Various Security Risks, Threats and Standards of Information Security in Internet Banking

Gagandeep Singh Sodhi[1], Dr. R.K Sehgal[2]
[1] Assistant Professor, Jasdev Singh Sandhu Institute Of Engineering & Technology, Patiala, Punjab, India
[2]Professor, Jasdev Singh Sandhu Institute Of Engineering & Technology, Patiala, Punjab, India
[1]gag_2k4@yahoo.com, [2]sehgal48@yahoo.com

Abstract- In the paper we discuss key security risks, which we feel pose danger to banking Sector and the government.The banking sector is always looking for new services delivery platforms to improve customer confidence and satisfaction. To achieve this, the banking service delivery platform must provide end-to-end security to safeguard the information exchange between the bank and the customer. The major cause for concern across banking sector is financial loss, data loss and not to mention the loss of credibility and reputation. We mentions the survey of organizations across India to find the figures that how seriously they tackle information security threats. Various communication channels used by employees, security incidents occurred in past, security solutions deployed and standards used for information security are also discussed. We haven`t mentioned the security threats like viruses, spam etc. in this paper.

I. INTRODUCTION

In the world of E-Commerce internet banking is one of the indispensable applications. Security issues are to be addressed critically in internet banking applications and it directly influences the comfort. Even though the existing mechanisms ensure security the hackers succeed in breaking these mechanisms.Security is a major concern in organizations because of identity and data theft. Due to lack of security organizations are facing financial loss,data loss and not to mention loss of credibility and reputation. Before talking about security we need to understand the current security landscape and the risk it involves. Top management in most organizations understands the possible security risks and what kind of impact they can have on organizations. In India, 65% of the CIOs feel that the security threats have become more dangerous than ever before [1].Clearly, cyber-crime is on the rise because there are monetary gains involved.According to various research reports from key security vendors, most cybercrime today are targeted at stealing critical data for financial gain.However this does not directly translate into allocating a significant part of IT budget on information security.42% of CIOs had less than 10% of their IT budget devoted to information security.19% had 10-20% of their budgets devoted to information security and the interesting fact is that 25% of organizations have not any separate budget for security. Most of the organizations just using anti-virus software.But the above clearly indicates the anti-virus softwares are not completely effective in combating security threats.

II. INFORMATION SECURUTY RISKS &THREATS

A. Entry points for security treats

There are various channels through which malicious code can enter.Security treats can comefrom anywhere,be it outside or inside the network. Information can be stolen from anywhere, anytime from your network,desktops,servers,Internet portal or wireless networks. Configuration of network also play vital role in information theft especially in wireless network. Firstly we need to identify the possible channels from where information can be stolen-USB ports, remote access , wireless networks, VoIP, laptops etc.Here are some communications Channels that are offered to employees in Indian enterprises [2].

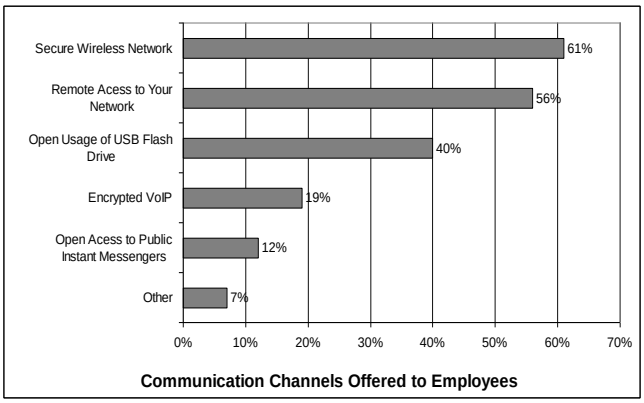

Fig.1. Communication Channels for Employees

Fig. 1 shows that 61% organizations are secure wireless networks remaining 41% organizations don't have wireless networks or use wireless network that is not secure.The real interesting one is open access to public IMs, free access to public IMs means employees can send whatever information they want to anybody.40% organizations allow open usage of flash drives, then there is obviously more danger of information theft. USB ports have become the default interface for every device you plug into computer or laptop. While they have increased the convenience, they have also increased the security risks. USB flash drives for instance, are commonly used to carry/share data besides flash drives, USB ports can also be used to connect to internet through internet data cards. While this makes it easy for your mobile workforce to connect to corporate network, or use the internet when on the move to check important mails, it also makes it easy to leak information.

B.Security incidents over past few years

Users are the key asset for every organization, but here is also most vulnerable point of entry.It`s easier to cajole a user into delving important information than breaking through a firewall. This makes educating users of various security threats extremely important. However, it is not as easy as it sounds.Have a look at the following result [3].

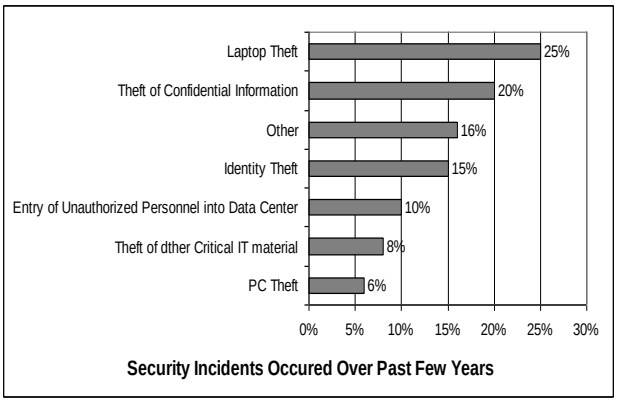

Fig. 2. Security incidents in past

Fig. 2. Shows that laptop thefts are the top of security incidents list.This means that user has to be more careful and stronger focus needs to be put in training users on how to protect their laptops.The second one is about the theft of confidential information .This could be caused by weak passwords or authentication, but it could also be caused by employees walking away with confidential data on USB drives.

C. How important is user training

If educating usercould resolve the problem of incoming security threats,then no organization would be combating so many security threats today and facing major financial loss.The thing to observe here is how much to really expect from user?Do you seriously expect them to remember long, complicated passwords without writing them down somewhere? Or do you expect them not to open an attachment that pretends to come from their boss? Or click on an email that comes from a bank where they don`t have an account? Every single user today has dozens of passwords and it's impossible for them to keep track of all of them without writing them down somewhere. Using the same password for all applications is anyways a bad idea, because if it gets hacked, the hacker gains entry into all of the users accounts so obviously ever user today is expected to remember multiple passwords. Now if you make the passwords too complex so that they were difficult to hack then you were also making them difficult to remember so a user would obviously have to write them down somewhere. You could teach the user to store his passwords in password protected document or implemented other mechanisms like finger prints scanning, cards scanners, etc.

III. STANDARDS

A. Before implementing security solutions

We first identify what kind of security threats with which we are fighting most. Only then we can identify the right solution to implement. As per the below chart [4], organizations are spending mostof their time combatting virus attacks,despite having anti-virus software in place.This indicates we need to train users on how to identify suspicious activity that could be linked to virus attack. Likewise they have to identify spam, because that`s the next biggest threat. Besides identifying the area where most of the time is going, it is equally important to identify the major security incidents that have happened in your organizations and their financial implications.

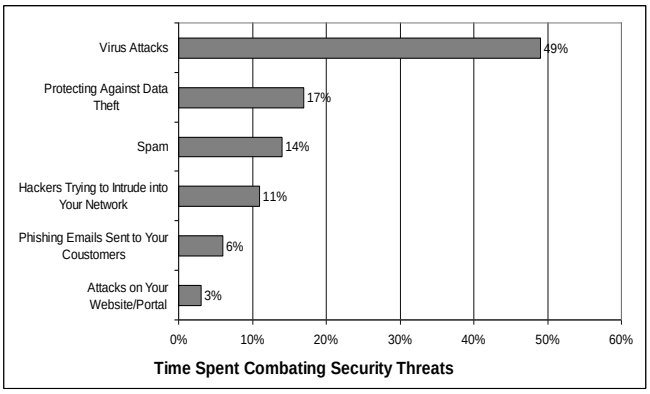

Fig. 3. Time spent in security Threats

B. Security policies

Security solutions alone are not enough.You also need well documented security policies and moreover you need to conduct regular formal assessment of network. Having the written policy is always good idea. We can`t stress enough on its importance. But even more important than that is to visit it regularly and keep updating the same. For instance, suppose that despite having a document policy, you keep getting security threats. In such a case you need to find a solution to that threat and update your security policy.

C. Security Standards

You need to conduct the regular assessment of security at your network. With the change in IT infrastructure security should be changed.Today two key standards are available for information technology.These are BS7799 and ISO 27000[5].

*1) BS 7799:*BS 7799 was a standard originally published by the British Standards Institution (BSI) in 1995. It was written by the United Kingdom Government's Department of Trade and Industry (DTI), and consisted of several parts.The first part, containing the best practices for Information Security Management, was revised in 1998,after a lengthy discussion in the worldwide standards bodies, was eventually adopted by ISO as ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000. ISO/IEC 17799

was then revised in June 2005 and finally incorporated in the ISO 27000 series of standards as ISO/IEC 27002 in July 2007 [6].The second part to BS7799 was first published by BSI in 1999, known as BS 7799 Part 2, titled "Information Security Management Systems - Specification with guidance for use." BS 7799-2 focused on how to implement an Information security management system (ISMS), referring to the information security management structure and controls identified in BS 7799-2, which later became ISO/IEC 27001. The 2002 version of BS 7799-2 introduced the Plan-Do-Check-Act (PDCA) (Deming quality assurance model), aligning it with quality standards such as ISO 9000. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.

2) ISO/IEC 27001: It formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements[7]. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

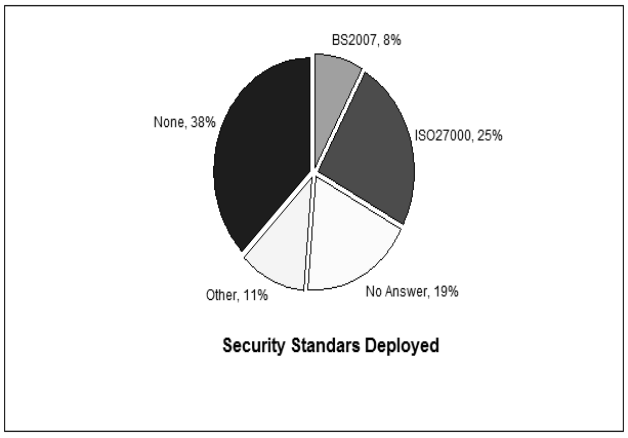

Fig. 4. Various security standards

Most organizations have a number of information security controls. Without an ISMS however, the controls tend to be somewhat disorganized and disjointed, having been implemented often as point solutions to specific situations or simply as a matter of convention. Maturity models typically refer to this stage as "ad hoc". The security controls in operation typically address certain aspects of IT or data security, specifically, leaving non-IT information assets (such as paperwork and proprietary knowledge) less well protected on the whole. Business continuity planning and physical security, for examples, may be managed quite independently of IT or information security while Human Resources practices may make little reference to the need to define and assign information security roles and responsibilities throughout the organization.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts.
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable.
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

D. Which is the best solution?

In below diagram various security solutions are shown which are implemented amongst the Indian enterprises. Most of the Organizations still depend on firewall and anti-virus. Which solution is to deploy depends on the type of data and budget of organization [8].Analysis on information technology gave us hope for new solutions. For example hard disk encryption techniques, data loss prevention methods and random password encryption etc.If data security through these techniques is not enough for your organization then get physical network security solutions at your data center.

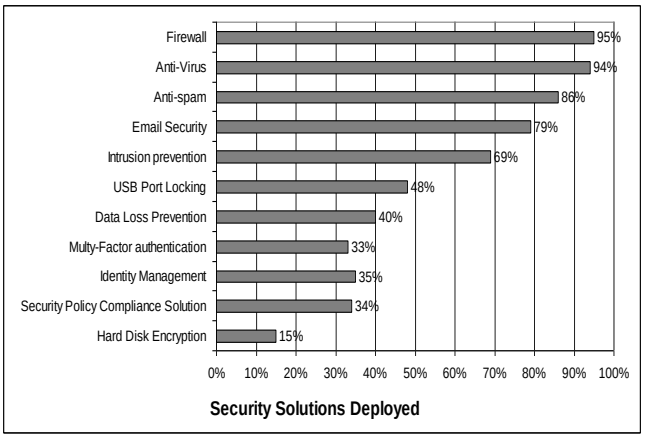

Fig. 5. Security solutions deployed

E. Other Security solutions

If information security at data center is not enough then apply physical security .Physical security at data centers starts right from the planning of data center [9].

1) Physical access control can be done using access cards to restrict the entry into data centers.

2) Surveillance with video camera at data center within an organization.

3) Deploying of authentication devises such as biometrics.

III. CONCLUSIONS

Information no longer resides inside the four walls of an organization given the business outsourcing. Any leakage of information can cause you to lose not only money but also credibility, so apart from securing PC`s from viruses, spyware etc. What seems very important for an organization is defending data against all vulnerable ends and this is now becoming a big concern for many enterprises. Even if you block the ports, scans

all the emails, or work offline it cannot guarantee data security. The issues regarding the information security are endless.

REFRENCES

[1] A Chopra, R sharma and V Jaitly, “Security risks in the new economy,” A Cybermedia publication, PC Quest, pp.39-53, May-2009.

[2] Survey by PC Quest, May-2009.

[3] Zhenfu Cao, "An Identity Based Proxy Signature Scheme Secure in the Standard Model," grc, pp.67-72, 2010 IEEE International Conference on Granular Computing, 2010.

[4] Giovanni Iachello, "Protecting Personal Data: Can IT Security Management Standards Help?" acsac, pp.266, 19th Annual Computer Security Applications Conference (ACSAC '03), 2003.

[5] Wolfgang Boehmer, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001," ares, pp.392-399, 2009 International Conference on Availability, Reliability and Security, 2009.

[6]George S. Oreku, Fredrick J. Mtenzi, "Using Nature to Best Clarify Computer Security and Threats," dasc, pp.702-707, 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing,2009.

[7]Eyal Adar, Andreas Wuchner, "Risk Management for Critical Infrastructure Protection (CIP) Challenges, Best Practices & Tools," iwcip, pp.90-100, First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05), 2005.

[8] Naaliel Mendes, AfonsoAraujoNeto, Joao Duraes, Marco Vieira, Henrique Madeira, "Assessing and Comparing Security of Web Servers," pp.313-322, 2008 14th IEEE Pacific Rim International Symposium on Dependable Computing, 2008.

[9]Yiming Yang, ShinjaeYoo, Frank Lin, Il-Chul Moon, "Personalized Email Prioritization Based on Content and Social Network Analysis," IEEE Intelligent Systems, vol. 25, no. 4, pp. 12-18, July/Aug. 2010, doi:10.1109/MIS.2010.56.

[10]Arti Mann, "Information Technology and the Related Services Industry: Evaluating India's Success Factors," hicss, pp.1-10, 42nd Hawaii International Conference on System Sciences, 2009.