الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

QDB
بنك قطر للتنمية
Qatar Development Bank

Cyber security Manual for SMEs

Providing practical guidance in recognizing cyber security risks faced by SMEs and offering actionable advice to safeguard their businesses

Version 1.0
June 2024
Public

Table of Content

Disclaimer / Legal Rights

Qatar Development Bank (QDB) and National Cyber Security Agency (NCSA) has designed and created this publication, titled "Cyber Security Manual", in order to help small & medium enterprises understand cyber security risks in the digital realm, and mitigate these risks by applying the fundamental requirements identified in this document.

QDB and NCSA are responsible for the review and maintenance of this document. Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge QDB and NCSA as the source and owner of the Cyber security Manual for SMEs.

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from QDB & NCSA. QDB & NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from QDB & NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

Introduction

1.1. Context

With digital information and technology now so heavily integrated into day-to-day work and the vast amount of information stored digitally and on networked systems, organizations have become more vulnerable to cyberattacks. The attacks, which target information and infrastructure, are also becoming far more sophisticated.

Cyberattacks can take many forms. Some attacks target legitimate users by tricking them into taking actions that open the door for unauthorized users. Other attacks target your applications by overwhelming them to cause a temporary shutdown or slowdown. Some attacks target your password-related account, like your business email, to gain access to confidential systems or data. Attacks can also infect your organization's systems and restrict your ability to access your applications and information until a ransom is paid to the attacker.

The impact of cyberattacks on small and medium-sized enterprises (SMEs) can be severe. It can result in operational disruptions that may cause downtime or the loss of critical data and information. This can lead to delays and missed business opportunities. Furthermore, the disruption caused by cyberattacks can have a ripple effect and significantly affect the ability of your organization to meet customer demands and deliver orders on time.

Attackers target organizations with security weaknesses regardless of their size, shape, or industry. Cybercriminals often perceive small businesses as having weaker defenses than larger organizations, making them easy targets with potentially higher rewards.

As cyberattacks targeting SMEs are on the rise, it is crucial for business owners and managers to ensure that they are properly prepared. Simply by relying on out-of-the-box cyber security solutions such as antivirus software is no longer sufficient, since cyber criminals are getting smarter, the attack surface is increasing, malicious tools are readily available, and their attacks are becoming more resilient to conventional cyber defenses. Implementing appropriate cyber security measures is essential for SMEs to safeguard their business and protect their customers' data. Cyber security measures can be in form of deploying people, policies, processes, and technologies to protect your organization, systems, and information from digital attacks. In light of these threats, Qatar Development Bank (QDB) along with National Cyber Security Agency (NCSA) has developed this Cyber Security Manual for SMEs as a minimum requirement to secure their businesses from cyberattacks.

Introduction

About Qatar Development Bank (QDB)

Qatar Development Bank (QDB) was established in 1997 as Qatar Industrial Development Bank, a 100% government-owned financial institution. Its primary aim was to develop investments within local industries, thereby accelerating growth and economic diversification in Qatar through support for the private sector.

QDB has achieved significant milestones in recent years, playing a chief role in growing Qatar's private sector. QDB has also played an integral role in stimulating national economic and social development, through funding a variety of local projects and providing support to the private sector through a range of innovative services. By adopting this strategy, QDB has contributed to empowering and enabling Qatari entrepreneurs to benefit from a wide range of promising investment opportunities and to develop their exporting potential while supporting their entry to new international markets.

QDB's strategy is entirely in line with the Qatar National Vision 2030. It is focused on promoting and facilitating the growth of the private sector in key economic sectors, with the aim of building a diversified, sustainable economy.

QDB aims to promote an anentrepreneurship spirit within the private sector in Qatar through providing the necessary services that shall ease the growth, development, and diversification of this sector. In doing so, QDB offers access to information, incubation, and capabilities to SMEs, in addition to access to capital through direct and indirect financial services, investment and access to local and international markets for Qatari exporters though export insurance and funding services.

PURPOSE, SCOPE, USAGE & AUTHORITY

2.1. Purpose

To help SMEs build a functional cyber security system and guide them in building their knowledge and capabilities, thus strengthening the overall cyber security maturity in Qatar.

2.2. Scope

The fundamental cyber security requirements outlined in this document apply to all SMEs and their corresponding information assets.

This guide is designed to help citizens and residents of Qatar who own or manage a small or medium business understand the cyber security risks they face and provide them with practical advice on how to protect their business and employees from cybercrime.

In other words, if you are a small or medium business owner, this guide is for you. Cyber security is a shared responsibility, and depending on how your business is structured, there are likely other people — co-owners, managers, or employees — who should also be familiar with the information you'll find in this guide.

2.3. Usage

This document is designed to be used by SME business owners to understand the minimum cyber security requirements they need to apply to their businesses. The minimum requirements have been segregated in two sections namely Process controls and Technical Controls.

You do not need to be a computer or Web expert to read or implement the measures in this guide. Although some cyber security terms are used, you can look up any terms you are unfamiliar with in the glossary at the end of this guide or online.

To apply the requirements in this document, you may also take assistance of the accompanying guidelines that will be published with this document.

Definitions

3.1. Key Definitions

QDB	Qatar Development Bank.
SMEs	Small and Medium Enterprises as per the QDB's national definition for SMEs.
Organization	In this document, whenever "Organization" is mentioned, it refers to an SME operating within the State of Qatar unless otherwise specified.
NCSA	National Cyber security Agency – State of Qatar.
NIAS	National Information Assurance Standard.

3.2. Glossary

Term	Definition
Applicable	Relevant; appropriate; adequate; possible to apply.
Appropriate	This term indicates suitable measures in the case of the SME.
Can	The modal verb shall entail possibility or capability.
Cloud Adoption	The process of moving to or implementing cloud computing in an organization.
Cloud Zero-Trust model	No one is trusted by default from inside or outside the network. Zero Trust requires that every transaction between systems (user identity, device, network, and applications) be validated and proven trustworthy before the transaction can occur.
Cyber security	The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.
Data Encryption	The method by which information is converted into a different form that hides the information's true meaning.
DDoS (distributed denial-of-service) attack	An attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic to force it to shut down and deny service to legitimate users.

Definitions

Term	Definition
Firewall	A software or a hardware device that monitors and controls the flow of data between networks. Acts as a security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside.
May	The modal verb shall entail permission.
Media Sanitization	A process through which data is deliberately, irreversibly removed from media by destroying the data stored on a memory device to make it unrecoverable.
MFA (Multi-Factor Authentication)	A multi-step account login process that requires users to enter more information than just a password, like a code sent through email or answering a secret question.
Must	The modal verb shall entail requirement.
OWASP top 10	OWASP top 10 A regularly updated report outlining security concerns for web application security, focusing on the 10 most critical risks.
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, which they may then use to commit fraudulent acts.
Ransomware attack	A type of malware that locks and encrypts a victim's data, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment.
Shall	The modal verb shall entail requirement.
Should	The modal verb should entail recommendation. Ignoring the recommendation could result in undesirable results.
Virtual Private Net work (VPN)	An encrypted connection over the Internet from a device to a network. VPN communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the VPN.
Web Application Firewall	A software or a device that protects web applications from a variety of application layer attacks such as cross-site scripting (XSS), SQL injection, and cookie poisoning, among others.

Risks and Threats

Understanding the cyber security threat landscape and its risks is vital for all SMEs in their journey towards enhancing the organization's security posture. One of the early steps is to inform yourself of the common types of cyber security threats out there and to establish how to protect your company against them.

Cyber security threats are acts performed by individuals that can damage or cause disruption to systems. Usually, these are done with harmful intent, and originate from different sources, like cybercriminals, hackers, and malicious insiders.

Vulnerability by definition is a weakness in a system, such as a missing patch, a bug, or a faulty hardware.

Cyber security risk is the likelihood and potential of a threat being able to exploit a vulnerability in the system and leading to harmful consequences such as financial loss, reputational damage, or operational disruption for the SME, which could result in significant costs.

4.1. Cyber security threats encompass various forms of attacks, such as:

Phishing attack:

Phishing is a common cyberattack that targets individuals through various forms of communication, such as email, text messages, and phone calls. Phishing attacks occur when an attacker poses as a trusted entity and tricks the victim into opening an email, instant message, or text message. The victim is then deceived by clicking a malicious link. This could lead to installing malware, freezing the system as part of a ransomware attack, or exposing sensitive user information such as account numbers, credit card numbers, passwords, or birth dates.

A phishing attack can result in a direct financial loss, such as paying invoices to a fraudster posing as a legitimate vendor or an illegitimate use of your credit card that is stolen because of the attack. Ransomware attacks, which may have more severe financial risks, often use phishing attacks as the delivery method.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:

A denial of service attack (DoS) is the process of flooding the target with many requests, consuming its capacity, and rendering it unable to respond to legitimate requests. If successful, a DoS attack prevents people from accessing online services (e.g. email, websites, online accounts), information, and other network resources.

A distributed DoS (DDoS) attack has the same goal of disrupting and preventing access to services and information, as a DoS, but it looks a bit different. To carry out a DDoS, the attacker uses multiple machines to attack one target. While a DDoS attack can be a coordinated effort between a group of attackers, it can also be carried out by one person.

Risks and Threats

The risk of the DoS and DDoS attacks is the financial loss associated with your online services being no longer available or the decreased productivity of your company resulting from losing access to or slow access to your resources. This attack can also result in undermining public confidence in your brand.

Malicious software (Malware) attack:

Malware is a blanket term used for malicious software designed to cause harm, such as ransomware, viruses, spyware and trojans. Malware can:

- steal or lock the files on your device
- steal your bank or credit card numbers
- steal your usernames and passwords
- take control of or spy on your computer

Malware can stop your device from working properly, delete or corrupt your files, or allow others to access your personal or business information. If your device is infected with malware, you could be vulnerable to other attacks. The malware could also spread to other devices on your network.

Ransomware attack:

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cyber-criminals might also threaten to publish or sell data online unless the victim pays the ransom.

Ransomware is a common threat to any business, large or small. The risk of ransomware is that it can put a company out of business or disrupt operations for an extended period of time. Nearly all ransomware victims will face financial losses, data losses, and reputational damage. If customer data is stolen, it may also lead to regulatory repercussions.

Paying the ransom is not really an option, because there is no guarantee that the attackers will ever send you the decryption key to recover the data. Also, paying the ransom does not actually remove the malware from oyour network. Lastly, dealing in crypto currency is not yet legal in Qatar.

Fundamental Security Requirements – Process Controls

5.1. Know your information systems and assets

You shall list the information systems and assets you use to operate your business.

Information systems and assets in this context refer to all computers, servers, network devices, mobile devices, information systems, applications, services, cloud applications, and the data and information, that an SME uses to conduct its business.

The information systems and assets shall be the scope of your implementation of the following fundamental security requirements: If any systems or assets are to be excluded from the fundamental security requirements, the SME shall provide the rationale behind this exclusion.

5.2. Identify the data classification of the assets

Information is the lifeblood of any organization; it is often the most valuable of an organization's intangible assets. As an organization, you must know where this information resides, what applications and networks store and process that information and build security into and around these. Cyber security is about protecting your information. It is based on three fundamental goals / criteria:

Confidentiality: What is the effect of an unauthorized disclosure of sensitive information (e.g., if someone discloses sensitive information publicly or to a competitor)? Sensitive information can be any information that you do not want unauthorized individuals to see because of the financial, security, legal, or privacy impact that could occur.

Integrity: What is the effect of an unauthorized modification of information (e.g., if someone modified sensitive information to be incorrect)?

Availability: What is the effect of information being either unavailable for use for a period or lost permanently (e.g., if someone took down an organization's website or deleted sensitive information)?

You shall classify and label all information assets and systems within the organization. You shall follow the classification and labeling schema described in the National Data Classification Policy. Implement the security requirements identified in this document to protect your organization.

Fundamental Security Requirements – Process Controls

5.3. Understand the importance of cyber security

Cyber security is everybody's responsibility. Your awareness (as a leader) of the business drives cyber security to be a significant part of your operational resilience strategy, which requires time and money. Your investment drives actions and activities that build and sustain a culture of cyber security.

All co-owners, managers and employees must do their best to follow cyber security policies, and help others in the organization.

You should assign a specific person as an information security owner to oversee the company's information security program. The Information Security Owner is the main contact point for cyber security-related decisions and directions. The information security owner should be familiar with information security and the SME's main systems and have support from the executive management.

You shall allocate an appropriate budget to cyber security. Determine how much of your organization's operations are dependent on IT. The budget allocated for cyber security is relative to the SME itself and can depend on the organization's size and needs. The budget can span various key areas: infrastructure, employee cyber security training, tools, third-party services, and responding proactively to diverse threats.

5.4. Raise the security awareness of your employees

Cyber security awareness is the level of understanding your employees have about cyber security best practices and cyber threats that their network, application, and organization face daily.

You must raise cyber security awareness by making users aware of the current cyber threats, the best practices relevant to the business, and helping them understand how to avoid the common mistakes and conduct their business securely. Such awareness must be conducted at regular intervals.

Further, new hires or onboarding training, which introduces employees to the skills and systems needed for their job functions, shall include basic cyber security elements.

You shall conduct yearly training to prepare employees for the changing business environment, covering updates to cyber security policies, strategies, and tactics to mitigate new threats.

Fundamental Security Requirements – Process Controls

5.5. Keep track of changes you make to your systems

Changes to your environment can be as simple as installing a new printer, or major change to your servers, or an emergency change to one of your IT applications.

You shall manage changes to your business environment, regardless of the size of the change to minimize the likelihood of disruptions, unauthorized alterations, and errors. To do this, you need to identify what you're changing, why you're making the change, and how it might affect your information security.

5.6. Develop a cyber incident response plan

An organization should always be ready and be able to respond promptly when faced with a cyber-attack or any other type of cyber security incident.

You shall create an incident response plan, a written document that can help your organization prepare for an incident, and respond adequately during and after the incident.

This plan will ensure your organization has the ability to detect, respond to, and recover from cyber incidents as quickly as possible, and thereby limit disruptions to internal services, clients, and partners, and reduce data loss and reputational damage.

A typical cyber incident response plans includes the following on a minimum:

- Defined procedures to detect, evaluate, and respond to incidents.
- Specify the roles and responsibilities of those involved in the response.
- Report all critical incidents to NCSA within two (2) hours of incident identification.

Cyber incidents can be reported to NCSA through the following channels:

- Email: ncsoc@ncsa.gov.qa
- NCSA Hotline at 16555 (24 x 7 service)

After recovering from an incident, you must conduct a root cause analysis, to understand why an incident occurred and take steps to remediate these causes and ensure that in future such things do not happen.

Fundamental Security Requirements – Technical Controls

6.1. Establish a basic perimeter defense.

Perimeter defense is protecting the boundaries of the organization's network to secure its data and resources from online threats. Examples of perimeter defense:

- Firewalls are software or hardware devices that monitor and control network data flow. A firewall is essential to defend your SME network from unauthorized external access.
- Wireless network: Your Wi-Fi network can be a target for cybercriminals. Ensure that your wireless network password is unique and robust. Enable network encryption, turn off network name broadcasting, and keep your router's software up-to-date.
- Virtual Private Network (VPN) is a secure connection between two points, such as your laptop and your organization's network. For cases where employees are permitted to connect remotely to the organization's network, set up a VPN connection. When connecting to your VPN network, the users shall use multi-factor authentication.

Devices like firewalls, routers, and VPNs must be used to protect your network from unauthorized online access and it must be configured accurately and securely. If such devices aren't properly configured or maintained, they can be exploited by threat actors, putting your data at risk of being compromised.

6.2. Improve physical security

It is crucial to understand that the cyber security measures implemented by your organization may not be entirely effective if you don't have appropriate physical security in place.

You shall secure physical spaces and assets with adequate controls to protect against theft, damage, or destruction. This includes securing and protecting servers, computers, routers, and other IT & network devices.

Fundamental Security Requirements – Technical Controls

6.3. Secure portable devices

A portable device in this context is any device (personal or official) accessing work files or data, be it a smart phone, tablet, laptop, USB drive, or any other memory device.

Using portable devices to send and receive your organization's information can expose your organization to the risk of sensitive information being viewed or used by people you have not authorized to do so. Allowing employees to use their organization-owned portable device for personal use, such as installing non-business apps, or vice versa allowing your employees to use their personal portable devices to access work related data, can sometimes expose your organization to the loss of sensitive information, malware, and other threats. Also, since most of these devices are small and/or valuable, they are at risk of being lost, stolen, and/or misplaced easily. Whether compromised through malware, misuse, loss, or theft, the impact on your organization may be significant, especially if the portable device contains sensitive information or communications tools for connection to your organization network. Portable devices can hold massive amounts of information on a tiny device. Your organization may even be able to store all of its electronic files on a portable storage device.

To address portable device security in your organization, you shall:

1. Examine the pros and cons of using portable devices in your organization.
2. Determine which types of portable devices will be allowed for use in the organization.
3. Decide whether personally owned portable devices can be used by employees for business purposes.
4. Integrate rules of use into your organization's cyber security policy.

Fundamental Security Requirements – Technical Controls

6.4. Update your systems and applications

Patches are software updates for applications and operating system (OS), that address security vulnerabilities within the application, product or the Operating System. Software vendors may also release updates to fix performance issues or provide better features and enhancements.

You must update your systems as soon as possible. One way to ensure your systems and applications are always up-to-date is by enabling automatic updates. Where possible, systems must be configured to download the updates as soon as they are available. However, where possible it is recommended to test the updates on a single system to ensure that they don't break any application or operating system feature.

You shall only use licensed software; since legitimate software is free from viruses and malware, manufacturers regularly send security updates.

6.5. Securely configure devices

Security misconfigurations, such as default administrative passwords and unsecured default settings on devices, are among the most common weaknesses that hackers look to exploit.

You must review & modify the default settings when installing a new device or software.

Accepting the default settings without reviewing them can create serious security issues and allow cyber attackers to gain access to your systems and your data easily.

You should consider adopting secure product configuration baseline, a set of minimum-security configurations required on the device to safeguard systems against cyber threats.

Fundamental Security Requirements – Technical Controls

6.6. Secure user accounts

The authority and access you grant employees, managers, and customers into your digital environment need limits, just as those set in the physical work environment do.

You shall provide each employee who uses electronic devices in an SME their login credentials, consisting of a username and a password. This credential must allow them to access resources or applications based on the concept of least privileges. All users' accounts shall be unique, identifiable, and attributed to individual users.

You should apply the least privileges principle and ensure that your employees should only have access to the specific data, resources, and applications needed to complete their tasks.

Employees who have supervisor or administrative privileges should have an administrative account separate from their standard account.

You shall create an appropriate password policy that balances security and usability.

Wherever possible you must use strong passwords and multi-factor authentication. Employees should be educated to avoid using passwords that can be guessed easily. Example using birthdates, names of family members or pets, simple numerical sequences such as 1234 etc.

6.7. Back up your data and encrypt the backups

Having a backup (a copy) of your organization's information is one step you can take to improve your organization's cyber security resilience. Suppose a cyber incident or attack compromises your networks, systems, or information. In that case, a backup enables your organization to reduce the risk of data loss, minimize downtime, and restore its essential services.

You shall regularly backup your organization's information to an external, secure location. How do you decide what information and applications to back up? Think about what is essential for your SME to run smoothly, and then regularly back up every file and application related to those processes.

You must have a process for restoring or recovering the data from your backups and these must be tested at regular intervals.

The backups should be encrypted to ensure that only authorized employees from your SME can access company files and information.

Fundamental Security Requirements – Technical Controls

6.8. Secure your online presence

Your online presence may include an e-commerce platform like an online shop, a customer web-facing application, or a social media platform.

You shall secure your websites and social media accounts.

Your website is a crucial tool for interacting with consumers, providing services, or selling products, and it establishes your digital identity. The best way to secure your website depends on its technical properties, the IT ecosystem in which it's managed, and where it's hosted.

Social media security refers to the measures organizations and individuals take to protect their social media accounts. If your organization uses social networking sites for marketing or professional purposes, you shall ensure that it is secured with strong passwords and multi factor authentication. Only designated employees should have access and the ability to post content in your official social media accounts.

6.9. Use cloud securely

Cloud computing delivers computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

You shall consider all aspects of cloud computing and assess the benefits and risks associated with the cloud solutions before adopting it. The Qatar government has made a strong push for Cloud adoption as part of its digital transformation vision and this is reflected through its Cloud First Policy.

You should strongly consider adopting a Government endorsed Cloud Service Provider.

Your team shall obtain the required skills to access and operate the cloud infrastructure and have to familiarize themselves with the cloud providers' security best practices.

Appendix

7.1. References

1	National Data Classification Policy v3.0, NCSA
2	2023 National Information Assurance Standard v2.1 , NCSA
3	CS Guidelines for Securing Social Media Accounts v3.0, NCSA
4	National Incident Management Framework, NCSA
5	Cloud First Policy, MCIT