VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

BCI 3002: Disaster Recovery and Business Continuity Management (DRBCM)

Slot: A1+TA1

Review 3

TITLE: PREVENTION OF ATTACKS USING ONE CLASS CLASSIFICATION AND AUTOENCODERS

26th November 2021

Team Leader:
Rohan Allen 18BCI0247

Team Members:
Rakshith Sachdev 18BCI0109
Harshita Pundir 18BCI0192

5. TESTING:

5.1 RISK MANAGEMENT

5.1.1 RISK MANAGEMENT LIFE CYCLE POLICIES AND PROCEDURES

The risk management process is a framework for the actions that need to be taken. There are five basic steps that are taken to manage risk; these steps are referred to as the risk management process. It begins with identifying risks, goes on to analyze risks, then the risk is prioritized, a solution is implemented, and finally, the risk is monitored. In manual systems, each step involves a lot of documentation and administration.

Step 1: Identify the Risk

The first step is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible. In a manual environment, these risks are noted down manually. If the organization has a risk management solution employed all this information is inserted directly into the system. The advantage of this approach is that these risks are now visible to every stakeholder in the organization with access to the system. Instead of this vital information being locked away in a report which has to be requested via email, anyone who wants to see which risks have been identified can access the information in the risk management system.

Step 2: Analyze the Risk

Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many business functions the risk affects. There are risks that can bring the whole business to a standstill if actualized, while there are risks that will only be minor inconveniences in the analysis. In a manual risk management environment, this analysis must be done manually. When a risk management solution is implemented one of the most important basic steps is to map risks to different documents, policies, procedures, and business processes. This means that the system will already have a mapped risk framework that will evaluate risks and let you know the far-reaching effects of each risk.

Step 3: Evaluate or Rank the Risk

Risks that need to be ranked and prioritized. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization. The business may be vulnerable to several low-level risks, but it may not require upper management intervention. On the other hand, just one of the highest-rated risks is enough to require immediate intervention.

Step 4: Treat the Risk
Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs. In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues. The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls. In a risk management solution, all the relevant stakeholders can be sent notifications from within the system. The discussion regarding the risk and its possible solution can take place from within the system. Upper management can also keep a close eye on the solutions being suggested and the progress being made within the system. Instead of everyone contacting each other to get updates, everyone can get updates directly from within the risk management solution.

Step 5: Monitor and Review the Risk
Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. These professionals must make sure that they keep a close watch on all risk factors. Under a digital environment, the risk management system monitors the entire risk framework of the organization. If any factor or risk changes, it is immediately visible to everyone. Computers are also much better at continuously monitoring risks than people. Monitoring risks also allows your business to ensure continuity.

5.2 ASSESSMENT AND EVALUATION

5.2.1 DEVELOPMENT OF RISK ASSESSMENT METHODOLOGY

5.2.1.1 CBA

To form the Cost-Benefit Analysis metric we follow the following steps:

1. Identification of the Assets and Values - In order to start our analysis, we must identify the assets of a network system and their values. Similarly to computer systems, the assets of a network system can be divided into several categories: Equipment and Hardware(computers, disks, tape drivers, printers, telecommunication, network systems, modems), Software (operating systems, utility programs, diagnostic programs, application programs.), Services (commercially provided services, such as teleprocessing, local batch processing, on-line processing, internet access, e-mail, voice mail, telephone, fax, and packet switch of data), Supplies (any consumable item designed specifically for use with equipment, software, service or support service), Personnel (salaries and benefits for persons who perform functions, such as development, support, management, operation and analysis for running this system) and other resources.

To properly assign values to assets, we need to consider their market value, depreciation, and discount value. When an asset is first purchased, it is purchased at its market or book value. After a certain amount of time, the value of the asset will decrease, thus resulting in depreciation. We then use the following formula to calculate the actual value of an asset at any given point in time:

$P= F(1/(1+I)n)$
Where P = present value, F = Future Value, I=Interest rate, and n = number of years.

2. Identification of Threats and Vulnerabilities - A threat is any action that can affect the security of assets and cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. Vulnerabilities are the weaknesses in the defense mechanisms of an information system. A threat is manifested by a threat agent using a specific technique, methodology, or spontaneous occurrence to produce an undesired effect on a network system. To clearly identify risks, we must identify the various threat agents and the methodologies that they use.

3. Risk Assessment and Prediction of the Likelihood of Occurrence - items and procedures to the likelihood of occurrence relate to the stringency of the existing controls:
i) Calculate the probability that the risk may happen, found in the observed data for the specific system.
ii) Estimate the number of occurrences in a given time period.
iii) Estimate the likelihood from a table. The analyst gives a rating based on several different risk analysis methodologies and then creates a table to hold and compare the ratings.
iv) The Delphi approach: several raters individually estimate the probable likelihood of an event, combine their estimates, and choose the best one.

4. Computation of Annual Loss Expectancy (ALE) - Because of the complication of assets and threats, it is difficult to estimate the precise value of each event. We use annual loss expectancy (ALE) to represent the cost of every event in a year. Once we determine the cost of one event, we can calculate the ALE by multiplying that cost by the number of incidents. For example, one event, with an expected cost of $20,000, may happen 2 times a year, while another event that costs $500,000 may occur once every 4 years. The ALE of the first event is $40,000, while the ALE of the second event is $125,000. We calculate the total ALE for this organization by adding the ALE's of the events together.

5. Management and Control - The purpose of management and control is to evaluate identified risks according to the degree of their acceptability/unacceptability, in consideration of the nature of the threats and vulnerabilities as they relate to risk, as well as identifying and selecting countermeasures to effectively reduce the risk. In other words, with the existing control, we calculate the expected loss. If the loss is unacceptably high, then we implement new controls. For

example, if a network intrusion's cost is too high, we evaluate and implement new network intrusion detection software and countermeasures. To effectively enforce the new controls, we need to develop and execute a plan to implement the countermeasures required to improve security and provide an acceptable degree of risk. This process includes selecting countermeasures, testing their effectiveness, and performing a cost-benefit analysis. Some suggested countermeasures are cryptographic controls, such as secure protocol and operating system protection features. Also available are identification and authentication countermeasures, such as access controls and physical controls

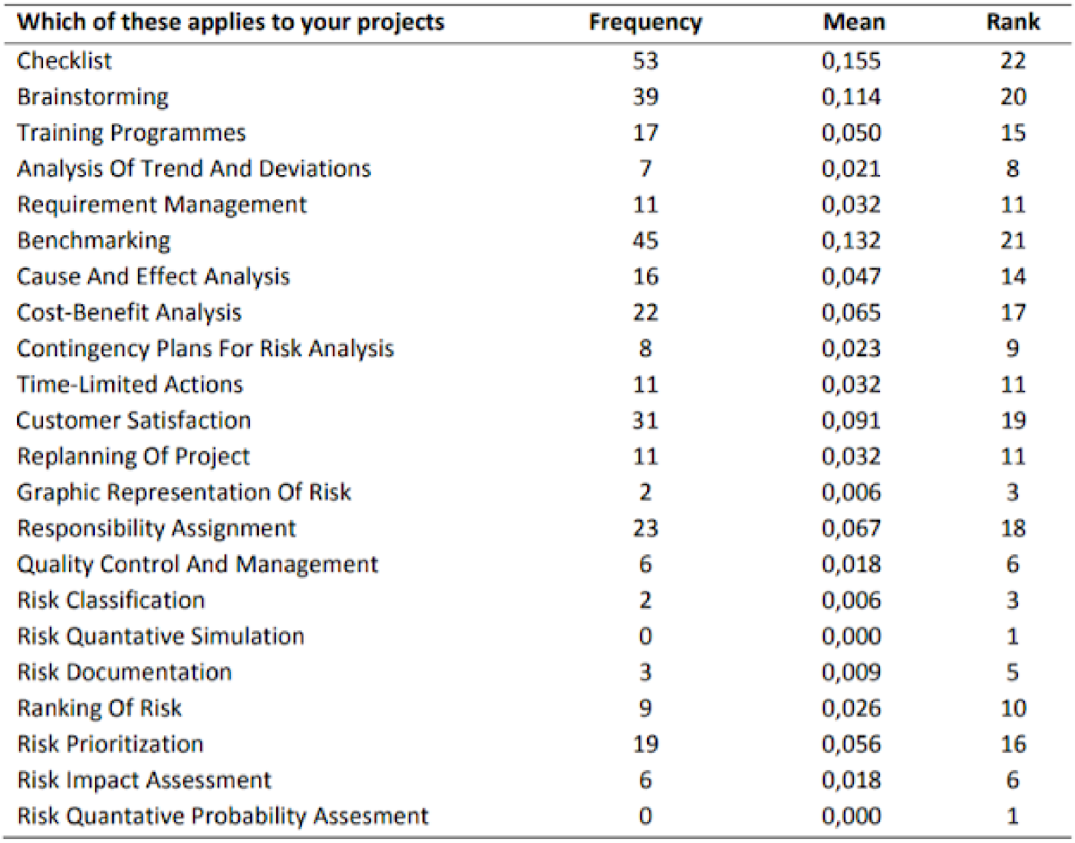
6. Cost-Benefit Analysis - The purpose of the cost-benefit analysis is to periodically review the effectiveness of planned and implemented security controls to determine if they are doing what they are supposed to do, rather than creating additional vulnerabilities. It is used to support the management and control actions. After completing steps 1 to 5, we compute the true cost or savings from the implementation of new countermeasures. We then calculate the effective cost, which is the new countermeasure cost minus any reduction in ALE from the use of the new countermeasure.

Justification of an Intrusion Detection System

ITEM	**AMOUNT**
Risk: disclosure and damage of company confidential data	
Cost to recover data: $200,000 @ 50% likelihood per year	$100,000
Effectiveness of the tool: 85%	-$85,000
Cost of tool	$40,000
ALE due to loss and control: $100,000 -$85,000 + $40,000	$55,000
Savings: $100,000 -$55,000	$45,000

5.3 TOOLS AND TECHNIQUES

Selected tools and techniques commonly applied to risk management in projects were presented to respondents to select as it applies to projects in their organisations. The data as presented in the table below shows checklist, brainstorming, and benchmarking as the most ranked. Risk simulation, risk probability assessment, graphical representation of risk, and risk classification were the listed ranked. The results here indicate that though factors of risk quantification and impact assessment were not used, by experience respondents or organizations are able to prioritize according to their perceived impact on the project using prior project experience or perception.



Which of these applies to your projects	Frequency	Mean	Rank
Checklist	53	0,155	22
Brainstorming	39	0,114	20
Training Programmes	17	0,050	15
Analysis Of Trend And Deviations	7	0,021	8
Requirement Management	11	0,032	11
Benchmarking	45	0,132	21
Cause And Effect Analysis	16	0,047	14
Cost-Benefit Analysis	22	0,065	17
Contingency Plans For Risk Analysis	8	0,023	9
Time-Limited Actions	11	0,032	11
Customer Satisfaction	31	0,091	19
Replanning Of Project	11	0,032	11
Graphic Representation Of Risk	2	0,006	3
Responsibility Assignment	23	0,067	18
Quality Control And Management	6	0,018	6
Risk Classification	2	0,006	3
Risk Quantative Simulation	0	0,000	1
Risk Documentation	3	0,009	5
Ranking Of Risk	9	0,026	10
Risk Prioritization	19	0,056	16
Risk Impact Assessment	6	0,018	6
Risk Quantative Probability Assesment	0	0,000	1

The result in the table above could be interpreted that a more qualitative analysis based on experience, perception, or expert opinion is applied by SMEs in which case prior project experience or length of work experience in the project is vital to the organization. The problem here is that in such a situation, experienced staff within the organization could undermine the contribution or opinion of the less experienced staff and ultimately impose their decision on them. As shown in the figure below, the top three most influenced decision-makers in the order of highest ranked are site managers, entrepreneurs, and project managers. Most previous research suggests entrepreneurs in general, have the most influence in decision-making among SMEs. This could perhaps be attributed to on-site decision makings by site managers in the construction sector rather than the overall decision-making of entrepreneurs or project managers on the project. The reality here also is that most of the entrepreneurs double as the project manager or site manager. This presents a conflicting issue in answering the questionnaire. Respondents are more likely to select the title as it applies to their organization. It is therefore possible respondents are talking of the same person under different role or title names.

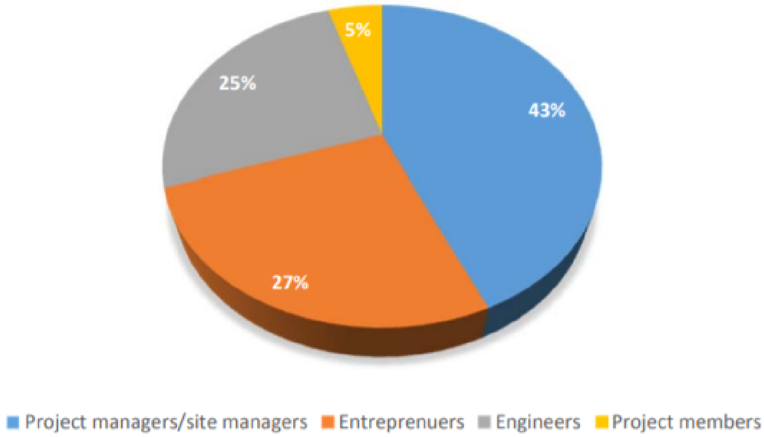
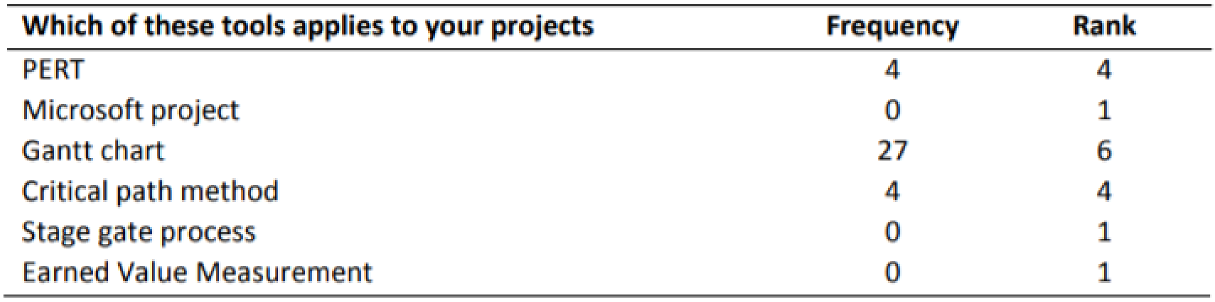


Figure: Most influenced decision-makers in Projects

Data for selected software tools for project decisions presented in the table below shows that the most commonly used software tool, as indicated by respondents, is the Gantt chart. More advanced tools such as the Microsoft project were not being applied. Advanced software is more expensive for these small organizations to usually invest in. The low level of training and skills in project management among respondents means their organizations are less likely to give priority and invest in such expensive management tools where no staff are likely to utilize in their operations for the benefit of the organization. Gantt chart as used by some organizations is simpler and required less training to use. This result shows the extent of application in project management among SMEs organizations in the construction sector. An indication that only time among the three project constraints is more likely to be tracked in projects in SMEs using modern project management tools.



Which of these tools applies to your projects	Frequency	Rank
PERT	4	4
Microsoft project	0	1
Gantt chart	27	6
Critical path method	4	4
Stage gate process	0	1
Earned Value Measurement	0	1

5.4 RISK CONTROL POLICIES AND COUNTERMEASURES

Control policies and Analysis policies

SHSU considers all electronic information transported over the university network to have the potential to be private and confidential. Network and system administrators are expected to treat the contents of electronic packets as such.

While it is not the policy of SHSU to actively monitor internet activity on the network, it is sometimes necessary to examine such activity when a problem has occurred or when optimizing traffic on the university's internet links. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by SHSU policies.

Audit logging, alarms, and alert functions of operating systems, user accounting, application software, firewalls, and other network perimeter access control systems will be enabled and reviewed annually. System integrity checks of the firewalls and other network perimeter access control systems will be performed annually. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported to the Information Security Officer.

Automated tools will provide real-time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:

- Internet traffic
- Electronic mail traffic
- Local Area Network (LAN) traffic; protocols, and device inventory
- Operating system security parameters

The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- System error logs
- Application logs
- Data backup and recovery logs
- Service desk trouble tickets and telephone call logs
- Network printer logs

The following checks will be performed at least annually by assigned individuals:

- Password strength
- Unauthorized network devices
- Unauthorized personal web servers
- Unsecured sharing of devices
- Operating system and software licenses

Any security issues discovered will be reported immediately to the Information Security Officer (ISO).

Attack methods and countermeasures

Any machine learning-based IDS attack has three basic criteria that describe the type of attack it will be, categorizing it into one of eight possible attack classes. It's worth noting that the positive is assumed to be malevolent, while the negative is assumed to be normal. The three distinct classes are listed below, each with two distinct characteristics:

Influence:
Causative attacks have an impact on learning since they have control over the training data (alter training process)
Exploratory assaults produce Denial of Service (DoS) (by exploiting existing flaws), and are frequently accompanied by false positives (rejects good input)

Security Violation:
Integrity assaults harm assets by producing false negatives (accepts malicious input)
Availability attacks result in a denial of service, which is mainly caused by false positives (rejects good input)

Specificity:
Targeted assaults are those that are focused on a specific instance (lets certain input pass)
Indiscriminate attacks include a wide range of scenarios (lets a lot of things pass)

These assaults are then divided into four categories: DoS, Probe, User to Root (U2R), and Root to Local (R2L). These assault kinds are focused on various results, with each attack's goal listed below:

A denial-of-service (DoS) attack attempts to halt traffic flow to and from the target system. The IDS receives an unusual volume of traffic that it cannot handle, and it shuts down to protect itself. This makes it impossible for typical traffic to access a network. An online business might be inundated with online orders on a major sale day, and because the network can't handle all of the requests, it would shut down, preventing paying consumers from making purchases.

A probe or surveillance attack attempts to obtain data from a network. The purpose is to impersonate a thief and steal vital information, such as client personal information or banking information.

U2R is a type of attack that starts with a regular user account and attempts to achieve super-user access to the system or network (root). The attacker attempts to get root privileges/access by exploiting system vulnerabilities.

R2L is a method of gaining local access to a remote machine. An attacker who does not have local access to the system or network attempts to "hack" their way in.

6. STORAGE DISASTER RECOVERY SERVICE TOOLS:

6.1 DATABASE DETAILS

As flash-based solid-state drive (SSD) becomes more prevalent because of the rapid fall in price and the significant increase in capacity, customers expect better data services than traditional disk-based systems. However, the order of magnitude performance provided and new characteristics of flash require a rethinking of data services. For example, backup and recovery are important to service in a database system since it protects data against unexpected hardware and software failures. To provide backup and recovery, backup/recovery tools or backup/recovery methods by operating systems can be used. However, the tools perform time-consuming jobs, and the methods may negatively affect run-time performance during normal operation even though high-performance SSDs are used. To handle these issues, we use an SSD-assisted backup/recovery scheme for database systems.

6.1.1 DATA BACKUP TECHNIQUES AND RECOVERY TOOLS

Overview of flash-based SSD

The FTL is one of the core engines in flash-based SSDs. In flash memory, any update of the data in a page must be written to a free page due to the out-of-place update nature of the flash memory. To hide this unique characteristic of flash memory from the host, the FTL maps the logical page number (LPN) from the host to the physical page number (PPN) in flash memory. The old page that has the original copy of the data becomes unreachable and obsolete. FTL erases dirty blocks which have obsolete pages and recycles these pages (garbage collection). To offer high performance and reliability, enterprise SSDs are equipped with supercapacitors that protect data on the DRAM buffer from a power outage. This guarantees that any writes sent to the DRAM buffer are successfully written to the flash memory even in the event of a power loss. Such supercapacitors also minimize the overhead caused by a flushing command for ordering and durability.

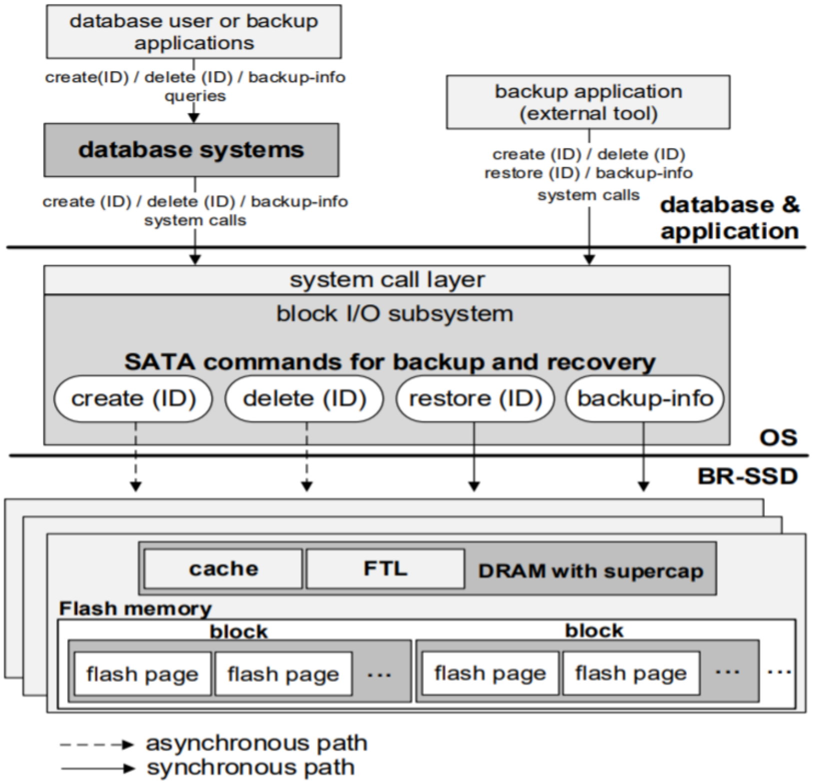

database user or backup applications
create(ID) / delete (ID) / backup-info queries
database systems
create (ID) / delete (ID) / backup-info system calls
backup application (external tool)
create (ID) / delete (ID) restore (ID) / backup-info system calls
database & application
system call layer
block I/O subsystem
SATA commands for backup and recovery
create (ID)
delete (ID)
restore (ID)
backup-info
OS
BR-SSD
cache
FTL
DRAM with supercap
Flash memory
block
block
flash page
flash page
flash page
flash page
asynchronous path
synchronous path

Figure: overall architecture

Backup and recovery operations in BR-SSD

We describe the internal procedure of BR-SSD while processing the create, delete, and restore operations. We add a reference count (refcount) to each block in SSD as the metadata for the operations. The refcount value represents the number of preserved pages in a block for backups. For example, when the page is preserved by a create operation, refcount of the corresponding block is increased by one. Meanwhile, refcount is decreased by one when the page is dereferenced by a delete operation.

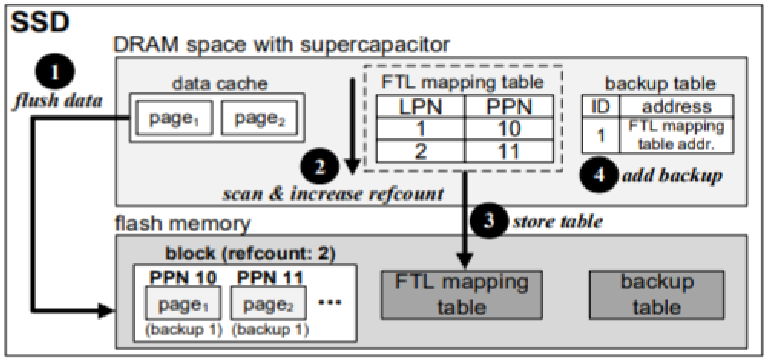


Figure: creating a backup

Create operation: We describe create operation(s) for backup(s) in BR-SSD as shown in the figure above. When a create command is issued from the host, a create operation is performed by BR-SSD in the following steps:

- BR-SSD flushes the current dirty pages from DRAM to persistent flash memory. This operation preserves the pages at a given point.
- BR-SSD scans for all entries in the FTL mapping table while increasing the refcount of blocks corresponding to the entries.
- BR-SSD flushes the FTL mapping table to flash memory in order to save the mapping information for the preserved pages.
- BR-SSD adds the address of the stored FTL mapping table to the backup table.

The figure above illustrates an example of a create operation inside BR-SSD. In this example, there are two pages, such as page 1 (LPN 1) and page 2 (LPN 2) in the data cache, and each page is mapped to PPN 10 and 11, respectively. When the host issues a create command to BR-SSD, the SSD flushes the current data (two pages mapped to PPN 10 and PPN 11) from the data cache (DRAM space) to flash memory. After flushing the data, BR-SSD traverses two entries in the FTL mapping table while increasing refcount to two so that these pages do not get garbage collected. And then, the SSD flushes the FTL mapping table to flash memory. Then, an entry that includes the address for the stored FTL mapping table is added to a backup table which is written into the flash memory asynchronously. The FTL mapping table is the space overhead from the create operation. In our storage device, the size of the FTL mapping table is about 70 MiB. A more detailed explanation of the create operation can be referenced from our previous work.

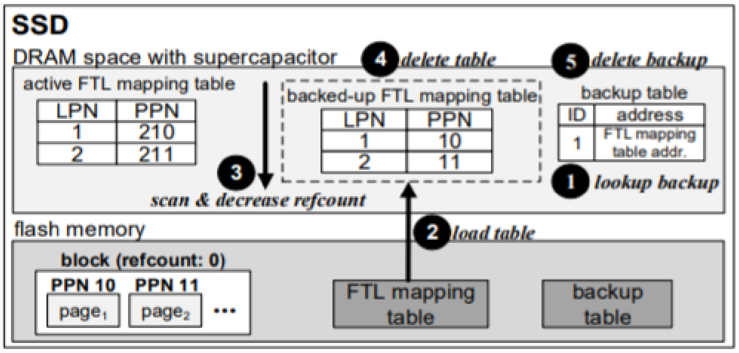


Figure: Deleting a backup

Delete operation: the figure above illustrates an example of a delete operation inside BR-SSD. When the host issues a delete command with a given backup ID to BR-SSD, the SSD searches the entry in the backup table according to the backup ID. If BR-SSD finds the entry in the backup table, the SSD obtains the address of the FTL mapping table to be deleted. Otherwise, BR-SSD returns an error message for this delete command to the host. After BR-SSD obtains the address, the SSD loads the backed-up FTL mapping table from flash memory to DRAM. Then, BR-SSD scans all entries in the backed-up FTL mapping table while decreasing refcount of the block, including the preserved pages to invalidate the pages. In this example, refcount of the block including the two pages is decreased and the pages will be garbage collected since refcount is zero; if the pages are associated with another backup, refcount is not zero. Then, BR-SSD deletes the backed-up FTL mapping table and the entry including the address of the stored FTL mapping table. During the delete operation, BR-SSD does not touch the active FTL mapping table. Consequently, this delete operation allows the backup to be deleted independently from other backups due to the full backup strategy

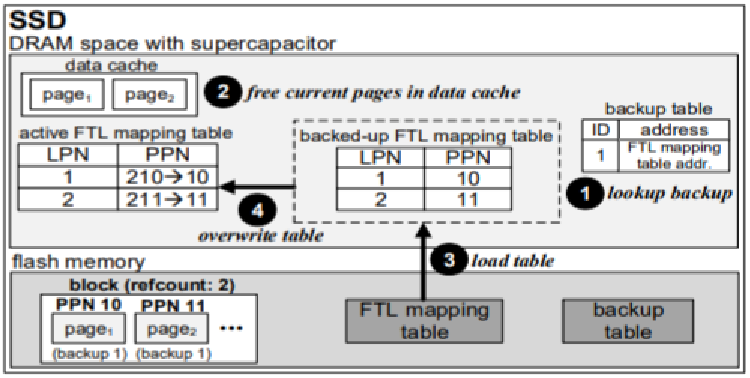


Figure: Restoring a backup

Restore operation: the figure above illustrates an example of a restore operation in BR-SSD. When the host issues a restore command with a given backup ID to BR-SSD, the SSD searches the entry in the backup table according to the backup ID. If BR-SSD finds the entry, the SSD obtains the address of the backed-up FTL mapping table in the backup table. Otherwise, the SSD returns an error message for this restore command to the host. After BR-SSD obtains the address, the SSD frees the current pages in the data cache. And then, BR-SSD loads the FTL mapping table from flash memory to DRAM. Then, BR-SSD overwrites all entries in the backed-up FTL mapping table to those in the active FTL mapping table. In this example, the active FTL mapping table contains page 1 and page 2 mapped to PPN 210 and PPN 211, respectively. During the restore operation, each PPN field of page 1 and page 2 in the active FTL mapping table is overwritten to 10 and 11, respectively. The two pages mapped to PPN 210 and PPN 211 will be garbage collected if the pages are not referenced by any backup. Consequently, this restore operation provides the full backup restoration by replacing all current entries with backed-up entries without data copies.

7. BUSINESS RECOVERY:

7.1 BUSINESS RECOVERY TEAM

For today's businesses, disaster can entail a variety of things. A natural calamity that affects power and infrastructure, or a cyberattack that cripples their network systems, are both possibilities. Whether a natural or man-made disaster strikes, it can jeopardize an organization's capacity to access and use the data and network technologies that enable it to operate. As a result, it's vital that businesses prepare for disaster by putting together a disaster recovery plan and forming a disaster recovery team.

A disaster recovery team should ideally be a cross-functional group capable of leveraging expertise from several departments and addressing a variety of system availability and business demands, as catastrophe recovery can affect all levels of an organization. While each business is different, there are several basic kinds of employees who should be involved in disaster recovery planning and execution.

Executive Management

Although senior management may not need to be involved in all parts of disaster recovery planning, they must be present at all meetings about disaster mitigation initiatives because they will be the ones to sign off on budget proposals and broader policies in the end. Although some CEOs may lack the technical competence required for comprehensive catastrophe planning, their position of power allows them to assist the team in overcoming hurdles and gaining organizational support.

IT Administration

Members of the organization's IT department will handle the majority of the more technical components of the disaster recovery plan. They have the best understanding of current network and computer infrastructure requirements and how to assure system availability in the case of a crisis. Any disaster recovery planning process should include senior IT managers who are familiar with the organization's storage and database systems, networking, and applications.

Advisors to Critical Business Units

Although IT workers are familiar with the ins and outs of the company's systems, they may not be aware of how important they are to other departments. The team can more effectively assess downtime tolerance by incorporating members from those departments in the planning phase. Some departments may be able to design workarounds that provide the recovery team more time to get systems back up and operating. As a result, the whole catastrophe recovery budget might be reduced. On the other side, the team may discover that even a few minutes of downtime for particular business units might result in unacceptable expenditures.

Management of Security and Compliance

Data availability and security may be harmed as a result of a disaster, exposing the company to significant legal consequences. Compliance requirements are frequently complicated, and the team must ensure that the methods it implements to mitigate a disaster meet those criteria. This is especially crucial if the company is bound by service level agreements (SLAs) that outline its obligations to its consumers. It's not worth taking chances when it comes to data integrity and security.

7.2 ASSESSMENT OF DAMAGE AND BUSINESS IMPACT

A business impact analysis (BIA) is the process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. The BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs), and recovery point objectives (RPOs). These recovery requirements are then used to develop strategies, solutions, and plans.

It is critically important for the survival of your business to identify processes, systems, and operations that are of eminent priority; that is the central focus of the business impact analysis (BIA). Its purpose is to determine how the interruption of your business operations may affect your organization. Potential effects include the loss of data, equipment, and revenue, loss of staff, reputational damage, and other types of business losses. Business impact analysis is an important stage in developing a disaster recovery (DR) plan, the mission of which is to ensure the operation of a company's infrastructure and applications in case of a major outage. A comprehensive disaster recovery BIA report is one of the most crucial elements required to devise an emergency response strategy. In this system, functionality like machine learning classifiers and malware detection is critical to the mission, and feature generation and feature databases are critical to the business. With this, the priority of the functions can be set to get the impact analysis.

Risk lurks in all corners of any business: from operational, financial, and strategic risk, to IT and security risk. The potential consequences of those risks include loss of revenue and possible legal action, to application outages, and inability to deliver key customer services. To address these issues, enterprises typically use a range of approaches - from the non-technical (such as business risk assessments) to the highly specialized, such as deploying vulnerability scanners and code inspectors.

However, these solutions typically produce such overwhelming volumes of risk-related data that it simply isn't possible for the business to properly review, assess and prioritize it. So, to counter this, many organizations have adopted a business impact analysis (BIA) approach to risk, aiming to identify and evaluate the potential effect of risks on critical business operations, and thereby enable organizations to prioritize and address them according to the likely impact on the business.

One of the most critical risks organizations face is a disruption to their key business applications, such as e-commerce, email, purchasing, etc, leading to loss of revenue or productivity. As such, it’s important that the network and security operations teams focus their risk mitigation efforts on ensuring that the applications, servers, and network infrastructure that support and drive key revenue-generating business processes are hardened against potential disruption or compromise. So how can IT teams approach this?

Identifying network security risk

First and foremost, organizations must identify the potential risks points within their enterprise networks. The key to this is identifying all firewalls and routers in the network, and then conducting an in-depth examination of each device including all the policies and rules that each device supports. When done manually, this is an extremely time-consuming process of mapping and documenting flows; it can be accelerated dramatically with an automated security management solution.

Once every device’s policies and rules are fully documented and traffic flows mapped, it is then possible to identify the risks that exist within the network and security infrastructure – which will generally speak fall into one of three categories.

The first of these is incorrect device configuration, which occurs when IT teams fail to ensure that each network security device is configured in accordance with vendor guidelines.

Risk is also introduced into the security fabric in instances where it fails to support the compliance and regulatory requirements of the organization, either in terms of the capabilities of the solutions deployed, or the rule sets that must be implemented.

The final risk category is where security is not configured in accordance with industry best practices, such as utilizing good network segmentation.

7.3 PLANNING RECOVERY ACTIVITIES

A network disaster recovery plan is a set of procedures designed to prepare an organization to respond to an interruption of network services during a natural or manmade catastrophe.

Voice, data, internet access, and other network services often share the same network resources. A network disaster recovery (DR) plan ensures that all resources and services that rely on the network are back up and running in the event of an interruption within certain a certain specified time frame.

Such a plan usually includes procedures for recovering an organization's local area networks (LANs), wide area networks (WANs), and wireless networks. It may cover network applications and services, servers, computers, and other devices, along with the data at issue.

Network services are critical to ensuring uninterrupted internal and external communication and data sharing within an organization. A network infrastructure can be disrupted by any number of disasters, including fire, flood, earthquake, hurricane, carrier issues, hardware or software malfunction or failure, human error, and cybersecurity incidents and attacks.

Any interruption of network services can affect an organization's ability to access, collect or use data and communicate with staff, partners, and customers. Interruptions put business continuity (BC) and data at risk and can result in huge customer service and public relations problems. A contingency plan for dealing with any sort of network interruption is vital to an organization's survival.

Some important caveats to consider when preparing a network disaster recovery plan include the following:

- Use business continuity standards. There are nearly two dozen BC/DR standards and they are a useful place to start when creating a contingency plan.
- Determine recovery objectives. Before starting on a plan, the organization must determine its recovery time objective (RTO) and recovery point objective (RPO) for each key service and data type. RTO is the time an organization has to make a function or service available following an interruption. RPO determines the acceptable age of files that an organization can recover from its backup storage to successfully resume operations after a network outage. RPO will vary for each type of data.
- Stick to the basics. A network DR plan should reflect the complexity of the network itself and should include only the information needed to respond to and recover from specific network-related incidents.
- Test and update regularly. Once complete, a network DR plan should be tested at least twice a year and more often if the network configuration changes. It should be reviewed regularly to ensure it reflects changes to the network, staff, potential threats, as well as the organization's business objectives.
- Stay flexible. No one approach to creating a network disaster recovery plan will work for every organization. Check out different types of plan templates and consider whether specialized network DR software or services might be useful.

Network disaster recovery planning provides guidelines for restoring network services and normal operations following a disaster. The plan outlines resources needed to perform network recovery procedures, such as equipment suppliers and information on data storage. It describes how off-site backups are maintained, and it identifies key staff members and departments and outlines their responsibilities in an emergency. The plan spells out responses unique to specific types of worst-case scenarios, such as a fire, flood, earthquake, and terrorist attack or cyberattack.

A network disaster recovery plan also identifies specific issues or threats related to an organization's network operations. These can include interruptions caused by loss of voice or data connectivity as a result of network provider problems or disasters caused by nature or human activities.

Like any other disaster recovery plan, this one should include information about contacting key staff members in case an emergency occurs after business hours, such as late at night or on weekends.

Some specific sections that should be included in a network disaster recovery plan include the following:

- Emergency contacts and actions. List the IT network emergency team members and their contact information at the front of the plan for fast access. A list of initial emergency response actions should also be up front.
- Purpose and scope. Outline the purpose of the plan and its scope, along with assumptions, team descriptions, and other background information.
- Instructions for activating the plan. Describe the circumstances under which the contingency plan will be activated, including outage time frames, who declares a disaster, who is contacted and all communication procedures to be used.
- Policy information. Include any relevant IT BC/DR policies, such as data backup policies.
- Emergency management procedures. Provide step-by-step procedures on how networks will be reconfigured and data accessed, what outside help might be needed and how staff will be accommodated for each different kind of potential disaster.
- Checklists and diagrams. Include checklists that prioritize hardware and software restoration and network flow diagrams that make it easy for technical support staff to quickly access the information they may need.
- Data collection. Describe the information that might be needed before officially declaring a network disruption, including network performance data and staff and first responder reports.
- Disaster declaration. Identify actions to take once the network emergency team determines it's necessary to declare a network disaster, including how the decision is communicated, who is contacted, and what additional damage assessments are needed.
- Disaster recovery. Provide instructions on restoring network operations, connectivity, devices, and related activities.
- Appendices. Provide names and contact information of IT and non-IT emergency teams, as well as information on internet service providers and other key vendors,

alternate network configuration data, forms that emergency response teams will need, and other relevant information.

The network disaster recovery plan doesn't exist in a vacuum, but rather is part of an organization's broader IT disaster recovery plan. Data backup is a key part of both the overall IT plan and the network plan, and information on an organization's backup policies and procedures should be included in DR planning.

Options for data backup range from having dual data centers in different locations, each of which can handle all of an organization's data processing needs. The data centers run in parallel and synchronize or mirror data between them. Operations can be shifted from one data center to another in an emergency. Dual data centers are not an option open to every organization. Leased colocation facilities are an alternative.

Other options include backing up data to dedicated backup disk appliances with management software that's either integrated in the appliance or run on a separate server. The backup software runs the data copying process and enforces backup policies for an organization. A backup appliance is an effective option as long as it's located where it won't be hit by the same disasters as an organization's original data.

Cloud backup and cloud-based disaster recovery are other options, either in-house or through a cloud data backup service. Cloud storage as a service provides low-cost, scalable capacity and eliminates the need to buy and maintain backup hardware. However, cloud providers fees vary depending on the types of services and accessibility required. And cloud services can require organizations to encrypt data and take other steps to secure the information they're sending to the cloud.

Cloud-to-cloud data backup is an emerging alternative. It uses software as a service (SaaS) platforms, such as Salesforce and Microsoft Office 365, to protect data. This data often exists only in the cloud. Backed up SaaS data is copied to another cloud from where it can be restored in an emergency.

7.4 COMMUNICATION SYSTEMS

You'll be dead in the water and losing clients if you don't have a way to continue consumer engagement during a calamity. Many businesses have basic disaster recovery strategies in place. Unfortunately, many of those same businesses do not include telecom in their disaster recovery plans.

Why is it necessary to use hosted VoIP?
There are a variety of advantages to using VoIP. Of course, the biggest benefit is that you will always be able to keep communication lines up, even in the event of a natural disaster. All that is necessary is access to the Internet. As a result, if your office loses Internet access for any reason, all you have to do is go to another location with an Internet connection, whether it's your home or somewhere else. This will ensure that your business continues to operate. You'll be able to easily reach your staff, ensuring their safety while also reducing operational disturbance by keeping lines of communication open.

In the event of an emergency, you'll also have a sound backup plan. You may lose data if there is a power outage or if your Internet goes down for any reason. If there is a data breach, this is also true. However, because hosted VoIP is cloud-based, recovering from such situations is much easier. Early detection tools are also provided by real-time monitoring capabilities. This ensures that your plan can be implemented before your operations are seriously harmed. With VoIP, tracking and monitoring suspicious activities is much easier. You'll be able to see a breach right away.

7.5 HUMAN RESOURCES

The most important factors to consider when creating an HR business continuity strategy
There are two major factors to consider while creating an HR business continuity plan: 2) talent and 1) furniture, fixtures, and equipment (commonly known as FF&E). Businesses are generally extremely excellent at designing plans to safeguard their FF&E; the difficult part is putting the talent component of the strategy together. And here is where human resources' input is crucial. Here are some things to think about

1. Include human resources in the development of the plan and as a member of the response team. This is also a moment when job descriptions are less crucial than having people who are capable and willing to complete the work. Being a member of any form of emergency response team necessitates flexibility and dedication. Anyone requested to take on this responsibility will need to buy-in from the organization.

2. Examine current emergency communications best practices within your organization. There's no need to start again with your plans. Some of the organization's current communication tactics for hurricanes, snowstorms, flooding, and other disasters might be applied here as well. A critical examination of what currently works and is deemed a true best practice is required.

3. Establish a central location for staff to get information. One of the things that every employee is seeking for during any type of disaster is information. HR case management software can be

used to manage employee questions and streamline the flow of information. Employees can self-serve through a knowledge portal, and HR can route-specific situations to the appropriate professionals more quickly.

4. Keep HR technology up to date. Keeping the HR department operational is critical to providing employees with timely information. HR departments, for example, were considered important corporate operations under COVID-19. Even if HR teams work from home, digital file management ensures that files are safe and available from any location, allowing HR to keep employees informed.

7.6 IT SYSTEMS SOFTWARE ARCHITECTURE RECOVERY

Based on the research gaps identified in previous techniques, we have provided an architecture for securing systems towards network-based attacks. Our proposed network intrusion detection system is an architecture that presents an autoencoder based anomaly detection model for intrusion detection, we use the NSL-KDD dataset, this dataset is a benchmark for machine learning-based intrusion detection, however, it suffers from several inefficiencies such as class imbalance, where for instance in the NSL-KDD training dataset only 0.04% of the samples belong to the u2r attack type making it severely underrepresented, the case is similar for the r2l and probe attack types whereas the majority of attack records are representing the DDOS attack type, this fact made it difficult for classifiers to detect these underrepresented types resulting in poor accuracy. Another issue is that this dataset is unrealistic, in reality, most traffic in a network is benign and only a small percentage might be malicious, while in the NSL-KDD training set, for example, attack samples compose 80% of the entire dataset which makes the models trained using this dataset ineffective in real-life situations. Our autoencoder-based approach attempts to overcome these problems.

The 37 attack types available in the dataset can be clustered into four general attack types

- Denial of service attacks
- Remote to Local attacks
- User to Root
- Probe attacks

Our model will perform binary classification of the data to two classes indicating whether the traffic is normal or an Attack, however, we will use the four attack types to analyze the results and calculate performance metrics for each general attack type.

The next section replaces the current outcome field with a Class field that has one of the following values:

- Normal

- Dos
- R2L
- U2R
- Probe

In order to avoid the imbalance of the samples representing each attack type in the training data, and to avoid the model's inability to learn about new attack types by observing existing ones, we present an approach that utilizes autoencoders and reconstruction error to detect anomalies.

In this approach we implemented a sparse autoencoder with dropout on the inputs, it consists of an input layer of 122 neurons due to the fact that the number of features for each sample is 122 followed by a dropout layer and a hidden layer of 8 neuron units so the hidden representation of the autoencoder has a compression ratio of 122/8 forcing it to learn interesting patterns and relations between the features, finally, there is an output layer of 122 units, the activation of both the hidden layer and the output layer is the relu function.

The autoencoder was trained to reconstruct its input, in other words, it learns the identity function, the model was trained using only the samples labeled "Normal" in the training dataset allowing it to capture the nature of normal behavior, this was accomplished by training the model to minimize the mean squared error between its output and its input.

The regularization constraints enforced over the autoencoder prevent it from simply copying the input to the output and overfitting the data, furthermore, the dropout presented on the inputs makes the autoencoder a special case of a denoising autoencoder, this kind of autoencoders is trained to reconstruct the input from a distorted corrupted version of itself, forcing the autoencoder to learn even more properties of the data.

The model is trained for 10 epochs using an Adam optimizer with a batch size of 100, furthermore, we held out 10% of the normal training samples to validate the model.

The model performs anomaly detection by calculating the reconstruction error of samples, since the model was trained using normal data samples only the reconstruction error of samples that represent attacks should be relatively high compared to the reconstruction error of normal data samples, this intuition allows us to detect attacks by setting a threshold for the reconstruction error, if a data sample has a reconstruction error higher than the preset threshold then the sample is classified as an attack, otherwise, it's classified as normal traffic.

For the choice of a threshold two values can be helpful for guiding the process, the model loss over the training data and over the validation data, we found by experiment that a choice around these values produces acceptable results, for our experiments we use the model loss over the training data as a threshold.

Due to the nature of this approach, it can only be used for 2-Class classification as it is purely for anomaly detection and not classification.