NETWORK SECURITY AND SECURITY LAWS AND REGULATIONS (LITERATURE REVIEW)

KADAM NILIMA PANDURANG
Vidya Pratishthan's Commerce and Science College, Indapur Dist- Pune, Department of BCS , 9130505063, nilimakadam15@gmail.com

RAUT TRUPTI SANTOSH
Vidya Pratishthan's Commerce and Science College, Indapur Dist- Pune, Department of BCA, 7709875583, santrupt14@gmail.com

SHINDE VIJAY BABAN
Vidya Pratishthan's Commerce and Science College, Indapur Dist- Pune, Department of BCS, 9730145654, vijayshindevpcscindapur@gmail.com

ABSTRACT

Today world becomes on internet. Not only all transactions are done on online but communication is also done online, but when data is transmitted on network there are many possibilities of hacking of confidential data and chances of misuse it. Whenever we use internet, network security issue arises. Online a cybercrimes, also leaves physical, electronic evidence, but unless good security measures are taken, it may be difficult to trace the source of cybercrime. In certain e-commerce-related areas, such as networking, data transfer and data storage, researchers applied scanning and testing methods, modeling analysis to detect potential risks. This paper focuses on e-commerce, net banking users are secure or not. This paper also includes laws, regulations and industry guidelines with significant security and privacy impact and requirements.

KEY WORDS: network Security, bank Security , regulation.

Introduction:

In digital world everyone give preference to online transaction and the government of indias new program "Digital india in place" more people are suffers trough internet for different purpose. One of the major concerns when purchasing online and accessing financial information is security. "Information security is the protection of information and the systems used to store and transmit data".

Internet banking provides following facility

-Information and data related to account and transactions
- Facility to check balance after deposit or withdrawal
-Provision to transfer money one account to other
-Provision for shopping,
-Paying electricity bill ,mobile bill etc
-Railway ticket booking and many more

But when we uses internet ,one of the most common question comes in our mind ."how to make transaction secure?" Because every one having money . but some peoples getting money by doing work and some peoples by doing misuse of technology with the help of skilled brain. when we are using internet then we must be aware about laws and regulation related to internet.

Network Basics

Why Security?

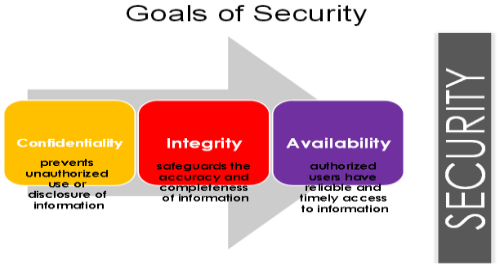
Security threats are real... And need protection against
Fundamental aspects of information must be protected
We can't keep ourselves isolated from the INTERNET

Types of Security

♣Computer Security generic name for the collection of tools designed to protect data and to thwart hackers

♣Network Security -measures to protect data during their transmission

♣Internet Security -measures to protect data during their transmission over a collection of interconnected network


Goals of Security
Confidentiality
prevents unauthorized use or disclosure of information
Integrity
safeguards the accuracy and completeness of information
Availability
authorized users have reliable and timely access to information
SECURITY

Threat

♣Any circumstance or event with the potential to cause harm to a networked system

-Denial of service

Attacks make computer resources (e.g., bandwidth, disk space, or CPU time) unavailable to its intended users

-Unauthorized access

Access without permission issues by a rightful owner of devices or networks

-Impersonation
-Worms
-Viruses

Risk management vs. cost of security

♣Risk mitigation

-The process of selecting appropriate controls to reduce risk to an acceptable level

♣The level of acceptable risk

-Determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy

♣Assess the cost of certain losses and do not spend more to protect something than it is actually worth

SECURITY MEASURES

Many threats can be minimized or prevented through various procedures. For instance, the threat of user errors could be minimized with validation procedures upon data entry and increased training for information users. While some threats are a result of user error, other threats may occur for malicious purposes. For malicious threats to occur there has to be motivation and the capability for the threat agent to carry out the threat, which are modified by access, catalysts, inhibitors, and amplifiers (Kovacich, 2003). Motivations for malicious attacks stem from various reasons such as personal gain, political, religious, curiosity, revenge, and so on. Motivation alone is not enough for a threat to occur; the threat agent must also have the capability to perform the act Capabilities that could enable a threat agent to perform a malicious act might include personality, access to facilities, software, technology, and education. Inhibitors can be implemented to reduce motivations in order to deter a threat agent from performing malicious acts. Inhibitors may consist of increasing security, resulting in higher capabilities required to perform malicious acts, or more severe consequences for improper use or harm to corporate data. While inhibitors are put in place to deter malicious acts, amplifiers may exist that could increase the likelihood of threat agents to perform these acts. Amplifiers may include peer pressure, fame, easy access to information, and increased skill and educational levels which result in higher capabilities.

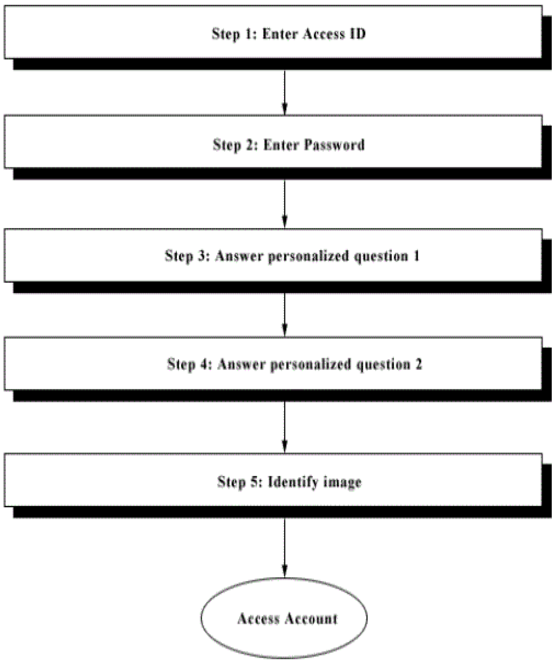


Fig. Online bank and security

Online bank's five step approach to security.

Online banks have invested heavily to make efforts in securing the financial information of their customers. Many online banks throughout the United States have implemented a five-step approach for online banking access in efforts to protect against external threats. Figure 1 outlines the steps required for customers to access their bank accounts online.

Step 1, the user must enter the access ID for their account that is provided by the bank. The immediate problem associated with this access number is the length of the number and lack of relevance to the user. If the user is unable to remember this access ID easily, then they are likely to write their login information on a piece of paper as person A did in the case previously discussed. This creates poor security habits on the part of the user and leaves the opportunity for someone to steal the paper containing their login information. Users may also be vulnerable to social engineering by home service technicians or others who may try to gain access to areas where password information may be stored.

Step 2 requires the user to enter a password to gain access to their account. A password alone is vulnerable to several security issues that were discussed above. By implementing a password with other security measures, as seen in the banking example, several vulnerabilities can be decreased compared to the use of passwords alone. However, in the instance that a user forgets their password, as was the case of person B in the case presented above, there should be procedures in place to help the user recover the password or reset it to a default without allowing unauthorized individuals aware of this situation. In the case described above, the security threat could have been eliminated through proper training and the use of an encrypted email to contact the user with their account information.

Steps 3 and 4 ask the user to answer security questions that were previously answered by the user. A list of common security questions used includes:

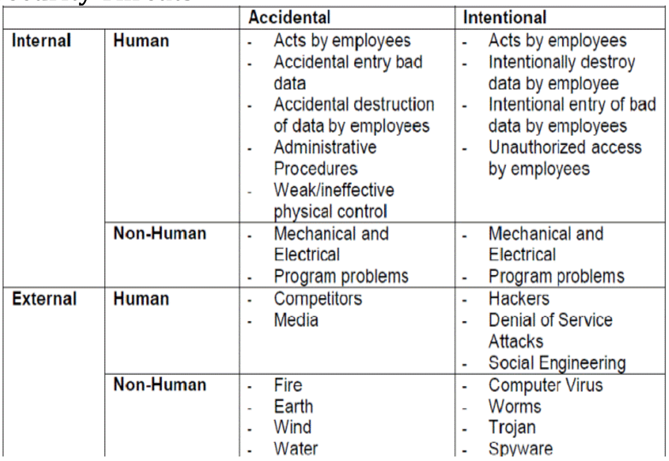
- What is your mother's maiden name?
- What is the name of your favorite restaurant?
- Who is your favorite actor?
- What is your favorite color?
- What is the name of your first pet?

While these questions add additional security, they are also subject to vulnerabilities from people who know the user intimately or from others engaging in social engineering. Creating questions that are too complicated might result in the user not remembering the answers and leave them unable to access their account. In this situation, the user would likely revert to writing their answers on a piece of paper along with their access ID. Once again, displaying poor security habits as demonstrated in the case of person A.

Step 5, is where the user identifies a picture that they have previously marked and labeled. This uses a form of hash visualization that was described previously in this article.

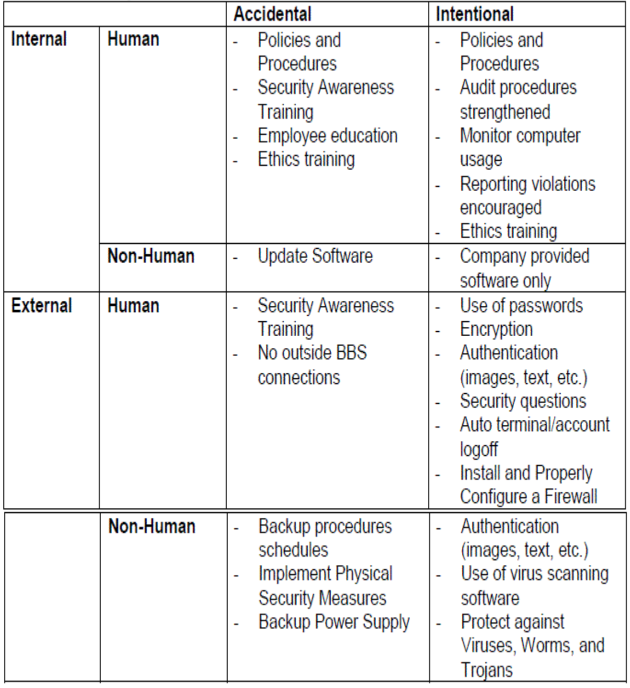
This five-step approach creates a very secure environment protecting against external threat agents but can significantly decrease usability among the users of the system. In

Security Threats



		Accidental	Intentional
Internal	Human	- Acts by employees - Accidental entry bad data - Accidental destruction of data by employees - Administrative Procedures - Weak/ineffective physical control	- Acts by employees - Intentionally destroy data by employee - Intentional entry of bad data by employees - Unauthorized access by employees
	Non-Human	- Mechanical and Electrical - Program problems	- Mechanical and Electrical - Program problems
External	Human	- Competitors - Media	- Hackers - Denial of Service Attacks - Social Engineering
	Non-Human	- Fire - Earth - Wind - Water	- Computer Virus - Worms - Trojan - Spyware

Security Methods



		Accidental	Intentional
Internal	Human	- Policies and Procedures - Security Awareness Training - Employee education - Ethics training	- Policies and Procedures - Audit procedures strengthened - Monitor computer usage - Reporting violations encouraged - Ethics training
	Non-Human	- Update Software	- Company provided software only
External	Human	- Security Awareness Training - No outside BBS connections	- Use of passwords - Encryption - Authentication (images, text, etc.) - Security questions - Auto terminal/account logoff - Install and Properly Configure a Firewall
	Non-Human	- Backup procedures schedules - Implement Physical Security Measures - Backup Power Supply	- Authentication (images, text, etc.) - Use of virus scanning software - Protect against Viruses, Worms, and Trojans

A **cybersecurity regulation** comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber-attacks. Cyber-attacks include viruses, worms, Trojan horses, phishing, denial of service (DOS) attacks, unauthorized access (stealing intellectual property or confidential information) and control system attacks. There are numerous measures available to prevent cyber-attacks. Cyber-security measures include firewalls, anti-virus software, intrusion detection and prevention systems, encryption and login passwords. There have been attempts to improve cybersecurity through regulation and collaborative efforts between government and the private-sector to encourage voluntary improvements to cybersecurity. Industry regulators including banking regulators have taken notice of the risk from cybersecurity and have either begun or are planning to begin to include cybersecurity as an aspect of regulatory examinations.[1]

Bank regulation is a form of government regulation which subjects banks to certain requirements, restrictions and guidelines, designed to create market transparency between banking institutions and the individuals and corporations with whom they conduct business, among other things.

Given the interconnectedness of the banking industry and the reliance that the national (and global) economy hold on banks, it is important for regulatory agencies to maintain control over the standardized practices of these institutions. Supporters of such regulation often base their arguments on the "too big to fail" notion. This holds that many financial institutions (particularly investment banks with a commercial arm) hold too much control over the economy to fail without enormous consequences. This is the premise for government bailouts, in which government financial assistance is provided to banks or other financial institutions who appear to be on the brink of collapse. The belief is that without this aid, the crippled banks would not only become bankrupt, but would create rippling effects throughout the economy leading to systemic failure.

Objectives of bank regulation

The objectives of bank regulation, and the emphasis, vary between jurisdictions. The most common objectives are:

- prudential — to reduce the level of risk to which bank creditors are exposed (i.e. to protect depositors)[11]
- systemic risk reduction — to reduce the risk of disruption resulting from adverse trading conditions for banks causing multiple or major bank failures[12]
- to avoid misuse of banks — to reduce the risk of banks being used for criminal purposes, e.g. laundering the proceeds of crime
- to protect banking confidentiality
- credit allocation — to direct credit to favored sectors
- it may also include rules about treating customers fairly and having corporate social responsibility.

Indian regulation

In the light of the hacking of the website of the Indian Space Agency's commercial arm in 2015, Antrix Corporation and government's Digital India programme, cyber law expert and advocate Supreme Court of India, Pavan Duggal stated that "a dedicated cyber security legislation as a key requirement for India. It is not sufficient to merely put cyber security as a part of the IT Act. We have to see cyber security not only from the sectoral perspective, but also from the national perspective."

Conclusion

As technology continues to advance, security measures also continue to improve and become more sophisticated. Many threats can be minimized or prevented through various procedures. For instance, the threat of user errors could be minimized with validation procedures upon data entry and increased training for information users. While some threats are a result of user error, other threats may occur for malicious purposes. Due to lack of security common sense and not applying security procedures all system faces the problem of security. Network security is playing very important role in our society ,Nation For providing protection against different attacks of network. It is our responsibility to aware about network security laws and regulations and cooperate our government. Now A days To cultivate ethics is very important then and then only person use technology for good actions with food motives. In digital world one important message is that ”Use the technology but do not misuse it

REFERENCES

1) http://www.iosrjournals.org/iosr-jce/papers/Vol13-issue1/R0131114121.pdf?id=7416
2) http://www.icommercecentral.com/open-access/a-case-study-on-ebanking-security-when-security-becomes-too-sophisticated-for-the-user-to-access-their-information.php?aid=38102
3) http://www.potaroo.net/t4/pdf/security.pdf
4) https://www.pacnog.org/pacnog10/track3/Security-Part-1.pdf
5) http://www.icommercecentral.com/open-access/a-case-study-on-ebanking-security-when-security-becomes-too-sophisticated-for-the-user-to-access-their-information.php?aid=38102
6) http://www.icommercecentral.com/articles-images/JIBC-04-g001.html
7) http://www.icommercecentral.com/articles-images/JIBC-04-t002.html
8) "A chronology of data breaches reported since the ChoicePoint incident." (2005). Retrieved October 13, 2005.
9) "Electronic privacy information center bill track: Tracking privacy, speech and civil liberties in the 109th congress." (2005). Retrieved October 23, 2005.
10) *Federal Deposit Insurance Corporation. "Risk Management Manual of Exam Policies, Section 1.1". Retrieved 17 August 2011.*
11) *Section 115, Dodd–Frank Wall Street Reform and Consumer Protection Act. "Pub. L. 111-203" (PDF). Archived (PDF) from the original on 8 July 2011. Retrieved 17 August 2011.*
12) https://en.wikipedia.org/wiki/Bank_regulation