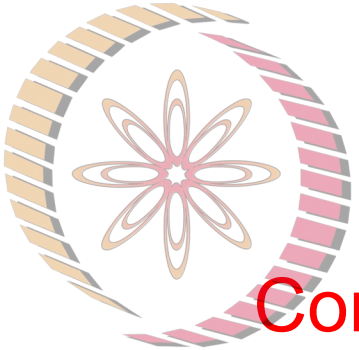
Cyber Security and Privacy
MS6880



Contingency Planning

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

IT project at IVK

- The IT department of IVK proposed an upgrade of their security infrastructure
- The steering committee responsible for prioritizing IT projects of IVK rejected the proposal for two consecutive years
- Reason: No ROI

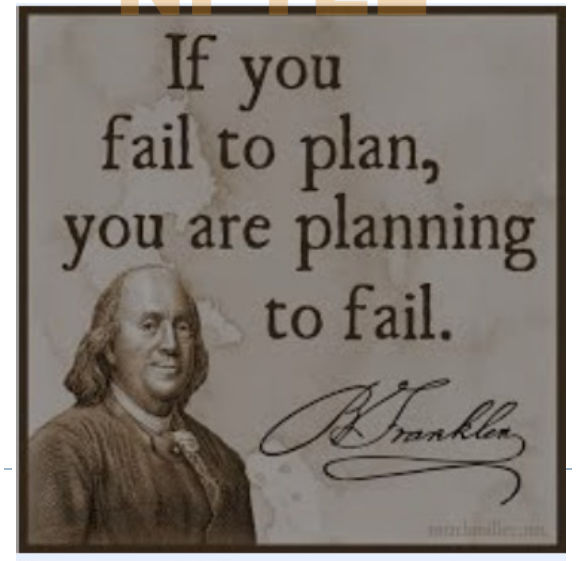
NPTEL

Security a low priority?

- Tangible drove out the significant!
- Poor articulation by IT dept
- Prioritization process issue
  - Selective, convenient, political

Planning

- Planning is creating action steps toward goals and then controlling them
  - Provides direction for the organization's future
  - Allows managing resources
  - Optimizes the use of the resources
  - Coordinates the effort of independent organizational units

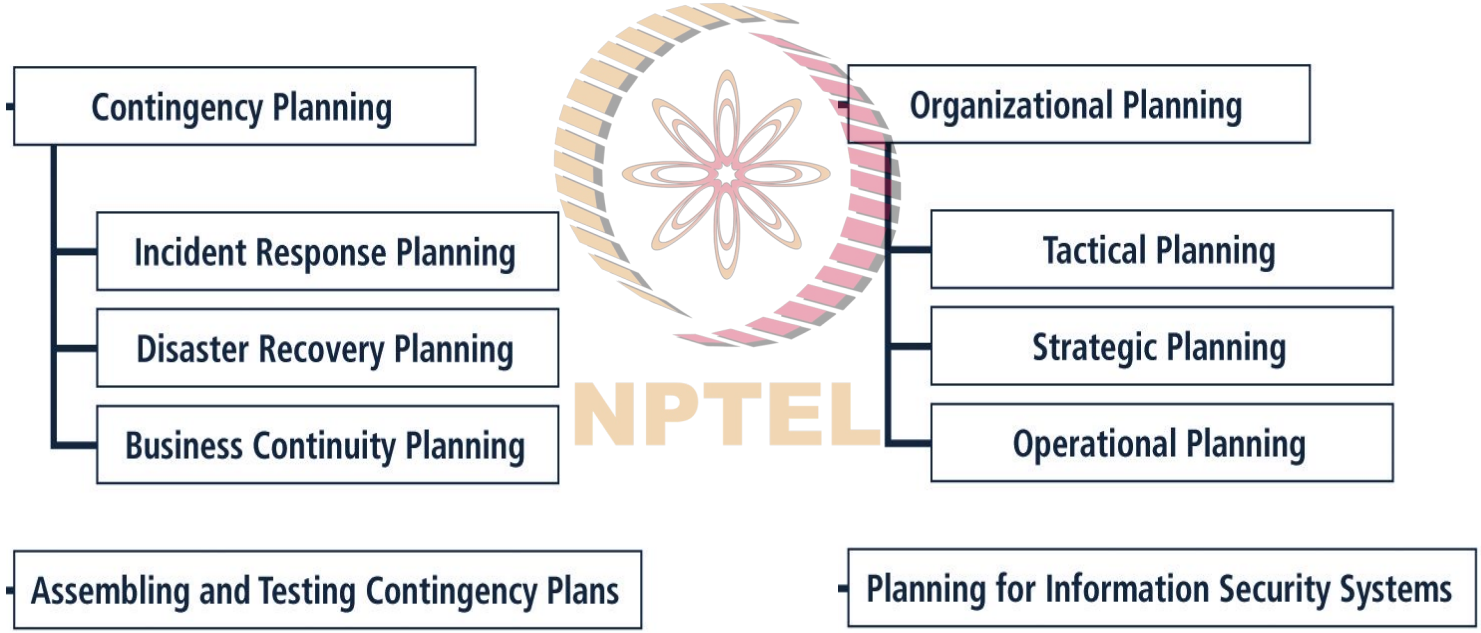


Security in planning

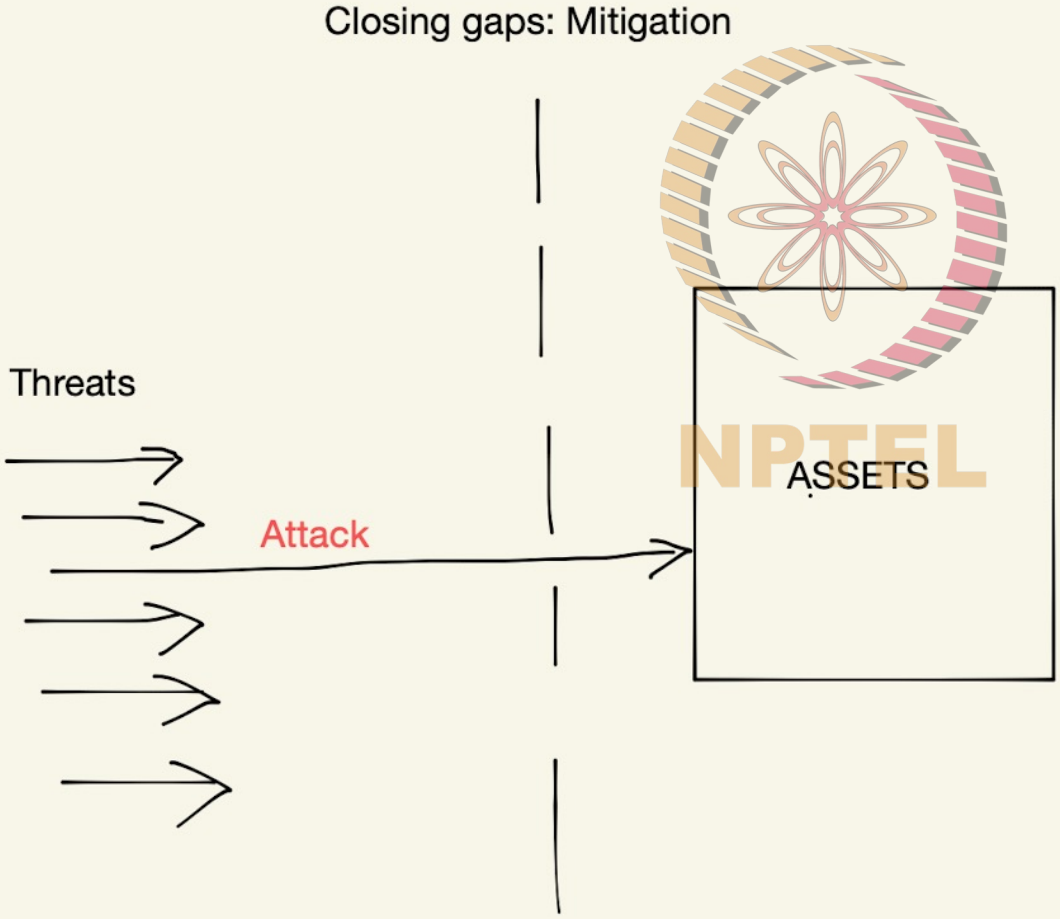
This nation should dedicate itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to Earth.

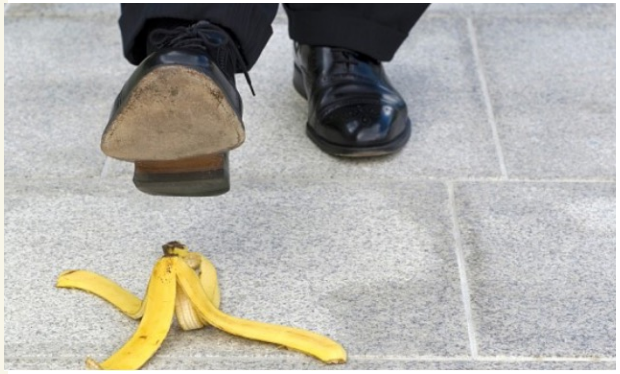
--JFK: May 25,1961

Information security planning



Threats, Attack, Vulnerability, Risk





Precursors to planning

- **Value Statement**

Integrity, honesty, passion, and respectfulness are significant parts of Microsoft's corporate philosophy

- **Vision Statement**

A personal computer in every home running Microsoft software ([old]

- **Mission Statement**

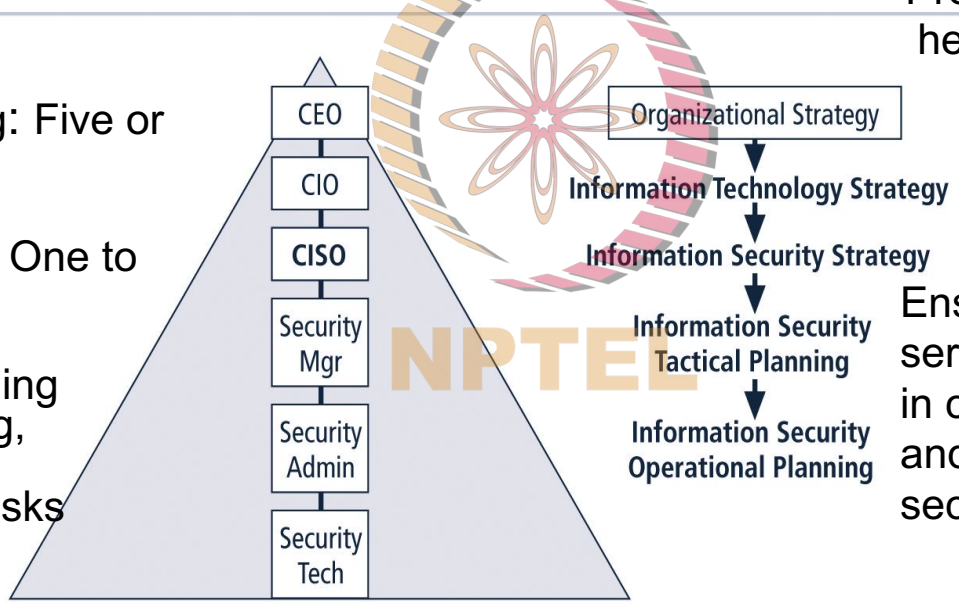
Organize the world's information and make it universally accessible and useful. [Google]

Top-down strategic planning

Strategic planning: Five or more year focus

Tactical planning: One to three year focus

Operational planning organizes ongoing, day-to-day performance of tasks



Providing the highest quality healthcare service in the industry

Providing high-level healthcare info service in support of the highest qual..

Ensuring that quality healthcare info services are provided securely and in compliance with all local, state, and national info processing, info security and privacy regulations.

CISO job description

- Creates strategic information security plan with a vision for the future of information security
- Understands fundamental business activities performed by the company
  - Suggests appropriate information security solutions that uniquely protect these activities
- Improves status of information security by developing
  - action plans
  - schedules
  - budgets
  - status reports
  - top management communications

NPTEL

What is contingency planning (CP)?

- The overall planning for unexpected events is called contingency planning (CP).
- It is how organizational planners position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets
- Main goal: restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event
- Contingency Plan Management Committee (CPMT) typically oversees the process

NPTEL

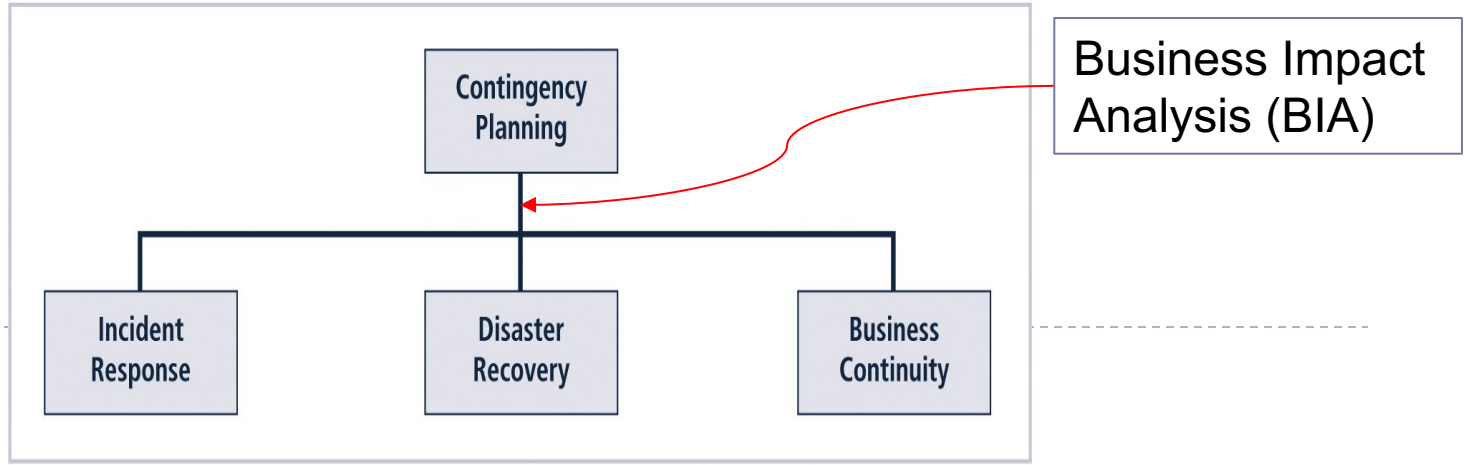
- Key open resource: Contingency planning guide for Federal information systems, NIST

Components of CP

Incident response planning (IRP) focuses on immediate response

Disaster recovery planning (DRP) focuses on restoring operations at the primary site after disasters occur

Business continuity planning (BCP) facilitates establishment of operations at an alternate site



Business processes and recovery criticality

BIA starts with prioritization of business processes

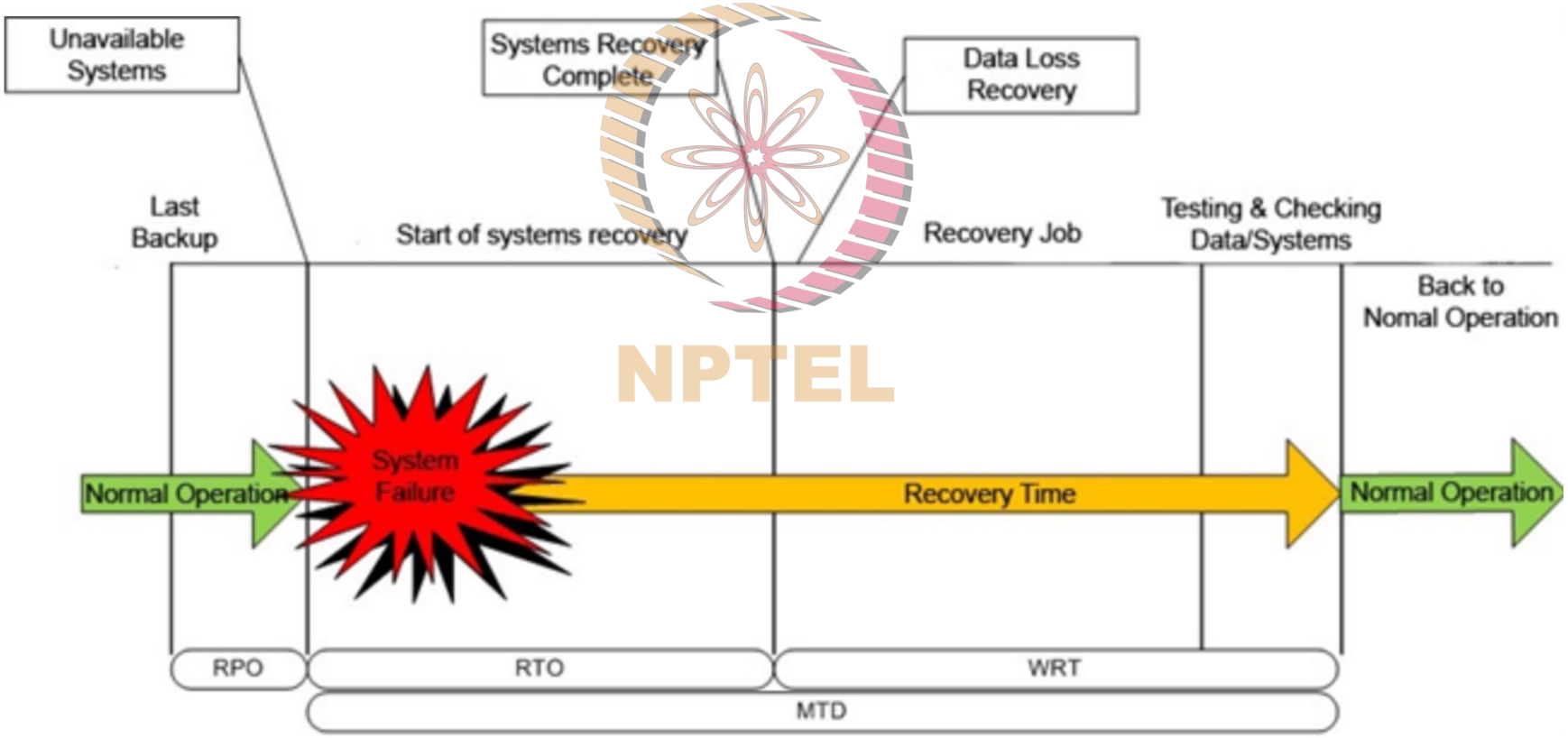
- Assembly line restoration vs recruitment process
- BIA questionnaire, experts, senior management

- Maximum Tolerable Downtime (MTD):
  - The total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage..
- Recovery Time Objective (RTO):
  - The max amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, other business processes and MTD
- Work Recovery Time (WRT):
  - The amount of effort (time) required to make business function after technology is recovered, with tasks such a testing and validation

$$MTD = RTO + WRT$$

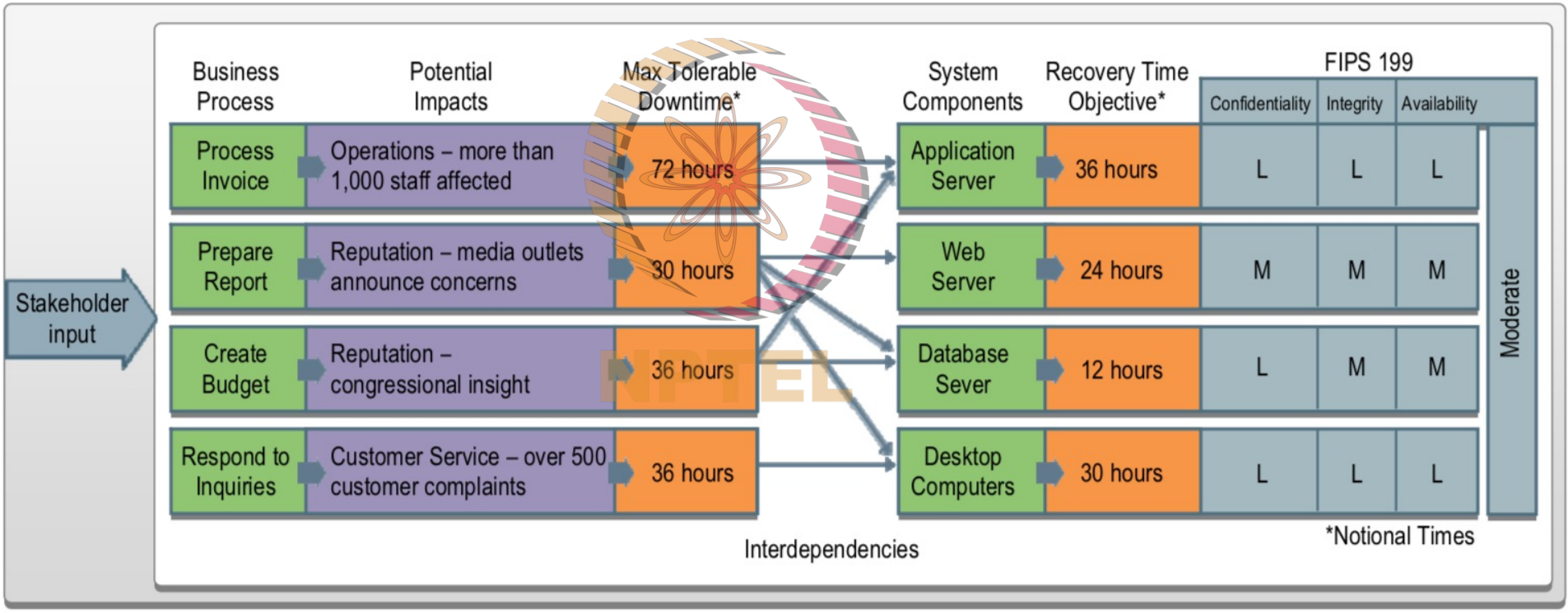
- Recovery Point Objective (RPO):
  - The point in time prior to disruption, to which business process data can be recovered upto, for a given backup

Recovery time lines

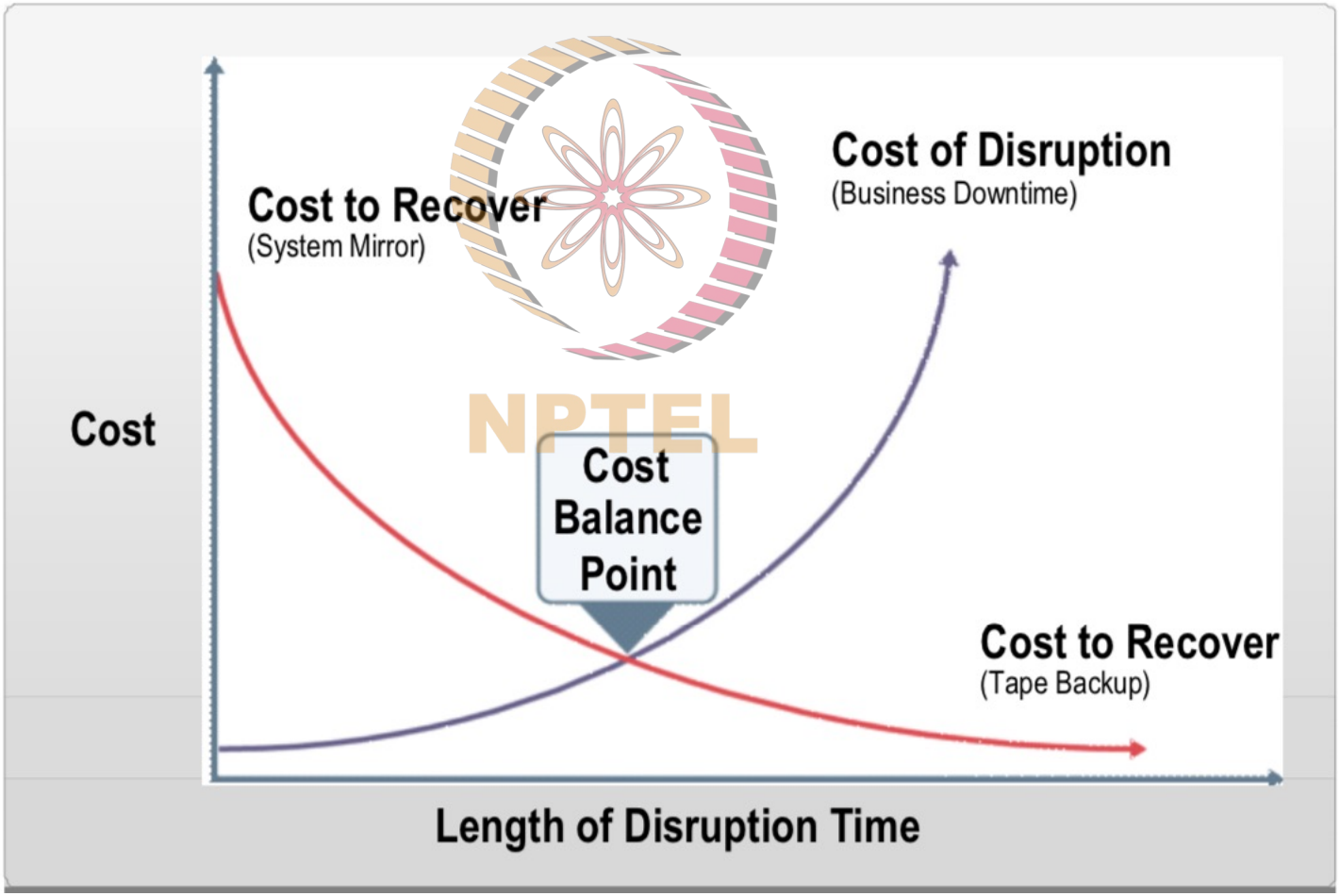


Ref: https://networksandservers.blogspot.com/2011/02/high-availability-terminology-ii.html

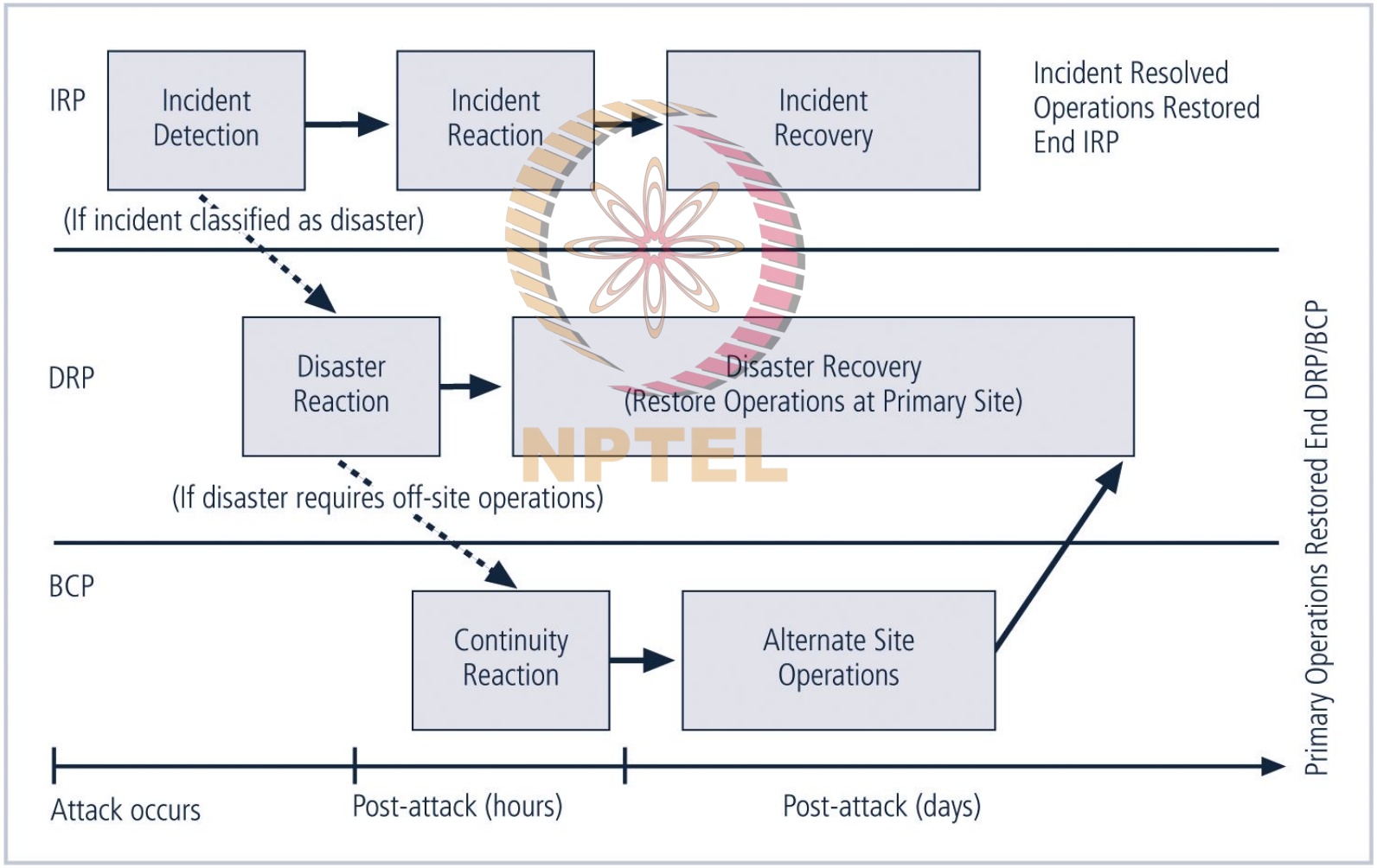
BIA process


Stakeholder input
Business Process
Potential Impacts
Max Tolerable Downtime*
Process Invoice
Operations – more than 1,000 staff affected
72 hours
Prepare Report
Reputation – media outlets announce concerns
30 hours
Create Budget
Reputation – congressional insight
36 hours
Respond to Inquiries
Customer Service – over 500 customer complaints
36 hours
System Components
Recovery Time Objective*
FIPS 199
Confidentiality
Integrity
Availability
Application Server
36 hours
L
L
L
Web Server
24 hours
M
M
M
Database Sever
12 hours
L
M
M
Desktop Computers
30 hours
L
L
L
Moderate
Interdependencies
*Notional Times

Cost balancing



Contingency plan implementation



In general, an incident is a disaster when:

- organization is unable to contain or control the impact of an incident **OR**
- level of damage or destruction from incident is so severe, the organization is unable to quickly recover

Incident Response Plan

- IRP:
  - Detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets
- Incident response (IR):
  - Set of procedures that commence when an incident is detected

NPTEL

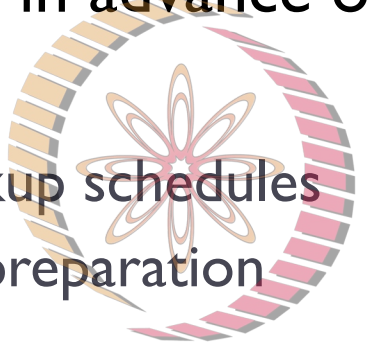
Incident Response Plan (Contd.)

- When a threat becomes a valid attack, it is classified as an information security incident if:
  - It is directed against information assets
  - It has a realistic chance of success
  - It threatens the confidentiality, integrity, or availability of information assets
- It is important to understand that IR is a reactive measure, not a preventative one

NPTEL

Before the Incident

- Planners draft a third set of procedures, those tasks that must be performed in advance of the incident
- Include:
  - Details of data backup schedules
  - Disaster recovery preparation
  - Training schedules
  - Testing plans
  - Copies of service agreements
  - Business continuity plans



During the Incident

- Planners develop and document the procedures that must be performed during the incident
- These procedures are grouped and assigned to various roles
- Planning committee drafts a set of function-specific procedures

After the Incident

- Once the procedures for handling an incident are drafted, planners develop and document the procedures that must be performed immediately after the incident has ceased

- Separate functional areas may develop different procedures

NPTEL

Incident detection

- Challenge is determining whether an event is routine system use or an actual incident
- Incident classification: process of examining a possible incident and determining whether or not it constitutes actual incident
- Initial reports from end users, intrusion detection systems, host- and network-based virus detection software, and systems administrators are all ways to track and detect incident candidates
- Careful training allows everyone to relay vital information to the IR team

Incident indicators*

- Possible Indicators
  - Presence of unfamiliar files
  - Presence or execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes
- Probable Indicators
  - Activities at unexpected times
  - Presence of new accounts
  - Reported attacks
  - Notification from IDS
- Definite Indicators
  - Use of dormant accounts
  - Changes to logs
  - Presence of hacker tools
  - Notifications by partner or peer
  - Notification by hacker

*Pipkin, Donald, Information Security,: Protecting the global enterprise, Prentice Hall, 2000

Incident response

- Once an actual incident has been confirmed and properly classified, the IR team moves from detection phase to reaction phase
- In the incident response phase, a number of action steps taken by the IR team and others must occur quickly and may occur concurrently
- These steps include notification of key personnel, the assignment of tasks, and documentation of the incident

NPTEL

Notification of key personnel

- As soon as incident is declared, the right people must be immediately notified in the right order
- Alert roster: document containing contact information of individuals to be notified in the event of actual incident either sequentially or hierarchically
- Alert message: scripted description of incident
- Other key personnel: must also be notified only after incident has been confirmed, but before media or other external sources learn of it

NPTEL

Documenting an incident

- As soon as an incident has been confirmed and the notification process is underway, the team should begin documentation
  - Should record the who, what, when, where, why and how of each action taken while the incident is occurring
- Serves as a case study after the fact to determine if right actions were taken and if they were effective
  - Can also prove the organization did everything possible to deter the spread of the incident

Example of IRP

Carnegie Mellon
INFORMATION SECURITY OFFICE

Table of Contents

Incident escalation

- An incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident
- Each organization will have to determine, during the business impact analysis, the point at which the incident becomes a disaster
- The organization must also document when to involve outside response

NPTEL

After Action Review

- Before returning to routine duties, the IR team must conduct an after-action review, or AAR
- AAR: detailed examination of events that occurred
- All team members:
  - Review their actions during the incident
  - Identify areas where the IR plan worked, didn't work, or should improve

NPTEL

Law enforcement involvement

- When incident violates civil or criminal law, it is organization's responsibility to notify proper authorities
- Selecting appropriate law enforcement agency depends on the type of crime committed: Federal, State, or Local
- Involving law enforcement has both advantages and disadvantages:
  - Usually much better equipped at processing evidence, obtaining statements from witnesses, and building legal cases
  - However, involvement can result in loss of control of chain of events following an incident

NPTEL

Disaster Recovery

- Disaster recovery planning (DRP) is the preparation for and recovery from a disaster, whether natural or man made
- In general, an incident is a disaster when:
  - organization is unable to contain or control the impact of an incident

    OR
  - level of damage or destruction from incident is so severe, the organization is unable to quickly recover
- Key role of DRP: defining how to reestablish operations at location where organization is usually located

NPTEL

Disaster Classifications

- A DRP can classify disasters in a number of ways
- Most common method: separate natural disasters from man-made disasters
- Another way: by speed of development
  - Rapid onset disasters
  - Slow onset disasters

NPTEL

Crisis management

- Crisis management: set of focused steps taken during and after a disaster that deal primarily with people involved
- Crisis management team manages event:
  - Supporting personnel and their loved ones during crisis
  - Determining event's impact on normal business operations
  - When necessary, making a disaster declaration
  - Keeping public informed about event
  - Communicating with outside parties
- Two key tasks of crisis management team:
  - Verifying personnel status
  - Activating alert roster

NPTEL

Business Continuity Planning (BCP)

- BCP
  - Ensures critical business functions can continue in a disaster
  - Most properly managed by CEO of organization
  - Activated and executed concurrently with the DRP when needed
  - Reestablishes critical functions at alternate site (DRP focuses on reestablishment at primary site)
  - Relies on identification of critical business functions and the resources to support them

NPTEL

Continuity strategies

- Several continuity strategies for business continuity
  - Determining factor is usually cost
- Three exclusive-use options:
  - Hot sites
  - Warm sites
  - Cold sites
- Three shared-use options:
  - Timeshare
  - Service bureaus
  - Mutual agreements

Exclusive Use Options

- Hot Sites
  - Fully configured computer facility with all services
- Warm Sites
  - Like hot site, but software applications not kept fully prepared
- Cold Sites
  - Only rudimentary services and facilities kept in readiness

NPTEL

Shared use options

- Timeshares
  - Like an exclusive use site but leased
- Service Bureaus
  - Agency that provides physical facilities
- Mutual Agreements
  - Contract between two organizations to assist
- Specialized alternatives:
  - Rolling mobile site
  - Externally stored resources

NPTEL

Off-site disaster data storage

- To get any BCP site running quickly, organization must be able to recover data
- Options include:
  - Electronic vaulting: bulk batch-transfer of data to an off-site facility
  - Remote Journaling: transfer of live transactions to an off-site facility
  - Database shadowing: storage of duplicate online transaction data

NPTEL

Testing Contingency Plans

- Once problems are identified during the testing process, improvements can be made, and the resulting plan can be relied on in times of need
- There are five testing strategies that can be used to test contingency plans:
  - Desk Check
  - Structured walkthrough
  - Simulation
  - Parallel testing
  - Full interruption
- https://danielmiessler.com/study/red-blue-purple-teams/

NPTEL

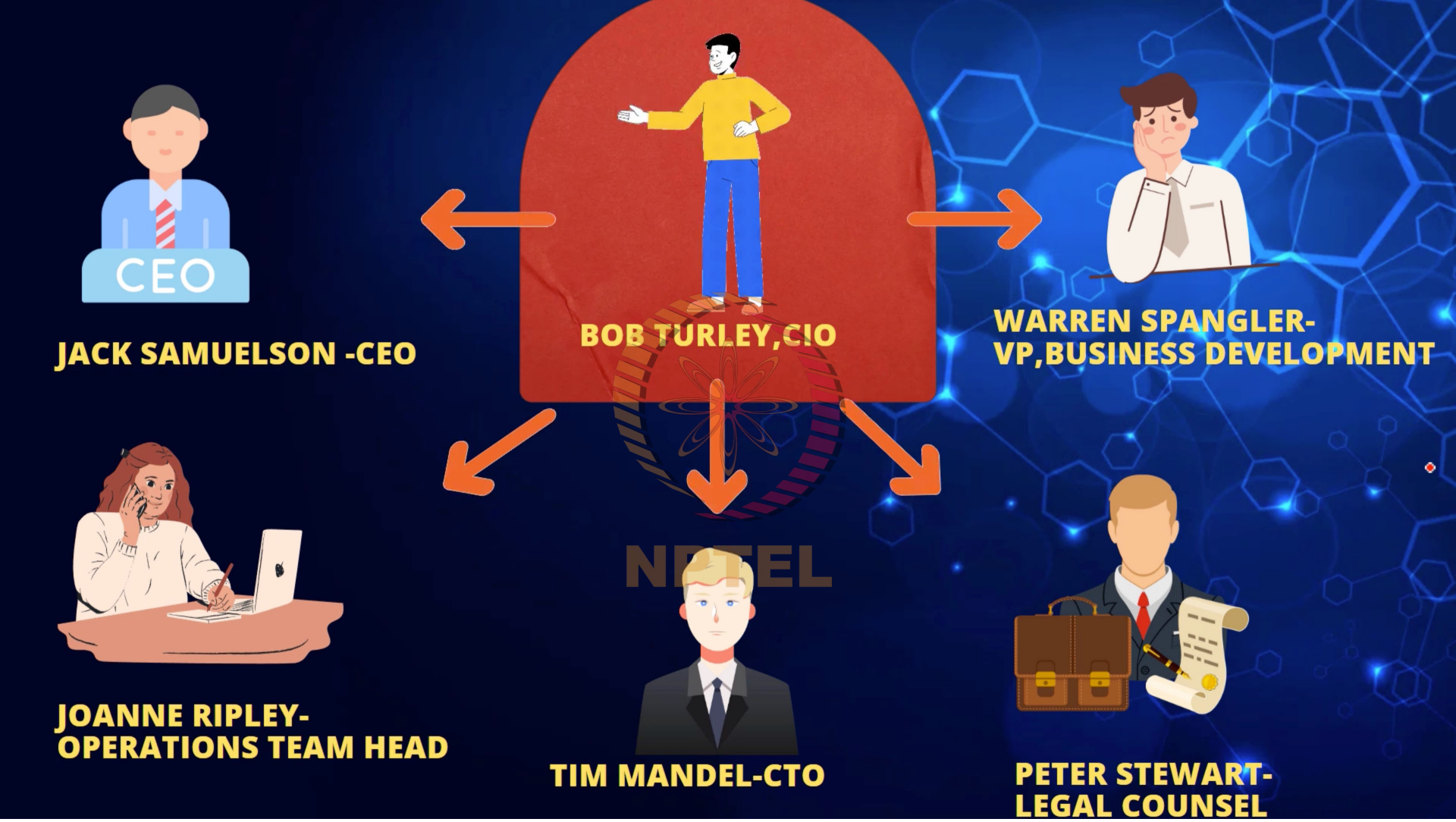
NPTEL

The iPremier company (B) & (C): Distributed Denial of Service Attack

GROUP MEMBERS:

1. K LOKESH - MS21A029
2. SANJANA ANAND - MS21A058
3. K R SUBISHA - MS21D026

PART A RECAP


CEO
JACK SAMUELSON -CEO
BOB TURLEY,CIO
WARREN SPANGLER-
VP,BUSINESS DEVELOPMENT
JOANNE RIPLEY-
OPERATIONS TEAM HEAD
TIM MANDEL-CTO
PETER STEWART-
LEGAL COUNSEL

THE STORY TILL NOW..

1

POSITION NOW

- one of top two retail chains
- most customers used credit cards
- only talented people were retained

2

TECHNICAL ARCHITECTURE:

- Yet to move to internal facility
- outdated,staffs attrition rate high

3

THE ATTACK

- DDoS Attack
- Detailed logging not enabled
- Not a good firewall to defend the attack

4

STATUS:

- No BCP
- No IRP
- No DRP

5

END OF ATTACK

- Automatic
- unsure whether firewall breached
- unsure whether customer info leaked

6

WAY FORWARD

- Shutting down completely
- disconnect from internet
- continue as usual

7

WHAT TO BE DONE NOW?

NPTEL

WHAT WENT WRONG??

TECHNICAL ISSUES

- No detailed logging in production computers
- No DDoS protection softwares
- outdated firewall
- Servers lacked capacity
- No Internal IT Team to firefight

MANAGERIAL PROBLEMS

- Young workforce, less experience
- Qdata still stands due to personal interests
- Greater investments required in security, infrastructure scaling and for a new Hosting facilities
- No emergency firefighting plans in place
- did not have routine checks of security infrastructure by simulating such possible attacks
- Didnt have a PR Strategy in place in case of similar Cyber threats
- Conflict of interests- No chain of command
- Monitoring of incompetent Qdata staff not monitored
- Bob hadnt taken serious action on Jack's initial caution that IPremier was running on deficit operating produres

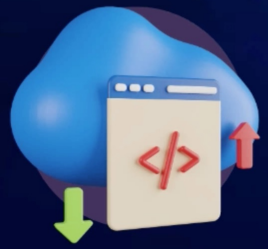
SEQUENCE OF EVENTS

iPremier disclosed publicly that it had been a victim of the DDoS attack

New secuity measures were implemented

Examination of files on every production computer

Ripley recommended that all the production computers be disconnected and Rebuild the software system



NPTEL

SECURITY MEASURES INSTITUTED

- Restarted all production computer equipment
- Conducted a file-file examination
- Study on technology solutions
- Project to move to a more modern hosting facility
- Modernized computing infrastucture
- Bought additional disk space and enabled high levels of logging
- Trained more staff in monitoring software
- Created Incidence response team
- Practices simulated attack
- Retained a cyber-security consulting firm
- Instituted third party security audits

THE DILEMMA

Option 1:
Go for Ripley's recommendation

- Disconnect all production computers from the Internet
- Rebuild software systems from development files
- Complete shut down for 24-36 hours to complete rebuild

Option 2:
Resistance to Ripley's recommendation

- Building a new site in a new facility from developmental files
- Later switch off old site only after new site is up and running

What do you recommend?
Let's open for discussion!

WEIGHING THE PROS & CONS

Option 1:

PROS

- Less time consuming
- Well documented process
- Provides guarantee w.r.t files

CONS

- Degrading customer satisfaction
- Increased competition from competitors

Option 2:

PROS

- No loss in sales
- New site - free of all vulnerabilities

CONS

- Costly to obtain space in a hosting facility & new equipment
- Keeping old system live can have negative consequences
- Time consuming

We suggest that the company should also diagnose the source of the issue and keep the services running in a parallel server until the issue is fixed.

SEQUENCE OF EVENTS

4 **Catastrophe**

Firewall had been penetrated, misdirected tactic "Suppressing fire during retreat"

3 **Call from FBI Agent**

MarketTop, biggest competitor is experiencing a DDoS attack from iPremier's production computing installation

2 **Accelerated Plan**

Create an iPremier site in a more up-to-date hosting facility

1 **Decision**

Senior Management decided not to shutdown the business for a comprehensive rebuild of all production platform.

NPTEL

3 ISSUES FACING THE COMPANY

Implement Ripley's recommendation

- Source of an Illegal attack
- Destruction of evidence of a crime

Handle situation between iPremier & MarketTop

- Lawsuit against iPremier
- How to approach MarketTop?

What to say publicly?

- Database server has been compromised
- Couldn't identify affected individual customer
- Violation of credit card processing agreement

HOW THE ISSUE CAN BE SOLVED

Implement Ripley's recommendation

- Run services from a parallel QData server, allow customers to surf while fixing issues
- Hold on credit card payments, Enable COD

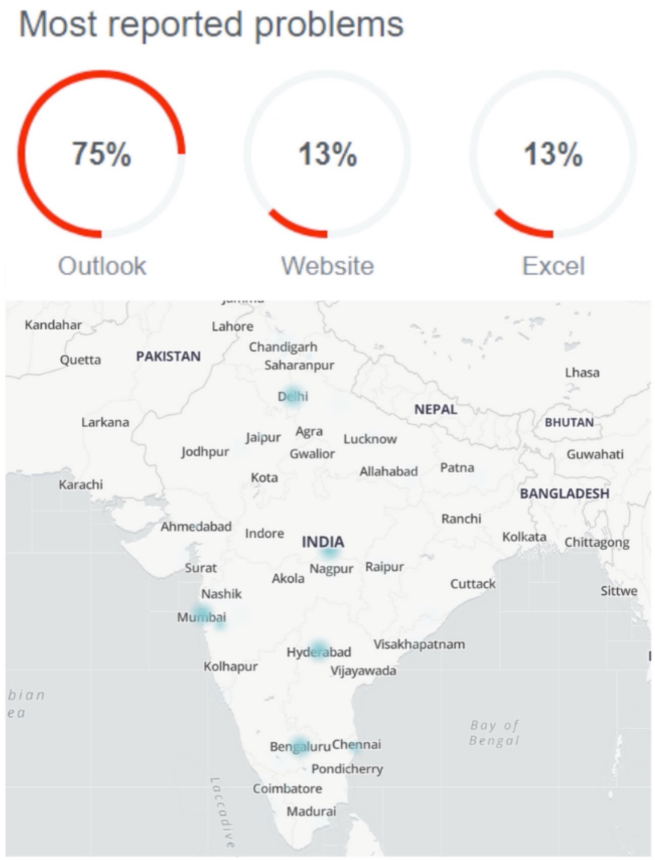
Handle situation between iPremier & MarketTop

- Request FBI to conduct diagnosis at iPremier and share report with MarketTop
- Collaborate with MarketTop and ensure security

What to say publicly?

- Publish the incident report and counter measures taken
- Flash a message saying that " Server is under Maintenance"

Microsoft services face major outage; Teams, Outlook, Store stop responding



Microsoft 365 Status @MSFT365Status · Jan 25

We've confirmed that the impacted services have recovered and remain stable. We're investigating some potential impact to the Exchange Online Service. Further, updates on the Exchange investigation will be available in your admin center under the SI# EX502694.

31 152 330 84.1K

Microsoft 365 Status @MSFT365Status · Jan 25

Replying to @MSFT365Status

We've isolated the problem to networking configuration issues, and we're analyzing the best mitigation strategy to address these without causing additional impact. Refer to the admin center MO502273 or msft.it/6018eAIdp for more information.

53 279 509 214.8K

Microsoft 365 Status @MSFT365Status · Jan 25

Replying to @MSFT365Status

We've rolled back a network change that we believe is causing impact. We're monitoring the service as the rollback takes effect.

114 469 960 262.2K

NPTEL

Microsoft services face major outage; Teams, Outlook, Store stop responding

[redacted] · Jan 25

Replying to @MSFT365Status

C'mmmon....it's up now. Y did you fix it so soon ??? The days when Exchange was on Prem were better. At least the outage used to be for few hours...

1 1 2,567

[redacted] · Jan 25

Replying to @MSFT365Status

thank you for service down, spent all the day solving issues for full inbox im enterprise plan, shall i move to google for 1tb plan

2 1,228

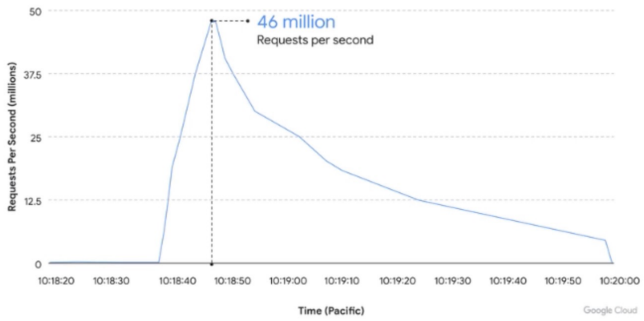
#MicrosoftTeams

Microsoft teams has stopped which means work has stopped

Everyone:

NPTEL

HOW GOOGLE CLOUD BLOCKED THE LARGEST LAYER 7 DDOS ATTACK AT 46 MILLION RPS

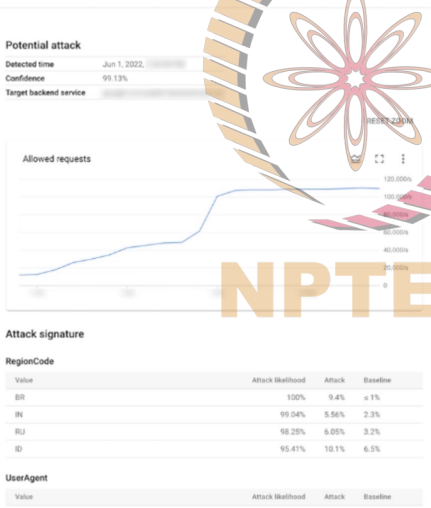


On June 1, 2022 a Google Cloud Armor customer was targeted with a series of HTTPS DDoS attacks which peaked at 46 million rps

- **Cloud Armor Adaptive Protection** was able to detect and analyze the traffic early in the attack lifecycle.
- It blocked the attack ensuring the customer's service stayed online and continued serving their end-users.

Open Systems Interconnection (OSI) Model:

#	Layer	Application
7	Application	Data
6	Presentation	Data
5	*Session*	*Data*
4	Transport	Segments
3	Network	Packets
2	*Datalinks*	*Frames*
1	*Physical*	*Bits*



How the attack was stopped?

- **Rate limiting** capability to throttle the attack traffic.
- A **defense-in-depth strategy** by deploying defenses and controls at multiple layers of the environment and infrastructure providers' network to protect your web applications and services from targeted web attacks.
- Performing **threat modeling** to understand your applications' attack surfaces, developing proactive and reactive strategies to protect them, and architecting your applications with sufficient capacity to manage unanticipated increases in traffic volume.

NPTEL

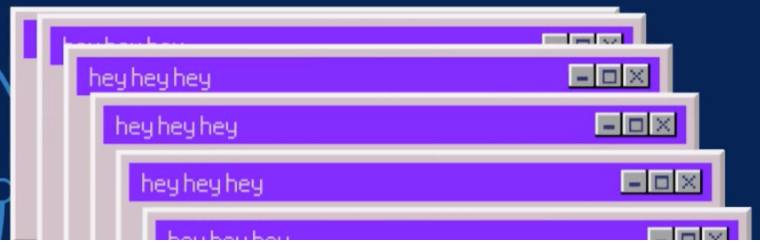
MITIGATION TECHNIQUES FOR DDOS ATTACKS

Reduce attack surface area

- Minimize surface area by limiting the options for attackers
- Not exposing the application or resources to ports or protocols where you do not expect any communication
- Placing computation resources behind load balancers/CDNs (Content delivery networks)

Know what is normal and abnormal traffic

- Rate limiting: Detecting elevated levels of traffic & handling accepted traffic



Plan for Scale

- Transit Capacity
  - Ample internet connectivity
  - Availability of resources and applications closer to the end user and internet exchanges
- Server Capacity
  - Running larger computation resources - for easy scale up or down
  - Load balancers - to shift loads

Deploy firewalls for Sophisticated Application attacks

- Deploying firewall -
  - Creating customized mitigation against illegetimate requests
  - Studying traffic patterns and create customized protections

NPTEL

CYBER RISK MANAGEMENT

- **CIA (Confidentiality, Integrity, Availability)**
  - Ripley didn't have access to Qdata server
- **Disaster Recovery Plan (DRP)** and **Incident Response Plan (IRP)** has to be implemented and practiced
- BCP (Business Continuity Plan) to be up to date
- Hardware and Software must be updated
- Improve network architecture
- Roles & Responsibilities to be adhered
- Identifying source of the attack - SOPs for cyber diagnosis - Forensic report to be recorded and maintained
- Maintain a parallel server, in case the original server stops functioning this can be turned on.

References

- https://www.businesstoday.in/technology/news/story/microsoft-services-face-major-outage-teams-outlook-store-stop-responding-367501-2023-01-25
- https://aws.amazon.com/shield/ddos-attack-protection/
- https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

THANK YOU!!