Information Booklet

Business Management

1

Crisis Management for SMEs

SMEDA

NBDP
National Business Development Program for SMEs

Introduction

Small and Medium Enterprises Development Authority (SMEDA) works under the Ministry of Industries and Production, Government of Pakistan and was established in 1988 with the objective to propel economic growth through development of SMEs. SMEDA serves as an SME strategy-advisory body for the Government of Pakistan and facilitates partners in meeting their SME development agendas.

SMEDA envisions growth of a globally competitive SME sector, through creating an enabling environment and support services for increase in the national economy. SMEDA strives to achieve this vision by providing assistance in employment generation and value addition to the national income, through development of the SME Sector, by helping increase the number, scale and competitiveness of SMEs.

National Business Development Program for SMEs (NBDP) is a project of SMEDA which intends to provide hands-on support services to SMEs. The aim of this business development support provided by NBDP is to advance new businesses and improve efficiencies in existing SME value chains to empower them to contend in global market. NBDP expects to facilitate around 314,000 SME beneficiaries over the period of five years.

Disclaimer

This information memorandum has been compiled to introduce the subject matter and to provide a general idea and information on the said matter. The information has been provided on as is where is basis without any warranties or assertions. Although, due care and diligence has been taken to compile this document, the contained information may vary due to any change in any of the concerned factors. NBDP/SMEDA, its employees or agents do not assume any liability for any financial or any other loss resulting from the information, as contained in this memorandum. The contained information does not preclude any further professional advice. The prospective user of this memorandum is encouraged to carry out additional diligence and gather any information which is necessary for making an informed decision, including taking professional advice from a qualified consultant/technical expert before taking any decision to act upon the information. For more information on services offered by NBDP/SMEDA, please visit http://www.nbdp.org.pk/ and www.smeda.org.pk

Objectives

- To elaborate the concept and importance of crisis management in small and medium businesses
- To provide an overview of crisis management plan for the preparation of possible risks and recovery

Table of Contents

a

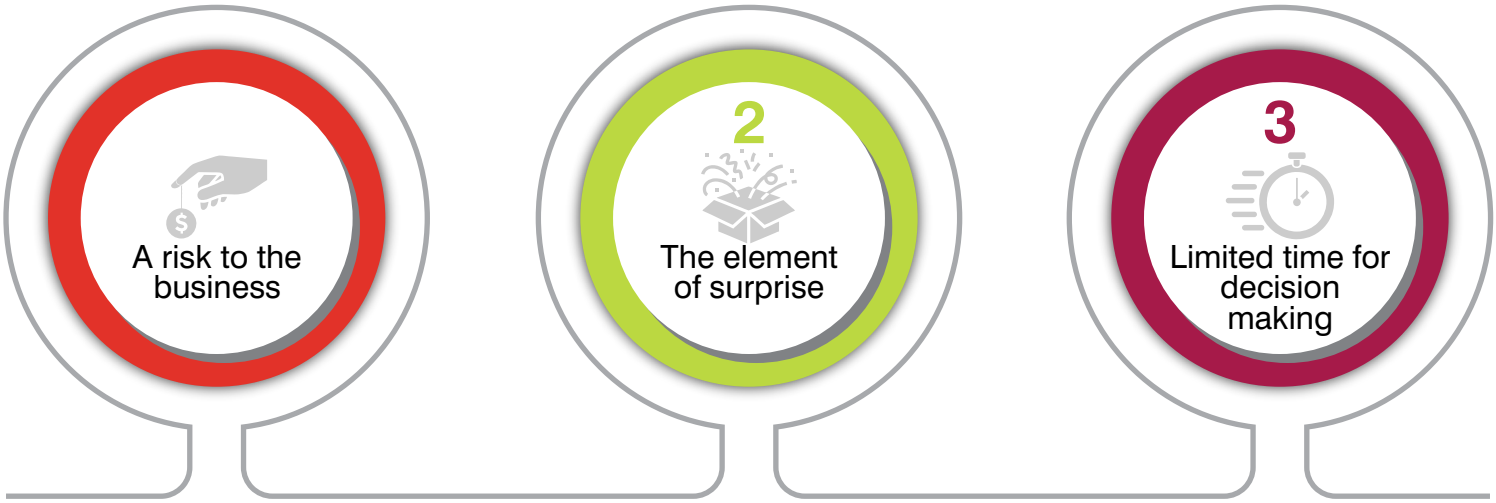
Crisis Management – What and Why?

What is Crisis Management?

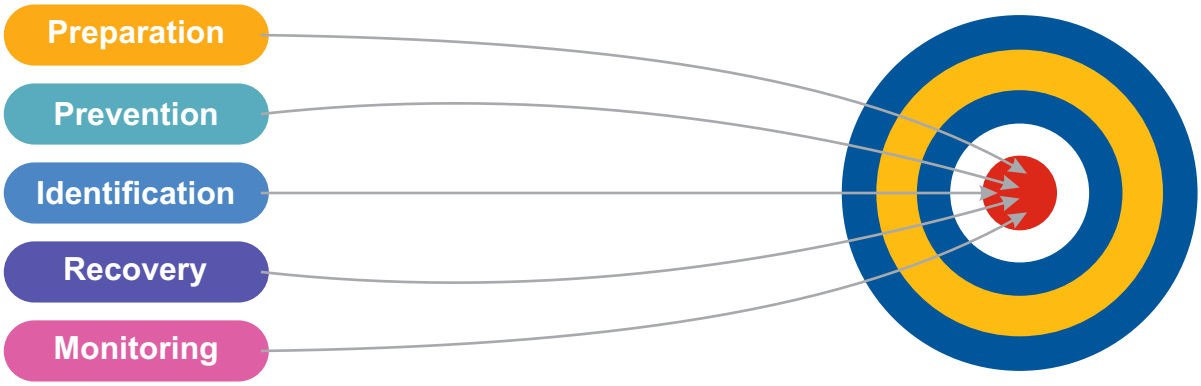
Crisis management refers to the techniques and methods to deal with a sudden or unexpected emergency situation of a business or its stakeholders. To manage the disruptive situation is called crisis management.

Every business seeks to protect itself from untoward situations which may have a detrimental impact on the business, however, there are situations and external factors that cannot be controlled such as natural disasters, political unrest, cyber attacks and market fluctuations. In such situations, it is important how the business reacts to a sudden event of incident.

Any crisis comprises of the following three aspects:



Process of Crisis Management include:



Importance of Crisis Management

Effectively managing the crisis provide opportunity to a business to timely deal with the situation without having a negative impact on business and its employees. Crisis management helps a business in following ways:

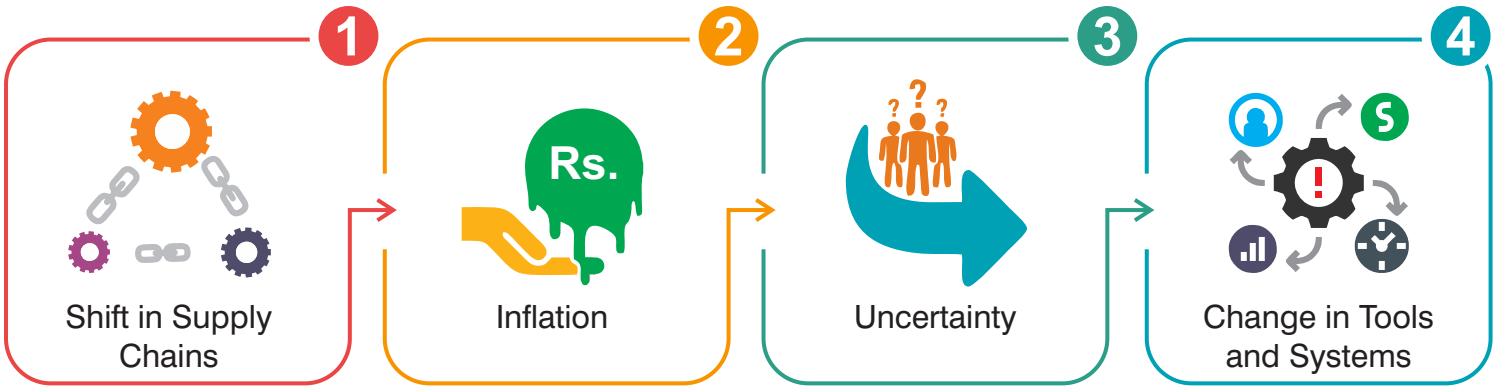
Helps to deal with the unexpected developments and adverse conditions.	Helps employees to adjust well to sudden changes in the business.
Helps the business owners to devise strategies to come out of uncertain conditions and also decide on the future course of action.	Helps the business owners to anticipate the early signs of crisis, warn the employees against the aftermaths and take necessary precautions for the same.

b Types of Crises in a Business

Following are the different types of crises a business may face:

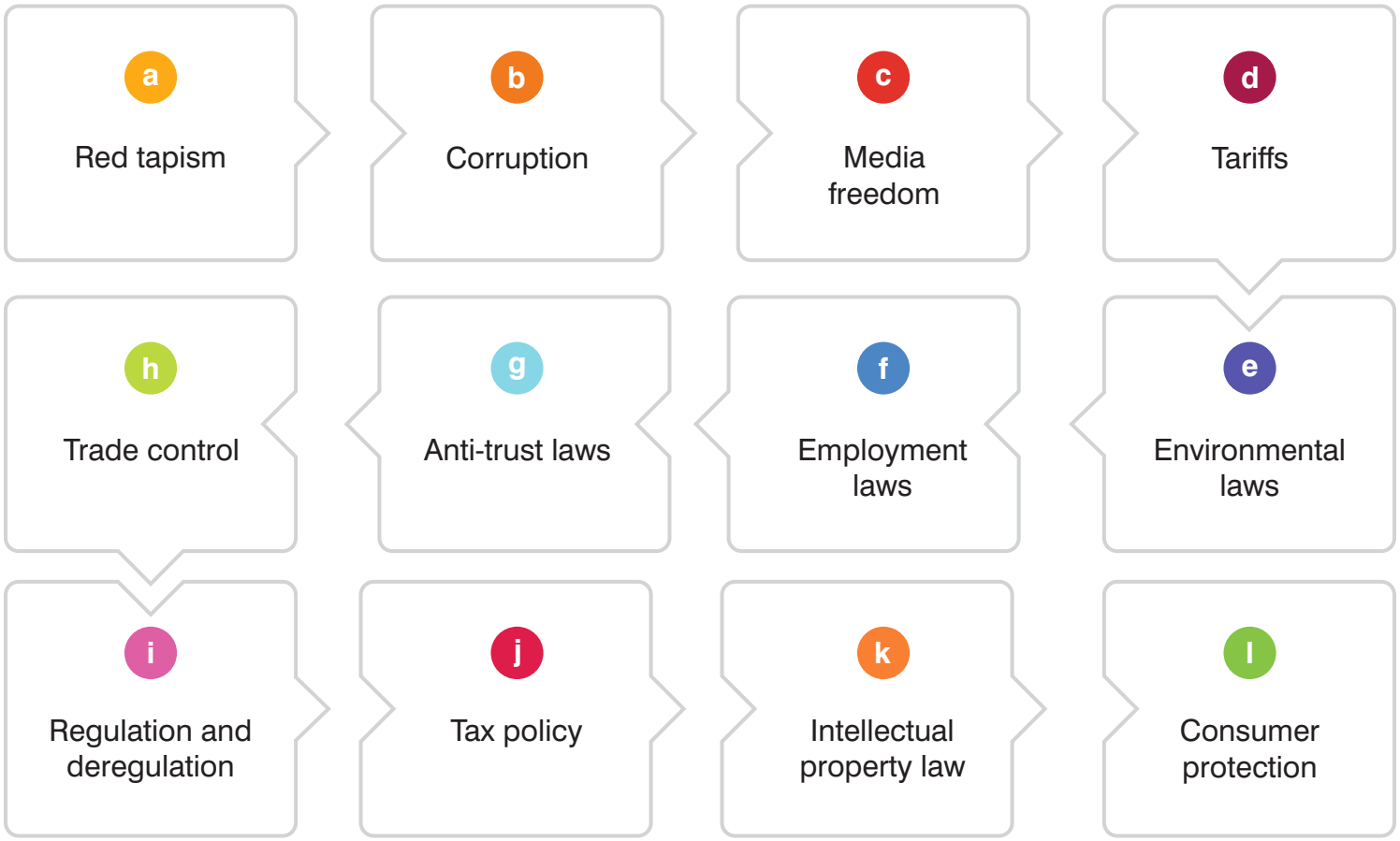
1 Environmental Factors

The effects of environmental factors include increased financial costs and risks etc. that increase the cost of doing business as it has a direct impact on the economic cycle at macro and micro level. Environmental factors include:



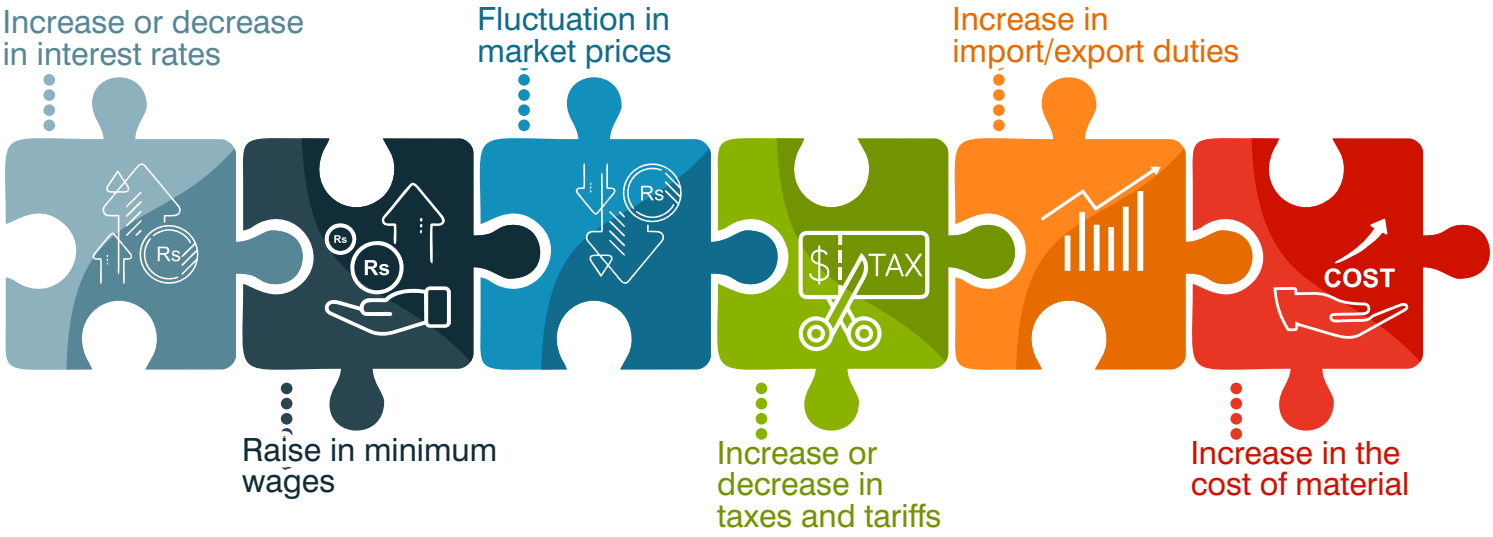
2 Political Situation

Political situation of a country is critical for businesses to function smoothly as any political uncertainty can cause the economy to crash or slow down considerably. Failure to comply with government regulations can result in hefty fees and fines for a business. Businesses should remain prepared to deal with changing government policies and political legislation that affect the business operations. For example, an increase in taxes by the government has a direct impact on the business. Other than this, some other political factors that can affect the business include:



3 Economic Effects and Situation

Macro-economic factors such as inflation, exchange rates, new government regulations and other decisions can adversely affect profits and lead to a substantial loss for a business. Economic risk is difficult to forecast and predict. However, inability to manage it properly can result in bankruptcy. Some of the more common economic risks are listed below:



Some other economic risks include hyperinflation, unstable exchange rates and government regulations that affect investment and businesses. All these conditions should be proactively recognized and monitored in the development of an economic risk management strategy.

4 Market Situation

Michael Porter identified five forces that make up the competitive environment and which can erode profitability of a business. These five factors are:

Competitive Rivalry

This looks at the number and strength of competitors of a business. How many competitors does a business have? Who are they, and how does the quality of their products and services compare with a specific business?

Where rivalry is intense, businesses can attract customers with aggressive price cuts and high-impact marketing campaigns. Also, in markets with lots of competitors, the suppliers and buyers can go elsewhere if they feel that they're not getting a good deal from a specific business. On the other hand, where competitive rivalry is minimal, and no one else is doing what a business does, it will have tremendous strength and healthy profits for the business.

Supplier Power

This is determined by how easy it is for suppliers to increase their prices. How many potential suppliers a business has? How unique is the product or service that they provide and how expensive would it be to switch from one supplier to another?

The more a business has to choose from, the easier it will be to switch to a cheaper alternative. This can impact the profit of business.

Buyer Power

When a business deals with only a few savvy customers, they have more power, but the power of business increases if it has many customers.

There is need to answer how easy it is for buyers to drive prices of a business down. How many buyers are there, and how big are their orders? How much would it cost them to switch products and services to those of a rival? Are the buyers of the business strong enough to dictate terms?

Threat of Substitution

This refers to the likelihood of customers finding a different way of doing what a business offers. For example, if a business supplies a unique software product that automates an important process, people may substitute it by doing the process manually or by outsourcing it. A substitution that is easy and cheap to make can weaken the position and threaten the profitability of the business.

Threat of New Entry

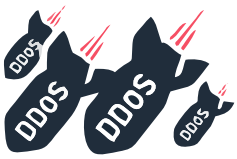
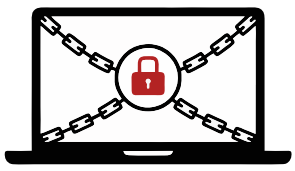
The position of a business can be affected by people's ability to enter the same market.

If it takes little money and effort to enter the market and compete effectively, or if a business has less protection for it key technologies, then rivals can quickly enter the same market and weaken the business's position. A business needs to have strong and durable barriers to entry to preserve a favorable position and take fair advantage of it.

5 Cyber Security

Businesses remain vulnerable to cyber security threats and need to take preventive measures to ensure that they remain protected. The most common types of cyber security threats that a business needs to be cautious about are listed below:

 Phishing:	Hackers or internet scammers may send distorted links or attachments using email or using social media sites, which when opened, it give access to sensitive information or business data. Upon clicking such links or attachments, is automatically downloaded to the target computer or server resulting in breach of information.

 Malware:	Malware is when the target of a phishing attack ends up downloading the link or file. This includes computer viruses, worms, Trojan horses and spyware. For example, a Trojan virus is a malware which is disguised as a legitimate software but is tasked with anything from spying on the system to manipulating its codes.
 Distributed Denial of Service (DDoS):	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic, which causes the system to fully crash or slow down.
 Brute Force or Password Attacks:	This is an attempt by the attacker to secure access to confidential passwords by using a software. Therefore, it is advised to use different passwords for different accounts and to change them regularly.
 Internet of Things (IoT) or Algorithm Manipulation:	As businesses expand, there is a need to rely on wearable tech, IoT applications, cloud and other devices. However, this exposes the data to risks and threats. It is necessary to protect the data by installing internet security software in the devices and use a strong password for the Wi-Fi, installed applications and login accounts.
 Ransomware:	Ransomware is a malware in which the data on a victim's computer is locked and payment is demanded before the ransomed data is decrypted and access is returned to the victim. Payment is often demanded in a virtual currency, such as Bitcoin, so that the cyber criminal's identity is not known. It can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites. Attacks have also used remote desktop protocol and other approaches that do not rely on any form of user interaction.

Protection and Safety Measures

It is a misconception that only large businesses are vulnerable to cyber attacks. In reality, all businesses remain vulnerable to such attacks. It is important to practice caution and take mitigating measures to avert such incidents. Some useful preventive measures that can be adopted in this regard are as follows:

1 Username and Passwords

It is important to follow some basic rules when creating and managing passwords for a business.

Always set strong usernames and passwords.	Do not use the same password for different accounts.
Ensure passwords are stored safely and cannot be easily accessed by others.	Follow the guidelines for developing a strong password. Use a combination of uppercase and lowercase letters, numbers, symbols, etc. so that it cannot be easily guessed.

2 Verifications and Other Code Numbers

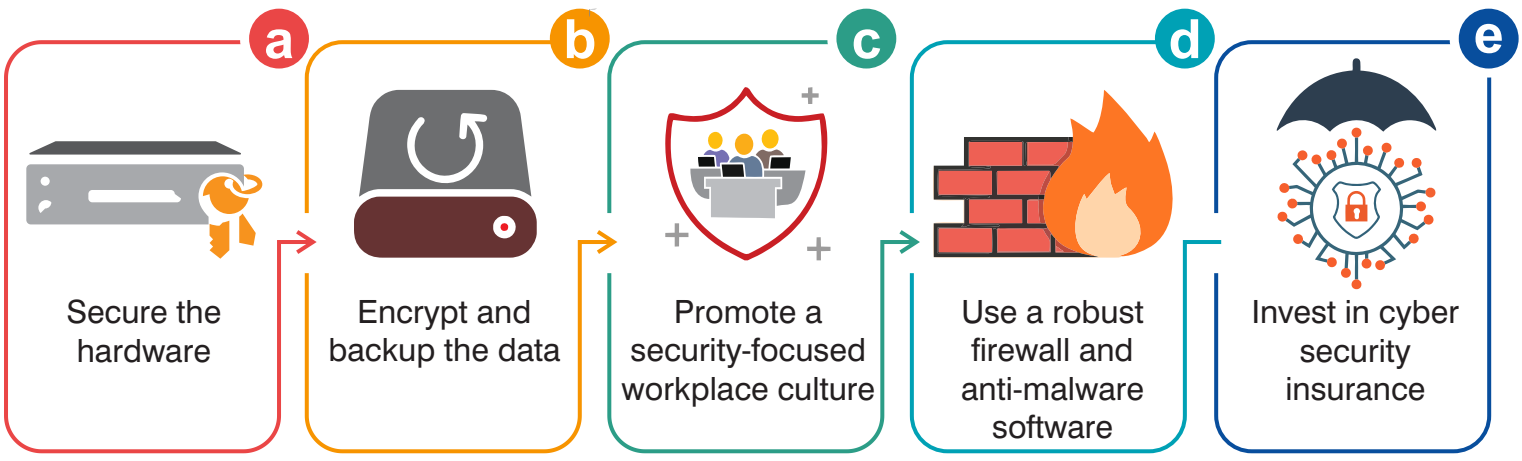
Verification and authentication codes are the second step in a log-in process. For example, an ATM withdrawal requires entering a unique PIN code which is only known to the user. When using credit or debit cards for online shopping, ZIP or postal codes are required without which one cannot carry out the transaction. A second step of authentication improves security and safety of online accounts.

3 Protecting Customer's Information

Businesses need to ensure that their customers remain protected from online fraud and identity theft. Ensuring a secure online environment for transactions is a key business priority. For many people who shop online it is important to know that their payment details and address are secure. It is also important for customers to know that their personal information will not be shared without their consent.

4 Creating a Cyber Security Policy

It is essential for businesses to create a cyber security policy so they are able to ensure a protected and safe environment for their customers and operations. Broadly, the policy must include the following steps:



C Crisis Management Measures in a Business

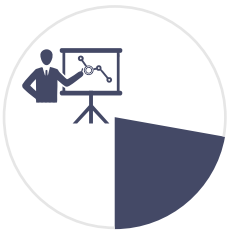
Businesses need to develop crisis management plan prior to the occurrence of any untoward event. Inability to respond effectively at the time of crisis can have severe operational, legal and public relations consequences.

Did you know?[1]

59%

According to a research, globally 59% of businesses have experienced a crisis, but only 54% of them have a plan in place to deal with them.

22%



Research suggests that businesses are at risk of losing 22% of their business when potential customers find just one negative article on the first page of their search result.

Responsive Crisis Management

When a plan of action is available to address the crisis that a business faces, it is called responsive crisis management. Responsive crisis management executes that plan and handles any unexpected obstructions that may come up.

For example a juice factory was blamed that syringes had been found in cans of juices they supply, the business urged its retailers not to remove the product from the shelves while the situation is investigated, the factory released videos and made public, showing the production process to demonstrate that such tempering is impossible within their factory. This also includes communicating with stakeholders, informing employees, and adaptive solutions. Responsive crisis management is used for scenarios like financial and personnel crises where a timely response is necessary.

Proactive Crisis Management

Proactive crisis management anticipates a potential crisis and works to prevent it or prepare for it. For example, building an earthquake-resistant office and sharing an evacuation plan with employees is one method to prepare for natural calamities or disasters. While not all crises can be prevented or planned for, actively monitoring threats to the business can mitigate the crisis.

Recovery Crisis Management

Occasionally, it can become difficult to forecast the risk and it becomes too late to prevent its affects. For example, technological crises can often blindside a business, causing long-term damage. In such situations, it is not possible to ensure full recovery but to begin recouping of what is left of the situation. At such times, it is best for the business to issue a public apology and look into the matter to identify what caused the unexpected crisis.

A crisis plan should include the following:

- Internal and external stakeholders
- Primary speaker for each communication channel
- Communication infrastructure and redundancies
- Decision-making chain of command
- Access to emergency funds
- Develop the holding statements
- Contingency plans

[1]Jonas Sickler, (June 8th, 2018, updated on 23 August, 2019) Crisis Management retrieved on: 25th August 2019 from: https://www.reputationmanagement.com/blog/crisis-management/

d Crisis Management Plan for the Business

A crisis management plan can be created by following the indicated steps:

1 Risk Assessment

Risk assessment is the first step towards developing a crisis management plan and entails identifying the possible crises that could affect the business activities and processes. For this purpose, business owners should develop a list of applicable and relevant threats to the business e.g. public relations slipups, social media blunders, product recalls, cyber attacks and data breaches etc.

2 Impact on the businesses

Business Impact Analysis (BIA) is a method to calculate the potential impact of a business-disrupting situation. A BIA can help reveal insights into the potential effects a crisis can have on the business including:

1. Customer satisfaction
2. Loss of public goodwill and reputation
3. Lost or delayed sales or revenues
4. Increased expenses (for example, paying for overtime labor or to expedite shipping of products)
5. Regulatory fines

BIA is an important step to ensure that the business is truly factoring in all possible threats to its activities and operations and make others realize the value of crisis management plans.

3 Identify Contingencies

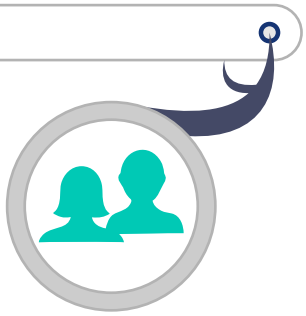
Once the relevant threats to the business have been identified, the second step is to identify the actions. These actions will help respond to those threats effectively and assess what resources would be required and how employees can help. For example a crisis plan for a product recall may require help from the Information Technology (IT) and logistics department to determine how to fix the problem, while customer service, sales, and public relations work together to answer customer questions and maintain the company's good standing.

4 Develop the Plan

Once an effective contingency plan for each potential crisis has been developed, the next step is to flesh out the plans with relevant stakeholders. Key employees, such as department heads, can help to provide insight into available resources and potential hurdles. For certain crisis scenarios, input may also be required from outside parties, such as contractors and partners that work closely with the business. It is important to remember any relevant regulatory requirements and determine how the business will continue to meet them, even in the midst of a crisis.

5 Familiarize Users

It is important that all employees understand their roles during a crisis. Ensure that all stakeholders have all the required information they need. During the tense moments of a crisis, people require very quick access to straightforward information.



6 Revisit the Plan Frequently

Once the plan is written and approved and has been tested, be sure to revisit it frequently. It is vital to keep the plan up to date, especially as employees join or leave the company, new technologies are implemented and other changes occur. It can be helpful to review and test the plan at least a few times a year to keep the content up to date.

HEAD OFFICE

Address:	3rd/4th Floor, 3rd Building, Aiwan-e-Iqbal Complex, Egerton Road, Lahore
Tel:	(042) 111-111-456, 99204701-12
Fax:	(042) 36304926-27
Email:	helpdesk@smeda.org.pk

REGIONAL OFFICES

Balochistan

Address:	Bungalow No. 15-A, Chaman Housing Scheme, Airport Road, Quetta
Tel:	(081)-2831623 - 2831702
Fax:	(081)-2831922
Email:	helpdesk.balochistan@smeda.org.pk

Punjab

Address:	4th Floor, 3rd Building, Aiwan-e-Iqbal Complex, Egerton Road, Lahore
Tel:	(042)-111-111-456
Fax:	(042)-36304926, 36304927
Email:	helpdesk.punjab@smeda.org.pk

Khyber Pakhtunkhwa

Address:	Ground Floor, State life Building, The Mall, Peshawar
Tel:	(091)-111-111-456, 091-9213046-7
Fax:	(091)- 5286908
Email:	helpdesk.KhyberPakhtunkhwa@smeda.org.pk

Sindh

Address:	5th Floor, Bahria Complex II, M.T. Khan Road, Karachi
Tel:	(021)-111-111-456
Fax:	(021)-35610572
Email:	helpdesk.sindh@smeda.org.pk