Business Continuity & Disaster Recovery

(Chapter - 3 : DISSA Course)

Arijit Chakraborty

June 5 , 2021

IT Rules 2021 : status update

- **IT & Law Minister Shri Ravi Shankar Prasad** :
- *''New (IT) Rules protect rights of users, were framed because of social media giants' refusal to do so ."*
- *'' Do business, earn profit, enhance user base … but be accountable to Constitution and laws of India."*
- Google, whatsapp, Google, Koo, ShareChat – complied : **CCO, Nodal & Grievance officers**
- Delhi HC Directed Twitter to comply with new IT Rules 2021- submit Compliance report in 3 weeks

Recent Cyber – fraud: ATM (Kolkata, May 25, 2021)

- Criminals in Kolkata hacked into 3 ATM of ICICI Bank between May 14 - 22 , stole INR 39.6 lakh
- Hackers connected to bank's server using small device attached to cables in ATM.
- Attackers used blocked card to withdraw cash.
- Reported in Delhi, Bangalore, Gurugram, Noida & Jalandhar before
- *Shri Murlidhar Sharma, JCP (crime) investigating*

Modus operandi

- End-to-end encryption in communication between ATM terminal & bank's server broken.
- RBI – in 22-page advisory : 18.02.21 (RBI/2020-21/74) asked all stakeholders **to upgrade ATM security** to thwart MiTM attacks
- **1. Banks told to ensure** : *network cables, input or output ports in ATM premises to be hidden & secure.*
- 2. **Banks to ensure : *end-to-end encryption of communication between ATM terminals or PCs & ATM switches/ authorization host***
- Specific types of ATM, not upgraded– were hacked

RBI Direction

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2020-21/74
DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21 February 18, 2021

The Chairman/ Managing Director/ Chief Executive Officer
All Scheduled Commercial Banks excluding RRBs/
Small Finance Banks/Payments Banks/ Credit Card issuing NBFCs.

Madam/ Dear Sir,

Master Direction on Digital Payment Security Controls

Please refer to para II (7) of the Statement on Developmental and Regulatory Policies of the Bi-monthly Monetary Policy Statement for 2020-21 dated December 4, 2020 (extract given below). The Master Direction provides necessary guidelines for the regulated entities to set up a robust governance structure and implement common minimum standards of security controls for digital payment products and services.

Yours faithfully,

(T.K. Rajan)
Chief General Manager

MITM Attack

- Fraudsters open hood of ATM machine,
- Intercept cable which connects ATM to bank server by attaching small device.
- Secretly intercept 2-way encrypted messaging & data transfer between ATM & bank servers -- manipulate
- Enables them to block or alter return SMS from server to ATM. Machine then starts dispensing Cash
- CCTV : hackers inserted cards, stayed for 30 minutes – 1 hour, walked away after pocketing cash.
- **ICICI bank statement** : ATM machines maintained by HITACHI but despite notice from them, HITACHI did not update system.

AdBlock working

- Ads served by servers with known addresses
- Ad blocker finds & hides directly in web page.
- AdBlock tool identify items & **delete them** or **set them as invisible.**
- **Risk**
- Some servers & websites **sell personal data** without User knowledge, some ad blockers do same.
- Ad blockers free,so **rely on this business model** to survive.

Online Gaming Industry

- **Key drivers :**

✓ Online fantasy sports leagues, quizzing & card games -poker.

✓ Affordable smartphones : users expected to reach 950 million in 2 years

✓ high-speed internet

✓ falling data prices.

- **Investments**
- **Mukesh Ambani :**
- gaming doesn't really exist in India
- sees a huge opportunity with increasing broadband connectivity
- India witnessing growth of online fantasy sports leagues
- **KPMG (March 2019 report) :**
- Revenue from online gaming expected to climb from 43.8 billion rupees ($610 million) in March 2018 to 118.8 billion rupees by fiscal 2023,

Cyber incidents

- **Gaming industry**
- 152 million web application attacks & billions of incidents of credential stuffing over a 2-year period.
- Gaming industry suffered 12 billion cyberattacks between Nov 2017 - March 2019

RBI : Compliance of System Audit Report (SAR)

- RBI : most banks yet to submit **system audit reports** certifying compliance with data store rules **even after 3 years of issuing circulars.**
- RBI : stated many foreign banks contesting : audit rules **do not apply to them** ‘’this was not acceptable”.
- RBI banks to submit compliance with plan by May 15, 2021.
- ‘’On soil” data storage

- **RBI : Data Localisation**
- several foreign banks unable to issue audit report stating : all personal & non personal data sent overseas for processing **has been deleted.**
- RBI barred **AmEx Bank & Diners Club** from adding new customers due to data storage rule violation.
- RBI's "on soil" data storage norms

BCP : Overview

Over 50% of businesses have experienced a disaster (either natural or man-made).

Businesses hit by disasters face many potential problems:

Communication Outages - difficult to locate key personnel

Transportation – unable to reach, unreliable or dangerous

Power – outage and lack of fuel for generators

Computer Systems – down and non retrievable

Facilities – damaged or destroyed

Underwater Infrastructure – offices, factories

Mail Service – interrupted or unavailable for weeks

Wide Area Networks – non functional

Reputation Damage – inability to reach customer's demands

WHAT IS BUSINESS CONTINUITY:

- Business continuity : **plan to deal with difficult situations**, so organization can continue with **as little disruption** as possible.
- Whether it's a business, PSU , or charity, - BCDR is vital

DISASTER RECOVERY PLANNING:

- **Disaster recovery plan (DRP)** : documented, structured approach that describes how an organization can quickly resume work after an unplanned incident.
- **DRP =** essential part of business continuity plan (BCP).
- Applied to aspects of organization that depend on functioning IT infrastructure.
- DRP : help an organization **resolve data loss & recover system functionality** so that it can perform after incident, even if it operates **at a minimal level**.

Natural Disasters

1. **Geological:** earthquakes, volcanoes, tsunamis, landslides
2. **Meteorological:** hurricanes, tornados, wind storms, hail, ice storms, snow storms, rainstorms, & lightning
3. **Other**: avalanches, fires, floods, meteors - meteorites, & solar storms
4. **Health:** widespread illnesses, quarantines, pandemics

Not all disruptions are disasters

Man-made Disasters

1. **Labor:** strikes, walkouts, & slow-downs that disrupt services and supplies
2. **Social**-political: war, terrorism, sabotage, vandalism, civil unrest, protests, demonstrations, cyber attacks, & blockades
3. **Materials**: fires, hazardous materials spills
4. **Utilities**: power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout from power plant accidents

BCP & DRP
= aid in CIA

- BCP & DRP
- Security pillars: C-I-A
  - Confidentiality
  - Integrity
  - Availability
- BCP and DRP **directly support availability**

Excerpt from DISSA Study Material

What is disaster recovery? A subset of BC

Disaster recovery includes the backup systems and IT contingency methods for organization's critical functions and applications.

Disaster recovery, as part of an overall BC plan, is about restoring IT systems and operations as efficiently as possible following a disaster. DR includes the backup systems and IT contingency methods for organization's critical functions and applications.

What's the difference between business continuity and disaster recovery?

The former is the overarching plans that guide operations and establish policy. Disaster recovery is what happens when an incident occurs.

Disaster recovery is the deployment of the teams and actions that are sprung. It is the net results of the work done to identify risks and remediate them. Disaster recovery is about specific incident responses, as opposed to broader planning.

After an incident, one fundamental task is to debrief and assess the response, and revising plans accordingly.

Business Impact Assessment

The impact assessment is a cataloguing process to identify the data of company holds, where it's stored, how it's collected, and how it's accessed. It determines which of those data are most critical and what the amount of downtime is that's acceptable should that data or apps be unavailable.

ELEMENTS OF BCP:

- **1. Threat Analysis**

Identification of potential disruptions, & potential damage they can cause to affected resources.

2. Role assignment

•Every organization needs a well-defined chain of command **to deal with crisis scenario**.
• Employees must be **cross-trained on their responsibilities**
•Internal departments (e.g., marketing, IT, human resources) to broken down into teams based on their skills and responsibilities.
•Team leaders can then assign roles and duties to individuals according to organization's threat analysis.

3. Communications

•A communications strategy details how information is disseminated **immediately following and during a disruptive event, as well as after it has been resolved.**

•Strategy should include:

✓**Methods of communication** (e.g., phone, email, text messages)
✓**Established points of contact** (e.g., managers, team leaders, human resources) responsible for communicating with employees
✓**Means of contacting** employee family members, media, government regulators, etc.

4. Backups

From **electrical power to communications and data**, every **critical business component** must have adequate backup plan that includes:

- **1. Data backups to be stored in different locations**. - prevents destruction of both original & backup copies at same time.
- If necessary, offline copies may be kept
- 2. **Backup power sources, such as generators & inverters** to deal with power outages.
- 3. **Backup communications** (e.g., mobile phones and text messaging to replace land lines) and backup services (e.g., cloud email services to replace on-premise servers).

BCP Policy Document

- **1. Plan Introduction**
- 1.1 Recovery Life Cycle - After a "Major Event"
- 1.2 Mission and Objectives
- 1.3 Disaster Recovery/Business Continuity Scope
- 1.4 Authorization
- 1.5 Responsibility
- 1.6 Key Plan Assumptions
- 1.7 Disaster Definition
- 1.8 Metrics
- 1.9 Disaster Recovery/Business Continuity and Security Basics

HFDC Bank – BCP Policy Document

- *HDFC Bank's mission is to be a world class Indian bank by adopting a single minded focus on service excellence and product quality.*
- *The Bank has adopted industry leading best practices in establishing a set of operating principles which govern how risks of a significant business disruption are mitigated to protect the Banks customers, employees and stakeholders.*
- *The Bank has a robust and well defined business continuity program which comprises of policies and procedures with clearly defined roles, responsibilities and ownership for Crisis Management, Emergency Response, Business recovery and IT Disaster Recovery Planning.*
- *The Bank's BCP steering committee, represented by the senior executive management of the Bank, approves and oversees the annual BCP strategy and road map.*

- *Regular drills and tests are conducted to cover all aspects of the Business Continuity Plan. Plans are reviewed and maintained regularly to incorporate any changes to environment, people, process and technology.*
- *The Bank's Business Continuity Office continuously works towards strengthening the business continuity preparedness of the Bank.*
- *The Bank's Business continuity program is developed to manage the impact of significant disruptions and will endeavor to resume business and operations to an acceptable level within a reasonable time in the event of a disaster.*
- *While the recovery time objectives (RTO) have been defined and documented in the plans, various external factors beyond our control could affect the actual recovery time.*
- *The Banks business continuity plan is in line with the guidelines issued by regulatory bodies and is subject to regular internal, external and regulatory reviews.*

- ***When a significant disruption occurs:***
- *After a significant disruption or a disaster, if your usual access to funds, transactions or branch is affected,* ***please contact us through our phone banking numbers****.*
- ***Phone banking numbers*** *of your nearest location are published on our website.*
- ***Contact numbers for credit card and debit cards*** *are also printed on the rear of your debit / credit / ATM card.*
- *If you are not able to contact us through phone banking, you could visit our web-site at www.hdfcbank.com and send us your queries and requests through online contact links*

- ***Alternative Channels for transacting Government Business during calamity / strike / disruptions***
- *The Bank provides multiple modes of payment for fulfilling Government business, such as payment through cash or cheque directly at the Bank's branches, payment through credit cards, debit cards or net banking accounts from the Bank's website.*
- ***If RBI or other Banks are not available**: Tax payments can be processed at our branches or any of the methods mentioned above*
- ***If cheque-based clearing facility is not available**: Funds Transfer can be processed from our branch or website (Net Banking) through NEFT or RTGS*