SECURITY RISKS AND IMPLICATIONS FROM THE UNCONTROLLED USE OF SOCIAL NETWORKS IN THE SANDF

BY: MAJ G.P.J. DE JAGER

SCOPE

Introduction

Offensive Information Collection

The Value of Information

Social Networking

The Importance of Information Security

Modern Day Information Security Challenges

Social Networking Risk Assessment

Control Measures

Conclusion & Recommendations

INTRODUCTION

Through the ages as one era brings about a new way of living, adaption to these new ‘technologies’ are prominent.

Within the age of information came the age of knowledge, characterised by the easy accessibility not only to information, but to knowledge.

Social networking is such an application of technology that has expanded into a vast array of applications to fit the modern lifestyle.

OFFENSIVE INFORMATION COLLECTION

Information collection started as early as warfare itself and was recognised as a valuable input to determine the outcome of battles and victories.

Various methods were applied to gain access to information, such as reconnaissance, patrols, infiltration techniques, bribery, etc.

The aim of information collection is to obtain sensitive or secret information that can be used as intelligence.

The following methods are used to collect sensitive information, specifically focussing on the online domain:

- Open Source Intelligence (OSINT)
- Eavesdropping
- Espionage.
- Social Engineering.

THE VALUE OF INFORMATION

It is important to note that the value of information is not a constant value, but it changes from situation to situation – OPSEC (wartime vs peacetime)

Due to the fluctuation in the value of information, it is important to realise the measures of control that can be implemented to mitigate the risk of losing valuable information to an undesired source

One major concern is that Military members are not happy with the effectiveness of official channels and some resort to unofficial channels such as social networking to convey official information.

Information obtained through social networks can add value to determine the bigger picture. The information shared on social networks will carry different weight pertaining to the situation in which it was shared with others.

SOCIAL NETWORKING

The number of people accessing the Internet via mobile phones may soon increase to exceed the numbers doing so via wire line devices. Wireless receivers combine as much as cell phones, PDA functions, MP3 players, cameras, GPS and remote control features into one device.

The results of global connectivity can already be seen, as nearly all members are having at least one device that has access to the internet. The focus has shifted from the traditional use of desktops and laptop to the more user preferred adaption of tablets and cellular phones. On average there are approximately 0.8 computers per person, while there are approximately 1.6 mobile devices per person.

There is a tendency that younger members are more prone to owning more than 1 mobile device. This is a clear indication of the shift to mobile devices as preferred devices to keep social networking activities on.

SOCIAL NETWORKING

People who tote digital cell phones could very well become the eyes and ears of a watchful society. They could provide information, including still or moving imagery, on events as they happen. Such reports could have excellent geospatial accuracy from knowing where the phone is plus maybe some rough-and-ready range finding from the caller to the event and valuable voice annotation.

The SANDF should take into consideration that there is a clear indication of the shift to mobile devices as preferred devices to keep social networking activities on, especially among the younger generation. This can be estimated to grow in numbers as younger members join the SANDF each year, thereby flagging it as a possible concern in new developments that current policies do not cover.

THE IMPORTANCE OF INFORMATION SECURITY

OPSEC: The protection of data against deliberate or incidental disclosure to unauthorised people and against unauthorised change.

Living in a free society with advanced technology contains harsh trade-offs for OPSEC.

As deployment situations can become very intense and critical to uphold information security it is important to note what method of communication members of the SANDF prefer to communicate home with, as this can cause certain breaches of security.

The SANDF may not be able to stop every member from participating online in social networks, but it should focus on ensuring that every member is aware about the importance of information security during the use of social networks. It is evident that there will only be more information exposed on social networks as the younger generation increase and mature within the organization, therefore it is essential to supply them with the correct knowledge of social network risks and implications.

MODERN DAY INFORMATION SECURITY CHALLENGES

Modern Information Security challenges in today's digital lifestyle include the following:

- Blending of corporate and personal lives
- Inconsistent enforcement of policies
- IT doesn't own and control all devices
- Covert attacks are no longer obvious

Due to the dynamic changes in the modern technologies and devices it is imperative that routine reviews be conducted.

The security risk review process is a detailed process that must be conducted by a skilled team in information security. The advantage of the review is that it does not entail an entire security assessment being conducted, but only a review on the existing security processes.

SOCIAL NETWORKING RISK ASSESSMENT

Risk Management is a foundation of information security programs; it is argued that the future of information security must focus on risk decisions in order to combat the ever-changing threat landscape. It does not address elimination of risk as that is not a reasonable goal, other than to mitigate the effects.

For a risk to be qualified the SANS Institute defined the following three ratings:

- Sensitivity – value relative to resource's tolerance for risk exposure.
- Severity – magnitude of consequences from threat realising.
- Likelihood – probability that threat will realise and how often it will occur.

Even though it can be determined how many devices and profiles members are having, it means little without knowing how much time is spend on social networking sites and applications. Daily access being the majority currently, of which 30% is hourly or less.

SOCIAL NETWORKING RISK ASSESSMENT

Frequency is the value assigned to measure how often an event could occur. Control is rated and the reverse rating used in calculating the likelihood score, it refers to the better the control, the less likely the threat would materialise.

Final Likelihood Score = ((Exposure + Frequency) / 2) x (Reverse Control)

Social Networks						
Threat (Agent & Action)		Vulnerability	Exposure	Freq	Ctrl	Likelihood
Users	Disclosing sensitive information	Aggrieved employees, Lack of controls	5	1	3 (0.6)	2

Final Risk Score = Impact x Likelihood

Social Networks					
Threat (Agent & Action)		Vulnerability	Impact Score	Likelihood Score	Risk Score
Users	Disclosing sensitive information	Aggrieved employees, Lack of controls	5	2	10

Risk Classification and Ranking (Low, Moderate and High)

Social Networks				
Threat (Agent & Action)		Vulnerability	Risk Score	Classification
Users	Disclosing sensitive information	Aggrieved employees, Lack of controls	10	Moderate Risk

CONTROL MEASURES

The DOD Information Communication system security policy.

Even though members are aware about disclosure of official information 75% of members agree that the current communication systems (Letters, Landlines, Lotus Notes, etc) of the Army are not sufficient to reach the correct people in time for official communication. To save time nearly half of all members make use of social network applications to inform others of certain work related aspects.

The Social Networking policy was developed much later than the ISS Policy.

Security awareness and training programs can serve to inform employees about their organisation's information security policy, to sensitise them to risks and potential losses, and to train them in the use of security practices and technologies.

Social networking must be incorporated in such a way that all members are aware of the regulations provided for social network usage. Information security awareness and training programs must be an integral part of development of all soldiers.

CONCLUSION & RECOMMENDATIONS

The value of information is changing continuously, trends on social networks may be short lived, but the information would stay available and exposed for far longer than expected.

There is a clear indication of the shift to mobile devices as preferred devices to keep social networking activities on, especially among the younger generation.

The security risk review process is a detailed process that must be conducted regularly by a skilled team in information security. This will serve as an indication to identify and mitigate risks not previously encountered.

The focus of security need to be shifted to compliance and that can only be achieved with a detailed training and awareness plan.

In order to have members comprehending the implications of using social networks, it must be explained to, and experienced by members little by little. Dramatic changes will lead to resistance from members and will be difficult to enforce.

THANK YOU

"IF YOU WANT TOTAL SECURITY, GO TO PRISON. THERE YOU'RE FED, CLOTHED, GIVEN MEDICAL CARE AND SO ON. THE ONLY THING LACKING… IS FREEDOM" – DWIGHT D. EISENHOWER