Incident Response and Recovery

What is Incident Response?

Incident response is the methodology an organization uses to respond to and manage a cyberattack.

Security Incidents vs IT Incidents

	IT Incidents	Security Incidents
Definition	Reduction or disruption of a service.	Reduction of security to networks, applications, data, or persons.
Purpose	Restore IT service. Not malicious.	Resolution of an attack, or security disruption. Often malicious.
Scope	IT service only.	Can span entire organization: HR, Compliance, facilities, legel,Vendors,etc.
Skills	IT technology	IT and offensive security, forensic knowledge, etc.

Why is Incident Response Important?

Protect Your Data

Protect Your Reputation

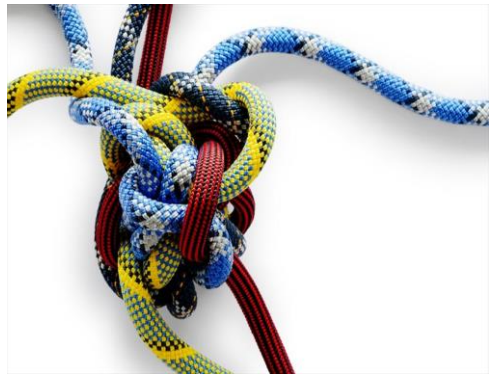
Protect Your Revenue

Incident Response Factors

Lack of resources

Lack of Skiles

Weak of security



Complexity

Lack of Visibility

Lack of Procedure

Lack of policy

Not learn from mistake

Incident Response Component

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Preparation phase

- Ensure your team are properly trained regarding their incident response roles and responsibilities in the event of data breach

- Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate your incident response plan.

- Ensure that all aspects of your incident response plan (training, execution, hardware and software resources, etc.) are approved and funded in advance

Questions to address

- Has everyone been trained on security policies?
- Have your security policies and incident response plan been approved by appropriate management?
- Does the Incident Response Team know their roles and the required notifications to make?
- Have all Incident Response Team members participated in mock drills?

Preparation phase

- How will you know about potential incident?
  Users, system alerts, SIEM, Third parties, others?

- Key decisions
  when dose management need to know?
  when dose legal get involved?
  when dose national CERT (NISSA) get involved?
  Prosecute, Yes , No it depends?

- What are the likely incidents you will encounter?

- What are the main steps?

- What resources are available and will be needed?

- What is the communication plan with in the investigation
  Who should be in the communication, how team will communicate

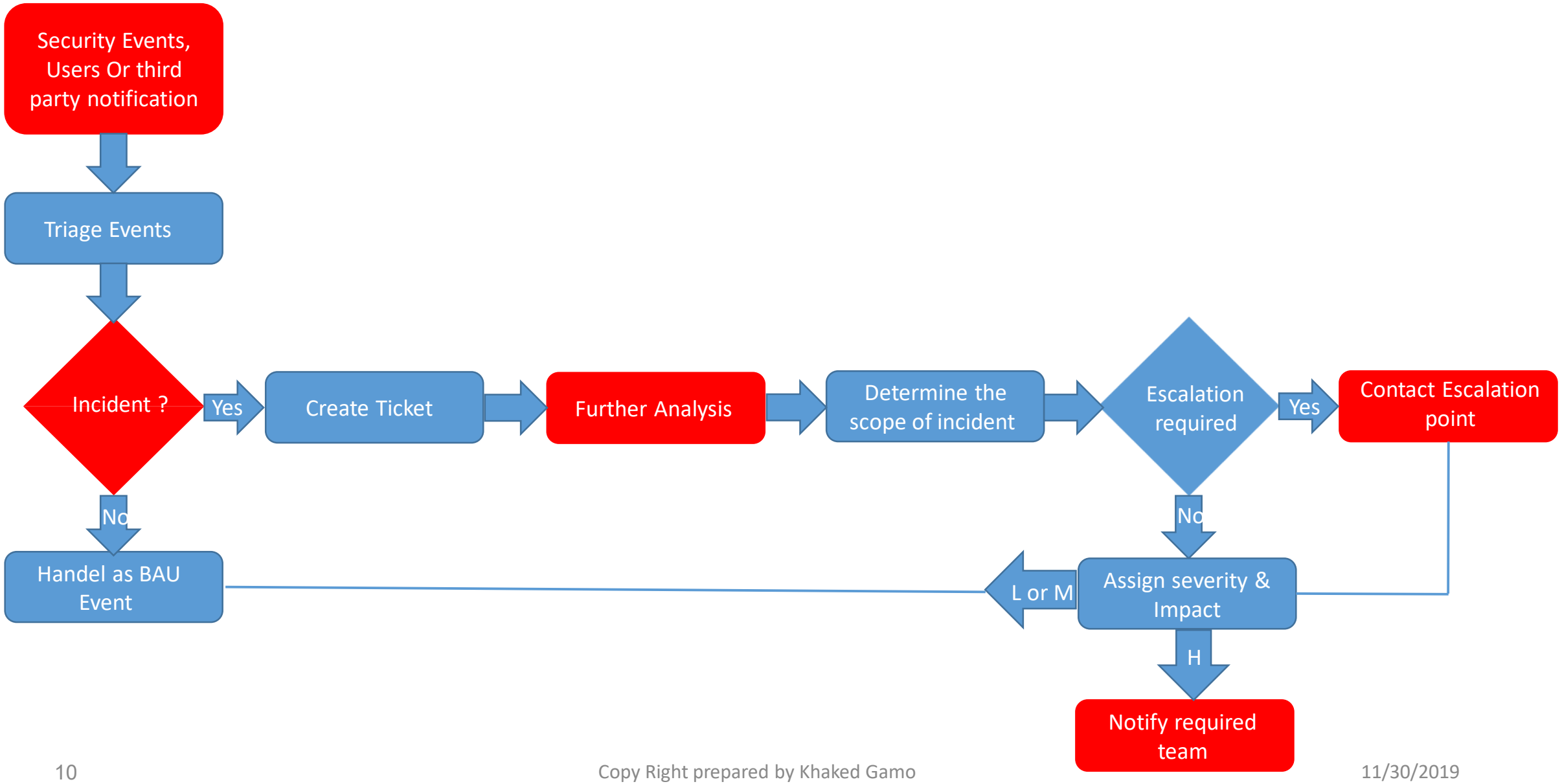
Identification phase

In this phase you will determine whether you've been breached.
A breach, or incident, could originate from many different areas.

Questions to address

- When did the event happen?
- How was it discovered?
- Who discovered it?
- Have any other areas been impacted?
- What is the scope of the compromise?
- Does it affect operations?
- Has the source (point of entry) of the event been discovered?

Identification Process



Containment phase

- What's been done to contain the breach short term?
- What's been done to contain the breach long term?
- Has any discovered malware been quarantined from the rest of the environment?
- What sort of backups are in place?
- Does your remote access require true multi-factor authentication?
- Have all access credentials been reviewed for legitimacy, hardened and changed?
- Have you applied all recent security patches and updates

Eradication

In this phase you need to be thorough. If any trace of malware or security issues remain in your systems, you may still be losing valuable data, and your liability could increase.

Questions to address

- Have artifacts/malware from the attacker been securely removed?
- Has the system be hardened, patched, and updates applied?
- Can the system be re-imaged?

Recovery Phase

During this time, it's important to get your systems and business operations up and running again without the fear of another breach.

Questions to address

- When can systems be returned to production?
- Have systems been patched, hardened and tested?
- Can the system be restored from a trusted back-up?
- How long will the affected systems be monitored and what will you look for when monitoring?
- What tools will ensure similar attacks will not reoccur? (File integrity monitoring, intrusion detection/protection, etc.)

Lesson learned

Once the investigation is complete, hold an after-action meeting with all Incident Response Team members and discuss what you've learned from the data breach.

Questions to address

- What changes need to be made to the security?
- How should employee be trained differently?
- What weakness did the breach exploit?
- How will you ensure a similar breach doesn't happen again?

Involved Team

- Representation from management
- Security analyst as primary handler
- Incident response SME
- Technical SME Networking, security, Data center Team
- Communication people
- Legal

Incident Response Framework

ISO/IEC 27035

INFORMATION SECURITY INCIDENT MANAGEMENT

NIST.SP.800-61

Computer Security
Incident Handling Guide

Incident Response Policy Sample

========== INCIDENT RESPONSE POLICY TEMPLATE ==========

Incident Response Program Policy

Statement of Management Commitment

The {organization name}'s leadership team is committed to information security and appropriate incident response to accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources. {Organization Name} has established the Incident Response Program to establish an actionable information security incident handling capability that includes preparation, detection, analysis, containment, recovery, and reporting for information security incidents.

The organization's {responsible executive} oversees the Incident Response Program as a whole and ensures that resources are appropriately maintained for preparedness and training for response to incidents that are reasonably foreseen or identified through continual activities associated with the Information Security Program.

Purpose

The Information Security Program includes an Incident Response Program provided to establish and maintain consistent Incident Response capabilities and processes enabling the organization to respond to cybersecurity threats and attacks swiftly and effectively. The Incident Response Program is designed to address the many factors that comprise typical attacks and the wide variety of considerations that go into ensuring your organization is prepared to handle all possible scenarios.

Scope

The scope of the Information Security Incident Response Program includes the span of authority and requirements assigned by the organization's executive leadership. All incidents impacting the confidentiality, integrity, availability of the organization's information or information systems as well as the privacy of individuals associated with the organization within the assigned authority are considered within the scope of the Incident Response Program.

Objectives

The Incident Response Program include objectives to:

Incident Response Report Forum Sample

Information Security Incident Report

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Security incident. All items completed should be based on information that is currently available. The report should be updated and modified during the course of the incident response process.

Incident ID (yyyymmdd-xxxx) **1. Incident Description.**	
Provide a brief description:	
2. Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	

Incident Response Plan Sample

Incident Response Plan Example

This document discusses the steps taken during an incident response plan. To create the plan, the steps in the following example should be replaced with contact information and specific courses of action for your organization.

1) The person who discovers the incident will call the grounds dispatch office. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
    a) Helpdesk
    b) Intrusion detection monitoring personnel
    c) A system administrator
    d) A firewall administrator
    e) A business partner
    f) A manager
    g) The security department or a security person.
    h) An outside source.

    List all sources and check off whether they have contact information and procedures. Usually each source would contact one 24/7 reachable entity such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.
2) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.
3) If the person discovering the incident is not a member of the IT department or affected department, they will call the 24/7 reachable grounds security department at xxx-xxx.

Understand Business Community Plan and Disaster Recovery Plan

Emergency Response Plans and Procedure

- Emergency Plans are greater scope than incident response
- Business Continuity Plan (BCP)
  - Broad in Scope
  - May include replacement location and staff
- Disaster Recovery Plans (DRP)
  - Recovery of specific service

Business Impact Analysis (BIA)

- Determine the impact to an organization and its operation due to a particular or complete loss
- Every business is different – need to determine critical from non critical function
- Perform impact analysis to understand and correct failures

Business Impact Analysis (BIA)

- Max Tolerable Downtime MTD

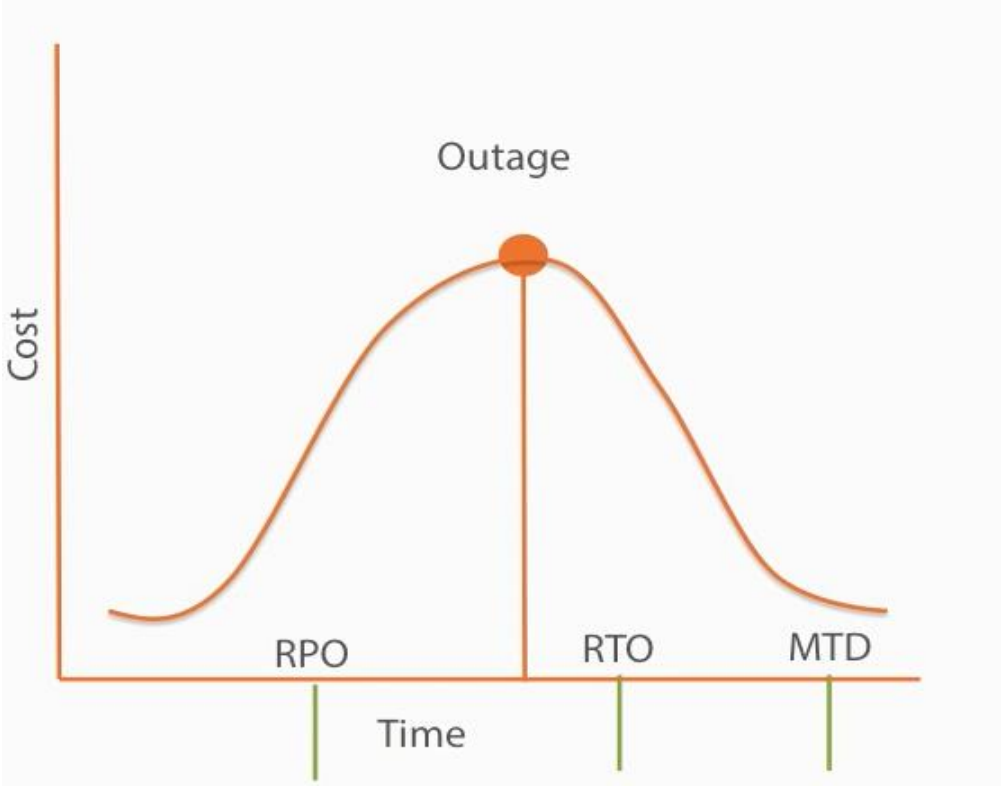
  Total time without business function before permanent harm

- Recovery Time Objective RTO

  Business function has been fully restored

- Recovery Point Objective

  Point at which reliable data can be restored



Disaster Recovery Plan (DRP)

- Documented process and procedures to recover and restore specific IT service
- Not the same as Incident management
  - Detect and stop
  - Recover and restore
- Classify disaster scenarios
- Availability of recovery assets
  - Hardware, Software, Location
  - Staff, good and services
- Communication Plans
  - often over looked

Interim or Alternative Processing strategies

- What to do of if entire site is lost?
- Alternative locations
  - Geographically separate
  - Can be cloud based
  - Different level of service

- Hot site
- Warm site
- Cold site
- Co-located site
- Mobile site

Backup and Redundancy Implementation

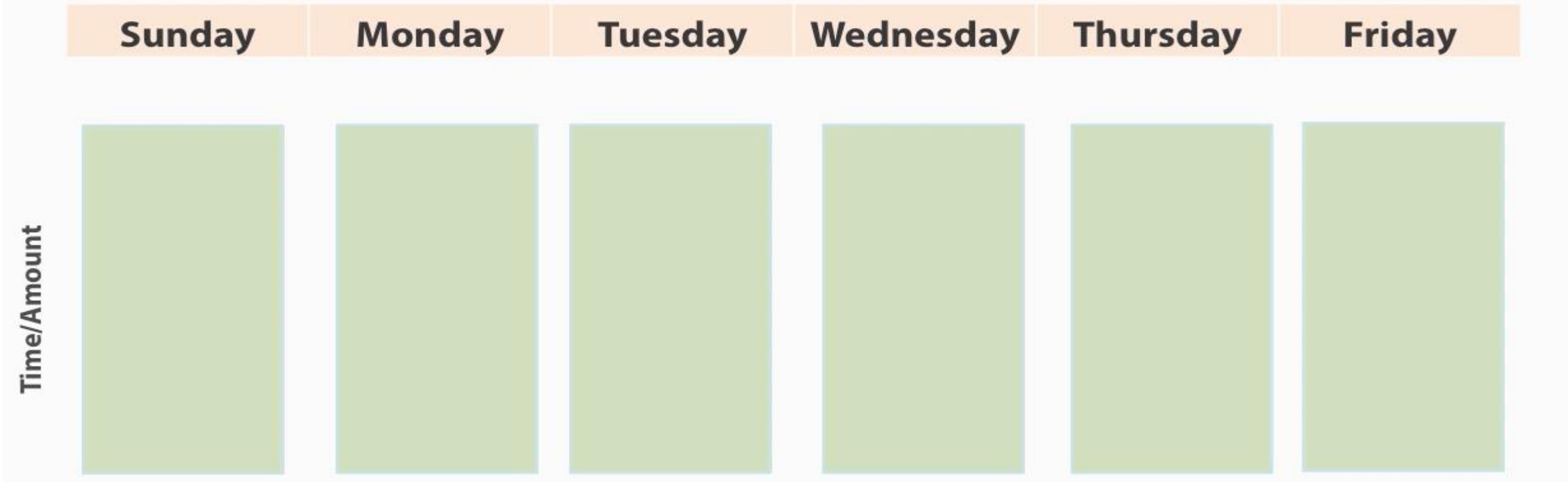
Fast Recovery time and minimum Data loss (RPO)
Time and Cost
Data Classification
How often does it need to be backed up?

Backup considerations

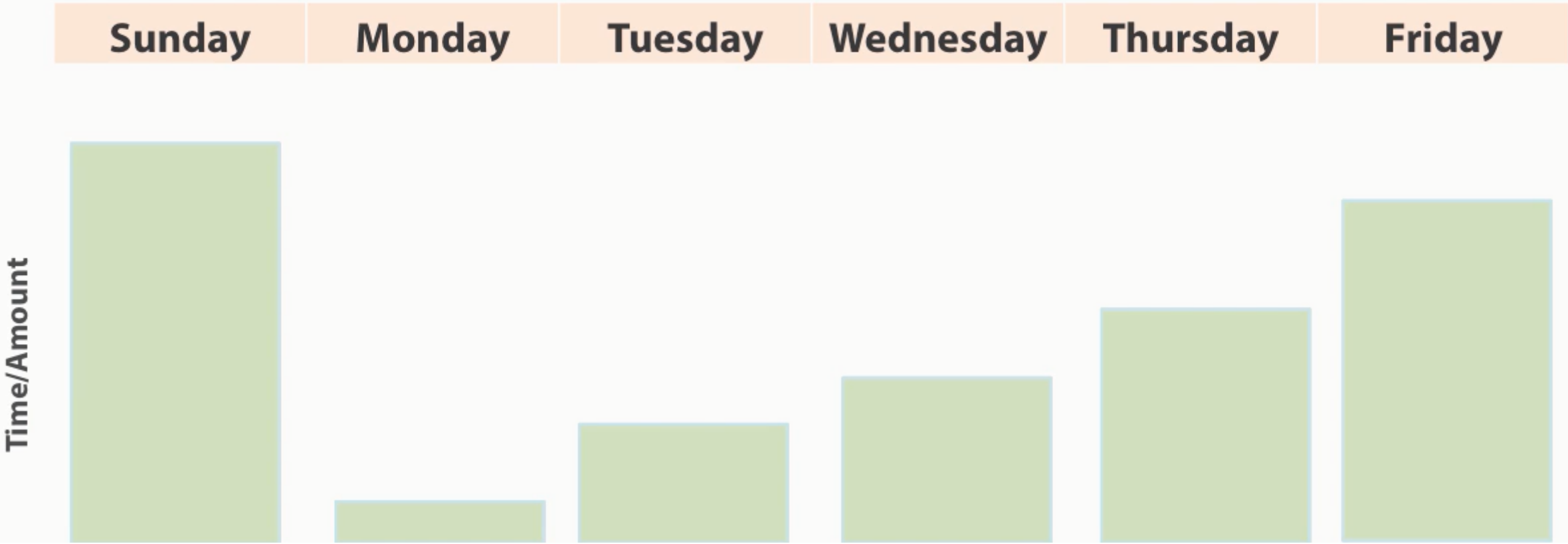
- Encryption
- Reliability
- Off site storage and recovery

Backup/Recovery methods

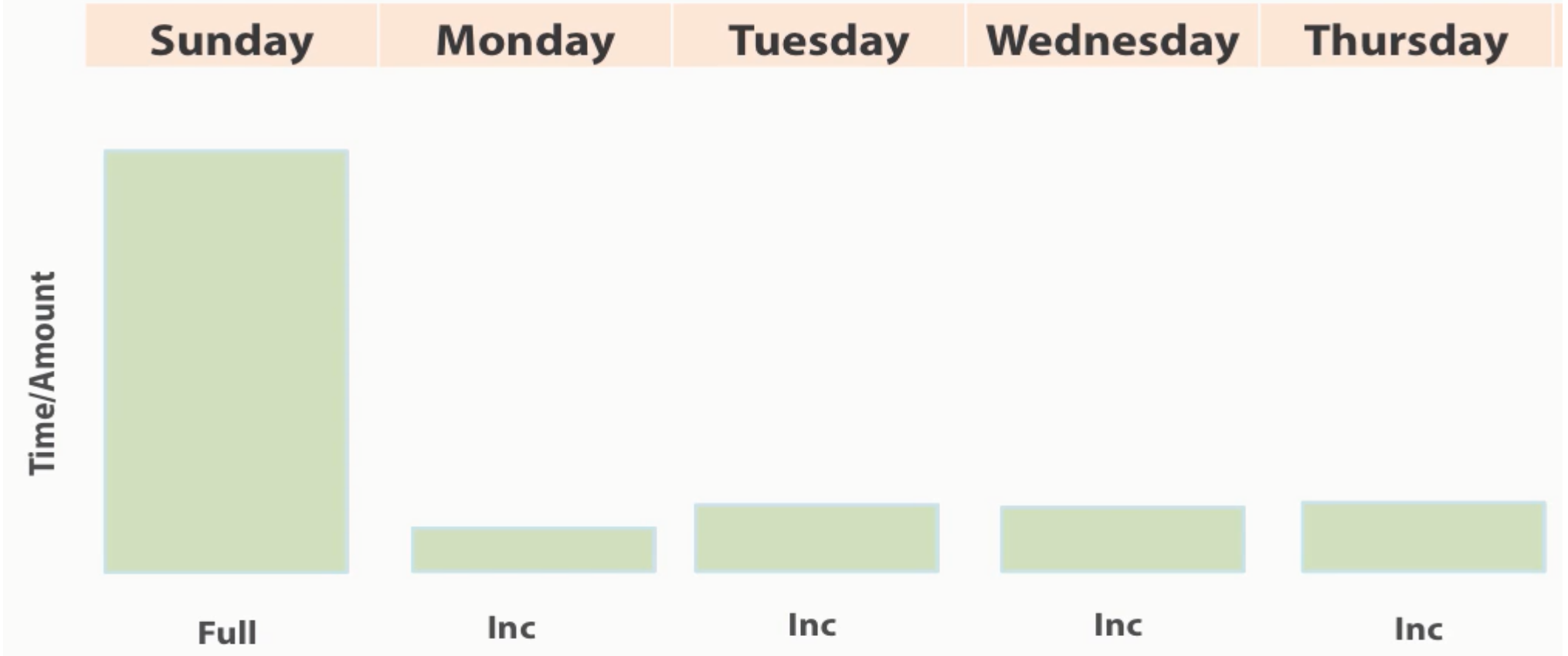
Backup Method: Full Backup



Backup Method: Differential



Backup Method: Incremental



Testing and Drill