International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 16 (2014), pp. 1647-1652

http://www. irphouse.com

Study of Cyber Frauds and BCP Related Attacks in Financial Institutes

Manpreet kaur, Divya Bansal, Sanjeev Sofat

Department of Computer Science and Engineering
PEC University of Technology Chandigarh, India,
manpreet1326@gmail.com divya@pec.edu.in
sanjeevsofat@pec.ac.in

Abstract

Banking sector has been hotspot for crime be it natural or unnatural attacks. Considering the present scenario of Technology covering all the sectors, technology is becoming indispensible part of banks it has become easy for users so as for attackers as now they have more mode to exploit the vulnerabilities. This paper reviews various threats in banks that appeared in the literature.

Keywords- Banks, technology, vulnerabilities, Threats

INTRODUCTION

Banks are the integral part of world's economy. With banks becoming an indispensable part of all business, it being on a halt for a small amount of time can adversely affect the businesses. Banks are becoming more vulnerable. With society's increasing dependency on information technology (IT), the consequences of cyber crime can be extremely grave. According to government of India Indians suffered a total loss of Rs 219.73 crore since 2011 due to cyber frauds and as many as 24,882 cases were registered by Banks. Banks are susceptible to many disruptions caused by various categories of threats; many threats are defined under various categories i.e. Business continuity planning, cyber fraud, and information security.

Business continuity planning

It can be defined as preparedness of an organization which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. It also includes identifying organization's exposure to internal and external threats, while maintaining competitive advantages and system integrity.

1. **Business continuity planning threats in banks**:
All the threats that are included in BCP can be defined under 4 categories i.e. as malicious activity, natural disaster, technical problems, and pandemics.

1.1 **Malicious activity:**
Malicious activity can be defined as any activity that causes disruption of operation, gain access to private and confidential information, cause financial, nonfinancial loss. Threats that can be categorized under malicious activities are:

1.1.1 Fraud, Theft, or Blackmail:
These are one of the common threats and most easy to be perpetrated these threats are mostly exploited by the insiders who have full access to the information, data etc. Such threats can be prevented by restricting access to confidential data or to information that can be altered or by implanting various awareness programs i.e. employee as well as customers.

1.1.2 Sabotage:
Can be destruction of property or obstruction of normal operation by someone who doesn't want them to succeed [6]. **Threats that can be included under sabotage are** intruders, bomb threats, and other disturbances.

1.1.3 Vandalism and Looting:
Vandalism and looting represent a threat because individuals often seek financial gain by exploiting security weaknesses exposed during an emergency or disaster situation.

1.1.4 Terrorism:
Terrorism is threat to all the business although it's not new threat but disruption and destruction caused by it is increasing continuously. Banks are affected by terrorism as it can cause disruption to financial flow, reputation loss; communication disruption etc. event in terrorism attack can leave facilities [3] intact but inaccessible for extended periods of time.

1.2 Natural Disasters:
It includes any natural calamities that can cause disruption of operations in banks, cause discontinuity in all the operations.

1.2.1. Fire:
Fire can be very easily caught even by short circuit but its loss can be highly immense. It can cause loss of life, equipment, and data. Authorities should know how to minimize the risks in case of fire, all facilities including back-up should be equipped with heat or smoke detectors.

1.2.2. Floods and Other Water Damage:
All financial institutions that are located near a flood plain exposes itself risk and should take the necessary actions to manage the level of exposure. Prevention can be

taken by using Water detectors.

1.2.3. Severe Weather:
The natural calamities i.e. earthquake, hurricane, tornado etc are included under this. Financial institutes must consider including appropriate scenarios in their business continuity planning process.

1.2.4. Air Contaminants:
[15]Air contaminants can be defined as all the particles, liquids, and gases which have harmful chemical properties that affect the health of the staff, BCP should consider the evacuation plans and the shutdown of HVAC systems to minimize the risks caused by the contamination [14].

1.2.5 Hazardous Spill:
The financial institutions that are close to chemical plants, railroad tracks, or roads used to transport hazardous materials. A leak or spill can result into air contamination. So all the institutes must make a effort to determine what is being produced or transported nearby, take steps to mitigate such risks.

1.3 Technical Disasters:
It includes threats due to technical disruption due to which various businesses can be affected in banks.

1.3.1 Communications Failure [7]:
Communication is the centre of all the business, in banks communication includes communicating to customers, employees, third party, affiliates, vendors, and service providers etc. Financial institutions lacking in their telecommunications infrastructures may be susceptible to single points of failure in disaster that disrupts their critical systems.

1.3.2. Electronic Payment System Providers:
Electronic payment system provider's failures may prevent the use of debit and credit cards and electronic funds transfers. Therefore, cash needs become critical when customers and employees do not have access to funds electronically.

1.3.3 Power Failure:
Storms, fires, malicious acts, brownouts, and blackouts and may result in widespread failure of the power grid and inoperable power distribution centers. A power failure could result in the loss of all the critical systems i.e computer systems; lighting, heating and cooling systems and security and protection systems.

1.3.4 Equipment and Software Failure:
Equipment and software failures may result in delay in deploying various polices or even extend the inability to implement the BCP, or stop ongoing work. The performance of preventive maintenance enhances system should be extended to all

supporting equipment, such as temperature and humidity control systems and alarm or detecting devices.

1.3.5 Transportation System Disruptions [5]:
It may be halted by natural or technical disasters, malicious activity, or accidents. This can adversely affect cash distribution, fuel delivery, check clearing, and relocation of staff to back-up sites.

1.4. Pandemics [10]:
Pandemics are defined as epidemics, or outbreaks in humans, of infectious diseases that have the ability to spread rapidly over large areas,the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. One of the most significant challenges likely from a severe pandemic event will be staffing shortages due to absenteeism

III. Cyber fraud

A deliberate act commission by any person, carried out in the course of a banking transaction under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank.

2. Cyber fraud threats in banks

All the threats those are included in cyber fraud

2.1 Phishing [11]:
Phishing is where a fraudster sends fake E-mail to large group of targets urging them to visit a fake website promising them resolve some issues. In this phished ask the victim for financial details like credit card numbers, passwords.

2.2 ATM:
ATM attacks can occur through various modes i.e. Cloning of ATM card, ATM database hacking, ATM card Skimming, ATM carding.

2.3 Hacking [13]:
It means an illegal intrusion into a computer and/or network. In case of banks the hacker hack the Internet banking account of the target and then get mobile number blocked to prevent the bank customer from receiving SMS alerts about illegal transactions made by them.

2.4 Cross site scripting:
The most common XSS attack method uses e-mail: A criminal appends special characters, such as those of a foreign language, to an ordinary URL. In this an attacker appends a script into bank's URL and e-mail it to victim, believing that it's legitimate e-mail from the bank, victim's browser sends the script to web server, which runs the

malicious code and in-turn passes browser cookie with your bank login.

2.5 Bot Network:
Bot network is a combination of two words remote and network. A cyber crime called 'bot network', in which spamsters and other perpetrators of cyber crime remotely take control of computers without users realizing that they are attacked, these attacks are increasing in banks.

2.6 Email related crimes:
The various e-mail related crimes in banks are email spamming, email bombing, sending malicious code through email.

2.7 Crime ware:
Crime ware is a class of malware designed specifically to automate cybercrime. Crime ware is designed to perpetrate identity theft in order to access a computer user's online accounts at financial services companies and online retailers for the purpose of taking funds from those accounts or completing unauthorized transactions that enrich the thief controlling the crime ware.

2.8 DDOS:
A recent example is Operation Ababil, which was a wave of DDoS attacks that targeted major banks. The first goal of a DDoS attack is disruption that shuts down a site, leading to increased call center activity, which drives up costs and in parallel, undermines customer trust in the organization. The other goal, more prevalent now than it's ever been, is to divert the bank's attention from other financial crimes.

IV Conclusion

Technology might have made easy access to attacker so has it brought many security measures that need to be taken care of, there are case where financial institutions are not even aware of the threat, So most important thing to be include in all the institutions is awareness. It is Impossible to eradicate attacks happening but they can be minimized by implementing security measures or the least we can do is to prevent more loss from happening.

V References

[1] Vanessa Pegueros (2012),Security of Mobile Banking and Payments the sans institute.
[2] Don macVittie Securing Banks In Changing Times.
[3] "Case study -Business Continuity Planning at the Bank of Japan case study. " September 2013.
[4] Nitin khanapurkar july –September 2008 cab calling Disaster management and Business Continuity Plan for banker.

[5] Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook
[6] http://www.thefreedictionary.com/sabotage
[7] R. Barry Johnston and Oana M. Nedelescu the Impact of Terrorism on Financial Markets.
[8] Swiss banking Recommendations for Business Continuity Management (BCM).
[9] Eliza M.Lis, Christiane Nickel (2009) The impact on extreme weather event on budget balance.
[10] Reserve Bank of India Mumbai, ―Report of the Working Group on Electronic Banking", January 2011, accessed on March 22, 2012.
[11] Weider D.Yu,Shruti Nargundkar,Nagapriya Tiruthani, -A Phishing Vulnerability Analysis of Web Based Systems (2008) IEEE.
[12] Atul Bamrara, Gajendra Singh and Mamta Bhatt. ―Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector‖. International Journal of Cyber Criminology Vol 7 Issue 1 January - June 2013.
[13] Namita Chandra,Ashwini Taksal, etal – Sensitive Data Protection using Bio-Metrics. Vol 4 IEEE 2014
[14] **Indoor air pollution, health and economic well-being E. Duflo**1**, M. Greenstone**1**, and R. Hanna**2 Copernicus Publications on behalf of the Institut Veolia Environnement Feb 2008
[15] http://www.ehib.org/page.jsp?page_key=149