People
4	Identity Hi-jacking	Often, social networking sites use fairly basic methods to verify a user's identity and simple password controls. This makes it relatively easy for one individual to pose as another, or to create a 'fake' organisational profile. This is usually done to inflict personal or reputational damage.	Reputational damage May lead to other attacks, including the distribution of 'malware' (see below), or financial scams such as asking 'online friends' for money	Information Security	People

No	Risk	Detail	Symptom	Area of Responsibility	Category
5	Physical Safety	Online activity can lead to actual physical attacks as users may post their address, family details and location (directly or indirectly). This is particularly relevant for individuals who have sensitive roles or positions within society. Some social networking sites, such as 'Twitter' or 'Twitter 360',can contain an individual's actual real-time location.	Physical attack	Information Security	People
6	Online Bullying	Bullying and harassment are sometimes conducted online. Children and adults can find themselves the subject of this type of activity and employers should remember that they have 'duty of care' for their staff.			
7	Malware	'Malware', such as computer viruses and worms, can be embedded in software, graphics and weblinks within social media sites. Although this is an existing internet-based risk, social networking provides new distribution methods which include mobile devices through SMS / MMS / Mobile Internet Browsing and 'Apps'.	Distribution of malware onto computers and mobile devices through staff or corporate profiles.	Information Security	Technology
8	Reputation	Organisations, as well as individuals, increasingly have an online presence within social networking sites. Reputational damage can occur through identity theft, or simply through online postings / responses made by others. Also, organisations that advertise within social media sites may be subject to abuse or modification of their advertising content.	Personal and/or corporate reputations are damaged through the posting of inappropriate and/or unwelcome content.	Public Relations / Marketing / Communications	Information
9	Legal and Regulatory	Content posted, accessed or distributed by individuals or staff can create legal and financial liabilities Some organisations may also have a regulatory requirement to record all customer contact. The legal framework around social networking is evolving and can vary greatly between sites and across countries.	Examples of exposure to legal liability include: slanderous, libellous, or defamatory comments; leakage of sensitive information; online bullying; breach of copyright; and, breach of intellectual property rights.	Information Security	Information

No	Risk	Detail	Symptom	Area of Responsibility	Category
10	Crisis Management	'Crisis management' is changing, due to widespread use of the Internet and social media. Full-blown crises can evolve very quickly, in a way that many organisations have never dealt with before.	Virtual pressure groups can form quickly, requiring prompt action. The increased pressure could result in an inappropriate response.	Public Relations / Marketing / Communications	Information
11	Data Leakage	Internal information, trade secrets or intellectual property may be leaked into the public domain via social networking sites. This could have financial implications. For those organisations that sell information, such as newspapers, information released through social media could undermine revenue-based services. Once posted online, it is virtually impossible to completely delete it.	Breach of intellectual property or internal information. Loss of income Loss of competitive advantage Loss of confidence / trust	Information Security	Information
12	Productivity	Social networking sites are generally accessible from a range of devices such as computers, phones and PDA's. This means that users can receive alerts and access sites almost 'anywhere, anytime'.	Reduced productivity in the work environment	HR / Business Managers	People
13	Professional Standards	Social networking tends to be based on a single identity or profile, often making it hard to separate work and personal life. By comparison, e-mail is more straightforward, as users can have a work and personal e-mail address.	Can contribute to a loss of productivity. Blurring of the line between personal and professional life.	HR / Business Managers	People
14	Governance	If social networking is embraced within an organisation, there is a risk that existing governance arrangements may be undermined.	New, informal work practices develop which don't conform to existing lines of authority.	HR / Business Managers	People
15	Recruitment	Social networking sites are increasingly used during recruitment processes. Given the possibility of identity theft, pertinent information should be verified through other channels.	People may be wrongly excluded from a position as a result of content linked to their identity, on social media sites.	HR	People
16	Inappropriate Activity	There is a tendency for people to engage in 'risky' behaviour on social networking sites.	Staff subject to disciplinary action as a result of their online conduct.	HR	People
17	Weak Authentication	Typically, user access to social networking applications is not sufficiently secured. This can lead to identity theft and 'hacking' attacks.	User accounts and identities can be compromised.	Information Security	Technology

No	Risk	Detail	Symptom	Area of Responsibility	Category
18	Audit Control	Communications and data transfers made through social networking sites are not easily audited. Some sites use a range of different applications or functions to encourage interaction with other sites, for example, combining social networking with 'online storage' sites, 'instant messaging' or e-mail.	Inability to monitor or record communications or to enforce copyright or distribution controls.	Information Security	Technology
19	Content Control	It is harder to control the distribution of information within social networks as the audience can be very large and effectively, anonymous. By comparison, e-mail tends to be aimed at specific people, allowing some control over content distribution. Some social networking sites may contain 'Adult' or otherwise 'inappropriate' content, particularly within adverts. In some cases, social networking sites have terms and conditions which mean that they actually own any information once it is posted.	Reduced control over distribution of information, potentially leading to data leakage and/or records management issues.	Information Security	Technology
20	Continuity	Attacks on social networking sites may render them unavailable. For organisations that utilise these sites for business purposes, this raises business continuity issues.	Loss of service	Business Managers	Technology
21	Technical Fault	There have been examples in the past where a technical fault has resulted in a failure to implement the user's privacy settings.	Release of sensitive and/or personal information.	Information Security	Technology
22	Bandwidth	Widespread use of social networking sites may increase the amount of internet bandwidth required. If the service is not properly planned, then it could impact other services that rely on the same bandwidth.	Loss of service	Business Managers	Technology