Global Scientific JOURNALS

GSJ: Volume 12, Issue 11, November 2024, Online: ISSN 2320-9186
www.globalscientificjournal.com

HEALTHCARE ORGANIZATIONS' BUSINESS CONTINUITY AND DISASTER RECOVERY

STUDY CASE

Arthor: Bashiru Seidu

(Affiliations): The Ghana National Information Technology Agency (NITA), Accra-Ghana, Cyber Security Expert Association (CSEAG), Accra-Ghana, Institute of ICT Professionals Ghana (IIPGH)-Accra-Ghana, Ghana Tertiary Education Commission (GTEC), Accra-Ghana

Email: bashiru.seidu@bsconsultgh.com

Company: BS CONSULT GH LTD

Address: Tema-Lashibi community 16, P.O. Box385, Accra-Ghana

INTRODUCTION

Information systems engineers are among the few sectors that prioritize catastrophe prevention and recovery in their daily operations. Furthermore, ensuring a quick return to the pre-disaster capabilities of systems is more crucial in other businesses than in the healthcare sector.

Healthcare businesses must prepare for the recovery of business operations, the foundational IT systems, and the data needed to treat patients since they rely heavily on Electronic Health Records (EHRs) and have low tolerances for system outages.

The integration points of disaster recovery, business continuity, and incident response are briefly discussed in this white paper.

To ensure a thorough grasp of each plan's breadth and to assist healthcare organizations in strengthening their resilience to setbacks and unfavorable circumstances, key components of these plans will be given.

Continuity of Business and Incident Response plans need to take into consideration both emerging cyber threats like ransomware and other harmful codes, as well as more conventional risks like floods and fires. The infrastructure of healthcare institutions has security flaws that hackers and other cybercriminals are exploiting. They breach the network's security, encrypt the information, and then charge the healthcare organization a premium for the key that will allow them to unlock and recover their patient data.

Recent attacks like NotPetya are much more pernicious because the hackers' goal was not extortion but rather data destruction and disruption of the affected enterprise.

Three strategies are essential for maintaining operations and restoring capacities in the event of any kind of emergency:

1. The continuity of business

2. Reaction to Incidents

3. Recovery from Disasters

IMPORTANT DISTINCTIONS

In many businesses, the terms disaster recovery and business continuity are sometimes used interchangeably. When reacting to an event, companies may have a propensity to rely entirely on Disaster Recovery, sometimes without a specific event Response Plan or Process.

In many companies, there may be a lack of definitions for each of these strategies and the combined use of them in a crisis.

Planning for, handling, and recovering from contingencies involves a lot of different parts; these plans and procedures are complementary to each other and flow from one another. But each kind of strategy has a very particular goal in mind:

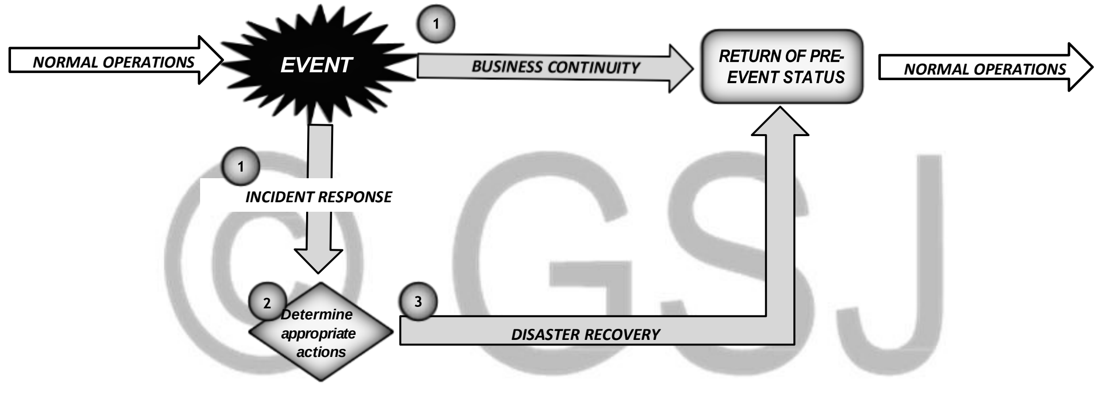
• The purpose of business continuity plans is to guarantee that vital business operations and procedures continue both during and after times of deterioration.

• Information system-focused disaster recovery plans are made to guarantee that the target system, infrastructure, or other elements are restored as quickly as possible after a contingency event.

• Information security professionals may detect, prevent, and recover from harmful computer events or occurrences by using incident response plans, often known as "cyber incident response plans" (NIST, 2012).

The image below serves as a straightforward yet powerful way to visualize the use of each of the three approaches under discussion and to draw attention to their distinctions.

Figure 1



Disaster Recovery is not the first response to an incident, as Figure 1 illustrates.

Using business continuity procedures and initiating an incident response are the first actions taken after an incident. Take the example of a clinical system outage:

1. The initial actions taken are to continue providing patient care in any way possible (for example, through business continuity measures) and to conduct some incident response work to evaluate the situation and collect as much data as you can.

2. A choice regarding the incident response's next course of action will only be made when the circumstance or incident has been fully comprehended.

Only once the situation or event is understood will a decision point be reached as part of the Incident Response regarding the next appropriate steps.

Among other security response actions, that decision point may at that point entail the choice to use Disaster Recovery operations.

The overall objective is to use the best incident response and disaster recovery plans to minimize the amount of time that business continuity plans need to be used.

Nonetheless, both short-term and long-term degradations must be taken into consideration while creating business continuity plans.

A BUSINESS IMPACT ANALYSIS'S SIGNIFICANCE

Doing a comprehensive Business Impact Analysis (BIA) should be the first step in creating disaster recovery and business continuity plans that work. According to NIST Special Publication 300-34, "Contingency Planning Guide for Federal Institutions," doing a BIA has three primary results:

1. The relationship between systems and the crucial business operations they influence or support

2. The effects on the company of a system availability interruption

3. Establishing (or verifying) the priorities for disaster recovery and business continuity plans (NIST, 2010).

Finding the appropriate stakeholders for each system and leading an organized discussion or discovery session are crucial initial steps in conducting a BIA. Employees from the business and information technology departments must be included.

Even the most seasoned employees always learn something new about their systems during BIA discovery sessions, which are most effective when both business and IT people are present. The following is a list of important topics to cover in these conversations:

GENERAL: A succinct explanation of the purpose of the system or application

• Which vital processes are impacted by the system? (Paidroll, billing, particular clinical workflows, etc.)

• What is the system's Maximum Tolerable Downtime (MTD)?

• How is the data handled or stored in the system classified?

• In what location is the system housed? Explain the surroundings and the interdependencies between the important systems.

CONTINGENCY STATUS

• Does this system have documented outage/downtime procedures?

• What is the frequency of system backups?

THE SYSTEM'S RECOVERY POINT OBJECTIVE (RPO) IS INFORMED BY THIS.

• How long does it take to restore the system and its data?

• How many personnel are required to restore the system?

- After the system has been restored, is there anything else the company needs to do before using the system again?

THE WORK RECOVERY TIME (WRT) OF THE SYSTEM IS INFORMED BY THIS.

Finding and analyzing the components thoroughly will provide the data needed to determine recovery priorities, create system criticality levels, and comprehend resource needs.

A straightforward formula must be remembered while assessing the RTO, WRT, and MTD metrics: the maximum tolerable downtime (MTD) must be exceeded by the time required to recover a system (RTO) plus any additional work required before system use may resume (WRT).

To guarantee that system availability is restored in a shorter period and within the MTD, senior leadership must assess compensating controls or additional resources if the BIA indicates that the MTD has been exceeded.

PLANNING FOR BUSINESS CONTINUITY

As previously stated in this article, disaster recovery and business continuity are not the same thing, and companies frequently mistakenly include both in the same plan. Maintaining business operations if premises, employees, or information systems deteriorate or become unavailable is known as business continuity.

Using downtime planning is a classic example of business continuity activities for healthcare providers. If a major office or facility is unavailable (due to fire, flood, etc.), business continuity activities for smaller business associates may involve employees working from home.

As incident response and, eventually, disaster recovery efforts are undertaken, business continuity plans are started and maintained.

The HITRUST Common Security Framework has specific instructions for creating a Business Continuity Plan (BCP). A BCP's essential components include, for instance:

- Guarantees of employee safety, information asset security, and organizational property protection

- Determining the essential company operations and procedures

Implementing preventive and detective controls for critical assets that support key business functions; identifying and prioritizing critical business processes; understanding the risk or risks the organization faces in terms of likelihood and impact over time; determining the financial, organizational, technical, and environmental resources required to address information security requirements during times of degradation; and recognizing the impact that disruptions caused by information security incidents are likely to have on the business.

- Making sure business continuity management is integrated into the organization's procedures and framework.

- Testing and upgrading the BCP at least once a year

• Determining the proper level of internal accountability for the business continuity management process (HITRUST Alliance, 2017)

After being recorded, BCPs should be shared with all relevant personnel in the company and copies should be kept in locations that are both staff-accessible and secure from outside threats. Simple examples of this include storing physical copies in a fireproof container or, more efficiently, storing electronic copies in a web-based file-sharing system that is secure and ensures high availability access for devices and authorized users.

PLANNING FOR INCIDENT RESPONSE

When reacting to an information security event, a highly particular set of documented protocols and procedures known as an incident response plan (IRP) must be followed. A consistent and thorough reaction to events is made possible by an effective IRP, which is essential for reducing service interruption and loss.

NIST SP 800-61 The following components or stages should be included in an organization's IRP, and Revision 1 offers great starting point recommendations for doing so:

1. Preparation (written plans, forms for collecting data, and controls to lessen consequences)

2. Identification and Evaluation

3. Recovery, Eradication, and Containment

4. Activity Following the Incident (Lessons Learned)

Responding to malicious incidents or assaults that impact data and information systems is the main topic of NIST 800-61. All possible risks to the availability, confidentiality, and integrity of data and information systems must be considered when creating an information security incident response plan (IRP). These risks must encompass malicious, unintentional, and environmental occurrences. NIST (2012).

The Federal Emergency Management Agency (FEMA) recommends an "all hazards approach" to emergency event planning in its Comprehensive Preparedness Guide for Developing and Maintaining Emergency Operations Plans. To use this publication as a straight quote:

Many of the impacts of crises are the same, even if their causes might vary widely. Rather than creating separate plans for each kind of danger, planners might handle common operational duties in their fundamental plans.

The Federal Emergency Management Agency recommends using an "all hazards approach" while making plans for handling emergency events in its Comprehensive Preparedness Guide (FEMA, 2010). It is highly recommended to use this method while creating strategies for information security IRPs. An IRP that takes into consideration both undiscovered and developing hazards in addition to the vast array of recognized threats is the aim.

These are regarded as "zero-day threats" in the context of information security. Loss of persons, facilities, or systems, as well as breaches to the confidentiality and integrity of systems and data, are the same consequences regardless of the assault or cause of deterioration.

PLANNING FOR DISASTER RECOVERY

The process by which an organization defines and records the specific procedures needed to recover from a disaster is known as disaster recovery planning. The Disaster Recovery Plan (DRP) and the Information System Contingency Plan (ISCP) are the two main plans used to restore IT systems, whilst the Business Continuity Plan (BCP) is used to recover business operations.

PLAN FOR DISASTER RECOVERY

When activities at a healthcare organization's primary site are adversely affected by a large disruptive event (such as a fire, hurricane, or flood), the DRP is intended to coordinate the recovery of IT systems at a backup location. The DRP offers an enterprise perspective on recovery sequencing for critical IT services that takes into account the healthcare organization's business requirements, system interdependencies, and conflicting stakeholder agendas.

It creates thorough protocols to swiftly and efficiently restore vital IT services after a catastrophe or protracted catastrophic outage.

CONTINGENCY PLAN FOR INFORMATION SYSTEMS

An ISCP is a strategy that focuses on an application or system and includes defined, comprehensive methods for evaluating and recovering the application or system at the primary site or a backup site.

An event that poses a risk of surpassing the application or system's RTO/RPO. An ISCP can be implemented apart from other plans or in conjunction with a DRP, COOP, and/or BCP as part of a broader recovery effort. There is only one DRP per site, although a healthcare company may have several ISCPs to restore different systems or applications. If there are several recovery locations, a DRP with site-specific recovery guidelines

TABLE 1 PROVIDES A COMPARISON OF THE DRP AND ISCP.

TABLE 1: COMPARISON BETWEEN DRP AND ISCP

DRP	ISCP
Orchestrates the recovery of data center operations in a different location	Orchestrates the recovery of a single information system
Focused on an individual site	Usually focused on an individual application
Executed to move site processing capabilities from a primary site to a recovery location	Executed to restore functionality to an application or system at the primary site (e.g. incident) or at another site (e.g. disaster)
Contains site-level procedures to accomplish a transition to another site	Contains detailed (e.g. keystroke level) recovery procedures for the individual application
Can activate one or more ISCPs for recovery of individual systems	May be activated independently from other plans (e.g. incident) or as part of a larger recovery effort (e.g. disaster)

PLANNING FOR BACKUP AND RECOVERY

The availability of medical records and other personal data has a direct influence on the capacity to provide patient care. One must wonder if there is a strategy to retrieve the data if an EHR or other crucial system crashes or is affected by ransomware.

Every healthcare company should have a data backup and recovery plan in place, as mandated by the HIPAA Security Rule. Although the HIPAA Security Rule mandates that ePHI be protected, it makes no mention of certain technologies. It does necessitate that backup data be shielded from dangers, the elements, and unwanted access.

The first step in creating a data backup strategy is making sure that an accurate inventory of the systems and locations where data is kept is in place.

Questions like: Is the data on the cloud or local (such as on servers, laptops, storage area networks, or SANs) must be considered? Are the network and system infrastructure settings and data recorded? To facilitate the recovery of systems and data at the alternative recovery location, all types of data must be routinely backed up and checked.

The frequency of backups and data recovery methods are determined by the RTO/RPO of IT systems. For instance, a real-time backup solution is necessary if an EHR requires a 15-minute RTO/RPO since a tape backup would not satisfy the system's recovery requirements. When determining the optimal way to backup an organization's systems, the RTO/RPO will be helpful.

Data must be backed up more often than less important data and cloud-based solutions are gaining popularity as a disaster recovery and business continuity solution. When adopting a cloud-based EHR, it's critical to comprehend the recovery plans of the cloud provider to make sure that patient information may still be accessed if the cloud provider's infrastructure fails or degrades.

Numerous cloud providers have options that allow for instant failover if one server fails, with both the primary and secondary servers in operational condition. In the case of a primary server failure, this design offers instant recovery; but, in the event of a compromised server, both servers will probably be compromised, necessitating the usage of backup data.

Regular data backups are necessary to provide the ability to restore data in the case of a cyberattack, in addition to protecting the company in the event of an outage or other unfavorable physical occurrence. Plans for both system-level and data-level backups should be included in regular IT system backups (such as those for the financial and EHR systems).

Data and system-level backups will be carried out at various times. For instance, the operating system (OS), any installed patches, and any applications that are installed on top of the OS are often included in system backups. Before and after an OS update, or more regularly if hardware, operating systems, and apps change less frequently, the system-level backup should be performed.

Data backups (e.g., PII, ePHI) may need a frequent backup solution (e.g., real-time, 15-to-30-minute intervals) depending on the system's RTO/RPO, whereas less essential data may need less frequent backups.

(For instance, hourly, daily, or monthly) As part of a BIA, it is crucial to determine the criticality of all systems and data since the frequency of backups has a cost. This categorization makes it possible to choose the backup plan that is most economical and compatible with the system's RTO/RPO criteria.

BACKUP TYPES

A health organization can back up its data in a few different methods. A popular backup method for important data is known as the "3-2-1" rule.

According to this guideline, you must have a minimum of three copies of your data (two copies plus the original data) in two distinct media (such as disk or tape) with at least

Off-site, one of them. (e.g. cloud, off-site tape storage) If one backup dataset is damaged or includes mistakes when retrieving data from a different location, restoration can still be done using the remaining backup copy.

The three most popular backup formats for local data backups (such as tape, NAS, or SANs) are differential, incremental, and complete backups. A full backup, which is typically carried out once a week, is a comprehensive backup of the system.

Only data changes since the last full or partial backup are backed up in an incremental backup. For an incremental backup, for instance, a full backup would be performed on Sunday, but only the changes made since Sunday would be backed up on Monday. The trend persists on Tuesday, with just the changes from Monday being backed up.

One of the less expensive backup techniques is incremental backups, which also reduces the amount of time needed to do daily backups. The drawback of incremental backups is that since each day needs to be restored sequentially, data recovery might take longer. Additionally, a complete system restoration might not be feasible if any of the days are missing or contain mistakes.

Since differential backups only include backing up data changes since the last complete backup, they are like incremental backups. Using the same scenario once more, we still do a complete backup on Sunday evening.

Like the incremental backup, we only backup the changes that have occurred since Sunday on Monday night. We are backing up Monday and Tuesday's changes because when we perform our backup on Tuesday, we are backing up anything that has changed from the Sunday complete backup.

The benefit of differential backups is that an organization just must save the differential with all the modifications and the whole backup. Because of this, restoring a differential backup is faster than restoring an incremental backup.

Performing backups of operating systems and running applications is essential in addition to backing up an organization's data. Backups are often performed at the host level rather than on each virtual machine when virtual machines are operating in a data center.

Although HIPAA mandates that ePHI backups be kept offsite, it is generally a good idea to keep all backup data elsewhere. It is best to save backup data somewhere that is not close to the organization's main location or geographic region. The likelihood that a natural disaster, such as a storm or flood, may impact both the primary and backup locations can be significantly decreased.

Although HIPAA considers encryption to be "addressable," it is nevertheless recommended practice to make sure ePHI is encrypted while data is in transit and at rest.

PLANS FOR INFORMATION SYSTEM RECOVERY

The sorts of information that may be found in a DRP and ISCP, as well as how they are used in a well-documented recovery plan, are covered in more detail in the sections that follow. This will be useful when thinking about the kinds of information required for creating these papers, but it is not a comprehensive description of every component of the DRP or ISCP.

Additional information and templates are available in NIST SP 800-34; some examples of the kinds of information included in an ISCP are listed below, NIST (2010).

ISCP IS THE CONCEPT OF OPERATIONS.

An ISCP is an application-specific plan that may be activated separately from the DRP, as was previously stated.

For example, if a data center has many virtual machines running different applications, one may create an ISCP for each application running on the virtual server and then include the recovery of the virtual machines in a common infrastructure ISCP.

Although a recovery plan may include any number of ISCPs, often only one DRP will offer the overall prioritizing of the ISCPs' recovery sequence. Activation and notification, recovery, and reconstitution are the three stages of ISCP recovery implementation (NIST, 2010).

ACTIVATION AND NOTIFICATION:

The ISCP should contain contact details as well as the roles and duties of each individual in charge of the system's recovery. This covers both in-house personnel and outside recovery assistance, including system suppliers.

ISCP RECOVERY

The IT system and system architecture should be fully described in the ISCP. A thorough component inventory, a list of all system dependencies and linkages, and any related plans should all be included. The ISCP offers a sequential and prioritized list of steps necessary for system recovery.

Keystroke-level recovery instructions should be given as part of an appendix to the plan because the ISCP is system-specific.

Primary personnel may or may not be available to restore the system, depending on the recovery event. As a result, thorough instructions, validation, and functional system testing significantly enhance an organization's capacity to restore systems as rapidly as feasible.

Plans for recovering the hardware, hypervisor, and virtual machine settings, together with any data and applications, should be included in the ISCP for servers that operate virtual machines.

Organizations may have an ISCP to recover the virtual machine environment, and the business organization may oversee restoring the data and applications, depending on who oversees the environment.

It's also critical to remember that every virtual machine may have a unique RTO or RPO, thus, to achieve their recovery goals, recovery operations need to be prioritized.

The recovery plan should include how to recover the hardware, operating system, business application, and data if the IT system is not working on a virtual machine. To guarantee that recovery documentation reflects the most recent changes, it is essential to relate it to asset and configuration management procedures.

The ISCP should provide instructions on how to restore backup data and system installation disks.

ISCP RECONSTITUTION

Following recovery, reconstitution involves actions to restore information systems to fully functional states. To confirm system capability, the recovered system is put through testing, and functioning, the recovery process is finished, and regular system operations are started again.

OPERATIONAL CONCEPT: DRP

The DRP serves as the main document that coordinates the network and IT system recovery operations. The phases that are carried out as part of the recovery should be guided by the DRP. Using checklists instead of long narratives will make it easier to keep track of the actions that have been taken.

This is particularly helpful if staff rotates during the event and the recuperation process takes days. Like the ISCP, the DRP recovery is carried out in three stages: reconstitution, recovery, and activation and notification (NIST, 2010).

DRP NOTIFICATION AND ACTIVATION

The steps necessary to activate the DRP and alert supporting recovery staff are outlined in the Activation and Notification Phase. In addition to defining what a catastrophe is, it also specifies who has the power to declare one and initiate the plan. To aid in the recovery, top management and IT personnel must be informed as soon as the plan is launched.

Key personnel's contact information and their participation in the recovery should be included in the DRP so that they may be informed. The notification procedure will be sped up with the use of automated notification-calling tree tools.

When establishing a disaster recovery plan, a typical error is thinking that existing IT professionals would be able to go to the recovery location and restore systems. In a disaster, as shown with recent storms, IT personnel may have difficulty getting from their houses to the recovery site. Preparing for this kind of scenario may involve measures to supplement workers with suppliers or other reliable sources.

A list of external stakeholders that need to be notified should be provided in the DRP. Contact and account information for other external stakeholders, such as telecom/internet providers, hardware/software suppliers, and insurance agents, must also be provided. If using an MSP or cloud provider for recovery services, they should also be informed that

Finally, a table outlining roles and responsibilities will help to ensure everyone knows what they are accountable for as part of the recovery. The table should include a leadership or decision-making role, a recovery or coordinator role, and other roles as needed to support disaster recovery operations.

RECOVERY: DRP

The recovery phase focuses on establishing recovery solutions to restore critical IT healthcare systems and data capabilities at the recovery location. The DRP should define a prioritized list of applications (for example, ISCPs) and actions that must be completed as part of the recovery process.

The BIA will have established the RTO/RPO of the IT systems, but assessing criticality must consider the many linkages between IT systems and processes. For example, data crucial to generating the whole picture required for clinical decision processes may come from several systems that feed into the EHR.

Focusing simply on crucial systems without comprehending critical linkages might jeopardize patient care.

Healthcare businesses may employ third-party services, such as cloud-based EHRs, thus it is critical to specify in the DRP which data applications run locally, and which are external to the company. Acquisitions, mergers, and strategic partnerships may also necessitate the need for external connectivity to access crucial data.

Identifying the locations of all applications and associated data will aid in determining which systems and data need to be restored at the recovery site, as well as any external links to third-party suppliers or business colleagues.

For systems housed outside of an organization's data center, it is critical that the information required to access that system from the recovery site be recorded and available to all essential personnel.

One advantage of using a cloud-based EHR or other web-based services is that you can view the data from any location with an internet connection.

Where dedicated, encrypted linkages to a third-party provider or business associate are used, it is critical to ensure access to the information needed to re-establish the connection to/from the recovery site (e.g. IP address, password, encryption keys).

RECOVERY SITES

The recovery site should, ideally, be placed outside of an organization's geographical region so that each facility/location would not be harmed by the same adverse event (e.g., hurricane, or earthquake).

RECOVERY LOCATIONS ARE COMMONLY CONFIGURED AS HOT, WARM, OR COLD.

A hot site, also known as an active/active architecture, is a replication of the existing systems in the primary data center. It normally works in parallel, with data being updated continuously at both places. If the first site fails, the backup site takes over-processing, so no data is lost, and no downtime occurs. This is also the most expensive recovery approach, as systems are replicated and operating at both the primary and secondary sites.

A warm site is a replica of the primary data center, but instead of having both sites running and updating continuously, the secondary site is up but not processing data.

Network infrastructure and servers are in place, and in the case of a disaster, data will be restored to the warm location to ensure complete functioning.

A cold site is just a facility that provides electricity and cooling. Everything needed to repair systems must be obtained and transported to the location. (servers, switches, routers, cables, access points) Recovering in a cold location is uncommon given today's reliance on fast access to electronic health data.

If a cold site is part of an organization's strategy, it is critical to plan for the recovery of common infrastructure, which must be operational before the recovery of critical systems.

A shared infrastructure contains all the hardware (servers, storage, network devices) and software (AD, WINS, virtualization) needed to run applications. System recovery cannot occur until the shared infrastructure is active.

The time when establishing a recovery strategy, consider the resources necessary to recover shared infrastructure.

Rather than restoring systems locally, it is feasible to use the services of Disaster Recovery as a Service (DRaaS) cloud provider to restore critical services. In the case of a disaster, servers, and storage may be installed in the DRaaS cloud service provider environment to restore critical IT services, eliminating the need for infrastructure maintenance at a recovery site.

When normal conditions are restored, the cloud infrastructure may be disassembled and normal activities resumed at the primary site.

RECONCILIATION – DRP

As previously stated, reconstitution occurs post-recovery and involves operations to restore information systems to a fully functioning status. In the context of the DRP, reconstitution refers to the return of the DRP's covered systems to full operational status.

PREVENTIVE CONTROLS

The goal of DRP is to reduce company downtime and get your technology back up and operating as soon as possible. BCP, on the other hand, focuses on ensuring the overall operation of the organization and encompasses a far broader range of activities, such as implementing preventative measures and managing employees and consumers.

Everyone on the team must understand that the BCP is the most significant corrective control the organization will have, and they should utilize the planning phase to develop it. The BCP involves more than simply remedial controls; it also includes preventative and detective measures. These three components are outlined here:

• Preventive controls to identify essential assets and prevent outages.

• Detective controls to immediately warn the organization of any outages or problems.

• Include corrective controls to swiftly restore normal functioning.

Traditionally, a disaster recovery system included cutover or switch-over recovery mechanisms. Such steps would enable a company to protect its technology and information by establishing a remote disaster recovery location that generates backups regularly. However, this method turned out to be expensive and time-consuming.

As a result, more economical and efficient cloud-based technologies were established.

HERE ARE SOME OF THE MOST FREQUENT DATA PROTECTION STRATEGIES:

• Regular tape backups and off-site storage.

• Backups can be made on-site and automatically transferred to an off-site drive or made straight to the off-site disk.

• Off-site data replication using storage area network (SAN) technology eliminates the requirement for data
restoration, leaving just the systems to be restored or synchronized.

• Private Cloud solutions duplicate management data (VMs, templates, and disks) to storage domains. These management data are specified in an XML format known as OVF (Open Virtualization Format) and may be recovered if a disaster happens.

• Hybrid Cloud solutions duplicate on-site and off-site data centers. These technologies allow for quick failover to local on-site hardware, but in the case of a physical disaster, servers may also be brought up in cloud data centers.

• High-availability systems duplicate data and systems off-site, allowing for ongoing access even after disasters (often through cloud storage).

In many circumstances, a company may choose to hire an outsourced disaster recovery provider to offer a stand-by site and systems rather than their distant facilities, which are increasingly being delivered through cloud computing.

In addition to planning for the need to restore systems, companies take preventative actions to avoid disasters in the first place. This may include:

• Use local mirrors for systems and data, as well as disk protection technologies like RAID.

• Surge protectors reduce the impact of power surges on sensitive electronic equipment.

• Use a backup generator or uninterruptible power supply (UPS) to keep systems operational during power outages.

- Fire protection and mitigation systems, including alarms and extinguishers.
- Anti-virus software and security measures.
- Water sensors in data center ceilings and floors.
- Plastic tarps can protect IT equipment from water damage.

PLAN TESTING, TRAINING, AND EXERCISE (TT&E).

It is insufficient to create a plan, put it on the shelf, and then forget about it until an unforeseen occurrence arises. Once a plan has been created, it must be tested to verify that it fits the RTO/RPO requirements of the systems being recovered.

Once a strategy has been prepared, the first step is to collect the plan's stakeholders and walk them through it on paper. This is known as a "tabletop" exercise, and it is the least disruptive method for testing a strategy. During a tabletop exercise, participants walk through the steps as they are written, searching for flaws in the method or stages that were overlooked.

After a tabletop exercise is completed, the next step may be to conduct a real exercise that tests all or portions of the organization's contingency preparations. However, live exercises may be costly and intrusive, thus using tabletop exercises as a first step is advised. Live exercises are critical because they reveal additional areas for plan improvement that the tabletop exercise did not identify.

Each time the rehabilitation staff goes through these activities, they get more comfortable with the process. Lessons learned, like those from the ISCP, should be put back into the strategy. As part of ISCP recovery testing, it is beneficial to incorporate staff members who are less familiar with the system to try and follow the recovery steps.

This ensures that the recovery procedures are thorough enough for someone unfamiliar with the system to efficiently follow the process. In the case of a natural catastrophe affecting an organization's local region, workers may have difficulty accessing the recovery site; dependence on individuals unfamiliar with the systems may be required to accomplish a recovery. The more thorough the strategy, the more likely the recovery will be effective.

PLAN MAINTENANCE.

All the strategies that comprise an IT Continuity response should be reevaluated at least once a year. Staff may leave or change jobs, vendors or equipment models change, and equipment configurations vary; all these factors have an influence on the capacity to recover systems if recovery documentation does not reflect these changes. Ideally, plans should be integrated into a comprehensive service management (SM) framework.

(Example: ITIL) A service management framework specifies procedures like asset, modification, and configuration management. If an SM process is built in, when a change happens, it not only updates the database tracking the change but also any documentation that is dependent on the change (e.g. DRP, ISCP).

In summary, disasters such as the increased frequency of catastrophic weather disasters and healthcare-targeted cyber activities have underlined the need to have contingency plans in place to ensure company continuity and speedy data recovery. The reliance on EHRs has resulted in low tolerance for system downtime, which may have a severe influence on quality of care and patient safety.

The implementation of strategies for incident response, business continuity, and disaster recovery are all critical components in assisting healthcare businesses in becoming more resilient to interruptions and adverse occurrences. It is no longer a matter of "if" but "when" a company will be impacted.

In addition to increasing an organization's chances of recovering from a catastrophic event, having recovery plans in place that are regularly tested and updated will demonstrate due care in your efforts to safeguard your patients and their data.

BIBLIOGRAPHY

1. Healthcare Emergency Management: A Communication Perspective"** by Michael B. McCafferty - This book discusses effective emergency management in healthcare, including disaster recovery protocols.

2. The Definitive Guide to Emergency Management and Disaster Recovery"** by Kevin C. Desouza and Michael D. Kirtman - It provides insights into best practices for disaster recovery in various sectors, including healthcare.

3. Pflanz, S. (2021). ** "A Framework for Business Continuity Management in Healthcare Organizations." *Journal of Healthcare Management*, 66(5), 321-330.

4. Vogt, L., & Haynes, A. (2020). ** "The Role of Business Continuity in Healthcare Resilience." *American Journal of Health Sciences*, 11(2), 88-94.

5. American Hospital Association (AHA)**: "Health Care System Preparedness: Developing a Comprehensive Approach to Disaster Preparedness." This report discusses strategies and frameworks for preparedness and recovery.

6. Centers for Disease Control and Prevention (CDC)**: "Public Health Preparedness Capabilities: National Standards for State and Local Planning." This resource outlines capabilities necessary for disaster readiness, including continuity planning.

7. Emergency Management Agency (FEMA)**: Offers guides on business continuity planning, specifically for healthcare organizations, including templates and resources.

8. Healthcare Information and Management Systems Society (HIMSS)**: Resources and white papers on health IT disaster recovery and business continuity planning.

9. Lessons Learned from the Hurricane Katrina Experience in Hospital Disaster Planning", published in *Disaster Medicine and Public Health Preparedness*, provides insights into effective disaster recovery strategies employed by healthcare organizations.

10. United States, National Institute of Standards and Technology (NIST), Department of Commerce. (August 2012) Special Publication 800-61 Revision 2 - Computer Security Incident Handling Guide.

11 United States, National Institute of Standards and Technology (NIST), Department of Commerce. (May 2010) Special Publication 800-34 Revision 1 – Contingency Planning Guide.

12. Authors: Jamie Watters, Book Title: Disaster Recovery, Crisis Response, and Business Continuity, Book Subtitle: A Management Desk Reference.

13. United States, Federal Emergency Management Agency (FEMA), Department of Homeland Security. (November 2010) Comprehensive Preparedness Guide (CPG) 101 Version 2 – Developing and Maintaining Emergency Operations Plans.