International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

CYBER SECURITY ISSUES IN SOCIAL MEDIAS

C.Theebendra[1], C.Kokila[2],
Asst. Professor, Department of Computer Science & Applications[1]
M.Phil Full time Research Scholar, PG and Research Department of Computer Science[2]
Vivekanandha College of Arts & Sciences for Women (Autonomous),
Tiruchengode,Namakkal-637 205,
Tamil Nadu, India
theebendra@gmail.com[1]
kokilachlm1994@gmail.com[2]

ABSTRACT- Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe.. Social networking websites such as Facebook, Twitter, Myspace, Google+, and LinkedIn are the popular social sites. Facebook is most popular social networking site. So we conducted a survey to find users view regarding security and privacy of social networking sites and regarding default privacy setting improvement particularly Facebook. In this paper The default settings share everything, users have to change their default privacy setting options to make their accounts and personal information more secure. we present several of these privacy and security issues of Social Networks

Keywords: Online Social Media, Social Networking, Security Risks,

I.INTRODUCTION

Social networking is the rage of this age. Social networks are formed when people sharing certain interests including hobbies, religion, politics, etc., coalesce into groups or communities.

In modern times it refers more to online communities because this is where most social networks tend to exist. To facilitate such social networking, there are many websites. These social networking sites include Face book, MySpace, Orkut, Twitter, Fropper, etc. Such sites help people to keep in touch with each other and also connect with long lost friends from school and college.

Though it began as a craze among the youth, people of all generations have caught the fad now. Membership can only be gained through existing members who will admit you into the circle as their friend. People can upload photos and videos through these sites and share them with their circle of friends.

Social networking comes in handy when one needs a job. We can use our contacts to learn of good job opportunities. Advertisers also have found social networking sites a useful tool to get feedback on their products as people tend to believe their peers' opinions on certain products rather than an advertisement. This has led them to use such sites to promote their products.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

II. SOCIAL MEDIA NETWORKING

As traditional social networking (i.e., club, party, seminar, etc.) communicates between people with similar interests in physical spaces, online social media networking is the same with it except for the place to meet; from physical space to cyberspace, especially the Internet. One of the strongest growth areas has been in the adoption of social networking sites, such as Facebook and currently more than 500 million users in Facebook enjoy games or sharing information in web applications.

With the popularity of mobile devices and applications combined with social networking technologies, communication using online social networking tools is becoming a new way of life to the people. Online social network services, such as Youtube, MySpace, Facebook, LinkedIn, and Twitter. Involving individual Internet users as well as multiple organizations are emerged as new communication platform in today's dynamic and complicated Internet based business world. However, with the explosive growth of social media coupled with applications, securing user's information and the related systems is extremely challenging. Figure 1 shows the generic network architecture for online social network services.

Social Media networking As traditional social networking (i.e., club, party, seminar, etc.) communicates between people with similar interests in physical spaces, online social media networking is the same with it except for the place to meet; from physical space to cyberspace, especially the Internet. One of the strongest growth areas has been in the adoption of social networking sites, such as Facebook and currently more than 500 million users in Facebook enjoy games or sharing information in web applications. With the popularity of mobile devices and applications combined with social networking technologies, communication using online social networking tools is becoming a new way of life to the people. Online social network services, such as Youtube, MySpace, Facebook, LinkedIn, and Twitter. involving individual Internet users as well as multiple organizations are emerged as new communication platform in today's dynamic and complicated Internetbased business world. However, with the explosive growth of social media coupled with applications, securing user's information and the related systems is extremely challenging. Figure 1 shows the generic network architecture for online social network services.

Individuals now bring their own computing devices to the office, mixing company and personal data on the same machine, and mobile devices are increasingly replacing desktops as the standard in business technology. All of these changes greatly increase the potential for data loss.business processes to partners, moved data and applications to "the Cloud" and embraced social media for communication with customers and collaboration with suppliers.

Sharing information is now the way of business and social life. Companies have outsourced .As the realities of these changes on modern business

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

practice take hold, it is quite possible

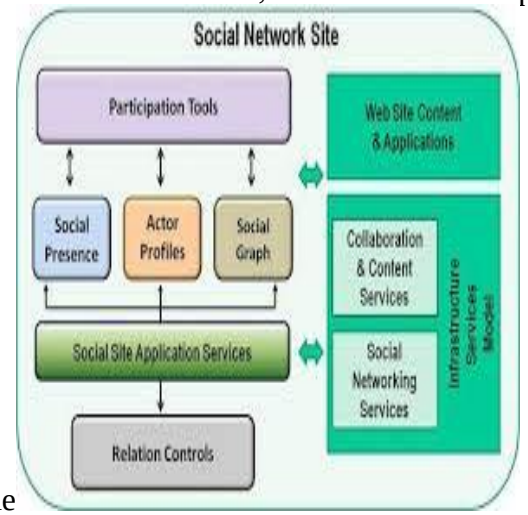

Figure 1. Social Media Network Architecture

III.CYBER SECURITY RISK IN A SOCIAL MEDIA WORLD

That we have crossed a dangerous line in this new information sharing culture. How are we to know if we are putting too much of our personal information on the Internet? And are we blurring the lines between what should and shouldn't be said in public?

We've come a long way since the "Loose Lips Sink Ships" campaign of World War II, when a "need to know" concept was enforced and warned against giving away anything that could help the enemy. Now, seemingly irrelevant snippets of personal data can be used to piece together intelligence to enable hackers to target individuals, facilities and organizations. We are now at war over information. Hacktivists, criminal gangs, terrorist groups

Figure 2.Risk of Social Media

III.CYBER SECURITY RISK IN A SOCIAL MEDIA WORLD

That we have crossed a dangerous line in this new information sharing culture. How are we to know if we are putting too much of our personal information on the Internet? And are we blurring the lines between what should and shouldn't be said in public?

We've come a long way since the "Loose Lips Sink Ships" campaign of World War II, when a "need to know" concept was enforced and warned against giving away anything that could help the enemy. Now, seemingly irrelevant snippets of personal data can be used to piece together intelligence to enable hackers to target individuals, facilities and organizations. We are now at war over information. Hacktivists, criminal gangs, terrorist groups and even rogue states are targeting valuable intellectual property, customer and employee personal details. Individuals must consider their Web profiles, behaviors and security

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

settings and wise up to the risks. Companies are also exposed to risks interacting with their supply chain, partners and customers.

A. New Business Strategy

To reduce cyber risk, companies need to develop a new business strategy that is "secure by design" and understand that this isn't just a technology issue, but a wide-ranging problem that encompasses culture, processes, staff behavior, training, and includes interactions with suppliers, partners and customers.

A key component in this strategy is to decide upon an information classification scheme. A decision must be made about what type of information should be kept secure, shared internally and published externally. Employees must be made to know what they should and shouldn't be sharing, so the information must be marked to make it clear. Furthermore, they must understand what criteria to apply when marking their own generated content and handling protectively marked documents. Rules should be in place on information handling to reduce chances of leakage and information should be shared on a "need to know" basis internally as well as externally.

The military have used a multi-level security system and protective marking scheme for many years. This six-tier system ranges from "Top Secret" to "Unclassified" and was designed to protect paper-based information stored in filing cabinets and moved between places physically. Companies should introduce similar schemes. Here is a pragmatic example of security classification levels for different types of data:

1. Private – Company-critical information including personnel records, customer data, intellectual property, for example inventions, the design of products, components or future products, concepts and plans.
2. Transactional / Confidential – Information that needs to be shared with suppliers and customers for the business to run including contracts, invoices, purchase orders, proposals.
3. Unclassified – Data that can be shared with the world in print or online.

Some, but not all, data may move from "Private" to "Unclassified" over time. For example, the marketing strategy starts as "Private" but then becomes "Transactional" (but embargoed) as events are planned with partners, with some data becoming "Unclassified" as the campaign is launched to the public. Website content will be considered "Confidential" until it is published, but even then the organization will still own the copyright.

Controls and measures need to be put in place appropriate for the security level and industry cyber risk profile.

B. Collaboration at All Security Levels is Required

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

A key issue is that companies need to share information with partners at all levels. For example, an aircraft component design may need to be shared with a third-party manufacturer. The key emphasis and business enabler is secure collaboration – making it easy for information to flow with the business activities that require it.

The partner organizations must then operate similar security models with appropriate controls in place such as identity and access management, encryption and partnering agreements and contracts that include terms for secure collaboration.

The Private security level necessitates stricter controls and procedures, limited device access, and most importantly, better-protected information. There will be fewer people with access privileges and a lower volume of data. Enterprise strategic information assets should be given the highest priority for security spending.

Network perimeter security is no longer enough as critical data is passed out of the company to partners, customers and cloud services. The data itself must therefore be protected with encryption - only visible to the intended recipient. It is little known that e-mail and attachments are sent over the internet "in the clear," with very little encrypted traffic. Companies should implement secure signed and encrypted e-mail, as the default standard for confidential information transfers between businesses.

C. Corrupting your other passwords

If you provide too much information on your facebookprofile,hackers can use it to guess your password this is a serious enough problem.However,it can get worse Hackers can use your facebook password to access your bank accounts and other online accounts.Tom clare,a cybersecurity expert,told CBS that is how many hackers break into other accounts. "understand that most users use the same password for everything"."if they can get your user credentials for your Facebook account,there's a good chance they have the password for your bank account."

IV.RISKS INVOLVED WITH SOCIAL MEDIA WEBSITES

A. Using social media for official purposes

- The primary security risk for using social media for official business is the possibility of data spills caused by employees posting too much information or information not authorised for public release. Agencies can significantly reduce the security risk by developing and communicating sound usage policies.
- There are also business risks that your agencies will need to consider when developing usage policies. For example, damage to agency reputation caused by negative posts by the public.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

B. Using social media for personal purposes

- According to recent reporting, only half of social media website users have privacy settings to control what information they share and with whom, and over a third accept friend requests from people they do not know. Poor security practices such as this increase the likelihood of users being targeted through socially-engineered communication campaigns by malicious adversaries.
- Users posting information about their personal life, their official duties, project details or government policy could unknowingly provide people with information that could be used to elicit government information from them or to tailor social engineering campaigns to compromise an agency's networks. Users should assume everything posted on social networking sites is permanent.
- Information that appears benign in isolation could, if collated with other information, have a considerable security impact on Australian government. Internet content is cached frequently, and information can be viewed, copied or forwarded on without the originator's knowledge. Once a person posts information, they effectively relinquish control over it. Information posted on the Internet is nearly impossible to completely remove.

 Carefully consider the type and amount of information you post regarding to your work duties. Do not post information that is not for public release from your current or previous job roles.

 Restrict the amount of personal information placed on social media websites. Avoid posting information such as your home or work address, phone numbers, place of employment and other personal information that can be used to target you.

 Monitor the information friends and colleagues post about you to prevent the unauthorised disclosure of your personal information.

 Consider limiting access to posted personal data to 'friends only'.

 Apply any available security and privacy options to your accounts and use a 'private' profile where applicable.

 Use a personal email address rather than an official email address when creating personal profiles, and use an alias rather than disclosing your full name. If possible, make your email address private to those viewing your page.

 Several social media websites allow users to 'opt-out' of allowing search engines to search and display your information. If possible, use this 'opt-out' feature.

 Review the website security and privacy policies regularly, as these can change with minimal communication to users.

 Be wary of accessing unknown website links or attachments, unsolicited contact and scams (such as through the use of fake profiles).

 Report any suspected security incidents when you or a colleague has posted sensitive or classified information on social media websites to your protective security team. Report any suspicious contact made to you or a colleague through social media websites.

V.CONCULSION

In conclusion our result states that users should be aware of their privacy quotient and Face book

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 13, 2017 ISSN: 2348-6600
Reference ID: IJCS-220 PAGE NO: 1372-1378
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

should work forward towards their security settings in order to save their users from privacy breach and various cyber-attacks. Apart from this still there is a lot of research work is required in the field of privacy and security of social network sites.

VI.REFERENECS

[1]Krishnamurthy B. 2010. I know what you will do next summer. acmsigcomm Computer Communication Review, 40(5):65-70, Oct. 2010.
[2] Leitch S and Warren M. Security Issues Challenging Facebook.
[3]Srivastava A. and Geethakumari G. 2013 Measuring Privacy Leaks in Online Social Networks, International Conference on Advances in Computing,Communications and Informatics (ICACCI), pp. 2095-2100, 2013.
[4] Srivastava A and Geethakumari G. A Framework to Customize Privacy Settings of Online Social Network Users. 2014 IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 187-192, 2013.
[5]"Facebookconnect,"http://developers.facebook.com/ connect.php.
[6]"Facebookstatistics,http ://www.facebook.com /press/info.php?statistics.