CYBER SECURITY FOR YOUR BUSINESS

Small and Medium Enterprises Development Authority

Ministry of Industries & Production

Government of Pakistan

www.smeda.org.pk

HEAD OFFICE

4th Floor, Building No. 3, Aiwan-e-Iqbal Complex, Edgerton Road,
Lahore
Tel: (92 42) 111 111 456, Fax: (92 42) 36304926-7
helpdesk@smeda.org.pk

REGIONAL OFFICE PUNJAB	REGIONAL OFFICE SINDH	REGIONAL OFFICE KPK	REGIONAL OFFICE BALOCHISTAN
3rd Floor, Building No. 3, Aiwan-e-Iqbal Complex, Edgerton Road Lahore, Tel: (042) 111-111-456 Fax: (042) 36304926-7	5TH Floor, Bahria Complex II, M.T. Khan Road, Karachi. Tel: (021) 111-111-456 Fax: (021) 5610572	Ground Floor State Life Building The Mall, Peshawar. Tel: (091) 9213046-47 Fax: (091) 286908	Bungalow No. 15-A Chaman Housing Scheme Airport Road, Quetta. Tel: (081) 831623, 831702 Fax: (081) 831922
helpdesk.punjab@smeda.org.pk	helpdesk-khi@smeda.org.pk	helpdesk-pew@smeda.org.pk	helpdesk-qta@smeda.org.pk

December, 2017

Table of Contents

1 INTRODUCTION OF SMEDA

The Small and Medium Enterprise Development Authority (SMEDA) was established with the objective to provide fresh impetus to the economy through the launch of an aggressive SME development strategy. Since its inception in October 1998, SMEDA had adopted a sectoral SME development approach. A few priority sectors were selected on the criterion of SME presence. In depth research was conducted and comprehensive development plans were formulated after identification of impediments and retardants. The all-encompassing sectoral development strategy involved overhauling of the regulatory environment by taking into consideration other important aspects including finance, marketing, technology and human resource development.

After successfully qualifying in the first phase of sector development SMEDA reorganized its operations in January 2001 with the task of SME development at a broader scale and enhanced outreach in terms of SMEDA's areas of operation. Currently, SMEDA along with sectoral focus offers a range of services to SMEs including over the counter support systems, exclusive business development facilities, training and development and information dissemination through a wide range of publications. SMEDA's activities can now be classified into the three following broad areas:

1. Creating a Conducive Environment; includes collaboration with policy makers to devise facilitating mechanisms for SMEs by removing regulatory impediments across numerous policy areas.
2. Cluster/Sector Development; comprises formulation and implementation of projects for SME clusters/sectors in collaboration with industry/trade associations and chambers
3. Enhancing Access to Business Development Services; development and provision of services to meet the business management, strategic and operational requirements of SMEs.

SMEDA has so far successfully formulated strategies for sectors, including fruits and vegetables, marble and granite, gems and jewelry, marine fisheries, leather and footwear, textiles, surgical instruments, transport and dairy. Whereas the task of SME development at a broader scale still requires more coverage and enhanced reach in terms of SMEDA's areas of operation.

2 DISCLAIMER

Form of this document and the contents therein are provided only for general information purpose and on an "as is" basis without any warranties of any kind. Use of this document is at the user's sole risk. SMEDA assumes no responsibility for the accuracy or completeness of this document, its form and any of the information provided therein and shall not be liable for any damages arising from its use.

Document No.	PUN/OTC/4
Prepared By	SMEDA-Punjab
Prepared In	December 2017
For information	uzmak@smeda.org.pk

3 WHAT IS CYBER SECURITY?

Computer security or otherwise known as cyber security is the protection of computers and systems from damage and theft of hardware, software and information. It includes controlling of physical access of hardware and also protecting it against misuse and harm of any form. Importance of cyber security is increasing as computer systems, networks, internet, Wi-Fi, etc. are being used in every field of work.

4 WHY CYBER SECURITY?

For the protection of computers, networks, programs and data, it is important to secure them with some form of technology processes and practices. It is important to earn the trust of online customers and to protect their information against any sort of fraud and crimes.

Cyber criminals not only work individually but also form small groups including criminal organizations working with corrupt technology professionals to violate cyber security. Cyber criminals may have various goals such as

i. Obtaining money to fund illegal activities.
ii. Attack on an organization's hardware and software network for confidential information.
iii. Financial crimes such as online fraud and fake schemes.
iv. Misuse of personal information.

5 ELEMENTS OF CYBER SECURITY

Cyber security requires coordinated efforts throughout an information system and it is important to secure the following elements:

i. **Application Security:** Use of software, hardware and procedural methods to protect applications from external threats. Security measures built into applications along with a sound application security routine minimizes the likelihood of an unauthorized user to manipulate applications to access, steal, modify or delete sensitive data.
ii. **Information Security:** Strategies to manage the processes, tools and policies necessary to prevent, detect, document and counter threats to digital as well as non-digital information.
iii. **Network Security:** Practices and policies to prevent and monitor unauthorized access, misuse, modification and denial of a computer network and related resources. It involves authorization of access to data in a network which is controlled by the network administrator. It protects and oversee operations being done in an organization and other types of institutions and enterprises.
iv. **Operational Security:** This process includes:
    a. Identification of critical information, analysis of threats and vulnerabilities and risks associated with them and then application of appropriate measures to secure information.
    b. Technologies such as security certifications and encryptions that immediately notify the user of any breaches in security can be used to make websites safer.

c. Companies and individuals who rely on software security should have backup plans also, as the cyberspace gets larger with technologies like cloud, mobile computing, etc., it also becomes difficult to control its safety completely and at the same time increases the risk of cyber-attacks.

Important cyber security measures every individual, company, business or e-commerce websites should practice are:

1. Firewalls
2. Anti-virus software
3. Intrusion detection system
4. Prevention systems
5. Encryption
6. Login passwords

6 IMPORTANCE OF CYBER SECURITY FOR BUSINESS

Cyber-attacks on business leads to attacks on customers. When a consumer does business with a company or vice versa, a lot of information and data is being exchanged and breach of such information can be harmful for both parties. It is of utmost importance to adopt ways of securing your business. If the hackers are able to access a marketing database, they may only need a person's email to use phishing techniques to trick one into providing more sensitive information. One might think they are communicating with a reputable business, but in reality they might be communicating with hackers who may steal or miss use their information.

Once a business is under cyber-attack there is no limitation to the amount of damage it can bring to the business and its consumers as all the information regarding its client data, products, specification, etc. would be at risk. Consumers and businesses both should be careful and should learn techniques to protect themselves from cyber threats and be very vigilant whenever interacting with suspicious email or online communication.

7 HOW TO AVOID BREACH OF CYBER SECURITY

Businesses should map IT assets to business strategy and adopt proactive cyber security programs. Data breaches can occur due to many reasons and it is always better to prevent than to cure. Businesses should adopt ways to prevent data security breaches as such:

i. Transfer of data from official devices to personal devices of employees or other external devices must be banned. Sensitive information must be protected whenever it is stored, sent or used.
ii. Software should be kept updated.
iii. Keep backup of all the information. The best possible way to prevent data is to back up regularly. Cloud based services such as Google Drive and One Drive can be utilized as a hard drive. Cloud based programs update and backup automatically.
iv. Restrict downloads. Any media that may serve as an allegiance to the hackers should be restricted to download.

v. Shred all the files and folders before disposing a storage equipment like a computer, laptop, external hard drives, etc. as there are applications that can retrieve information after formatting.
vi. Unencrypted devices should be banned. Laptops and other portable devices that are unencrypted are more prone to cyber-attacks.
vii. Use complex passwords that are unpredictable, hard to crack and keep changing them from time to time.
viii. Must use automotive security systems that regularly check the password settings, server and firewall configuration to reduce risk of losing sensitive information.
ix. Security team should have updated software that should be able to identify suspicious network activities and be prepared if the network is under cyber-attack.
x. Data within the organizational network should be tracked.
xi. Accessibility to data should be defined for those who are working on company's sensitive data and information.
xii. Privacy and security trainings should be given to all employees, clients and others related to data related activities.
xiii. Management, production and security solutions must be combined to prevent the targeted attacks.
xiv. Business should have a pre planed breach response in order to trigger quick responses to data breaches which will help in reduction of harm. The plan can contain notification of the concerned staff or the agency who could contain the breach.
xv. Cyber security teams have to be particularly vigilant that all user input specially the credit/debit card details, contact information, addresses, passwords or any other personal information provided is firmly protected.
xvi. Employees must be bound through written agreements to keep the confidential information protected.
xvii. Not all employees in an organization need the same level of access. Limiting the access to information to those who do not need it, greatly increases cyber security.
xviii. Businesses should regularly and actively challenge IT information security personals on information risk and its business impacts and also make sure to invest time to listen to them, comprehend and discuss the technology solutions that can solve the problem.

8 CYBER SECURITY AWARENESS

Cyber security awareness and education is important not only for the IT professionals in an organization/business but for all employees at every level starting from general rank up to the higher management. Start by raising awareness across the organization because people are an organization's biggest asset and also potentially its biggest risk. How these people take decisions and behave in key moments is essential to strengthening resilience.

Security awareness and changing employee comportment can definitely reduce the risk of a breach. Employees need to be made aware of the consequences one can face if they are targeted by hackers or an employee does any act that breaches cyber security of a business. Knowing the risks and damages associated with breach of cyber security will increase the

willingness of employees to take measures to prevent it. Some ways to create cyber security are as such:

i. Invest in awareness programs to educate employees on how to effectively deal with common threats from social media or phishing in order to save confidential data and information.
ii. Internal marketing materials such as posters and company-wide emails reminding employees of key security practices.
iii. Deploy phishing simulators to both raise awareness and track programs.
iv. Deploy up to date training programs and make them mandatory for employees to revisit to keep them updated and also to serve as a reminder for best practices.
v. Businesses can reward good security behavior as an encouragement for the employees and have strategies to address behavior requiring improvement.
vi. Employees should be made aware and be trained to communicate information risk as a business risk by treating it as something more than a technical issue and assess it in the context of customer services, public relation and business reputation.
vii. Businesses should also make the employees be aware of the punishable offences defined under the Prevention of Electronic Crimes 2016, Pakistan. Details of these offences may also be displayed on their websites and offices to discourage hackers. A list of these offences is given in Paragraph No. 11 of this document.
viii. Beyond technical processes and procedures, security professionals in an organization should be familiar with the latest legislation and regulations that companies have to abide by with a clear understanding of the various governance frameworks. Some of these offences are as such:
ix. **Unauthorized use of identity information:** whoever obtains, sells, possesses, transmits or uses another person's identity information without authorization shall be punished with imprisonment or with fine or with both.
x. **Unauthorized issuance of SIM cards, etc.:** whoever sells or otherwise provides subscriber identity module (SIM) card or any other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices without obtaining and verification of the subscriber's antecedences in the mode and manger from the time being approved by the relevant authority shall be punished with imprisonment or with fine or with both.
xi. **Tampering of communication equipment:** whoever unlawfully or without authorization changes, alters, tampers with or re-programs unique device identifier of any communication equipment including a cellular or wireless handset and starts using or marketing such device for transmitting and receiving information shall be punished with imprisonment or with fine or with both.
xii. **Retention of traffic data:** service provider shall within its existing or required technical capability, retain its specific traffic data for a minimum period of one year or such period as the relevant authority may notify from time to time and subject to production of a warrant issued by the court provide that data to the investigation agency or the authorized officer whenever so required.
xiii. **Limitation of liability of service providers:** no service provider shall be subject to any civil or criminal liability, unless it is established that the service provider had

specific actual knowledge and willful intent to proactively and positively participate and not merely through omission or failure to act and thereby facilitate or aid the use by any person of any information system, service, application, online platform or telecommunication system maintained, controlled or managed by the service provider.

xiv. **Confidentiality of information:** a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law or an unauthorized officer who has secured access to any material or data containing personal information about another person , discloses such material to another person, except when required by the law, without consent of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to harm, wrongful loss or gain to any person or compromise confidentiality of such material shall be punished with imprisonment or with fine or with both.

xv. **Spamming:** whoever with the intent to transmit harmful, fraudulent, misleading, illegal or unsolicited information without permission or shows any information for wrongful gain will be punished with imprisonment or with fine or with both Organizations engaged in direct marketing shall provide the option to the recipient of direct marketing to unsubscribe from such marketing.

xvi. **Making, obtaining or supplying device for use in offence:** whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device, with the intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence, without prejudice to any other liability that he may incur in this behalf be punished with imprisonment or with fine or with both.

xvii. Unlawful online content i.e., a content that is against the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, public order, morality, or in relation to contempt of court or commission of or incitement to an offence under the Electronic Crimes Act, 2016.

9 CYBER SECURITY STRATEGY AND RISK ANALYSIS FOR BUSINESS

Cyber-attacks are no longer single events but a combination of social engineering and technical skills to penetrate in a network and gain access to important assets. Therefore, there is no single solution to prevent cyber-attacks. Individual businesses should have an overall cyber security strategy focused on cyber resilience which can be derived by a threat led approach that focuses on the key assets of that particular business and motivation and capabilities of most likely attackers. This strategy may vary from business to business depending on its nature. However, some key principles that need to be taken care by every business while drafting such strategy are:

i. The first step for doing a threat and risk analysis is to identify and establish what information can be the likely target of a cyber-attack. Cyber attackers usually have a specific intent to access data that holds interest to them. Therefore, the value of this identified information is relative to the motivation of the attackers.

ii. Once the key assets are established, the need is to determine where it is stored and who has access to it because the more people having access to the information the greater the potential risks for a cyber-attack. IT staff usually have access to all data on the network. Cyber resilience requires the business / organization to have the ability to detect and diminish threats but also to be able to monitor and respond to successful cyber-attacks.

iii. The next step is to determine the controls that already exist to prevent, detect and respond to these threats. IT staff and information security officials need to be involved to compare these controls against the capabilities and methods likely to be used by the hackers. This will help identify vulnerabilities that exist in the organization's processes controls such as lack of staff awareness training, weak back up process, no off-site storage or excess permissions to data access, etc.

This whole exercise will help in developing a list of recommendations that a business can look into to address the vulnerabilities to better prepare for the attacks that they are most likely to face. These recommendations will also form a basis for a cyber-security framework specifically tailored for that particular business and can be used to plan the cyber resilience strategy.

10 E-COMMERCE AND CYBER SECURITY

Online commerce is a massive business and is growing larger day by day. However, lack of consumer confidence is also a growing concern for online merchants. Whether it is a small, medium or large business, everyone can fall as a prey to hackers. When it comes to protecting your business against such cyber-attacks specially business dealing with e-commerce, it is important to make sure your employees are educated on the most common types of attacks. Employees with such know how and training can take further steps to protect their customers' private date and ensure safe business transactions. To avoid falling victim to cyber-attacks companies' can protect their online brands by practicing the following:

i. Use a secure e-commerce platform that supports sophisticated object oriented programming languages.

ii. Use a secure connection for online checkout. If a strong secure sockets layer (SSL) authentication for the website and data protection is used then no third-party will be able to intrude due to the encryption. HTTPS should be a must to ensure security of all e-commerce transactions. This also helps increase customer's trust in the company's website.

iii. E-commerce websites should ask customers for a mix of special characters, numbers and symbols as passwords to make accounts on their websites, as once the account is made it's the company's responsibility to protect its customer's information. Complex and longer passwords make it difficult for hackers to crack.

iv. Awareness against social engineering scams must be given to the consumers through conspicuous banners placed on the website. Remember, social engineering scams involve emails or any sort of communication that raises fear or similar emotion in the

victim and tricks them to promptly reveal sensitive information or open a malicious link or file.

v. To keep online business safe it is best to layer your security, starting with firewalls that basically are essential for stopping attackers even before they are able to breach your network and gain access to sensitive information. Contact forms, login boxes, search queries, etc., can also be added to websites to ensure that your e-commerce portal is protected against application level-attacks.

vi. For e-commerce sites where the software is developed in-house it is important to reduce bugs and vulnerabilities at the coding level. Where an external software is used, cyber security professionals are responsible for validating the vendor and for ensuring privacy.

vii. If the server and application level functions of e-commerce sites are outsourced to cloud service providers, then the security analysts need to work closely with the cloud provider team and be particular of what aspects of security can be outsourced safely and which need to be done in-house.

11 LEGAL PROTECTIONS FOR CYBER SECURITY AVAILABLE IN PAKISTAN

When we think of the kinds of criminals infractions that could earn you a lifetime behind bars, cybercrimes is probably not something that comes to your mind. However, cybercrime is a serious offense and people who commit it should not be left unpunished. As the targeted individual or organization has to face damages of various kinds, therefore, it is essential for the hacker or cybercriminal to pay for their actions too. Punishment serves as a dual purpose, as it holds the criminal accountable and also deters others from making the same mistakes.

A cyber security regulation comprises of directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and information from cyber-attacks. If your cyber security has been breached by anyone in any manner you will have the right to approach the relevant forum under the Electronic Crimes Act, 2016.

You can visit the following link to view the list of cybercrimes and their punishments in Pakistan; https://propakistani.pk/2016/08/05/must-read-list-of-cyber-crimes-and-their-punishments-in-pakistan/.

As per the law of Prevention of Electronic Crimes Act 2016 (Pakistan), which can be viewed on the following link: http://www.na.gov.pk/uploads/documents/1470910659_707.pdf, some of the punishable offences are as such:

i. Unauthorized interference, access, copying or transmission of information system or data.

ii. Unauthorized access, copying or transmission of critical infrastructure information system or data.

iii. Electronic forgery and fraud i.e., interference or use of any information system or data to cause damage or injury to any person or public.

iv. Cyber stalking with an intent to coerce or intimidate or harass any person.

v. Spoofing – if with a dishonest intent one establishes a website or sends any information with counterfeit source intended to be believed by the recipient or visitor of the website to be authentic source.

vi. Unlawful online content i.e., a content that is against the glory of Islam or the integrity, security or defense of Pakistan or any part thereof, public order, morality, or in relation to contempt of court or commission of or incitement to an offence under the Electronic Crimes Act, 2016.