Information Security Protection and Planning for: Continuity and Security

Wael Alnahari (master@wjn.sa)
University of Bisha https://orcid.org/0000-0001-5247-3713

Case Report

Keywords: Disaster Recovery Plan, Business Continuity Plan, DRP, BCP, Sample Plan, SME, Project Management, Cybersecurity

Posted Date: February 16th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-244632/v1

Information Security Protection and Planning for: Continuity and Security

Wael Alnahari
College of Computers and Information Technologies, 24 Lab 1 , University of Bisha,
8338 Riyadh - Al Nakhil Dist.Unit No. 4 - 5693,
Bisha,
67716,
Asir,
Saudi Arabia, Tel.: +966506202244,
Fax: +966126700946
Email: master@wjn.sa
(Corresponding author)

***Abstract*—In this report, a sample of disaster recovery plan DRP and a business continuity plan BCP is made for WJN LLC. The plan includes risks from natural, environmental, technical, and other factors. The plans are ready to implement in the company.**

***Index Terms*—Disaster Recovery Plan, Business Continuity Plan, DRP, BCP, Sample Plan, SME, Project Management, Cybersecurity**

I. Introduction

This report contains five chapters. The chapters have been organized to represent the scientific steps toward initiating a Disaster Recovery Plan and Business Continuity Plan. Each chapter's content is briefly described below:

- **Chapter One :** This chapter includes the risk assessment and an introduction of the company for which the plans are to be implemented, the goals of the plans, the types of disasters which requires the plans implementation, quantitative and qualitative risk assessment, evaluation of emergency situations based on both encountered and expected disasters within the company.
- **Chapter Two:** This chapter discusses risk control and the team responsible to help the company recover.
- **Chapter Three:** This chapter discusses risk management via evaluating financial and environmental impacts both internally and externally.
- **Chapter Four:** This chapter contains emergency strategy and how to inform and build the recovery team to tackle the disaster as well as using alternative storage and sites to ensure business continuity.
- **Chapter Five:** This chapter includes the recovery strategy for central servers and systems as well as the conducted operations to recover from disasters.

II. Chapter One

A. 1-1 Introduction

WJN LLC is one of the companies specialized in information and database security, digital forensics, and provision of necessary programs and products for solutions in cyber and information security. WJN LLC depends on information technology systems and infrastructures to provide necessary services and securing records and data. Information technology is only one of various system resources which WJN LLC supports.

The risks that can face WJN LLC as a company or its data can be due to natural sources such as fire or earthquake, due to technological sources such as intentional hacks, computer or network viruses, and malicious acts from the company's staff, or due to other sources such as power loss in essential components. These risks impact WJN LLC either in the short-term or long-term and harm the company's reputation and contribute in bankrupting the company.

B. 1-2 Goals and Limits of Plan

This report is designed to show the essential points for disaster recovery plan and business continuity plan. The plans will guide to react to disastrous events which include the company and technological services interruption that aim to:

- Being able to continue providing services after having encountered interruption.
- Ensuring that all the staff understand their duties in implementing the plan.
- Ensuring the financial feasibility of implementing the plan.
- Ensuring that all operations are within the acceptable safety precautions.
- Providing necessary information to ensuring the continuity of workflow before, during, and after the risks.
- Identifying the requirements necessary to implement the risk management plan.
- Identifying the solutions and strategies necessary during the risk.
- Identifying and categorizing the expected risks.

C. 1-3 Assumptions

The disaster recovery plan and the reaction strategy depend on the following assumptions:

- Availability of the disaster recovery plan.

• Annual inspection during regular conditions at least once.
• Storage of the disaster recovery plan and record of staff members in a secure site outside the company.
• Updating the business continuity plan as needed based on the threats and disasters faced.

D. 1-4 Duration of Implementing the Disaster Recovery Plan

The duration which the plan is first initiated to recover from the disaster effectively and efficiently while ensuring the restoration of workflow as soon as possible and with least loss. The following figure (Fig. 1) illustrates the steps.

E. 1-5 Accident Types Requiring a Disaster Recovery Plan

There are various types of accidents that can face the company which differ in their magnitude of size, danger, impact, and side-effects. The disasters can cause various casualties such as human injuries or deaths, equipment damage or demolish, interruption of daily and essential services.

Identifying accidents requiring a disaster recovery plan:
• Natural threats: flooding and fire are the most dangerous incidents geographically.
• Environmental threats: sudden and unexpected loss of power in the company.
• Technological threats: sudden and unexpected malfunction of servers or databases.
• Thievery of company equipment by staff including office supplies, printers, phone. . . etc.
• Internal and/or external attacks on the company.
• Loss of data including intentional and unintentional loss or losses due to misuse of data.

F. 1-6 Qualitative and Quantitative Risk Evaluation

Eng. Wesam Ghazi Alnahari is responsible to evaluate and update both qualitative and quantitative risks by following an effective strategy to overcome the risks. His tasks also include listing all risks via analyzing and foreseeing possibilities of interrupting each task. Then, the risks are prioritized based on the magnitude of damage caused.

• The risk evaluation starts by quantifying the property within the company including:Estimating the financial loss and cost threats including the cost for financial, managemental, physical, and technical protection for the company.The following table 1 illustrates the risks which was evaluated by Eng. Wesam Ghazi Alnahari which shows that a fire incident will have the largest negative impact on the company since it has the largest annual financial cost. Moreover, table 1 shows that the highest possibility of occurrence is for computer malfunction then virus which means that the company should be highly prepared for the incident in the future.
• Cost and value of company property includes:
• Computers: 29,000 SAR.
• Storage media: 10,000 SAR.
• Servers: 150,000 SAR.
• Security software: 6,000 SAR.
• Potential risks and their priority based on the Annualized Rate of Occurrence as numbered:

1. Computer malfunction.
2. Viruses in data.
3. Storage media thievery.
4. Fire incident.

• The risk evaluation continues by using the qualitative risk evaluation including:Eng. Wesam Ghazi Alnahari evaluates the danger of a risk and the seriousness of a threat via estimating a level of the magnitude of impact to each threat or risk and proposing a counter-attack procedure which is then consulted by the rest of the company stakeholders.

A measurement method of five points will be made where 1 represents the least impact and 5 represents the highest impact as follows:

1. Very low: temporary interruption, there are no interruption necessary tasks or services.
2. Low: temporary interruption, there are short-term interruption in necessary tasks or services such as thievery of storage media.
3. Medium: short- or long-term interruption, there are short-term interruption in necessary tasks or services such as viruses in data.
4. High: short-, long-term, or permanent interruption in necessary tasks or services or inability in conducting most necessary tasks such as computers malfunction.
5. Very high: long-term or permanent interruption in necessary tasks or services or inability in conducting most necessary tasks such as fire incident.

G. 1-7 Followed Emergency Strategy

In this section the threats have been identified for which an emergency strategy is to be implemented within the company which includes the following aspects:
• Devices malfunction: interruption of functionality due to increased temperature or excessive dust from having the device work for long times.
• Internal security threats: unauthorized access to data centers, hack attacks, download of malicious software.
• Building threats: fire incidents or flooding due to rain.

All mentioned threats highly obstruct the company from functioning effectively. The threats cause excessive losses which can lead to bankruptcy. We aim to take all threats into account to deal with the situation and disasters as efficiently as possible in order to minimize the negative impacts and recover the company as soon as possible.

H. 1-8 Equipment Security Strategy

The following control measures were taken to prevent or reduce the negative consequences after disasters:
• Preventive control measures for computers:
Installation of appropriate fans for the power units and CPU or locating the computers in an air-conditioned environment.
• Preventive control measures for servers:
Installation of 6 extra fans to ensure heat reduction inside the servers.
• Preventive control measures for power utility:
Power generator of 11 kW working for 12 continuous hours.

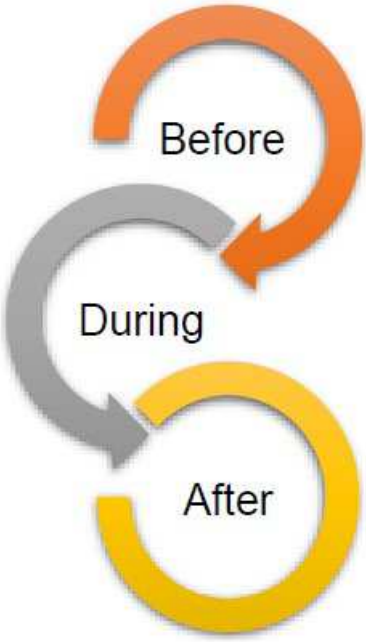

Chart 1. Steps and measures strategy.

TABLE I
THREATS AND RESOURCES.

Resource	Threat	SLE	ARO	ALE
Computers	Failure	5220 SAR	0.18	939.60 SAR
Data	Virus	720 SAR	0.12	86.40 SAR
Storage Media	Thievery	1000 SAR	0.10	100 SAR
Property	Fire	15000 SAR	0.10	1500 SAR

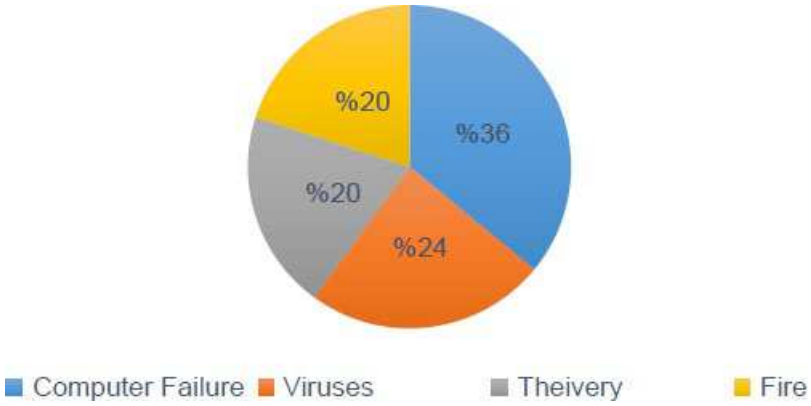

Chart 2. Threats and annualized rate of occurrence.

• Preventive control measures for fire incidents:

There are 3 fire extinguishers in the company floor and 5 fire detectors.

• Extra preventive control measures for maintenance and cleaning:

A contract has been made with a specialized company for periodic maintenance and cleaning every 3 months.

I. 1-9 Threats for Computers Interruption

There are many sources and reasons for interrupting computers functionality or operation; however, we will mention what has happened based on experience in Table 2:

J. 1-10 Company Insurance on Products and Equipment

A contract has been made with an insurance company for WJN LLC property which is categorized into:

TABLE II
COMPUTER SERVICES ISSUES.

Action	Consequences
Not inspecting the hard disk drive periodically	Workflow interruption due to full memory
Unexpected power loss	Loss of data which was not saved
Unexpected Internet service errors from the provider	Internet speed reduction or complete loss
Increase of ambient temperature	The computers might be unstable or suddenly stop functioning or even internal component permanent failure

A. Buildings: which means the building skeleton or structure and all that related which is included in the insurance policy whether it was mobile or stationary from threats such as fire, thievery, infrastructure failure such as piping, natural disasters. . . etc.

B. Equipment: which includes servers, computers, printers. . . etc.

C. Inventory: all company's products or property inside its storage.

III. CHAPTER TWO

A. 2-1 Recovery Team

The business continuity plan requires the emergency team to understand their duties and be able to apply them. In addition to the response, continuity, and recovery from disasters and catastrophes, the team was trained and certified to do the following:

Contact template with the team Table 3:

The responsibilities were assigned to the team members as follows Table 4, 5, and 6:

IV. CHAPTER THREE

A. 3-1 Disasters Strategy

In this section, the strategy is done via evaluating the risk probability on all aspects (physical – environmental – internal – external) as well as danger level, the magnitude of loss, and the effectiveness of control measures. The risks will be evaluated from 1 to 5 where 1 in the least threatening and 5 is the most threatening in tables 7 to 13.

1) *3-1-1 Physical and Security Risks:*
2) *3-1-2 Environmental Risks:*
3) *3-1-3 Internal Risks:*
4) *3-1-4 External Risks:*

B. 3-2 Summary of Evaluation

The following figures (Fig. 3, 4, 5) show the overall evaluation of risk and threats as well as its probability:

V. CHAPTER FOUR

A. 4-1 Escalation and Reporting to Staff

Wael Ghazi Alnahari is responsible to escalate and report the emergency situation directly to all team members of the recovery team according to the following situations:

Situation 1: if the emergency occurred during regular hours of operation, the team will be personally informed.

Situation 2: if the emergency occurred out of regular hours of operation, the team will be contacted via phone as follows

The following table 14 summarizes the role of each member:

B. 4-2 Contacting Resellers and Distributors

Eng. Wesam Ghazi Alnahari is responsible to identify the list of resellers and distributors and identifying communication strategy according to the disaster while phone contact is only during direct and great impacts otherwise email will suffice which is described in table 15.

C. 4-3 Use of Alternate Sites

Preparing an alternate site in Wael Ghazi Alnahri's house (in the roof) to manage disasters supplied by modern technologies to ensure the workflow.

The roof was chosen to avoid flooding and fire damage.

The site is approximately 3 km away from WJN LLC which means ease of accessibility in case of a disaster to minimize the harm. All staff will know the location before any disasters have happened.

- Essential equipment inside alternate site: in order to ensure the continuity of the business, the essential equipment should be available in the alternate site.
- Router 4G + Switch.
- Four laptops.
- Mobile with enough funds to make calls and its charger.
- 3in1 printer (printer scanner copier).
- Extension cords and 4 ethernet cables.
- One server.
- Computer backup tools, disks, and USB flash memory
- Office supplies (pens, pencils, papers. . . etc.)

Essential steps to operate alternate site:

The essential steps are performed when a disaster causes damage in the primary location requiring a different site of operation as follows:

1. Wael Ghazi Alnahari notifies the recovery team directly as explained in section 4-1 and give the order for initiation.
2. Wasem Ghazi Alnahari restores the backed-up data and extract the storage media from the secret vault.
3. The paused tasks of WJN LLC due to the disaster is resumed and is back to normal.
4. Wael Ghazi Alnahari contacts the insurance company to cover the financial damage.
5. Eng. Wesam Ghazi Alnahari contacts the distributors to ensure the availability of the products.

TABLE III
RECOVERY TEAM.

Employee name	Primary contact	E-mail
Wael Ghazi Alnahari	0506202244	master@wjn.sa
Wasem Ghazi Alnahari	0539155352	wasem@wjn.sa
Eng. Wesam Ghazi Alnahari	0537155352	wesam@wjn.sa

TABLE IV
RESPONSIBILITIES FOR TEAM MEMBER 1.

Role	Primary	Alternate
Leader of recovery team	Name: Wael Ghazi Alnahari Phone: 0506202244	Name: Wasem Ghazi Alnahari Phone: 0539155352
Responsibilities: Initiating the emergency strategy. Identifying the needs of using alternative sites and activating their use. Restoring backup data and documents and storage media.		

TABLE V
RESPONSIBILITIES FOR TEAM MEMBER 2.

Role	Primary
Board advisor	Name: Eng. Wesam Ghazi Alnahari Phone: 0537155352 Responsibilities: Contacting distributors. Evaluating risks and actual costs and losses after disasters. Reviewing and auditing the recovery plan. Data recovery after disasters and reporting damages.

TABLE VI
RESPONSIBILITIES FOR TEAM MEMBER 3.

Role	Primary
Legal counselor	Name: Wael Ghazi Alnahari Phone: 0506202244 Responsibilities: Contacting the insurance company. Initiating all contracts and agreements between WJN LLC and distributors during disasters Advocating in front of specialized authorities to make full report of the disaster and causes in lawsuit.

TABLE VII
PHYSICAL AND SECURITY RISKS.

Threat	Danger	Probability	Expected Loss
Sudden equipment failure	4	4	3
Failure due to power loss	3	2	3
Failure due to dust accumulation	2	2	1
Failure due to excessive heat	2	2	1
Failure due to excessive humidity	3	2	2
Failure due to working for too long	4	3	3

TABLE VIII
PHYSICAL AND SECURITY RISKS WITH CONTROL MEASURES.

Threat	Danger	Probability	Expected Loss	Effectiveness of Control Measures		
				Firewall	IDS	HoneyPot
Download of malicious software	3	3	4	4	4	4
Use of weak password	4	3	4	4	4	4
Use of hard disks without checking for viruses	5	4	5	4	4	4

TABLE IX
ENVIRONMENTAL RISKS.

Threat	Danger	Probability	Expected Loss
Flooding due to rain or other causes	4	3	4
Fire	3	3	3

TABLE X
INTERNAL RISKS.

Threat	Danger	Probability	Expected Loss
Thievery of equipment or storage media	5	4	4

TABLE XI
INTERNAL RISK WITH CONTROL MEASURES.

Threat	Danger	Probability	Expected Loss	Effectiveness of Control Measures		
				Firewall	IDS	HoneyPot
Server attack from within the company (intentional or unintentional)	5	3	4	4	3	3
Use of spyware by beneficiaries from within the organization	5	3	4	4	3	3
Visiting untrusted websites that allow malware to be downloaded	4	3	4	4	3	3
Unauthorized access to datacenters and disabling its components or functionality	4	3	4	4	4	4
Modify network device settings in a hard-to-track way to prolong outages	5	3	4	4	4	4

TABLE XII
EXTERNAL RISK.

Threat	Danger	Probability	Expected Loss
Cable comprise and sabotage	4	3	4
Thievery	4	3	4

TABLE XIII
EXTERNAL RISK WITH CONTROL MEASURES.

Threat	Danger	Probability	Expected Loss	Effectiveness of Control Measures		
				Firewall	IDS	HoneyPot
Attacks to modify, change or destroy data	5	3	4	4	4	4

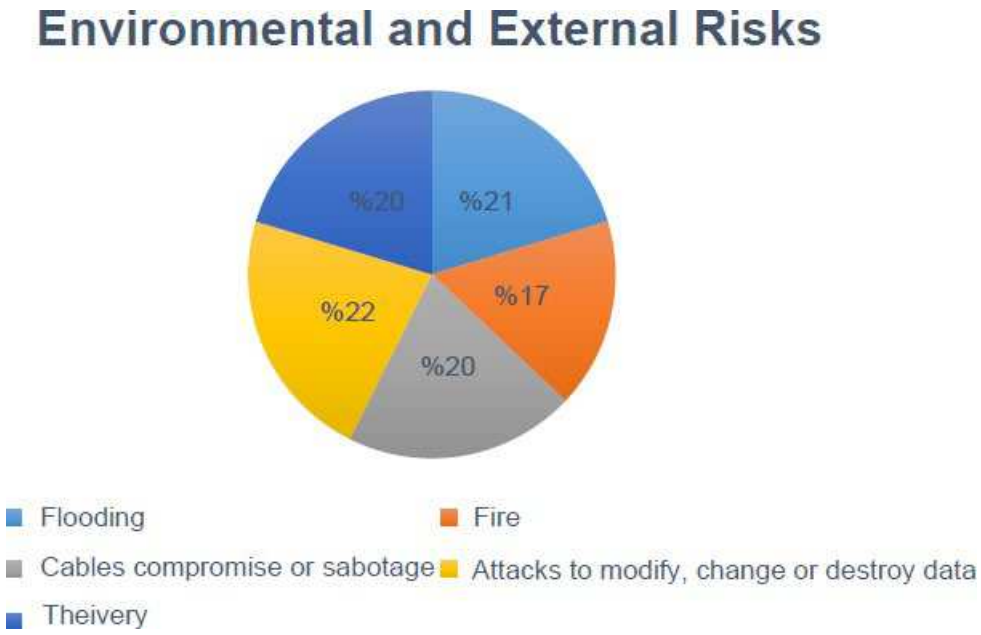

Chart 3. Environmental and external risks.

TABLE XIV
RECOVERY TEAM RESPONSIBILITIES.

Employee	Role	Responsibility
Wael Ghazi Alnahari	Head of emergency team	Notify the emergency team - activate the alternate site
Wasem Ghazi Alnahari	Deputy head of the emergency team	Restore backup - extract the required documents
Eng. Wesam Ghazi Alnahari	Board advisor of the emergency team	Assessing actual risks and costs after a disaster - communicating with distributors

TABLE XV
DISTRIBUTOR.

Distributor	Phone	E-mail
TheKernel - Mohammed Dawwas – Operations	00971508992030	dawwas@thekernel.com

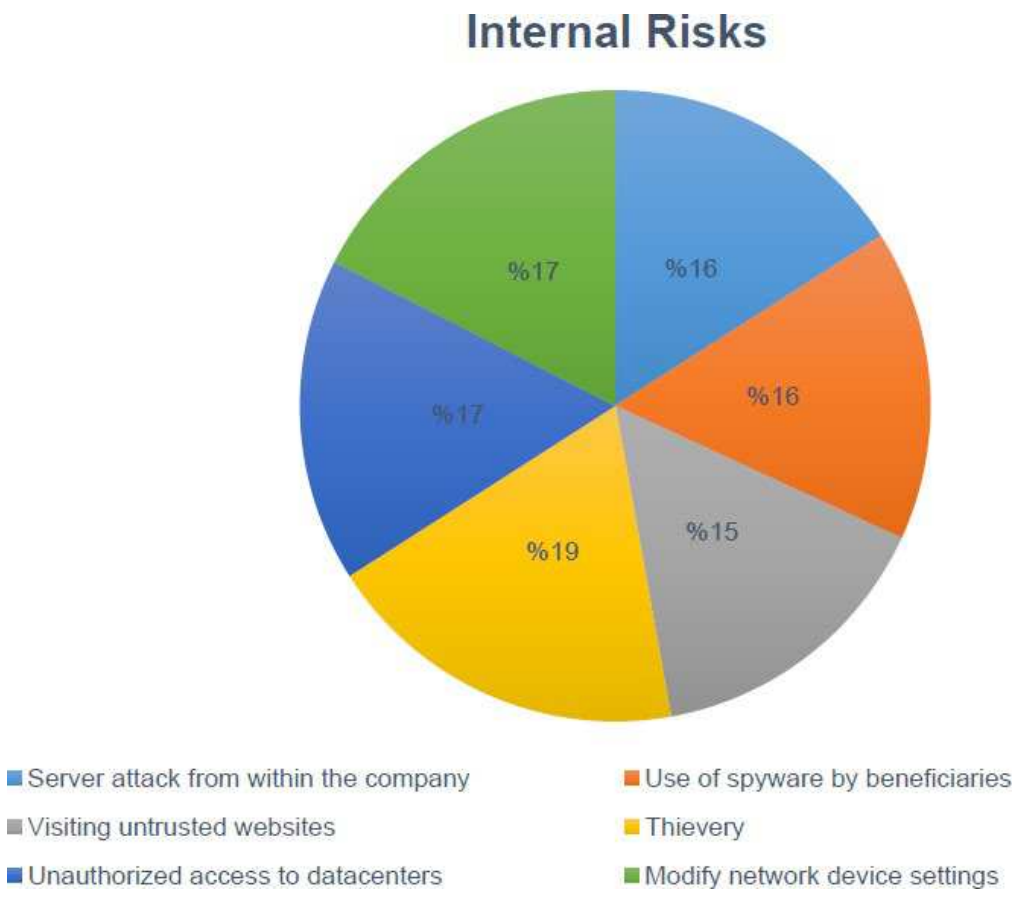

Chart 4. Internal risks.

D. 4-4 Storing Data Outside the Company

Wasem Ghazi Alnahari is authorized to store sensitive and confidential data essential to ensure the workflow in two forms:

- Form one:Storing the data in flash drives and paper forms in a password-protected vault inside the alternate site. The vault is inspected and updated weekly.
- Form two:Backup form separated in three different location as per its importance and are daily updated according to table 16.

VI. Chapter Five

A. 5-1 Procedures for Disaster Recovery

The responsibilities to recover from disasters within the company as mentioned in table 17:

Followed steps during recovery from disasters:

1. Estimation of loss according to the following table 18:
2. Qualification (activity resume stage) via compensating the loss according to table 18.
3. Evaluating the procedures taken to deal with the disaster during the facing and response phase while documenting the lessons and suggesting improvements according to the following table 19
4. Documenting the event and providing recommendations and suggestions necessary to ensure the workflow in order to benefit from the current experience and avoid the negativities in the future while improving and updating the situation according to the following table 20:

B. 5-2 Wired and Wireless Communication

Wael Ghazi Alnahri is responsible to operate the local wireless communication within WJN LLC for personal and commercial use according to the following restrictions:

1. Ensuring the method of operation and the appropriate location for installation especially with respect to increasing security.
2. The use of these communication channels is restricted by the rules of Communications and Information Technology Commission and the cybercrime law as well as related laws.

C. 5-3 Computers and Servers Data Recovery

- Media and documents storing procedures:

The following table 21 shows the backing-up procedures which requires full-version backup which duplicates the original data and can be immediately replaced between actual and alternate sites of WJN LLC.

- Control and preventive measure for servers:
- WHM v78.0.21 & cPanel
- Jailed Apache is enabled

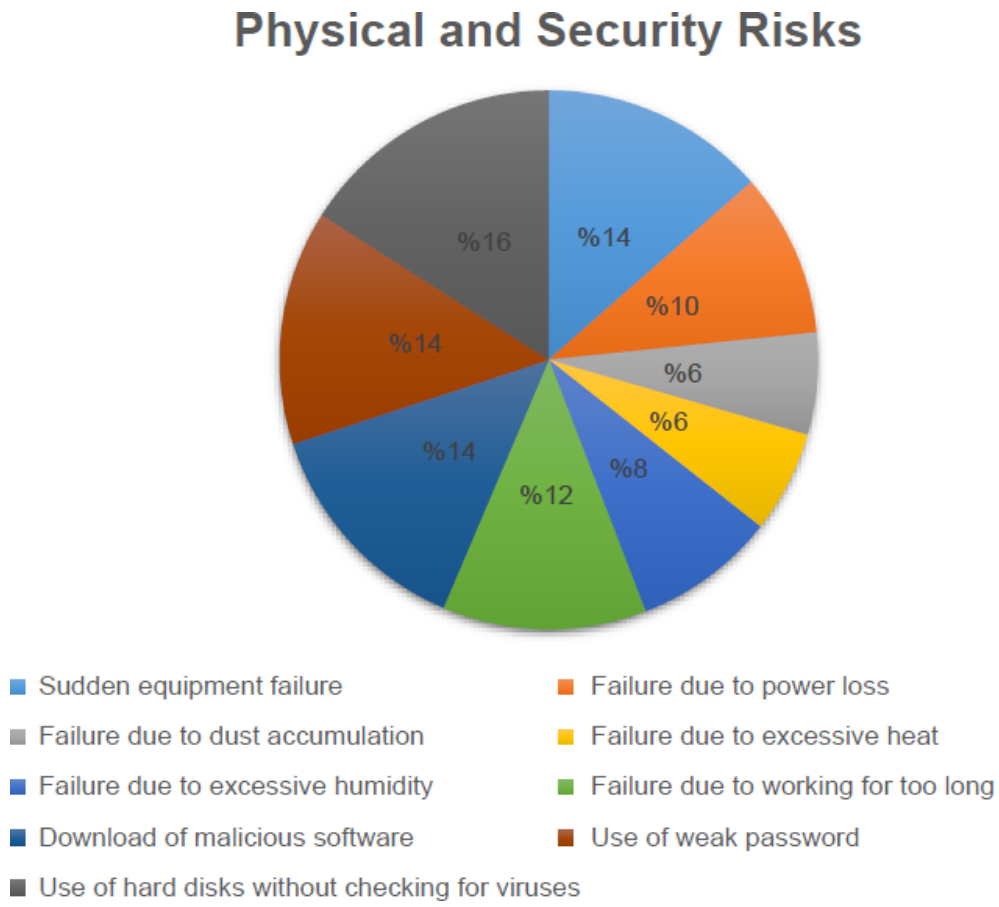

Chart 5. Physical and security risks

Chart 6. Team escalation and reporting.

TABLE XVI
BACKUP SEPARATION.

First backup copy	In the server, on the same device and is copied in an external hard disk via USB
Second backup copy	On Amazon S3 Cloud
Third backup copy	On Google Drive

TABLE XVII
RESPONSIBILITIES TO RECOVER FROM DISASTERS.

Responsibility	Employee
Estimating losses in the property and the company	Wael Ghazi Alnahari
Resume workflow	Wasem Ghazi Alnahari
Control measures evaluation and quality checks	Wael Ghazi Alnahari
Documentation of situation and making appropriate recommendations	Eng. Wesam Ghazi Alnahari

TABLE XVIII
LOSS ESTIMATION.

Loss	Quantity	Expected Loss

TABLE XIX
PROCEDURE EVALUATION.

Date	Information/Decision/Procedure	Recommendation

TABLE XX
IMPROVEMENTS TO RECENT EXPERIENCE.

Date	Event	Recommendation/Suggestion	Responsible

TABLE XXI
DATA BACKUP FOR ESSENTIAL TASKS.

Essential Task	Backup Type
Website data	Full backup
Database data	Full backup
Users data	Full backup
Users documents	Full backup
Access control data	Full backup
Accounting data	Full backup
Server data	Full backup
Router configuration data	Full backup

- Apache Symlink Protection is enabled
- .cPHulk Brute Force Protection is enabled
- .Password strength requirements are strong
- .The system did not detect processes with outdated binaries
- .SCGI is disabled, currently using the recommended suEXEC
- .is not permitted to send email ”nobody“ The pseudo-user
- .CSF has SMTP_BLOCK enabled
- pseudo- ”nobody“ Apache is being queried to determine the actual sender when mail originates from the user
- Shell Fork Bomb Protection is enabled
- SSH Password Authorization disabled
- Security Questions (asks questions to verify your identity when you log in from an unrecognized IP address. If correctly, you will be able to log in, and the unrecognized IP address will be added to the list of you answer) recognized IP addresses:Enable HSTS (Strict-Transport-Security)
- Serve HSTS headers with all HTTPS requests
- Max Age Header (max-age)
- Specify the duration HSTS headers are cached in browsers -12 months
- :Apply HSTS policy to subdomains (includeSubDomains) - • Every domain below this will inherit the same HSTS headers
- .Caution: If any of your subdomains do not support HTTPS, they will become inaccessible
- :Preload -
- Permit browsers to preload HSTS configuration automatically
- .Caution: Preload can make a website without HTTPS support completely inaccessible
- :No-Sniff Header -
- header to prevent Internet Explorer and Google Chrome from MIME- ”X-Content-Type-Options: nosniff“ Send the
- .sniffing away from the declared Content-Type
- Always Use HTTPS -
- Minimum TLS Version TLS 1.2 -
- enabled: Opportunistic Encryption -

• Opportunistic Encryption allows browsers to benefit from the improved performance of HTTP/2 by letting them
• in the address ”http“ know that your site is available over an encrypted connection. Browsers will continue to show
• .”https“ bar, not
• enabled: Onion Routing -
• s onion services ’Onion Routing allows routing traffic from legitimate users on the Tor network through Cloudflare
• .rather than exit nodes, thereby improving privacy of the users and enabling more fine-grained protection
• :RTT enabled + 0 TLS 1.3 -
• .Enable the latest version of the TLS protocol for improved security and performance
• enabled: Automatic HTTPS Rewrites -
• for all resources or links on your ”https“ to ”http“ Automatic HTTPS Rewrites helps fix mixed content by changing
• .web site that can be served with HTTPS
• unenabled: Disable Universal SSL -
• Disabling Universal SSL removes any currently active Universal SSL certificates for your zone from the edge and
• prevents any future Universal SSL certificates from being ordered. If there are no dedicated certificates or custom
• .certificates uploaded for the domain, visitors will be unable to access the domain over HTTPS
• : EV SSL – using security cerificate
• https://www.ssllabs.com/ssltest/analyze.html?d=wjn.sa&hideResults=on&latest
• Wildcard SSL *.wjn.sa subdomain -
• One month: Challenge Passage -
• Specify how long a visitor with a bad IP reputation is allowed access to your website after completing a challenge.
• .After the Challenge Passage TTL expires, the visitor in question will have to pass a new Challenge
• enabled: Privacy Pass Support -
• Privacy Pass is a browser extension developed by the Privacy Pass Team to improve the browsing experience for your
• .visitors. Enabling Privacy Pass will reduce the number of CAPTCHAs shown to your visitors
• enabled: Browser Integrity Check -
• .Evaluate HTTP headers from your visitors browser for threats. If a threat is found a block page will be delivered
• Email Address Obfuscation -
• Display obfuscated email addresses on your website to prevent harvesting by bots and spammers, without visible
• .changes to the address for human visitors
• enabled: Server-side Excludes -
• .Automatically hide specific content from disreputable visitors
• enabled: Hotlink Protection -
• Protect your images from off-site linking
• Enabling second factor authentication via security key
• Network preventive procedures:
• Specialized router to operate 4G for servers as backup operation
• Security level Medium
• Enable Attack Protection
• Medium: the other types of ICMP messages are blocked
• Dynamic IPs: hourly updates (Shell script update via API with CloudFlare)
• Email security: Spf1
• DMARC1
• DKIM
• https://mxtoolbox.com/dkim.aspx
• Domain Name: wjn.sa
• Selector: mail
• DNSsec -
• https://dnssec-analyzer.verisignlabs.com/wjn.sa
• CAA enable SSL
• "comodo.com" issue 0
• ";" issuewild 0
• Preventive measures for operating system:
• Daily updates and operating 24/7
• Red Hat Enterprise Linux Server 7.6
• .”el7.957.10.1-3.10.0“ The system kernel is up-to-date at version
• Preventive measures for databases
• Daily backup and retrieval of IOS and Image
• .MySQL test database doesn’t exist
• MySQL check for anonymous users -
• .The MySQL port is blocked by the firewall, effectively allowing only local connections
• Preventive measures for virus:
• Antivirus programs
• ClamAV Scanner
• Preventive measure for breaches:
• WAF (Web Application Firewall | Free ModSecurity Rules from Comodo)
• Firewall - csf v12.09 & ConfigServer Security
• ConfigServer ModSecurity Control - cmc v3.02

D. 5-4 Testing and Practicing the Recovery Plan

In the following table 22, the types of tests to be made on the plan for the whole recovery team is illustrated along with its periodic duration:

Eng. Wesam Ghazi Alnahari is responsible for auditing and updating the recovery plan and informing the whole team according to the following table 23:

VII. Appendix

A. Appendix A

1) Incident of malware infection: Dealing with malware infection is done according to the following steps which are organized from simple to complicated depending on the type and strength of malware:

1. Performing full computer scan on the infected computer by ClamAV Scanner or other anti-malware program.
2. Restore the device to factory defaults and keeping a copy of important data.
3. Using caution when dealing with storage device used for backup and ensuring its vacancy from malware before connecting it to the restored to defaults device.

TABLE XXII
RECOVERY PLAN TESTING.

Test Type	Duration
Testing the whole disaster recovery plan	Once every 6 months
Testing the restoration of backups	Once every 3 months

TABLE XXIII
RECOVERY PLAN REVISION.

Content to be reviewed	Duration
Officially reviewing and auditing the plan and its updates	Once every 3 months

4. Format and reinstall the operation system after having saved the extremely important data and ensured the backed-up data is clean before using it on the formatted device.

Peer-reviewed form for the malware infection incident is mentioned in table 24:

2) Fire incident: People present in the time of fire should call the authorities and try to deal with the situation with available tools such as fire extinguisher and breaking or opening windows.

1. Ensuring that the fire alarms have gone on.

2. If the fire was too big to take care of, the civil defense should be contacted immediately: 998 then inform a tree of three people.

3. In case of being the only person present, the person should do all possibility to stop fire and call 998 when the person cannot stop the fire and afterward try to contact someone in the company.

4. Everyone should evacuate the building and head to emergency exits in a calm and quick manner without the use of elevators.

5. Ensuring that the fire does not get close to accelerants as much as possible with the main objective being humans safety.

Peer-reviewed form for fire incident is mentioned in table 25:

B. Appendix B

1) External entities contact form: Use the following table 26 to update the data for contact

VIII. COMPETING INTERESTS

The authors declare no competing interests.

ACKNOWLEDGMENTS

I wish to thank my parents for their support and encouragement throughout my study. This research is supported by : WJN LLC (Sole Proprietorship) : Limited Liability Company (WJN LLC), Saudi Arabia. We are grateful to Eng. Wesam G. Alnahri for his contribution in the design of the sample of articles analyzed here, for improving the use of English in the manuscript.

TABLE XXIV
MALWARE DOCUMENTATION PEER-REVIEWED.

Malware Incident	**Location:**	**Time:**
Date:		
Name	**Signature**	

TABLE XXV
FIRE DOCUMENTATION PEER-REVIEWED.

Fire Incident	**Location:**	**Time:**
Date:		
Name	**Signature**	

TABLE XXVI
EXTERNALS CONTACT INFORMATION.

Contact	**Phone**
Insurance company	056202244
Communication company	909
Distributor	00971508992030

Figures

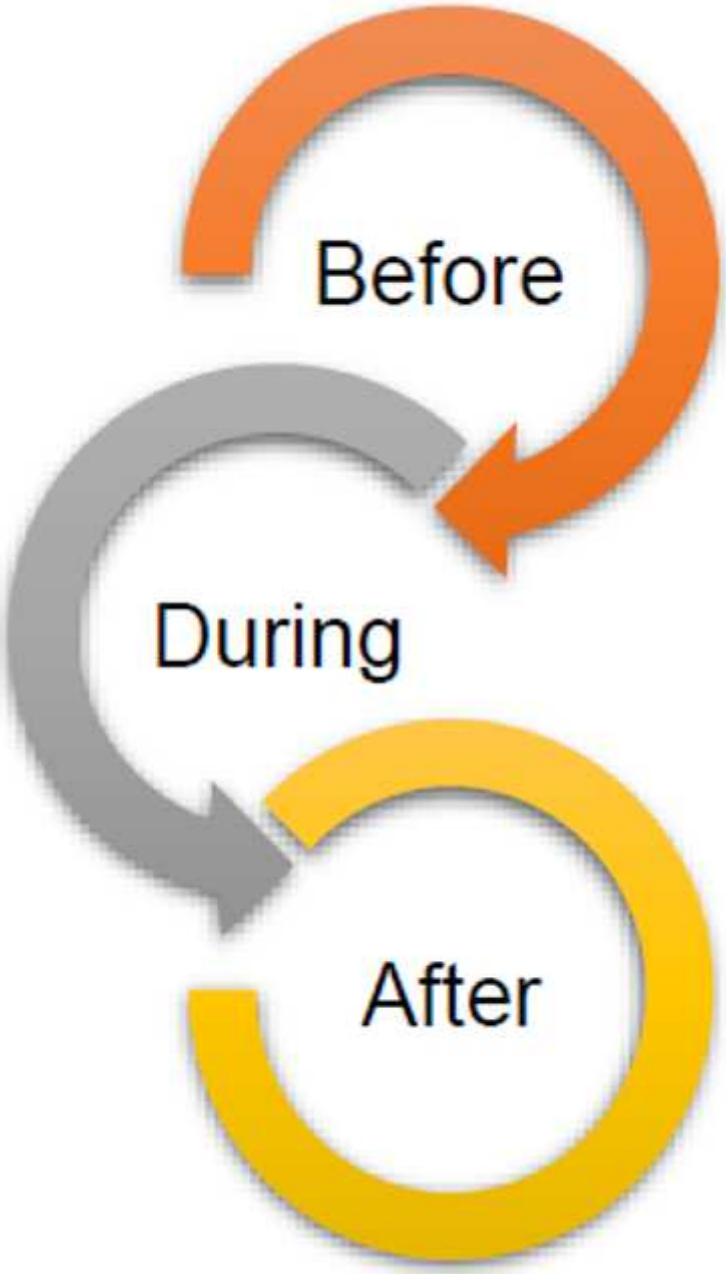

Figure 1

Steps and measures strategy.

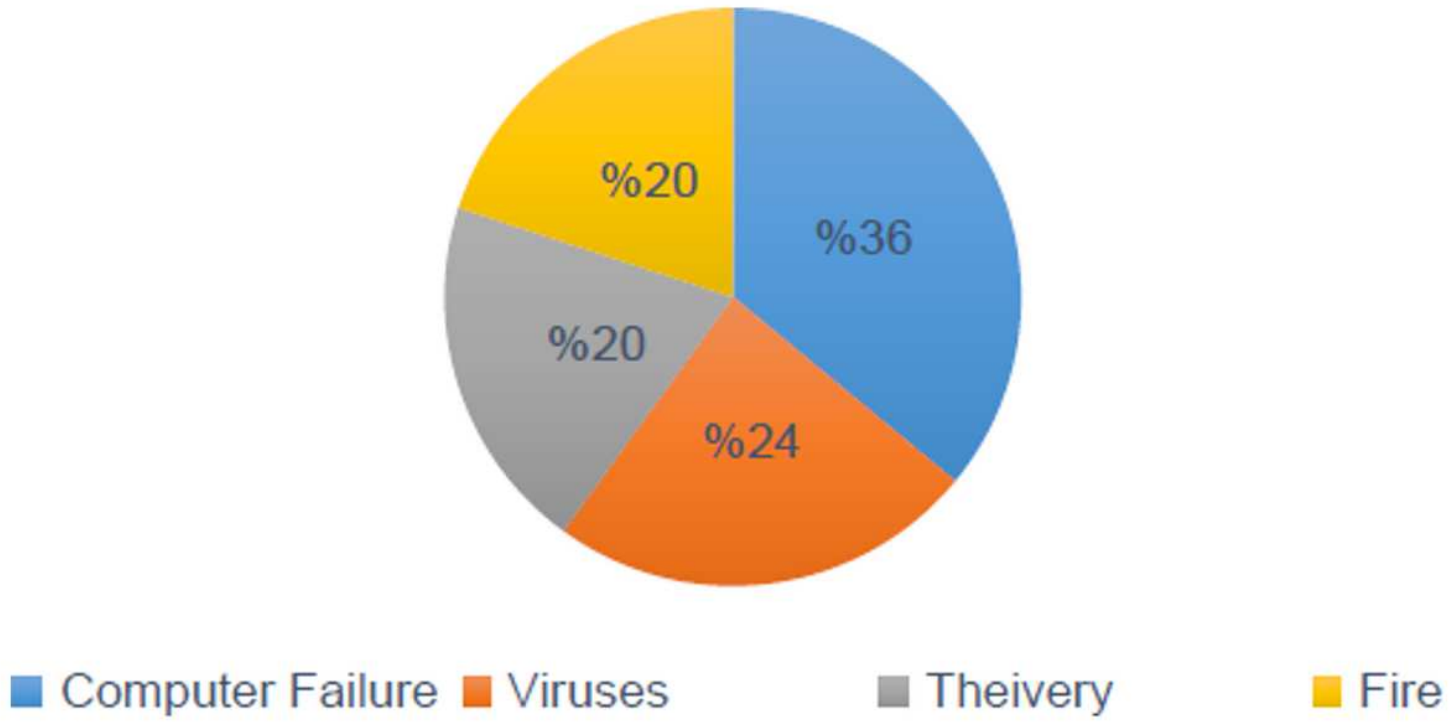

Figure 2

Threats and annualized rate of occurrence.

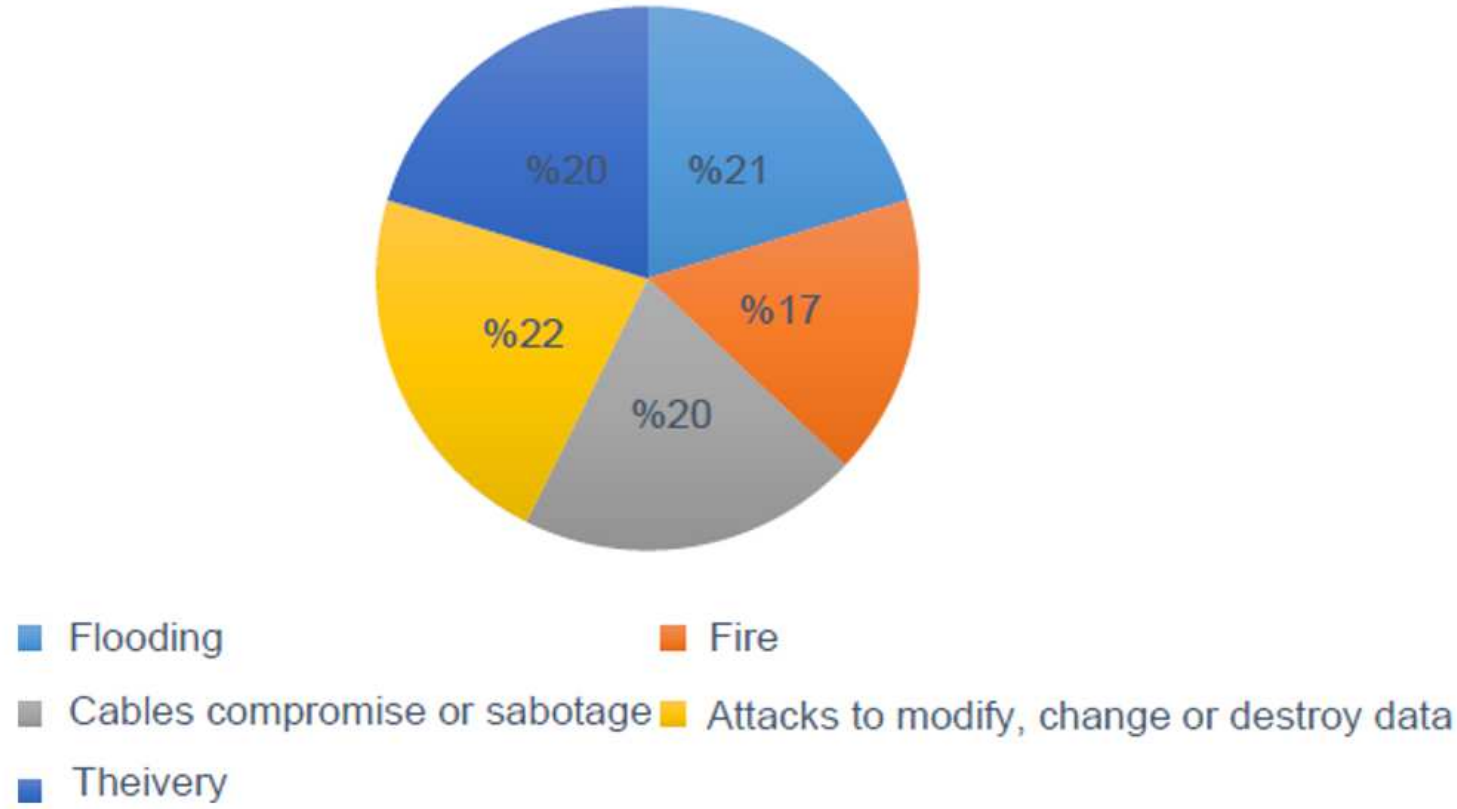

Figure 3

Environmental and external risks.

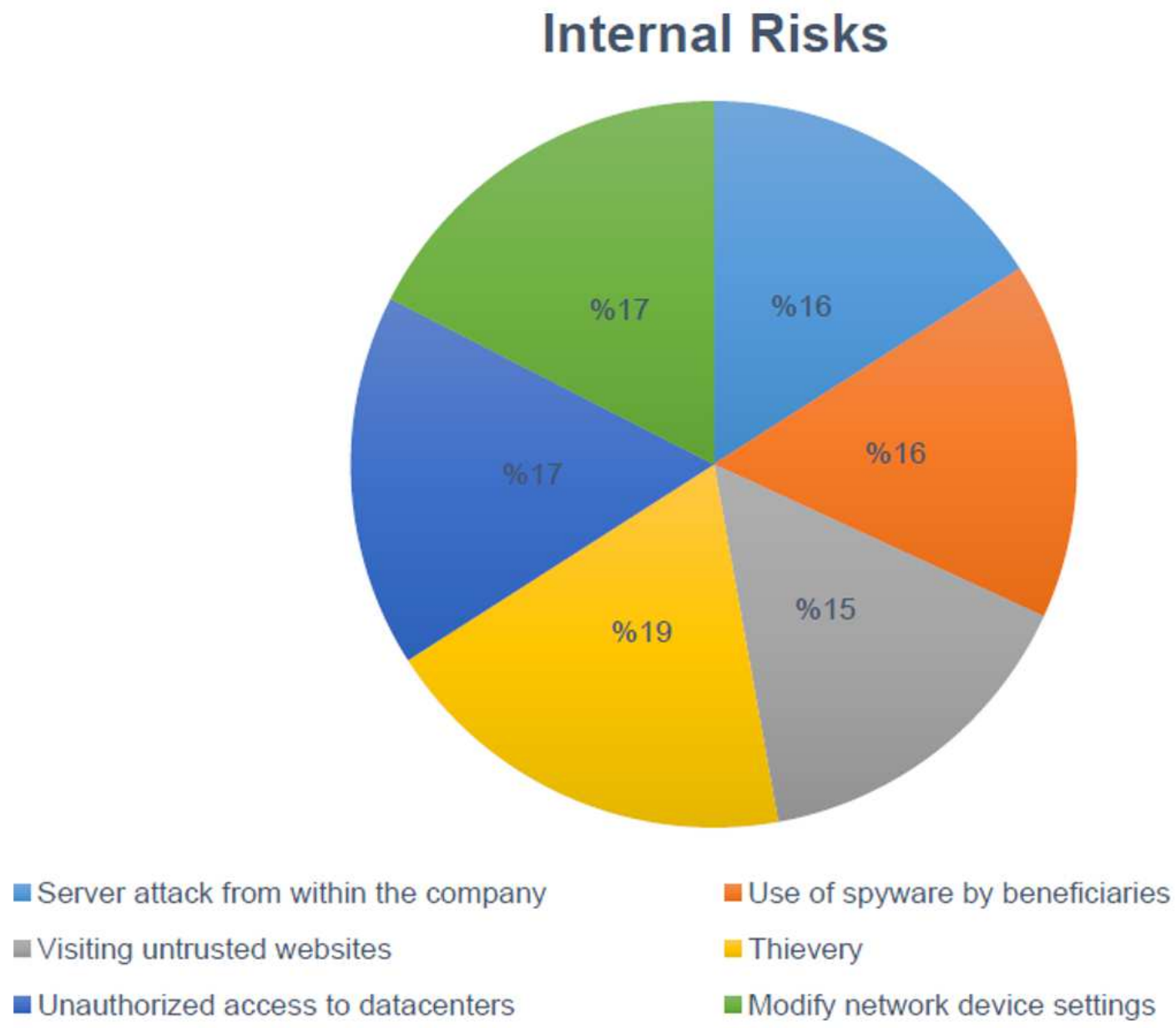

Figure 4

Internal risks.

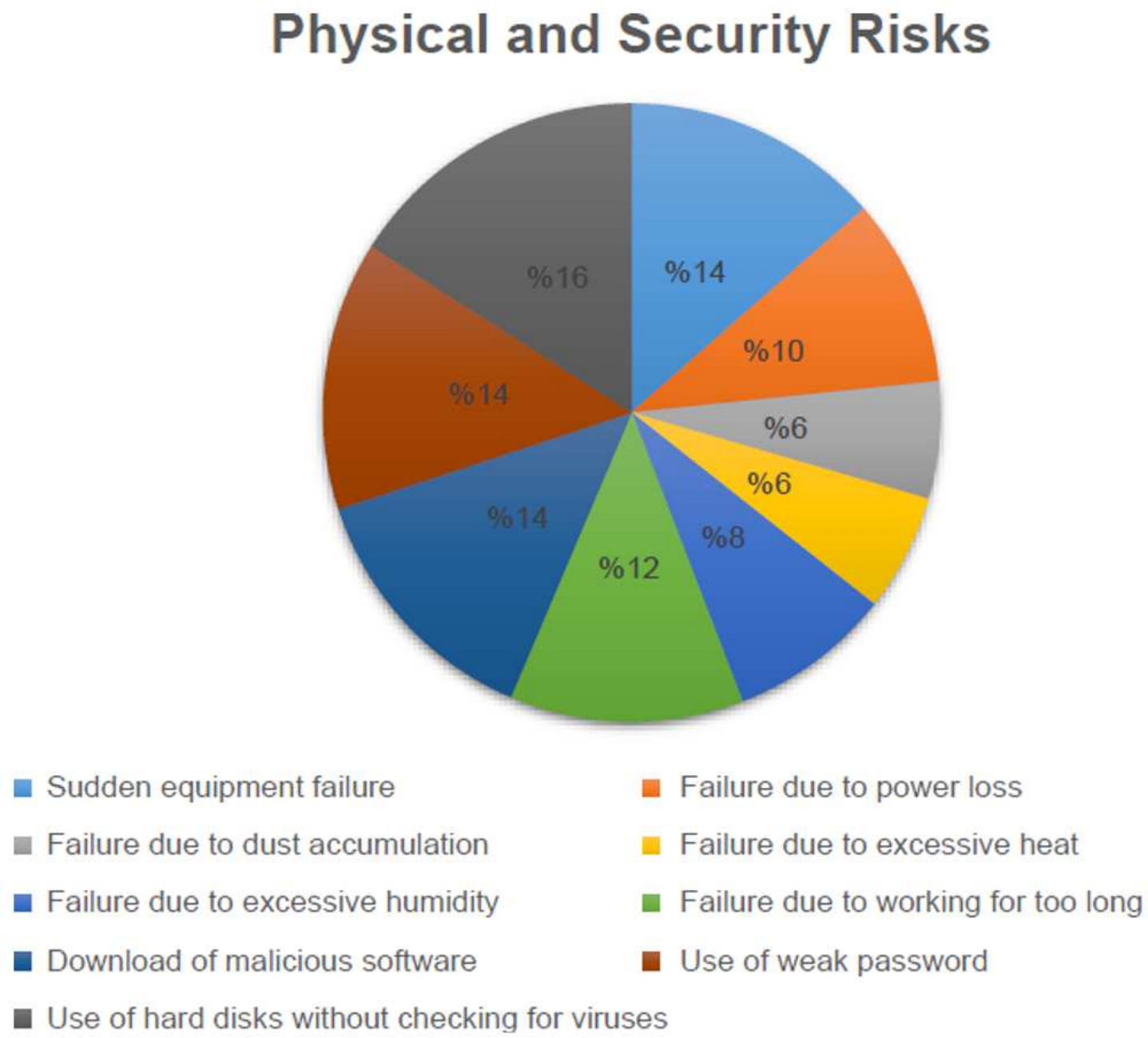

Figure 5

Physical and security risks.

Figure 6

Team escalation and reporting.