Implications of Risks in Online Social Networking and Framework for Measurement of Risks

Mr.Velmurugan.A[1] Dr.S.Balaji[2]
[1]Research scholar ,PG and Research [2]Associate professor, PG and Research
[1,2]Department of Computer Science Engineering
[1,2]Dhanraj Baid Jain College

Abstract— Exponential growth of online social networks resulted in fundamental shift in status of end users. Individual end users become content managers instead of just being content consumers. Today, for every single piece of data shared on online social networks, the uploader must decide which of his friends should be able to access the data. In Online Social Networks, term "friend" has become all-encompassing, it has become increasingly difficult for users to control which friends get to see what personal information. There is a need for to quantify the privacy risk attributed to friend relationship in online social networks. Hence it becomes absolutely necessary to enhance the safety and reduce the risk associated with the usage of social networks. The aim of this paper in exploring the consequences of the adoption of social networks by employees working in enterprises. The methodologies to answer questions related to the risks incurred in an organization due to the usage of social network by its employees, efficient approaches that can be taken to mitigate the different risks and the financial and organizational implications for an organization in implementing any of the possible risk mitigation approaches. aims at exploring the consequences of the adoption of social networks by employees working in enterprises. The methodologies to answer questions related to the risks incurred in an organization due to the usage of social network by its employees, efficient approaches that can be taken to mitigate the different risks and the financial and organizational implications for an organization in implementing any of the possible risk mitigation approaches.
Key words: Social Network, Facebook, Privacy, Enterprise, Risk Mitigation

I. INTRODUCTION

The Internet has become an inevitable part of lives of people today. Online social networks (Facebook, LinkedIn, Twitter etc) are top most visited sites on internet. These sites are an easy and cost effective way for people to reach out to their classmates, friends and family from across the globe. A large percentage of success of these social networking sites can be attributed to a fact that they give users the opportunity to create their own space and a great way to connect with likeminded people, learn and share knowledge. Online social networks are one of the most popular fora for self representation and user interactions. Individuals join social networks to present themselves. In OSNs user can present themselves by constructing a profile. The audience of social networks is so broad that besides customers and business competitors, hackers may also access such information. Thus the enterprises are subjected to serious security threats given the amount of accessible data available on the social network and the wide range of motivated attackers trying to access this data.CEOs and other decision makers of an enterprise are now getting serious about the social networks to understand its possible benefits and risks for the business. Enterprises are now realizing the potential risks that the social network sites expose their enterprise to and are looking for possible mitigation approaches.

II. LITERATURE SUPPORT

Exponential growth of online social networks resulted in fundamental shift in status of end users. Individual end users become content managers instead of just being content consumers. Today, for every single piece of data shared on OSNs, the uploader must decide which of his friends should be able to access the data. Several studies on Facebook usage have shown that the average number of friends per user is approximately 150. Anyone can make a request to join a user's friend circle{family members, colleagues, classmates, acquaintances, strangers etc. Current literature support the claim that users are willing to add strangers to their friend circle. Dissimilar communities of interests of computer science investigators consume undertook some of the troubles that grow in Social Networks, and stretched a various wander of "privacy problem solutions". These are accept intention precepts to address Social Network privacy consequences. Each of these solutions is formulated with a particular type of user, use, and privacy problem in bear in mind. We recognize three types of privacy problems that investigators in computer science fishing tackle. They are Social Privacy, Institutional Privacy and Surveillance Privacy troubles. The first approach "social privacy" addresses problems related to users fear of intrusion induced by other users. They capture, for example, the fear of constituting haunted, hectored, made turn of, or constituting exhibited to bitter content. Some users have a firm awareness of social privacy. Many of them demonstrate rigorous privacy settings, potently governing the access to and visibility of their profiles. The second approach "institutional privacy" analysed in Kate Raynes-Goldie's work addresses problems related to a)users fear about Private and Public institutions expend personal data for undesired intentions. b) users missing assure and supervision over the accumulation and processing of their data in Social Networks. The consciousness of institutional privacy is much less labeled. Only a small minority of study participants concern about institutions bothering and using their personal data. The third approach "surveillance privacy" addresses problems related to people's fear about when the personal data and social fundamental interaction of Social Network users are rendered by governments and service suppliers.

III. IMPLICATIONS OF RISKS IN OSN

The number of social networks and its users has been on an increase over the past couple of years. Social networks have been used by a wide range of users, in different contexts to fulfill various tasks and in the process expose both personal

and work related information. Recent surveys show that over the past couple of months there has been a steep increase in the amount of work related information on the social network

Employee's involvement in social network not only leads to a drop in the enterprise's productivity, but also poses a greater threat of information leakage. The risks associated with an individual and an enterprise increases with the amount of personal and professional information available on the social network. Recent surveys have shown that the amount of sensitive information exposed on the social network depends primarily on the users' security awareness and their education.

The exposure of sensitive data on the social networks can happen by the employee involving in any/all of the following activities

1) User's activity streams: An activity stream is a collection of events associated with a user. These streams may capture the changes that the user made to their profile page, applications added and their recent communications.
2) Media content and text files: Users may post media content that may reveal personal and/or professional information. Files such as resume, job descriptions and business itinerary would fall under this category.
3) User's Group: User's social network groups may reveal, either directly or indirectly, social and professional information of the users. In order to assess an enterprises' risk exposure, it is important for the decision maker to be aware of all these potential threats. This being an emerging issue, the precautionary measures that the enterprise needs to take is not evident. Some measures like banning access to social network could affect the enterprises' productivity and might not be completely effective. Other measures like control points to intercept and block data disclosure could have only limited effects. Educating, monitoring and punishing employees have their own pros and cons.

Attack Goal-Possibility	Approach	Impact	Level of Aggregation
Identity theft, Blackmail	Collect confidential data of employees and misuse this information	Information can be exploited from a single social network or from multiple social networks. Multi-site analysis leads to higher risk for the enterprise and the individual.	No aggregation – data of the same user is combined to generate a user's profile
Financial gain, Blackmail, Damage to company's reputation, Obtain Competitive insights	Get sensitive information related to the company. Analyze employees' posts/comments/ updates about ongoing projects etc.	Can be done on single or multi-site. Multi-site analysis leads to higher risk for the enterprise and the individual	Aggregation of the different types of data (job applications, comments, photos)
Sell confidential data to competitors	Get info about Projects	Can be Multi-Sites Or Single Site	----

Table 1: Goals of attackers

IV. Framework for Quantitative Risk Analysis

The proposed model aims at addressing the following concerns to help the decision makers secure their enterprise:

- The current level of risk and data exposure for a given organization and a threat environment.
- The risks and costs involved in making the different choices of investment and policy decisions.
- Most effective investment, given a limited set of resources.

The model helps decision makers in analyzing the different risk mitigation options and in arriving at the most effective and cost efficient mitigation technique. While arriving at the risk mitigation techniques in the model, the attacker's skill and motivation levels are also taken into account. While arriving at the risk mitigation techniques in the model, the attacker's skill and motivation levels are also taken into account.

The following actions, called levers are considered, which a decision maker can take to change the behavior of employees.

Education: Investments could be made to create awareness and educate employees about the current threats and privacy issues on the social network.

- Monitoring and Punishment: Investments could be made in monitoring
- employees' behavior, creating awareness of unacceptable behavior and punishing them based on the collected evidence.
- Control Points: Investments could also be made on software and hardware control points to monitor, intercept and block data leakages. Examples of control points would be email interceptors, black-listing and blocking of web sites.

Considering the practical resources available for an enterprise, the investments in the levers should be optimally chosen, to mitigate the risk up to a point where the marginal cost of implementing the lever is less than the value of additional savings from security incidents.

The overall investment cost for an enterprise and the total risk associated with an enterprise would be the two metrics that our model focuses on to help the decision makers arrive at such a conclusion.

The overall investment cost is calculated as a weighted sum of Fixed/Initial cost and Variable/Maintenance cost. The Fixed cost is an initial cost resulting from making investments in specific control points. The Fixed/Initial cost has been modeled by the linear equation as

Fixed Cost = A * CP_F + B * ED_F + C * MP_F. The variables CP_F, ED_F and MP_F can take values 0 or 1. These variables are set to 1 when the corresponding control levers are used by the enterprise and are set to 0 when the corresponding levers are not used by the enterprise. i.e. CP_F, ED_F and MP_F are 0 if the corresponding levers CP_L, ED_L and MP_L are 0; 1 otherwise. A, B and C are constant weights and are fixed at 50, 10 and 30 respectively in the model. The Variable/Maintenance cost is directly proportional to both the time duration for which the control levers are used and the number of employees in the enterprise. The linear equation used in calculating the Variable cost is based on the equation Variable_Cost(t) = D(t) * CP_L * t + E(t) * ED_L * t + F(t) * MP_L*t. The variables D(t), E(t) and F(t) are the variable weights reflecting the different impact and costs of the levers in different periods of time. The variables CP_L, ED_L and MP_L can take values between [0, 3]. The following would be the factors accounting for the variable/maintenance cost of an enterprise: Updating and renewing the license for software used to control the leakage of user information on the social network.

- Conducting regular training/education sessions to keep the employees updated
- with the current risk. The cost associated with this is also dependent on the
- number of employees in the enterprise every year.
- The employees might have found a way to bypass the monitoring system of the enterprise. Hence an upgrade of the monitoring system would be a mandatory requirement.

V. CONCLUSION

The work focused on the different risk mitigation techniques that a decision maker can take to enhance the security of the enterprise and its employees by modifying employees' interaction with the social network. The techniques involved provide threat awareness through training, monitoring user behavior and installing control points to intercept and block data leakage. All of the above mitigation approaches are taken by the decision maker as a countermeasure to overcome the security risks incurred on the enterprise due to the immoral behavior and the negligence of the employee.

The work illustrated how modeling can be used to simulate the user behavior on the social network and hence help the enterprise decision makers to explore the implications of employees using the social network and to arrive at their different investment choices on the control levers to mitigate these risks.

REFERENCES

[1] James Grimmelmann. Facebook and the social dynamics of privacy. Iowa Law Review, 95(4):1{52, 2009.
[2] Bibi van den Berg, Stefanie P• otzsch, Ronald Leenes, Katrin Borcea-Ptzmann, and Filipe Beato. Privacy in social software. In Privacy and Identity Management for Life, pages 33{60. Springer, 2011.
[3] Justin Lee Becker and Hao Chen. Measuring privacy risk in online social networks.PhD thesis, University of California, Davis, 2009.
[4] Ai Ho, Abdou Maiga, and Esma A• meur. Privacy protection issues in social networking sites. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on, pages 271{278. IEEE, 2009.
[5] Giles Hogben. Security issues and recommendations for online social networks.ENISA position paper, 2007.
[6] Balachander Krishnamurthy and Craig E Wills. Characterizing privacy in online social networks. In Proceedings of the frst workshop on Online social networks,pages 37{42. ACM, 2008.
[7] Chi Zhang, Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang. Privacy and security for online social networks: challenges and opportunities. Network, IEEE, 24(4):13{18,2010.
[8] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in facebook with an audience view. UPSEC, 8:1{8, 2008.
[9] Cuneyt Gurcan Akcora and Elena Ferrari. Graphical user interfaces for privacy settings.
[10] Cuneyt Gurcan Akcora, Barbara Carminati, and Elena Ferrari. Risks of friendships on social networks. arXiv preprint arXiv:1210.3234, 2012.
[11] Cuneyt Gurcan Akcora, Barbara Carminati, and Elena Ferrari. Privacy in social networks: How risky is your social graph? In Data Engineering (ICDE), 2012 IEEE 28th International Conference on, pages 9{19. IEEE, 2012.
[12] Javed Ahmed and Zubair Ahmed Shaikh. Privacy issues in social networking platforms: comparative study of facebook developers platform and opensocial. In Computer Networks and Information Technology (ICCNIT), 2011 International Conference on, pages 179{183. IEEE, 2011.
[13] Michael Beye, Arjan JP Jeckmans, Zekeriya Erkin, Pieter Hartel, Reginald L Lagendijk,and Qiang Tang. Privacy in online social networks. In Computational Social Networks, pages 87{113. Springer, 2012.
[14] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pages 71{80. ACM, 2005.
[15] Rongjing Xiang, Jennifer Neville, and Monica Rogati. Modeling relationship strength in online social networks. In Proceedings of the 19th international conference on World wide web, pages 981{990. ACM, 2010.
[16] Patrick Gage Kelley, Robin Brewer, Yael Mayer, Lorrie Faith Cranor, and Norman Sadeh. An investigation into facebook friend grouping. In Human-Computer Interaction{INTERACT 2011, pages 216{233. Springer, 2011.
[17] Fabeah Adu-Oppong, Casey K Gardiner, Apu Kapadia, and Patrick P Tsang.Social circles: Tackling privacy in social networks. In Symposium on Usable Privacy and Security (SOUPS), 2008.

[18] Alessandra Mazzia, Kristen LeFevre. and Eytan Adar. The pviz comprehension tool for social network privacy settings. In Proceedings of the Eighth Symposium on Usable Privacy and Security, page 13. ACM, 2012.
[19] Anna Cinzia Squicciarini, Dan Lin, Sushama Karumanchi, and Nicole DeSisto.Automatic social group organization and privacy management. In CollaborateCom,pages 89{96, 2012.
[20] Anna Squicciarini, Sushama Karumanchi, Dan Lin, and Nicole DeSisto. Identifying hidden social circles for advanced privacy con_guration. Computers & Security,41:40{51, 2014.
[21] Lujun Fang and Kristen LeFevre. Privacy wizards for social networking sites. In Proceedings of the 19th international conference on World wide web, pages 351{360.ACM, 2010.
[22] Lujun Fang, Heedo Kim, Kristen LeFevre, and Aaron Tami. A privacy recommendation wizard for users of social networking sites. In Proceedings of the 17th ACM conference on Computer and communications security, pages 630{632. ACM, 2010.
[23] Alexandra Cetto, Michael Netter, G• unther Pernul, Christian Richthammer, Moritz Riesner, Christian Roth, and Johannes S• anger. Friend inspector: A serious game to enhance privacy awareness in social networks. arXiv preprint arXiv:1402.5878,2014.

