EC-Council

How to Create an Effective Disaster Recovery Plan in 5 Steps

EC-Council Cyber Research

S K NIAMATHULLA,
Product Manager – Content Research,
EC-Council, India

RAKESH SHARMA,
Technical Information Security Officer (TISO)
Citi, Singapore.

TABLE OF CONTENT

Creating an Effective Disaster Recovery Plan

Abstract:

When organizations get hacked: How disaster recovery and business continuity professionals save the day.

Disaster Recovery can be described as the process of mitigating and recovering from the effects of a cyberattack. A disaster recovery plan/policy not only details a D-day protocol to be followed upon the realization of the incident, but also, at the core of its process operation, helps the organization recover the affected information and assets, and the damage done to the business operation is repaired and restored. As the gravity of this process suggests, any organization (government or private) that intend to store/ work with a vast amount of liable data for any reason, should consider various critical factors while developing and maintaining their disaster recovery plan. Generally, the most important step in this process is to identify critical assets, perform business impact assessment on them based on their value to the organization, use a formalized policy and plan to protect those assets, recover data, and restore systems and business operations

Why is this so significant? Year after year, the global cybersecurity market cultivates and supports a ballooning economy. With 71.1 billion in 2014 (7.9% over 2013), 75 billion in 2015 (4.7% from 2014), 101 billion in 2018 (8.7% over 2018), 112 billion in 2019, its growth is anticipated to escalate to 281.74 billion by 2027 [1]. Thus, considering its economic impact, this paper will focus on one of the elements of cybersecurity, which converges to a disaster recovery/business continuing plan and highlights data security challenges.

Keywords: Cybersecurity; Disaster Recovery; Business Continuity Plan; Data Security; Risk Analysis; Security Policies.

1. Introduction

In today's world, cybersecurity has become an integral part or component of the IT industry. In fact, cybersecurity will continue to play a greater role in the future, as all organizations link their IT networks to the internet, EDI, etc. But, all of this might pose an information security risk for an organization. Every organization aims to secure its network environment, but most organizations have little control over their network system due to external factors that are linked to them. If those external factors are not secure, then they create a threat to the security posture of the organization. The centralized computer network is replaced or connected to the distributed networks, and multiple servers are connected on a corporate network to balance their processing power. If one of these servers fail as a result of a cyberattack, a major issue arises, which may lead to loss of a massive amount of data or sometimes completely halting business operations. A disaster recovery plan plays a significant role in preventing or minimizing data loss and business disruption resulting from cyber disaster – everything from equipment failures to advanced cyberattacks in such situations.

Many organizations are reluctant to develop a reliable and practical disaster recovery plan, without which, they have little protection from the impact of significantly disruptive events. A disaster recovery plan involves strategizing, planning, deploying appropriate technology, continuous testing, maintenance, and back-up of data and critical systems.

In this paper, where we consider a disaster to be anything that threatens the function of a business, ranging from a computer virus to a huge earthquake, a well thought out disaster recovery plan can play a vital role in business continuity, even in adverse conditions. A disaster recovery plan covers a broad range of topics and includes practically everyone in an organization, from employees to managers and CISO's, who must be on the same page when an incident occurs. Ideally, a cooperative functioning between the employee, support function, and management yield smooth business continuity during the disaster recovery operations.

Business continuity planning

BCP is a network of pre-disaster processes and protocols, complied to ensure that all areas of the organization can resume business operations as quickly as possible in the event of an emergency.

2. What is a disaster?

A Disaster could be considered as an event that creates an inability to maintain the business operation. The different types of potential disasters that an organization needs to consider while building a recovery plan are:

1. Natural disasters – fires, earthquakes, storms, floods, etc.
2. Human error
3. Hardware malfunctions
4. System virus
5. Power outages and many more

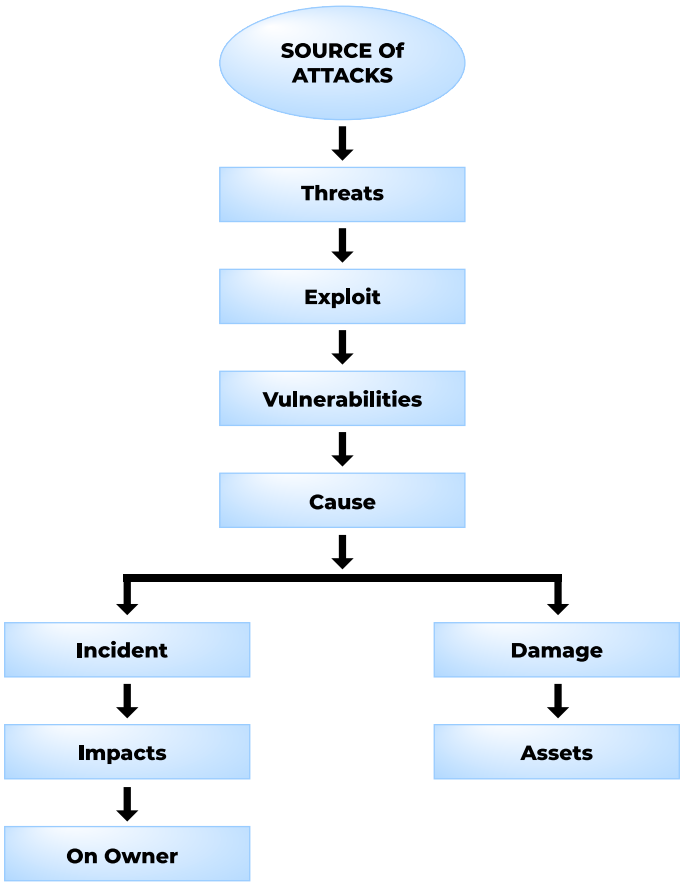


Figure – 1: Cyber incident and related concepts

As shown in Figure 1, assets are the elements of an information system that possess a value. A cyber incident, even if occurring on a single asset, may also impact the entire network. The source of any attack, such as malware, phishing, spam, DoS, etc., tend to exploit a certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined to provide a measure of the information security risk.

3. Disaster recovery

Disaster Recovery (DR) is a process of planning and compilation of procedures and protocols that helps an organization deal with critical events such as natural disaster, cyberattacks, hardware failures, etc. that affect their business activities.

In the wake of a disaster, the availability of such a document will reduce downtime of the business process due to technical failure. Documentation plays a vital role when a massive disruption takes place. It defines/shows which process should be recovered first and what should be the acceptable downtime. Thus, a documented generally consists of a Business Continuity Plan, which analyzes all the processes and prioritizes them according to their importance to business continuity.

Documentation also reduces possible risks, as it helps the network engineer/security analyst to understand what should be done in case of a cyberattack and helps the organization recover operations in an organized process.

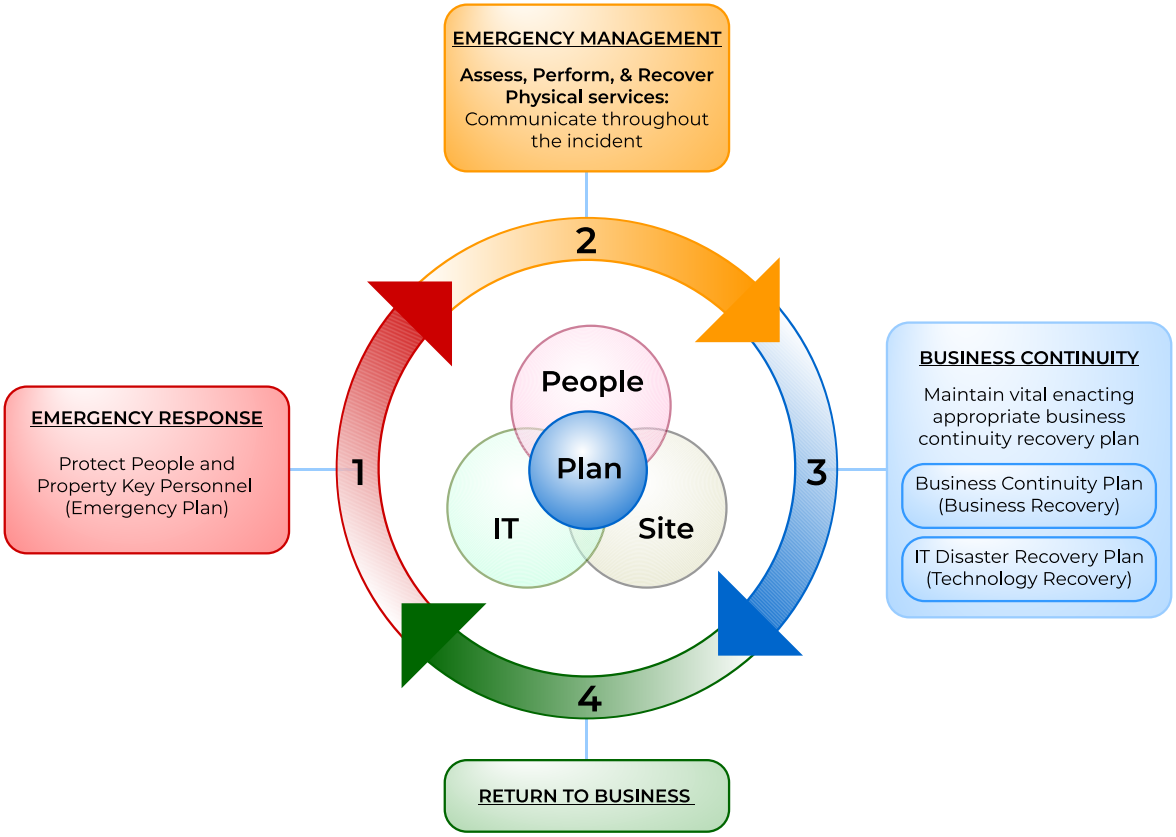


Figure – 2: Disaster Recovery Process

DR helps protect the organization from the effects of significant false events, recover data, minimize application interruption, and help the staff make informed decisions on what to do and what not to do in case of a disaster.

4. Disaster management cycle

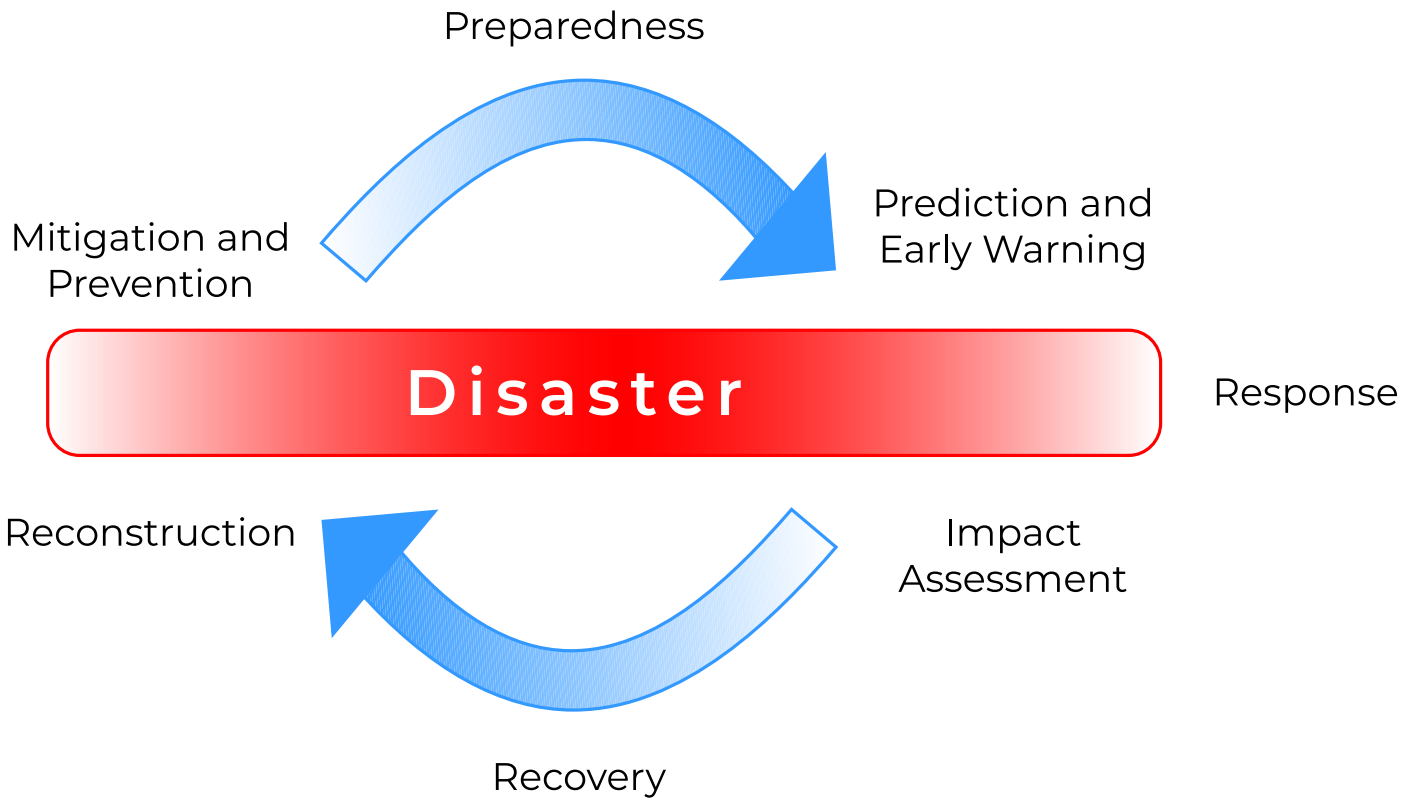


Figure – 3: Disaster Management Cycle

Three phases of disaster relief:

1. **Preparedness** – Identifying vulnerabilities and assess regional needs, build resilient and less vulnerable infrastructure, establish early warning systems and standard emergency operational procedures.
2. **Response -** Implement operational procedures such as message boards, evacuation instructions, and install temporary radio links.
3. **Rehabilitation and Recovery.**

5. Current weakness for data privacy

These days, organizations heavily rely on LAN/WAN networks in their global operations, which exposes them to several threats. These organizations can't rely on tools and technologies which have limitations.

The network security of this distributed network infrastructure needs improvement, and every organization must tackle the following four crucial areas that need improvement:

- Skilled workforce
- Effective management to control emergency situations
- Protecting the viability of the data, its integrity, and confidentiality
- Safeguarding the organization-wide network and platform availability

Many organizations have three major factors for data security issues in networks.

1. Availability
2. Management control
3. Data viability

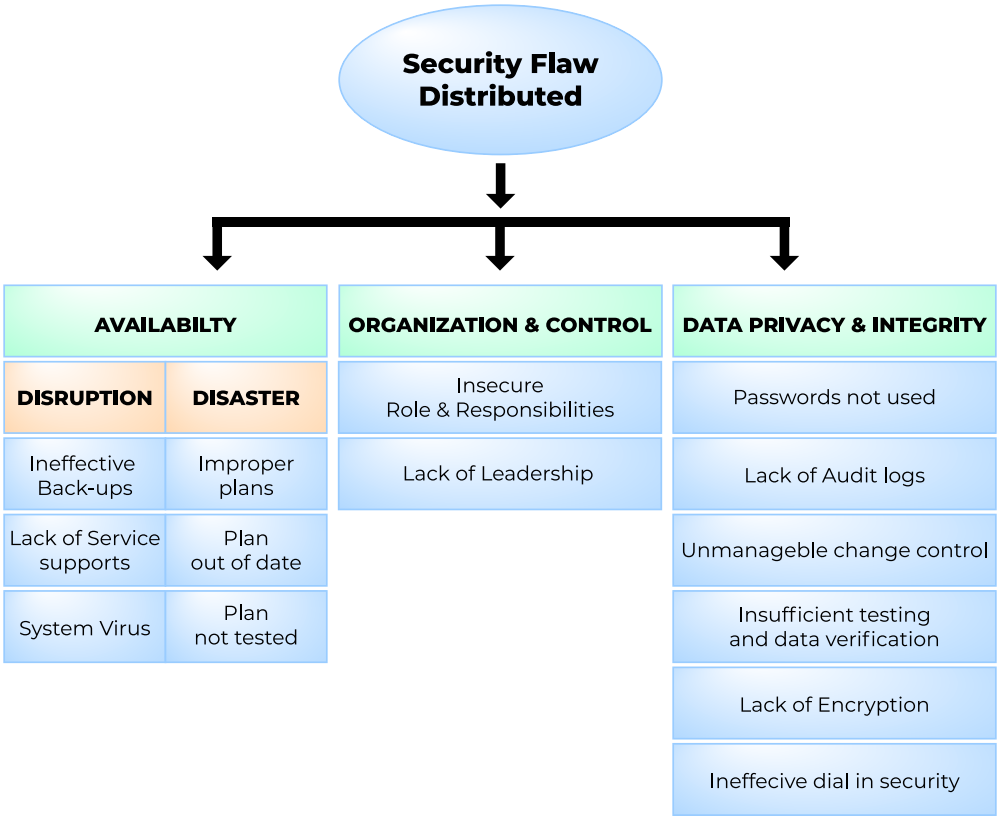


Figure -4: Security flaws in distributed networks

6. Disaster recovery plan

Disaster recovery starts with a list of all assets such as (a) computers (b) networks (c) servers and many more, and it is proposed to identify them using names or numbers uniquely

Every organization should prepare a list of all contacts, including your partners and reputed global service providers like EC-Council Global Service (EGS), to prevent sudden disasters where EGS plays a vital role in providing disaster recovery services globally. EGS offers 5 services that align with the NIST cybersecurity framework - identify, protect, detect, respond, and disaster recovery, which is further classified into 20 sub-services that help an organization prevent and recover from different cyber disasters.

Further, these organizations should also document IP addresses, usernames, and passwords of servers. With the support of EGS, every organization should follow a few basic and essential steps for disaster recovery:

1. The data center should be accessed only by authorized persons
2. Every organization's data center should be equipped with a humidity sensor, a surveillance camera, a temperature sensor, a smoke detector, and so on.

(a) Importance of disaster recovery planning

Many smaller organizations don't focus on the importance of a disaster recovery plan until it's too late.

> ***"Don't wait for a disaster to happen – implement a disaster recovery plan now."***

In the event of a disaster, first, the organization's data is lost, making their customers vulnerable. In addition to the loss of revenue, the reputation of the organization is also tarnished – then the course of action is to shut down the doors of the organizations permanently.
Prevent your organization and its critical data by initiating a disaster recovery plan that:

1. Involve many global service partners from across the business
2. Has a clear ownership
3. Is simple to execute
4. Leverages multi-layered approach
5. Is regularly practiced and continuously updated

The importance of cybersecurity in DRP

Every organization needs to prepare for cyberattacks and employ a workforce with a sound knowledge of cybersecurity.

- Train your employees in cybersecurity
- Every employee should know all possible security measures
- Maintain password policies and update them frequently

Train your employees in cybersecurity

Training your employees is not a one-time event. Every employee of an organization should be trained continuously because of rapidly evolving technology and hackers adopting new and sophisticated methods to launch cyber attacks.

(1) Train your employees on

a. How to avoid security disasters and how to respond immediately.
b. Why cybersecurity is so vital and how to keep security systems protected
c. Sharing a security tip with employees.
d. Disaster recovery certification and training courses to get more updated knowledge on the trends and technologies of the cybersecurity

Every employee should be aware of all possible security measures

All network security measures should be adequately documented, implemented, and updated to deal with the latest security threats. Every business should have the following in place:

a. Firewall
b. VPN
c. IDS/IPS
d. Secure wireless network
e. Security countermeasures against viruses, spyware, etc.

Implement strong password policies

Every organization should implement a password policy for its employees about the creation, usage, and safeguarding passwords.

(b) Why all organizations need a cybersecurity and Disaster Recovery Plan

The attackers have been one step ahead and tend to utilize advanced tools and technologies to target small businesses. WHY?

1. Cyber attackers know smaller organizations have fewer resources and are less invested in cybersecurity, making them easier targets.
2. Ransomware Attack: Sending legitimate-looking emails with malicious attachments to the victim to silently install malicious code on the system and encrypt all data with a private key and then mount an extortion attack, demanding a ransom in return for access to their data, is a ransomware attack.

"ONE CLICK CAN UNLOCK THE DOORS TO YOUR SENSITIVE DATA"

If an organization is using internal communication tools/software, the virus needs only to target a single user. From that user, it can quickly attack other users to penetrate deep within the organization's network infrastructure, which is quite similar to the COVID-19 virus, spreading like wildfire. Also, due to lockdowns imposed in countries after the Coronavirus outbreak, many organizations are at risk with employees now working from home and using their VPN network, saving sensitive data on their laptops, using WIFI, to name a few. On the other hand, cybercriminals are taking advantage of the situation and are sending phishing emails related to the COVID-19 epidemic with clickable links to infiltrate systems.

Disasters and cybercriminals don't care if organizations are ready or not. Take time to get things in motion and save time, money, and your business – in the future.

7. Ten key controls and policy implications

Every organization should implement the following 10 key controls in its security policies to prevent cyber disasters

Key Controls and Policy Implications	
Information and data security	A written policy document must be available to all organization's employees responsible for the information and data security
Awareness and training	Providing regular online information security training to the staff on the following: 1. OhPhish 2. Cybersecurity Training 3. Certification course programs Every employee must be given adequate security education and technical training to handle an emergency.
Assessment and continuous improvement	Conducting regular assessment and penetration test against your network will help an organization find and fix vulnerabilities
Allocation of security responsibilities	Security responsibilities for the protection of each software and hardware asset and for carrying out specific security processes and procedures must be explicitly defined
Security incident Handler:	A Security Incident handler must be available inhouse or through the collaboration of every organization, and all security incidents must be reported through the correct channels as quickly as possible.
Threat control	Intrusion detection and prevention measures and appropriate user awareness must be implemented
Business continuity-planning process	There must be a managed process in place for developing and maintaining business continuity plans.
Safeguarding of company records	Essential records must be safeguarded from loss, destruction, and falsification
Compliance with data protection legislation	All system applications handling personal data must comply with data protection legislation and principles.
Compliance with security policy	All systems must be regularly reviewed to ensure compliance with security policies and standards.

There are various reasons that can cause a system to crash. The lack of system security and employee intended sabotage are the primary concerns. While computer criminals stay outside company walls, they are not always the reason for a system failure.

8. Role of cybersecurity teams

A certified and skilled cybersecurity workforce always helps strengthen an organization and implement strategic plans and principles to protect its assets. The role of a cybersecurity team majorly focuses on identifying, protecting, detecting, and responding to mitigate the gaps and vulnerabilities in the organization's network. It is the responsibility of the cybersecurity team along with the disaster or emergency management team to implement the following:

a. A cybersecurity certified team (EDRP) to enable communication, collaboration, and co-operation in emergency/disaster management strategies to identify critical assets
b. Mitigate the company's vulnerabilities and threats
c. Protect the organization's data
d. Networks and systems
e. Perform weekly offsite full system back-ups
f. The awareness and training to handle DR and emergency
g. Update the organization's procedures and policies.
h. Monitor internal and external threats

The cybersecurity awareness and training help disaster recovery or emergency management teams disrupt two essential operational threats in during emergencies

1. Vulnerabilities associated with intended and unintended organization's internal threats due to lack of preparedness towards emergency responses.
2. Internal or external threats, causing damage to an organization's network, that could go unnoticed until a potential disaster forces an organization to perform restoration of operations.

Disaster recovery management and cybersecurity teams work together to train the workforce, create awareness plans, maintain resilience, and enforce operational procedures in the organization

9. Elements of cybersecurity

1. Information Security
2. Application Security
3. Network Security
4. Disaster Recovery/Business Continuity Planning
5. Operational Security
6. End-User Education

Disaster recovery management could be more appropriately described as guidelines or procedures that should be documented and implemented in the wake of a breach or cyberattack in order to restore business operations back to normal. These procedures could be classified under following different entities concerning their disposition.

1) Information security

In cybersecurity, information security is described as protecting the information through risk management, which includes reducing the probability of unauthorized access. In regards to digital information, there exist two different methods of data protection, i.e., through encryption and back-up, depending on the sensitivity of the information. Where encrypting or password protecting all the possible files will reduce the risk of integrity compromises upon breach, collecting and maintaining a back-up for all important files and data is comparatively easier and less financially taxing.

2) Application security

All the web or non-web based applications that use some or other forms of information sharing module need to be protected. According to Veracode's State of Software Security Vol. 10 reports, 83% of the 85,000 applications it tested had at least one security flaw [5]. Though the application itself can be restructured for the available back-up, the information needs risk management, and this can be achieved through disaster recovery planning that involves thorough testing of the application for any possible vulnerabilities.

3) Network security

Securing the network is one of the most laborious operations in the disaster recovery plan. It involves the inventory of all the network-related equipment and mapping the entire network structure. But, at the same time, it is the most crucial step as a network connects all the endpoints of business and flaws in network security, or its recovery could bring an entire business operation to a halt. Another mode that is applicable under disaster recovery protocol is performing a network penetration test to assess the resilience of the network defense and to identify and address all possible vulnerabilities.

4) Disaster recovery/business continuity planning

Business continuity planning revolves around the concept of keeping the business up and running during the time of disaster recovery. Hence, many disaster recovery protocols, by default, also involve business continuity modules. The most recent and affordable solution to this crisis is through cloud computing. If all the data is stored in the cloud, or the entire application platform is subjected to cloud computing, then the business operation can ceaselessly continue, even amid a cyberattack.

5) Operational security

Operational security procedures apply to cybersecurity professionals and decision-makers of an organization in order to bring into effect risk management policies that consider all the possibilities of a potential attack. Comprehensive risk management for complete business operations involves awareness and education of the employees, risk management, vulnerability assessment, penetration testing, incorporation of compliance and security guidelines, information protection, implementing changes to security protocol, authorizing access to confidential information and core applications, etc.

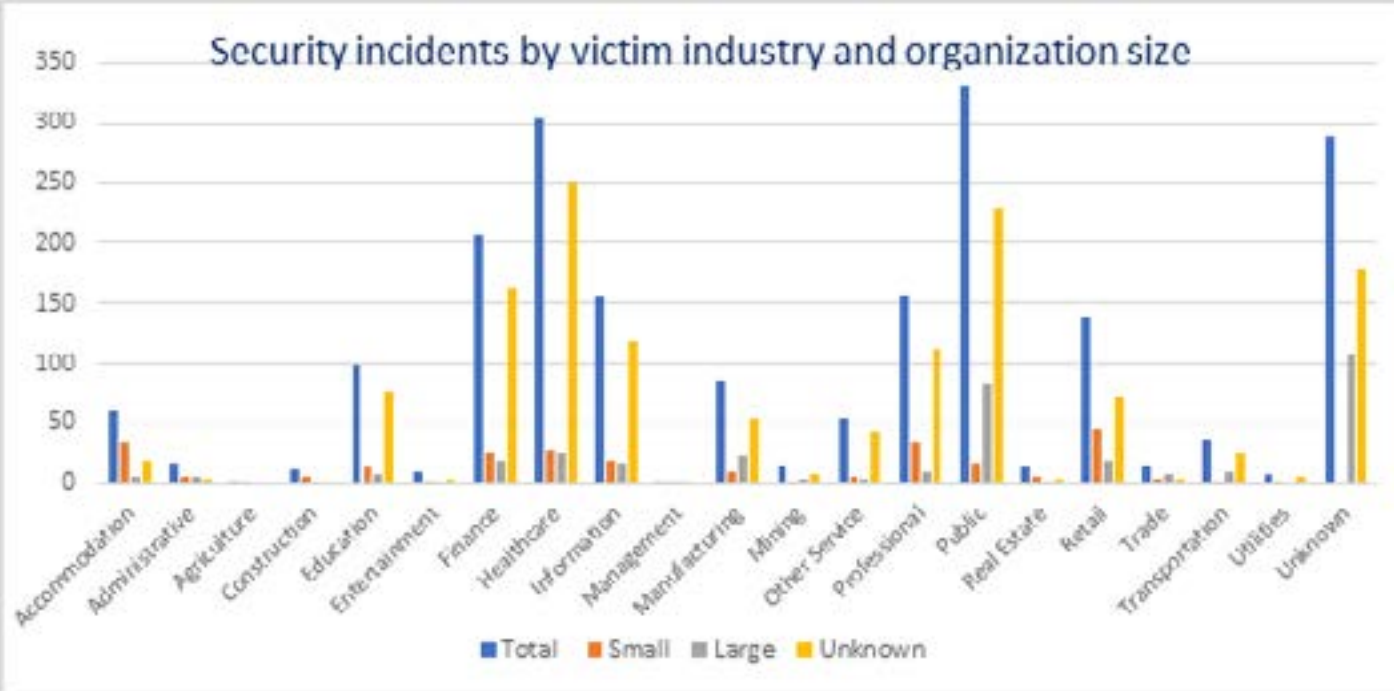
6) End-user education

The end-users, who may be a client or employees, are considered to be the first line of defense against cybersecurity threats. Hence, education and awareness among end-users pertaining to cybersecurity risks and their mitigation are considered the prominent course of action by all compliance and security guidelines. Monitoring behavior and automation of tasks to some extent could also help reduce the risk of human error.

Victim demographics and industry analysis

S.No	Industries	Total	Small	Large	Unknown
1	Accommodation	61	34	7	20
2	Administrative	17	6	6	5
3	Agriculture	2	2	0	0
4	Construction	11	7	3	1
5	Education	99	14	8	77
6	Entertainment	10	2	3	5
7	Finance	207	26	19	162
8	Healthcare	304	29	25	250

9	Information	155	20	18	117
10	Management	2	1	1	0
11	Manufacturing	87	10	22	55
12	Mining	15	2	5	8
13	Other Service	54	6	5	43
14	Professional	157	34	10	113
15	Public	330	17	83	230
16	Real Estate	14	6	3	5
17	Retail	139	46	19	74
18	Trade	16	4	8	4
19	Transportation	36	3	9	24
20	Utilities	8	2	0	6
21	Unknown	289	0	109	180



Source: Data breach report 2019

10. Disaster recovery planning steps

DRP steps will help your organization stay safe from sudden disasters and cyberattacks and will also help you establish disaster recovery and cybersecurity plan while considering the key points bulleted below:

Step 1: Establish an owner

The responsibility of protecting the organization from disasters and cybersecurity threats often falls on the IT department. Every small and big organization needs to identify a certified (EDRP) and skilled employee in the organization who can own the development of disaster recovery and cybersecurity plans. This user should be organized, comfortable collaborating with people across the organization, and be able to create, review, and maintain the plan.

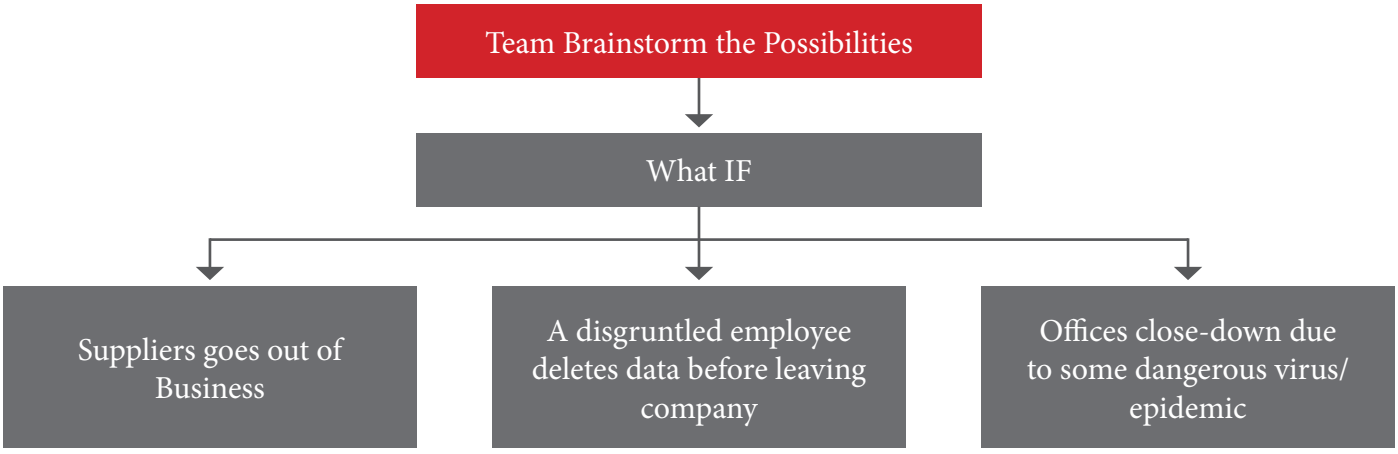
Step 2: Identify certified and skilled users from each area of the organization

Creating a plan that impacts the entire organization/business will require input from every area of the business.

a. Identify which systems and data are most critical for each team to do their work, and then document who has access to those systems and data.
b. These documents will need to be updated as employees come and go (in or out of the organization)
c. These users will also participate in a table-top exercise that will allow businesses to practice "what if" scenarios and will test plans before it is used in a real disaster situation.

Step 3: Detail your risks

Every business risk could include a multitude of events such as natural disasters, a vendor partner shutting down, a ransomware attack, and many more.



Discussing what steps organizations need to take in order to recover from each of these will help quickly identify and implement actions to mitigate risks and help prioritize tasks.

Step 4: Data, applications, and tools are the most critical

Every organization consists of different departments, and each department has data and systems that they need to function. Such as

- Accounting needs access to payroll data,
- Software teams need the code repository,
- Sales need their customer lists, etc.

All of these are important and in the event of a disaster, you can't fix everything at once. The disaster recovery expert team (EDRP) should determine the amount of time the businesses can reasonably survive without that system or data, who "owns" that system, and who will be responsible for restoring it.

Step 5: Back up of critical business information

More than 60% of all small organization's data is present on desktops and laptops. If you want to ensure all files of every department is safe, then a back-up solution is needed that includes the following features:

1. Protection for every computer
2. Cloud back up
3. Runs automatically
4. Prioritizes easy recovery

11. Data back-up in cloud computing

Cloud computing plays a vital role in every organization in protecting and storing the back-up of their data. It provides on-demand resources to users and these resources can be hardware or software. Software may include any application programming interface, application development kit, and any type of data file, etc. There are various resources to back up data and maintain its security among users, but cloud computing must be able to provide the reliability of operation of these resources such that users can upload their sensitive and essential data and use them when needed.

In its many advantages, we found that cloud technology can store huge amounts of data for various customers with sufficient security mechanisms in place.

In today's world, many organizations are uploading there private and essential data to the cloud environment and, at the same time, we found critical issues regarding this storage, i.e., if any of the cloud provider's data center gets destroyed due to any natural disaster then the back-up and recovery of systems depends on the service provider. To avoid such a scenario, the client should be able to connect to the back-up server, where private data is stored, and whenever access to the cloud environment fails, data should be easy to recover during the disaster.

The following essential cloud computing techniques are:

1. High-Security Distribution and Rake Technology (HS-DRT)
2. Parity Cloud Service Technique
3. Efficient Routing Grounded on Taxonomy (ERGOT)
4. Linux Box
5. Cold and Hot Backup Service Replacement Strategy (CBSRS)
6. Shared Back-up Router Resources (SBRR)
7. Rent Out the Rented Resources

S.No.	Techniques	Advantage	Disadvantage
1.	HSDRT	Used for handheld devices like – laptop, smart phone	Costly, Increase redundancy
2.	Parity Cloud Service	Reliable, privacy, low-cost	Implementation, Complexity is high
3.	ERGOT	Privacy, data retrieval	Time complexity, implementation complexity
4.	Linux Box	Simple, low cost for implementation	Required higher bandwidth, complete server back-up at a time, privacy
5.	CBSRS	Triggered only when failure detected	Cost increases as data gradually increases
6.	SBRR	Low cost, works even if the router fails	Inconsistencies between logical and physical configurations may lead to some performance problem
7.	Rent Out the rented resources	Cost depends on the infrastructure utilization	Implementation becomes complex

12. Training and awareness is a critical part of cybersecurity

Training and awareness of users is the most critical part of cybersecurity as employees are an integral component of each organization. Are you still not convinced? Major or minor mistakes made by untrained employees cause 25% - 40% of data breaches (according to the Ponemon Institute Report), causing reputation and revenue loss to the organization. The best way to address mistakes is with a proactive approach – provide online training and certifying your employees in disaster recovery, pen-testing, and many more with practical examples of what to do and what not to do in order to nip these mistakes or errors in the bud. Proper training includes education, testing, and imbibing a sense of accountability.

Why employees need cybersecurity training

According to a recent report, 91% of cyberattacks start with a phishing email, and many organizations notice that the gap is due to the lack of cybersecurity training for employees.

In this paper, we can suggest some learnings for the employees. OhPhish - a holistic solution for awareness and training, cybersecurity posture, and tips to improve with training. Every organization has to act now and begin grooming security habits in their employees. We suggest few certification courses:

Certified Ethical Hacker (C|EH),
EC-Council Disaster Recover Professionals (EDRP)

A comprehensive training leads to

1. Your employees knowing the right thing to do.
2. Accountability
3. A safer company

The attackers know how they can target and trick your employees, causing damage to your organization. Only certified and well-trained employees can reduce your organization's risk.

13. Performance of organizations and security controls (ISO 27001 License)

ISO 27001 certification is an information security standard that was published by the ISO Organization on the 25th of September 2013 to establish an Information Security Management System (ISMS). An ISMS is a systematic method for managing sensitive information of organizations so that it remains secure. It includes people, processes, and IT systems by applying a risk management process. An independent and qualified auditor may assess organizations to check if it meets the requirements of the ISO 27001 standard.

The latest version of the standard from ISO 27001:2013, and there are no references to the previous version of the standard from the year 2005. It contains 113 security controls, which are divided into 14 domains.

To measure the performance of the company, apply SWOT analysis as a technique to measure the actual performance with the potential performance for all security controls. ISO 27001 certification applies to every business to reduce an organization's cyber insurance premium of any size across the world. ISO 27001 plays a vital role in getting a cost-effective cyber insurance policy and improving your organization's overall information security posture. This ISO 27001 standard contains policies, processes, and controls that are designed to protect the information in all its forms, helping organizations to manage the data they collect and the threats they face. Although many organizations are put off by the cost of an ISO 27001 implementation project (depending on the size of your business), it will reduce your cyber insurance premium in the long run.

14. Open jobs for disaster recovery/business continuity

According to LinkedIn, the total number of jobs available for Business continuity domain worldwide is 20,392

According to LinkedIn, the total number of jobs available for Disaster Recovery domain worldwide is 31,096

The question that arises now is – how to select the best disaster recovery training from the available choices? There are several points to consider before enrolling in a disaster recovery and business continuity educational program. The overall objective of the program is to equip users with a skill set that helps them create and manage a disaster recovery plan. The most common assumption while creating such a program is about the audience. Only a few business continuity training programs are designed in a way that is suitable for beginners; on the other hand, only a few are designed for experts.

Primarily, the training/certification must be conducted from a well-recognized cybersecurity credentialing body, and secondly, the institution that offers the certifications should have attained globally recognized industry accreditations such as the ISO 17024. An organization must ensure that the course outline of a program they develop is aligned with their organization's educational and training requirements.

Here are a few topics, that a disaster recovery/business continuity certification should cover in detail:

1. Business Continuity Management (BCM)
2. Risk Assessment
3. Business Impact Analysis (BIA)
4. Business Continuity Planning (BCP)
5. Disaster Recovery Planning Process
6. Data Backup/Recovery Strategies
7. System Recovery
8. Business Continuity Plan (BCP) Review, Maintenance, and Training

15. Employability

As per an article posted on www.businessnewsdaily.com, where they performed an informal survey to identify the number of job postings against relevant certifications below table illustrates the statistics on job opportunities for the available certifications in Disaster Recovery and Business Continuity field.

Jobs are ready – get certified in EDRP

Certification	SimpleHired	Indeed	LinkedIn	LinkUp	Total
CBCI	73	96	37	42	248
CBCP	182	287	375	185	1029
EDRP	88	115	940	313	1456

source: www.businessnewsdaily.com

16. Assessment and continuous improvement

Third-party assessment

Third-party assessment for a nominal fee- This third-party assessment will provide a more comprehensive and independent review of the SMB's cybersecurity posture with advice on how to proceed.

Continuous improvement

The effectiveness of cybersecurity management requires continuous improvement. For each of the five core functions of the cybersecurity framework, there are many degrees/steps to which SMBs can opt for. For example

1. Network and equipment monitoring can be done manually and many organizations can purchase specialty software to assist/help.
2. 3rd Party organizations can provide assessment services, including ISO 27001, Pen-testing to validate the effectiveness of cybersecurity controls.

The choice of the degree to which many organizations should opt for depends on the level of risk they perceive, and this may vary with time.

In addition, the cybersecurity domain is continuously evolving, with advance vulnerabilities, exploits, and new threats arising all the time. Many organizations review their risk and adapt their mitigation strategies to suit this changing landscape.

17. Conclusion

Certified security professionals play a vital role in reducing the effects of cyberattacks with effective disaster recovery planning. Although disaster recovery was originally founded based on the principles of emergency management in response to natural disasters, in this paper, we highlighted the need to advance the disaster recovery planning process to include cybersecurity threats and also implement cybersecurity training and awareness programs in the DR process. The advanced threats from cybercriminals pose a serious risk to enterprises and creating awareness in the cybersecurity domain should improve the DR response to cyber intrusions. Therefore, we conclude that every organization must implement a robust cybersecurity framework, integrate their disaster recovery program with it and continue improving their strategies of disaster recovery management by investing in training and skilling of their workforce.

18. References

1. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
2. https://journals.sagepub.com/doi/full/10.1177/1550147719829960
3. https://nidm.gov.in/easindia2014/err/pdf/themes_issue/technology/disaster_comm.pdf
4. https://www.semanticscholar.org/paper/Emergency-Telecommunications-for Managing-A-Science-Serrano-Santoyo-Rojas-Mendizabal/0873ffa3c095f6cd30a9a97cd336cf642874159f
5. https://isaeurope.com/whitepaper-industrial-cybersecurity-for-small-and-medium-sized-businesses/
6. https://www.unisdr.org/files/2909_Disasterpreparednessforeffectiveresponse.pdf
7. https://www.csoonline.com/article/3315700/what-is-application-security-a-process-and-tools-for-securing-software.html
8. https://www.tutorialspoint.com/computer_security/computer_security_legal_compliance.htm
9. https://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704
10. https://www.businessnewsdaily.com/10802-business-continuity-disaster-recovery-certifications.html

EC-Council