Information Booklet

Business Management

2

Cyber Security for SMEs

SMEDA

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 understand cyber security for conventional and online business
- To address growing threats of identity theft, online fraud and disruptive business practices

Table of Contents

a Conventional vs Online Business

Thirty years ago, opening a business entailed purchasing or renting a space, setting up phone service and working on attracting customers. The internet changed all that and now business can be set up without leaving the house.

Even with a storefront, a business is expected to have an online presence that makes it easy for customers to get information or place orders. There are many differences between a conventional business and an online business, not the least of which are startup costs, personnel and logistics.

Conventional Business

Business which allows direct, face to face interaction with the customer is referred to as a "Conventional Business". It is a set-up where customers have to visit the facility in person to buy the products/goods or to get the service.

Online Business

Any business that sells products and/or services on the internet is referred to as an “Online Business”. It is pertinent to not confuse a business website or social media presence with an online business. A website provides information to customers about the business, whereas, an online business entails selling products/services using the global infrastructure setup of the internet through virtual presence.

Characteristics of:

Conventional Business

- Conventional businesses are important because while buying some products customers may not be comfortable to make a purchase without physically examining the product at the conventional business outlet.
- Most conventional businesses are not open 24 hours a day, close on holidays and many are open only five or six days in a week.
- Under certain business models, customers prefer human interaction which is provided by a conventional business.
- To setup a conventional business, a substantial initial investment is required to cover the costs of location rent, raw material, processed products etc.
- Conventional businesses remain vulnerable to robberies and theft.

Online Business

- Some business models are more suited to an online setup than a conventional store.
- Online businesses are always open, and sell products and services 24 hours a day throughout the week.
- It may be difficult to establish trust in customers for an online business. Not all businesses are adaptable for strict e-business models.
- Online business model generally has lower overhead and startup costs as it eliminates the need for location rent, staff and utilities.
- Online businesses are less prone to criminal threats and hazards but more vulnerable to cyber attacks.

b Cyber Security – Concept and Types

The practice of protecting systems, networks and programs from digital attacks is called cyber security. Digital attacks vary in nature and include attempts to access, change or destroy information which is sensitive to the business and its operations. Further, extorting money from users or using confidential information for fraudulent activities are included in digital attacks. In summary, any attempts to interrupt and negatively impact business operations is considered a digital attack. It is challenging to mitigate the risk of cyber and digital attacks since technology is constantly evolving and digital attacks are not easy to predict. However, there are precautionary measures that can be taken to minimize the threat and damage associated with cyber attacks.

In today's always-connected world where the private information of individuals and businesses is vulnerable to exposure and misuse, cyber security is everyone's responsibility because hackers or malicious threat actors who steal proprietary information are present everywhere.

What is Cyber Security All About?

Cyber security aims to protect the network, devices, programs or data spread across the network being used for business operations and online presence. To ensure optimum protection from cyber attacks and fraud, it is important to ensure active coordination between the people, processes and technology involved.

People

All users must understand and observe the basic data security principles such as selecting strong passwords, practicing caution while opening attachments in emails and maintaining a data backup.

Processes

Businesses must develop a framework and protocol to avert possible cyber attacks. Guidelines should be provided to identify attacks, protect devices, detect threats, and recovery options.

Technology

Employ judicious and proactive use of technology to ensure optimum security to protect the business and individuals from cyber attacks. There are three main entities which require protection:

Endpoint Devices
(computers, smart devices and routers)

Networks
(WAN, LAN, and WiFi)

Cloud
(g-drive, Dropbox and iDrive)

Five Basic Elements of Cyber Security

Application Security

Minimize the likelihood that unauthorized code is able to manipulate applications to access, steal, modify or delete sensitive data.

Information Security

Information security protects information assets, regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Network Security

Detect, prevent and respond to threats through the use of security policies, software tools and IT services.

Disaster Recovery

Maintain or quickly resume business-critical functions following a disaster.

End-User Education

Provide directives that describe what actions must be taken or avoided - in order to protect business assets.

Why is Cyber Security Important?

Cyber security is important because cyber security risk is increasing.

Cyber security programs have become increasingly important for businesses over the years. A cyber attack can result in significant financial loss for the business and expose it to identify theft, breach of information and compromise customer confidentiality and invasion of privacy.

Types of Cyber Security Threats

Common types of cyber security threats:

1 Phishing:

Hackers or internet scammers may send distorted links or attachments while sending an email or using social media sites, which when clicked upon or opened in the case of an attachment give access to sensitive information or business data. Upon clicking such links or attachments, certain software or content is automatically downloaded to the target computer or server resulting in breach of information.

2 Malware:

If the target of a phishing attack ends up downloading the link or file, then the installed program is a malicious software, which is harmful to a computer user. 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.

3 **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.

4 **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 a different password for multiple accounts and to change it regularly.

5 **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 which can be compromised without frequent monitoring and due diligence.

6 **Ransomware:**

This is a malware that locks the system down and encrypts the data and device so that no one can use it anymore. The affected computer or server remain locked until a significant financial amount is paid to lock it out.

C Cyber Risks and Threats for Businesses

A successful cyber attack can cause major damage to the business by affecting it financially, negatively impacting business reputation and loss of trust. The impact of a security breach can be financial, reputational and legal.

Financial Loss

Cyber attacks often result in substantial financial losses stemming from:

- Loss or theft of business information and data
- Information theft i.e. bank details, payment and financial information.
- Monetary theft
- Disruption of business operations and trading e.g. inability to conduct online transactions
- Loss of business or contract

Business that experience a cyber breach incur significant repair costs to restore the affected systems, devices and networks.

Reputational Loss

A cyber attack can have a detrimental impact on the business reputation and credibility. In particular, it can lead to loss of customers, sales and reduced profits and revenues. Additionally, it can affect suppliers and investors causing loss of trust in the business.

Legal Significance of a Cyber Breach

Business owners need to protect and manage data and information as per the prevalent data protection and privacy laws and regulations. In case of a cyber breach, a business may face legal exposure, which could result in business and financial losses.

d Assessing Cyber Risks to Business

Identifying, investigating and assessing risks is referred to as a risk assessment. It identifies cyber security measures that are suitable for a business to mitigate risks associated with cyber attacks. A business needs to undertake a risk assessment to ensure it is prepared to act in case of any untoward situation.

What Does a Cyber Security Risk Assessment Include?

A cyber security risk assessment identifies cyber risks that businesses remain vulnerable to. It covers the overall data and information of a business e.g. customer data, intellectual business property, patents, business intelligence, and information available on laptops, systems, hard drives and back up devices, and the applicable risks.

A risk estimation and evaluation exercise is carried out as part of the cyber security risk assessment, followed by selection of controls to treat the identified risks. The risk environment needs to be frequently monitored and reviewed to remain updated of any change in the business, and to maintain an overview of the complete risk management process.

The Prevention of Electronic Crimes Act, 2016 introduced a range of offenses in Pakistan involving the unauthorized access, transmission, copying, or interference in an information system or data. Harsher penalties are set for these crimes if they involve information systems or data connected to critical infrastructure.

ISO 27001 and Cyber Risks

ISO 27001 is the cyber security standard that a business should strive for; using this family of standards helps the business to manage the security of assets such as financial information, intellectual property, employee details or information entrusted to the business by third parties.

ISO/IEC 27001 is the best-known standard providing requirements for an information security management system (ISMS)

Some standard protocols as part of information security risk assessment process are:

- Develop and maintain the criteria for certain information security risks.
- Ensure that repetitive risk assessments “produce regular, valid and comparable results”.
- Find out “risks related to the loss of confidentiality, integrity and availability for information within the scope of the information security management system” and identify the risk sources.
- Examine and assess the information security risks as per the established standards.

e Protection and Safety Measures

It is wrong to assume only large businesses are vulnerable to cyber attacks. In reality, all businesses are vulnerable to cyber attacks and should take measures to avoid such incidents. Some useful preventive measures that can be adopted are:

i. Username and Passwords

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

- Do use the default username and passwords.
- Do not use the same password for different accounts.
- Ensure passwords are stored safely and are not accessible to 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, for example, (?%&@!).
- Make sure to change passwords at least every nine months to one year.

Using a password manager helps track the age of each password, and indicates what additional security controls have been applied, and helps generate complex passwords for all accounts, which reduces cyber fatigue and makes life easier - and more secure.

ii. Verifications and Other Code Numbers

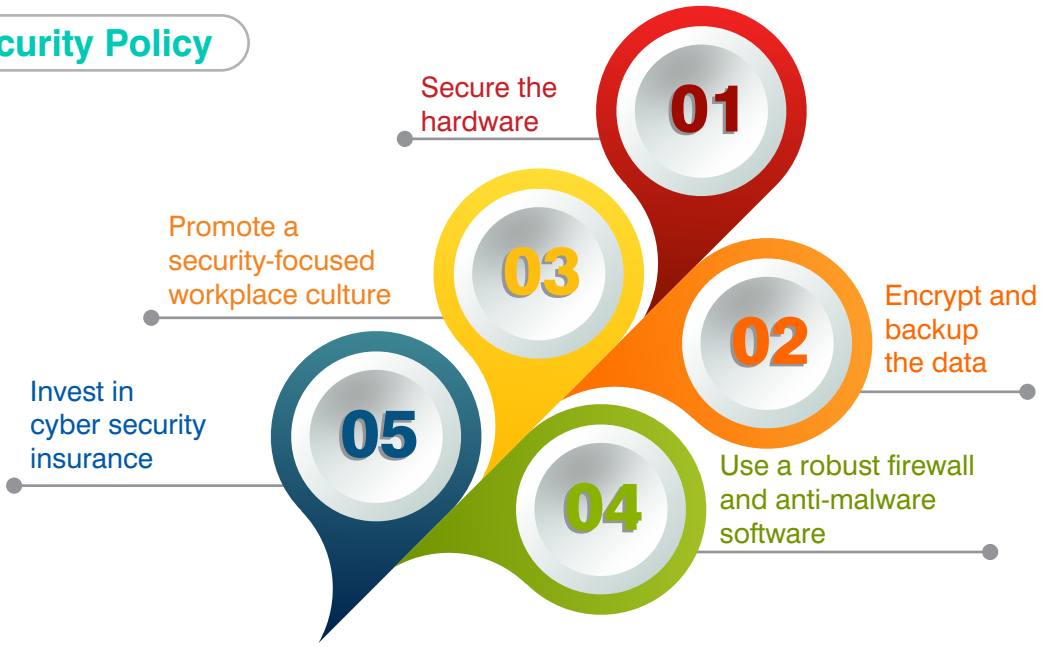
Verification and authentication codes are the second step in a log-in process and are shared via text messages or email. For example, an ATM withdrawal requires entering a unique PIN code which is only known to the user. When using credit or debit cards for online shopping, ZIP or postal codes are required for carrying out the transaction. A second step of authentication improves security and safety of online accounts.

iii. Protecting Customer Information

Cyber crime is one of the most prevalent form of criminal activities related to business. That is why protection of customer information should be one of the main priorities of any business. Businesses should work on preventing cyber attacks by implementing cyber security policies to protect customer information, prevent online fraud and identity theft.

iv. 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. The policy must include the following steps:



1. Secure the Hardware

Securing the hardware and the software from cyber threats is equally important. To do so, the business must protect all hardware devices with strong passwords to restrict access and loss/theft of devices. Business owners and staff must limit the access to passwords and avoid writing passwords on diaries or sticky notes where they can be easily viewed by others.

2. Encrypt and Backup the Data

To protect business information from cyber risks, a risk mitigation strategy must contain the following components:

I. Averting physical access to sensitive data

II. Rendering the data useless if it falls into the wrong hands

Remember!
Once the data is encrypted, back up all data and store it separately.

Businesses can achieve the latter by always encrypting data. Full-disk encryption software is included in virtually all operating systems today and can encrypt data on a desktop or laptop computer when it is not being used. Ensure encryption software is activated and updated in all devices. Devices should be set to auto lock or sleep mode after five minutes if not in use.

3. Promote a Security-Focused Workplace Culture

Employees should be provided knowledge and training regarding cyber security measures to mitigate the threat of data and security breaches. The following steps can be taken to promote a cyber secure workplace culture:

- Prohibit employees from using their personal devices for work.
- Teach employees about the secure use of personal and work devices.
- Inform employees about the risk of using unsecured networks such as public Wi-Fi.
- Only use a secure network that requires a key/password to access.
- Avoid using unsecured websites on work devices.
- Discourage password sharing and instruct employees to temporarily log in with guest accounts.
- Restrict the Information Technology (IT) and administration access rights to employees.
- Ensure safe and encrypted storage of the data by the IT department.

4. Use Robust Firewall and Anti-Malware Software

Ransomware is the most common security threat to small businesses. A ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Ransomware can be devastating to a business and it is necessary to take precautionary measures to remain protected from such attacks. A specific software is needed to protect a business from ransomware.

What is a Malware?

Malware is malicious software or code that typically dam- ages or disables, takes control of, or steals information from a computer system. Malware broadly includes botnets, viruses, worms, Trojan horses, logic bombs, rootkits, bootkits, back- doors, spyware, and adware.

5. Invest in Cyber Security Insurance

The insurance sector has been issued a directive from Securities and Exchange Commission of Pakistan (SECP) to provide protection against cyber attacks as cyber criminals continue to find innovative and advanced means to breach security defense. Even the most security-conscious businesses remain vulnerable to attacks. Businesses need to obtain cyber security insurance to mitigate losses or damages from a variety of cyber incidents, including data breaches, business interruption and network damage.

f Responding to a Cyber Security Incident

Cyber security incidents should be immediately reported to the National Response Center for Cyber Crime (NR3C). The following crimes can be reported to NR3C:

- Un-authorized access to the physical information system, digital data, personal identity.
- Email hacking, fake id on social media (Facebook, Twitter, Google Plus).
- Online fund transfer fraud through bank, ATM, Easypaisa, U-paisa, TimePay or any other online fund transfer facility.
- Impersonation and threats on social media (Facebook, Twitter, Google Plus).

Following are some methods for registering the complaints:

a Write a comprehensive application in simple English/Urdu text indicating details about the offense(s). Evidence such as email printouts (screenshots) should be attached with the application.

b A written application can be sent by hand or via courier with complete credentials (name, address, Computerized National Identity Card (CNIC) details, and contact number) stating the complaint to the Director NR3C-Federal Investigation Authority (FIA), National Police Foundation Building, 2nd Floor, Mauve Area, G-10/4, Islamabad.

c A complaint registration form can also be filled out and is available at: http://complaint.fia.gov.pk/

d The complaint application and details of the incident can also be sent via email on: helpdesk@nr3c.gov.pk

e Once the complaint is received with proper and complete information, Helpdesk responds by assigning CCHD/# (Cyber Crime Helpdesk Number) within 24 hours.

Note: Complaints will be sent to the Cyber Crime Circle Zone for further enquiry and verification.

In case of any query and update/progress about the complaints, an email can be sent to the following address:
helpdesk@nr3c.gov.pk or the authorities can be contacted telephonically on
051-9106384 or **0336-6006060**

g Cyber Security Management Plan

All businesses must develop a cyber security risk management plan. Legal Experts and IT Professionals can be consulted to formulate this plan. Some general guidelines for developing the cyber security plan are as below:

- Identify the data and information that the business stores and uses.
- Define the worth of the information. For example:
  - What would happen to the business if the data is made public?
  - What if the information was improper or changed?
  - What would happen if the data is lost?
- Develop an inventory where different types of information is being stored. An IT professional can assist with this step.
- Define threats and vulnerabilities.
- Evaluate the likelihood of each event and the significance of the potential impact. Develop a ratings matrix of high, medium and low for each event. This will help in segregating the levels of risk and the impact each risk holds.
- Take steps to help mitigate the risks and safeguard the information. Work to develop a plan and create a budget and implementation timetable.
- Monitor the progress on a regular basis.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Control Recommendations
Malicious human (Interference) – DDOS attack	Firewall is configured properly and has good DDOS mitigation	Website	Website resources will be unavailable	DDOS was discovered once in 2 years	Potential loss of 10,000 per hour of downtime	Monitor the firewall
High	Low	Critical	Critical	Medium	Medium	

ID	Activity / Security Control	Rationale	Associated Documentation
1	Define the system	Careful system definitions are essential to define the accuracy of vulnerability and risk assessments. These also help in selection of controls that will provide adequate protection against cyber threats.	
2	Identify and classify critical cyber assets	It is important to identify the assets that may need to be protected, along with their classification (e.g., confidential information, private information, etc.). That way, an informed decision can be made regarding the controls needed to protect these assets, commensurate with risk severity and impact on the business.	
3	Provide active executive sponsorship	Active and visible support from executive management at each stage of planning, deploying and monitoring security efforts is crucial to success.	
4	Identify and analyze the electronic security perimeter(s) (ESPs)	It is important to understand the entry points that an adversary may use to attack the business assets develop a “Threat Model Matrix”. The threat model matrix then becomes an important component of the risk assessment.	
5	Perform a vulnerability assessment	Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities; create the basis for estimating the likelihood of successful attacks. These also help to prioritize remedial actions.	
6	Assess risks to system information and assets	The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the mission and goals of a business. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the business.	
7	Select security controls	Security control selection culminates in the specification of a tailored set of security controls that will satisfy the minimum security requirements for the business.	
8	Monitor and assess the effectiveness of controls	Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate perceived risks.	
9	Assign responsibility for security risk management to a senior manager	Assigning responsibility ensures that security risk mitigation, resource-allocation decisions and policy enforcement roll up to a clearly defined executive with the requisite authority.	

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