وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Security Guidelines for Hotel Information Systems

Version: 1.0

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: July 2018

Document History			
Version	Date	Description	Comments
1.0	19 July 2018	Document Released	

Table of Contents

Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This guideline has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Introduction

Guests look at Hotels with a pseudo home feeling. They expect it to be comfortable, private and secure. Traditionally hotels have focused on these expectations. There is a considerable focus on physical security within the hotels, doors have lock (smart card based locks for additional comfort and security), and rooms have electronic safes with pin codes that can be set by the guest.

Guests expect that the same level of protection extend to their digital assets when they are connected to the Hotel's digital infrastructure i.e. LAN or Wireless LAN to access internet.

Hotels need to reassure their guests that Digital security is as important a priority as the physical security and that information provided by the guests (be it physical (paper format) or digital) will be secured against potential threats including cyber threats.

Objective

The objective of this guideline is to help businesses within the hospitality sector understand the potential information security risks they face and identify suitable controls to mitigate minimize or avoid such risks.

Scope and Audience

Businesses such as Hotels, Hotel Apartments, restaurants within Qatar.

Understand the Risks

As any business, the biggest risks for the hotel and leisure industry emanates from the biggest expectations from their guests i.e. Comfort, Privacy and Security. Although by the nature of its business, such organizations may be deemed non-critical, in effect such businesses are a trove of information that may be very attractive for the cyber criminals, hacktivists and state actors. Information held by such businesses include personal information such as details about passport, any other identity cards, credit cards, personal or business addresses, travel itineraries, personal likes and habits etc. A malicious actor can use such information to impersonate identity, mount social engineering or phishing attacks or commit financial frauds amongst other things. As such the business itself is at risk as they may become the focus of attack for such information.

The key risks that the businesses faces include:

1. Loss of personal data relating to guests, resulting in breaches of privacy law obligations and, potentially, individual loss claims.
2. Loss of confidential information, which may amount to a breach of contract and/or loss of commercial advantage.
3. Denial-of-service attacks, preventing the use of operational systems, including booking systems.

4. Financial fraud with customer credit card information, including bookings made using stolen identities.
5. Reputational damage caused as the consequence of any of these risks occurring
6. Third party risks related to loss of personal or confidential information due to criminals targeting sensitive data via third-party providers – e.g. room booking sites or car rental companies, which maintain information on guests.

Evolving Threats

The following are some of the leading threats faced by the hotel and leisure industry.

Phishing attacks: Phishing attacks is primarily a pre-step to a full blown targeted malicious attack towards an organization. The primary objective being to gain user credentials through social engineering techniques and infiltrate an agency's system to plant and launch advanced persistent threats.

WiFi-based attacks: Unless secured adequately, traditional WiFi systems are vulnerable and malicious actors (This could be insiders such as employees or hotel guests or external actors such as hackers, cyber criminals etc.) could use them to breach into corporate systems or fellow users.

Dark Hotel: A new variant is a targeted spear phishing and malware spreading attack dubbed as "**Dark Hotel**" DarkHotel (or Darkhotel). It selectively attacks business hotel visitors through the hotel's in-house Wi-Fi network. The attacks are specifically targeted at senior company executives, using forged digital certificates, generated by factoring the underlying weak public keys of real certificates, to convince victims that prompted software downloads are valid.

DDoS and botnet attacks: Distributed-denial-of-service attacks have grown in popularity to carry out a range of malware injection activities. Within such attacks, hackers utilize botnets of compromised networks to flood critical systems (e.g. online ticket booking) with traffic, which results in a crash of the platform. Attackers may also ask for a ransom amount from the authorities to prevent disruption of such critical systems.

Ransomware: These attacks have grown in popularity in the last few years and we have some real crippling attacks wherein the attackers gain access to the organizations system and encrypts the data. The businesses are then asked to pay a ransom to be able to get a key to decrypt the data.

Data Leakage: These are attacks where malicious actor gain access to your systems and stay there as much as possible and try to identify and exfiltrate critical data outside the organization. The data includes business data as well as guests information (personal / financial (credit cards) etc.)

Guidelines

Reliance on technology is increasing within the hospitality sector where image and competitive advantage matters significantly and the ultimate objective being to provide a comfortable and luxurious experience to the guests and visitors. Information systems can be a game changer in achieving this objective.

However, with the increased dependence on technology comes increased risks of information security breach (loss of confidentiality, integrity and availability of customer data). The Hospitality sector and

the entities within must observe information security hygiene and adequately protect their information systems and the underlying infrastructure.

As part of their duties, sensitize staff at all levels about handling customer data. Information security hygiene should become part of their duties.

Governance

Establishing leadership for the information security program within the organization is very important. All security standards such as the National Information Assurance Policy have duly emphasized it.

Each organizations should develop a comprehensive framework of Information Security and Privacy policies and procedures to effectively implement and manage the enterprise information security / privacy management system.

The framework must include a Corporate Information Security Policy (CISP)[1] outlining the organizations commitment to adopt information security / privacy practices within the business and to implement an effective management system to deliver the objectives. The Head of the organization must sign the policy.

A policy manual covering various processes and specific domain areas should complement the CISP.

Legislations

The management system and the associated policy manual should define controls in line with regulatory requirements. The regulatory requirements include local as well as international (where applicable) requirements.

Some of the key regulatory requirements include:

1. Adherence to National Information Assurance Policy (Qatar)
2. Adherence to Personal Information Privacy Protection Law (Qatar)
3. Adherence to Cyber Crime Law (Qatar)
4. Adherence to Electronic Commerce and Transaction Law
5. Adherence to GDPR if applicable

Privacy

Protection of Personal Information is a key regulatory requirement both locally as well as internationally. The regulation enshrines a number of rights to the individuals such as Right to be forgotten, Right to information, Need for consent etc. It is necessary that the systems be designed in line with the privacy regulatory requirements. Organizations should only collect data that is required for the business. A key strategy in effective Privacy Management is to ensure reduction in risk by reducing the amount of data that is collected, ensuring its usage based on the consent received and disposal of data as soon as the need (business as well as legal /regulatory) has been finished.

Cyber insurance

A data security breach is an incident in which the confidentiality, integrity or availability of data (often stored electronically) is compromised, such that the data is vulnerable to access or acquisition by

[1] A template for Corporate Information Security Policy is available on the Q-CERT website.

unauthorized persons. Hackers or malevolent individuals do not cause all data breaches; some are caused by individual carelessness, such as leaving an unsecured laptop somewhere and exposing the data to an unsecured environment. With personally identifiable information — such as QID numbers, financial account numbers or access credentials — the loss of confidentiality potentially can lead to identity theft, unauthorized credit or debit card charges, and bank account fraud. Organizations could experience direct and indirect losses, including fines and penalties imposed by the card associations. Companies may also face third-party liability in the form of lawsuits and claims, regulatory fines, and, in some cases, even civil and criminal penalties.

Cyber Insurance is not a line of defense, however in case of a breach, it can help organizations manage some of the liabilities at least from a financial perspective. This makes sense in a strong regulatory environment where organizations may be liable of disciplinary fines and / or costs related to breach notification.

Agencies should be careful and due diligence should be conducted, including involving business stakeholders such as Legal department while negotiating an appropriate Cyber insurance policy for the agency. All definitions and its interpretations by both the policy owner and the cyber insurance provider should be vetted by the legal department. Some of the factors to consider while choosing a cyber insurance cover are:

Type of Cover: Typically the policy should cover both first-party and third-party losses suffered as a result of a cybersecurity breach.

Scope of Coverage: The scope of coverage can be tailored to a variety of risk scenarios and should cover the following:

- **Asset Liability** covers digital assets replacement expense coverage, business incomes loss and dependent business income loss coverage, cyber extortion threat and reward payments coverage.
- **Network Security Liability** covers third-party damages resulting from a failure to protect against destruction, deletion, or corruption of a third party's electronic data. This could be the result of a denial of service attacks against websites or computers, or through the transmission of a virus from third-party computers and systems.
- **Privacy Liability** covers third-party damages that result from the disclosure of confidential information collected or handled by you, or that is under your custody or control. This includes coverage for vicarious liability where a vendor loses information you had entrusted to them.
- **Electronic Media Content Liability** covers personal injury, and trademark/copyright claims that arise from the creation and dissemination of electronic content.
- **Regulatory Defense and Penalties** covers costs arising from an alleged violation of privacy law caused by a security breach.
- **Network Extortion** provides reimbursement for payments made under duress in response to an extortion threat.
- **Network Business Interruption** provides reimbursement for your loss of income and extra expenses that result from an interruption or suspension of computer systems. This includes limits placed - dependent business interruption losses.
- **Breach Event Expenses** covers costs associated with privacy regulation compliance. This includes retaining a crisis management firm, outside counsel, legal costs, regulatory fines, breach notification or forensic investigators.

- **Data Asset Protection** covers recovery of costs and expenses that you may incur to restore, recreate, or recollect your data and other intangible assets.
- **Multimedia/Media liability** covers can include specific defacement of website and intellectual property rights infringement.
- **Extortion liability** covers losses due to a threat of extortion, professional fees related to dealing with the extortion.
- **Third-party claims**. This includes claims for damages brought by customers, consumers or outside business entities for damages, they incurred because of the insured company's breach of security, namely their losses from the inability to transact business, including punitive and exemplary damages, settlements and costs.

The above lists are not exhaustive; Carriers may offer additional coverage, especially for companies with specialized risks.

Time Limit: is defined as the duration for remediation coverage, the most common time period is one year after the breach.

Defining and Implementing Processes

Having established the necessary governance in place, a key step is to establish the right processes in place to implement an effective program.

The section below highlights some of the key processes that needs to be in place. Organizations are advised to review the National Information Assurance Policy V2.0 and any regulations issued by the local or international regulators and any other sector specific best practices such as the one issued by IATA.

Information Asset Classification and Labelling

1. Create an inventory of all information assets across the business.
2. Evaluate the aggregate Security Value of the Information asset using an Information Asset Classification Model[2]
3. Evaluate the Data Privacy Impact Assessment to ascertain if the Information asset has any Personal Identifiable Information (PII).
4. Label the information asset based on the Confidentiality and Privacy ratings of the asset.
5. The labels should be clear, unambiguous and visible.
6. For electronic data, it is also recommended to use meta tags or machine readable formats.

Change Management

1. Define and implement a Change Management process in line with the NIA Policy[3].
2. Establish a Change Management Board (CMB) or Change Advisory Board (CAB) to review and approve any changes to the system.
3. The CMB / CAB should draw its members from the business verticals, IT Department, Information Security Head, Business Continuity Head and any other members as may be required.
4. The CMB / CAB should approve all the changes.

[2] National Information Assurance Policy also proposes an Information Asset Classification Model.
[3] Templates for Change Management Process maps. Change management forms are available on Q-CERT website.

5. Define an Emergency approval process to carry out any emergency changes, if any are required. This may involve verbal approvals, direct approval from a senior management etc.
6. Notwithstanding, all changes (including emergency changes) should be documented in the system.
7. Any change requests should include a rollback process in case if the proposed change is not successful.
8. The process should include regular reviews to ensure that the executed changes have achieved their objectives and are performing well, as well as rolling back changes that were temporary in nature.

System Acceptance and Commissioning

1. Define a process to validate any new system (software / hardware) introduced into the business network.
2. The validation process on a minimum should include:
    a. The business justification and the need for the information asset within the business network.
    b. The information asset classification and labeling of the information asset.
    c. A minimum baseline security assessment that includes:
        i. A check to confirm that standard security controls such as end-point protection, hardening etc. have been implemented.
        ii. A vulnerability assessment exercise or a penetration testing exercise for critical and public (internet) facing systems to identify any known vulnerabilities.
        iii. An execution plan to either eliminate or mitigate the identified vulnerabilities in line with the risk appetite of the organization.
3. Update the Asset Inventory list after the system has been commissioned.
4. Update the System monitoring solution to collect and monitor security event from the commissioned device.

Logging and Monitoring

1. Define and implement a Logging and Monitoring process in line with the NIA Policy[4].
2. Configure all information assets to log critical system and security logs. Organizations should ensure that adequate events are logged necessary to identify and assist in investigation of security incidents.[5]
3. Maintain logs for a minimum of 120 day in line with Cyber Crime Law.
4. Monitor the security logs on a 24x7 basis, at least for the critical systems.
5. It is recommended to correlate logs from various systems be co-related to get a holistic view of the operations.

[4] NIA Policy provides controls to enable Logging and Monitoring.
[5] "Guidelines for Incident Management – Pre-requisite Measures also provides additional system specific guidance.

6. The Logging and Monitoring process should work closely with the Incident Management process and the logging and monitoring system should be able to route incidents identified through the system for incident response.

Security Awareness

1. Define and implement an information security awareness program for the employees and contractors that work within your organization.
2. Ensure that security awareness programs are conducted at regular intervals through the use of various mediums.
3. On a minimum the security awareness program should include:
    a. Organizations internal security policies and procedures.
    b. Legal and regulatory requirements
    c. Acceptable usage of information processing facilities and information assets.
    d. Information on enforcement and disciplinary process.
    e. Information on reporting security incidents.
    f. Information on who to contact for security incidents.

Incident Reporting and Management

1. Define and implement an incident management process in line with the NIA Policy.
2. Establish mechanisms for users and employees to report information security incidents in a responsible manner.
3. Define a SLA (internal and external) for responding and closing all reported incidents.
4. The information security program should require reporting of all cyber security incidents to Q-CERT and Qatar Tourism Authority (if applicable).
5. Report any cyber-attacks / incidents ASAP, or within two days of its discovery.

Data Breach Notification

1. Regulations especially in the realm of privacy make it mandatory to inform the data subjects in case of a breach of their personal information with the organization.
2. Define a procedure to notify data subjects upon discovery of a data breach incident.
3. The procedure should ensure that:
    a. The process integrates with the corporate Incident Management / Crisis Management processes.
    b. Regulations may dictate the period upon breach discovery, within which to carry out such a notification.
    c. The organization has an inventory of data subjects whose personal information exists within the organizations business data.
    d. The organization identifies appropriate communication mediums and tools for notification to data subjects in case of an identified data breach incident.

Business Continuity and Resilience

1. Considering that Qatar is focusing to be a tourism and sports destination, Hotel industry is an important sector for Qatar and organizations should ensure that the business is designed to be resilient in the face of natural / man-made calamities, technological disasters and / or accidents.

2. Assign a person to own and manage the Business Continuity program and the associated Business Continuity Management System.
3. Develop a comprehensive Business Continuity Plan (BCP)[6] covering all the critical systems.
4. The BCP should adequately cover the People (Most Important), Processes and Technology.
5. Design critical systems to be fault tolerant and resilient.
6. Test the BCP at regular intervals including live tests and failovers to ensure that the BCP will work in case of a disaster.

Technical Controls

Section A: General IT Controls

System and Network Design

Organizations should ensure that security is imbibed in the architecture (Systems and Networks) by design rather than add-ons put in to mitigate design flaws. On a minimum, consider the following factors:

1. Segmentation: Segregate information assets in different segments (security zones) based on their sensitivity.
2. Access Surface: Access to information assets should be restricted to limited and regulated communication channels only. Further, only make available information that is required. Hide all other information as much as possible reinforcing the concept of "Security by Obscurity".
3. Defense in Depth: Protect the Information asset at multiple levels and points using multiple techniques and technology. The security of the system should be assessed against the least secured asset in the system (weakest link).
4. Adequate Protection: The security controls chosen should be adequate and appropriate based on the Risk profile of the organization and the risk to the asset itself as well as the value of the asset itself.
5. Least Privilege / Need to Know: Access to the information assets should be carefully controlled and restricted based on the concepts of least privilege or a Need to Know basis. Special attention should be placed on Administrative or Privileged accounts.
6. Privacy By Design: Protection of Personal Information is a key regulatory requirement both locally as well as internationally. The regulation enshrines a number of rights to the individuals such as Right to be forgotten, Right to information, Need for consent etc. It is necessary that the systems be designed in line with the privacy regulatory requirements.
7. Availability: Protect against single point of failures, using redundant elements and high availability concepts.

System and Network Security

The NIA Policy covers in depth controls for system and network security. The section below reprises the most important ones:

1. Configuration:
    a. Secure the configuration of all network and security devices.

[6] Refer to National Information Assurance Policy V2.0 and Industry Standards such as ISO 22301 for additional guidance.

   b. A copy of updated and tested configuration should be stored in a secure location to be used in case of a disaster.
2. Firewalls / Proxy Servers:
   a. Use Firewalls to compartmentalize the systems as per different security zones.
   b. Use an appropriate firewall to regulate traffic (application / packets / protocols / ports) based on the OSI Network model.
   c. Configure the firewall with appropriate and granular rules.
   d. Route any traffic from internet through a proxy server.
3. Clock Synchronization:
   a. Configure a Network Time Server to synchronize all devices on the network to the same time source.
4. Wireless Security
   a. Maintain an inventory of Wireless Access Points. Monitor, detect and remove rogue wireless access points.
   b. Configure the system to use adequate authentication and encryption.
   c. Use firewall / routers to segregate the networks. Use different SSIDs and different configurations for networks of varying security zones.
   d. Also, refer to our Cyber Security Guidelines for Securing Home and Small Office Routers[7] for your routers and access points setup recommendations.
5. DNS
   a. Use separate Domain Name Servers for resolving internal and external addresses.
   b. Zones files are digitally signed, and cryptographic mutual authentication and data integrity of zone transfers and dynamic updates is provided. Cryptographic origin authentication and integrity assurance of DNS data is provided.
6. VPN
   a. Any remote connections to the business systems should be through a VPN.
   b. Connections to business critical systems should be through a VPN, even when connecting through business wireless systems.
   c. Treat the traffic from a VPN connection in the same way as business traffic and filter them through the same checks (monitoring and control).
7. System Hardening
   a. All systems should conform to a minimum baseline posture. On a minimum these should include:
      i. Application of all known security patches.
      ii. Disable all unwanted services and uninstall all unwanted applications.
      iii. Enable necessary logs for audit and system and security monitoring[8].
      iv. Install endpoint protection program e.g. Anti-Malicious software, HIDS, Application Firewall etc.
      v. A Vulnerability assessment (esp. for servers) to identify known vulnerabilities.
   b. The organization should define Hardening Profiles for the various systems it uses based on the security requirements.

[7] http://www.qcert.org/sites/default/files/public/documents/cs-csps_guidelines_home_office_routers_en_v1.0.pdf
[8] Refer to Guidelines to Incident Management – Pre-requisite Measures

c. Ensure protection against DDOS attacks. The Cyber Security Guidelines for Distributed Denial of Service[9] (DDoS) Attacks provides guidance and recommendations for the same.

8. Endpoint Security
    a. Register each endpoint in the Information Asset register.
    b. Install a tested Anti-Malicious program on all systems.
    c. Log, monitor and address alerts from the endpoint security system.
    d. Configure Host based Intrusion Detection Systems (HIDS) and / or Application Firewalls on servers.
    e. Evaluate and install Data Leakage Protection solutions for endpoints that have access to business critical data and / or PII data of your customers / employees.
9. Privacy By Design
    a. For every new information asset introduced into the system:
        i. Update the Information Asset Register.
        ii. Identify the PII that it creates, processes or stores.
        iii. Conduct a Data Privacy Impact Assessment (DPIA) to identify the criticality of the data and the potential security controls to secure the PII.

Product Security

The NIA Policy covers in depth controls for product security. The section below reprises the most important ones:

1. Any product chosen to solve a business problem or meet a business requirement should:
    a. Be supported by a vendor of good standing and commitment.
    b. Be selected through an independent and unbiased process of vendor / product selection.
    c. Be independently tested to ensure that it meets all the business and security requirements of the business.
2. A minimum-security assurance levels is assured for products chosen for critical business functions.
3. Ensure that the products do not contain any hardcoded usernames and passwords. All default passwords should be changed prior use in business networks.

Software Security

The NIA Policy covers in depth controls for software security. The section below reprises the most important ones:

1. Adhere to and imbibe security controls within the software development cycle (SDLC).
2. Secure SDLC include BSIMM and OSAMM methodology amongst others.
3. Test the security of any software deployed in business networks. Testing includes Vulnerability Testing, Penetration Testing, Code Reviews etc. Perform code reviews for the most critical applications. For critical and / or internet facing applications the testing should be carried out at regular intervals (at least on a semi-annual basis).

[9] http://www.qcert.org/sites/default/files/public/documents/cs-csps_cs_guidelines_ddos_attacks__eng_v1.0.pdf

4. Review and adhere to the guidelines provided by MoTC[10], if the organization intends to use Open Source Software.

Cloud Security

The Cloud Security Policy[11] covers in depth controls for software security. Further, the Data Location advisory[12] provides additional guidance on using CSPs located outside Qatar.

1. Organizations should host critical business data inside Qatar (to the extent possible) or in countries that have friendly (political) relations with and regulatory regimes similar to Qatar.
2. Encrypt data stored outside Qatar for regulatory or business continuity requirements.

Personal data (PII) stored / processed in clouds should meet the Data Privacy regulatory requirements both locally as well as internationally.

Identity and Access Management / Privilege Access Management

The Qatar e-Authentication Framework[13] provides a strong framework for building an e-Authentication solution within an organization.

The NIA Policy covers in depth security controls for Identity and Authentication Management.

Media Security

The NIA Policy covers in depth security controls for Media Security. The section below reprises the most important ones:

1. Security controls for media should consider privacy impacts along with security considerations.
2. By design, do not retain data / media beyond what is required. For as long as data / media is retained (throughout its life cycle and in all forms), it should be protected as per its security profile.
3. Practical and adequate data disposal means should be implemented to dispose data that has served its purpose and needs to be destroyed.

BYOD

The BYOD Security Policy[14] covers in depth security controls for any personal device used in the business network / system. This includes any devices such as storage (USBs), wireless routers, mobiles / tablets etc. In addition, the NIA Policy also includes controls for BYODs.

---

[10] http://www.qcert.org/sites/default/files/public/documents/cs_guidelines_open_source_software_eng_v1.0_0.pdf

[11] http://www.qcert.org/sites/default/files/public/documents/cs_cloud_security_policy-2017_english_v1.2.pdf

[12] http://www.qcert.org/alerts/data-location-advisory-v20

[13] http://www.qcert.org/sites/default/files/public/documents/cs-gima-qatar_e-authentication_framework_v1.0_0.pdf

[14] http://www.qcert.org/sites/default/files/public/documents/cs-csps_byod_policy_v1.0.pdf

Social Media Security

Reputation is critical for the hotel and leisure industry. Social media plays an important role in defining the organization's image and perception in the virtual world. As such, it is important that the social media channels be secured against potential cyber threats. The Security Guidelines for Securing Social Media Accounts[15] provides detailed recommendations to businesses to help them secure their social media channels.

Critical Systems

Website & Online-booking

The security controls mentioned in the Software security and the Product security section above, along with the NIA Policy are applicable for the e-commerce (Hotel Booking) portal as well. You may also refer to Information Security Controls for Website Development and Hosting guidelines[16] for additional information. Pay special attention to the following aspects:

1. Authentication: Use digital certificates from trusted authorities (CSPs, preferably Qatari CSPs) to validate the identity of portal service provider.
2. Privacy:
    a. Only collect data that is required. Dispose of data once the requirement is complete (including regulatory requirements).
    b. Encrypt data throughout its life cycle from collection, processing, storage and disposal.

   Integrity: Integrity of information means ensuring that a communication received has not been altered or tampered with. In an e-commerce portal, this can be achieved by using digital certificates to digitally "sign" messages.
4. Segmentation: Ensure proper segmentation between web servers and database servers. Utilize a DMZ for internet facing assets to prevent an attacker from gaining direct access to internal assets in the event of a breach.
5. Availability: Define a back-up strategy for databases and applications. Consider off-site storage for critical data.
6. Non-repudiation: Non-repudiation is the ability, to legally prove that a person has sent a specific email, requested a service, or made a purchase approval from a website. In the realm of e-commerce, nonrepudiation is achieved by using digital signatures.
7. PCI Compliance: Ensure that your payment gateway is in compliance to PCI standards. The organizations should take extra care in selecting their POS system vendors and credit card processors. The third party agreements with these entities should be vetted and security obligations should become part of such agreements
8. Testing: Regular testing of the e-commerce portal to:
    a. Verify the security requirement specification such as location of the asset(s), access control mechanism for the assets, operational context of the organization, existing

[15] http://www.qcert.org/sites/default/files/public/documents/cs-ciip-guidelines_for_securing_social_media_accounts_eng_v2_0.pdf

[16] http://www.qcert.org/sites/default/files/public/documents/giap-information_security_controls_for_website_development_and_hosting-en-v1.0.pdf

system services and their access control mechanisms, and the connectivity within the organization and connectivity of the organization to the outside world

b. Verify the configuration of the security tools specified in the security infrastructure i.e. whether the security tools are properly installed and configured to maintain the security of the asset
c. Verify that all known patches are updated or suitably mitigated.
d. Verify if any gap exists between the proposed security infrastructure and the implemented security infrastructure
e. Verify the limitation of the proposed security infrastructure with respect to the known vulnerabilities

Point of Sale Terminals (Restaurants)

A general tendency amongst users is to believe that only the computers are at cyber risk. Electro-mechanical devices such as printers, Multi-Function devices (Printer cum scanners cum copiers etc.), or micro terminals (POS machines, Display or Information systems) are generally ignored when it comes to patching or protecting them from vulnerabilities although they may reside on the same network as business systems.

POS terminals are a sweet spot for malicious actors that are looking for personal information such as credit card details, personal details / information of hotel guests. As a result, malicious actors attack POS terminals to exploit credit card data and guest information held on them.

1. Ensure that the corporate password policy is applicable on POS systems as well.
2. Regularly patch the POS systems (hardware / software) to mitigate any known vulnerabilities.
3. Segregate POS machines on a separate network to restrict spread of malware or loss of information from other systems in case of a breach.
4. POS malware variants are difficult to identify, so it is critical that organizations have experts regularly conduct deep-dive penetration to sniff out potential vulnerabilities before malicious actors can take advantage of them.
5. Restrict Access to Internet: Apply access control lists on the router configuration to limit un-authorized traffic to and from the POS devices.
6. Disallow Remote Access: Cyber Criminals can exploit remote access configurations on POS systems to gain access to these networks. To prevent unauthorized access of POS systems, disallow remote access to the POS network at all times.
7. Disable unwanted wireless protocols such as Blue Tooth, GPRS if not required.
8. Use End-to-End encryption if possible.

Guest Wi-Fi Internet

Wireless internet is one of the most sought after service for guests within a hotel. These include guests that are staying in the hotel or those that patronize certain services / facilities (such as using Health facilities / Attending Events / Restaurants / visitors to the hotel guests etc.). However, the service is at risk of being misused by the guests or malicious actors who may get access to hotel's wi-fi one way or the other.

The Cyber Security Guidelines for Public Wi-Fi[17] provide recommendations for deploying a secure Public Wi-Fi system. The section below reprises the most important ones:

a. Maintain an inventory of Wireless Access Points. Monitor, detect and remove rogue wireless access points.
b. Configure the system to use adequate authentication and encryption.
c. Use firewall / routers to segregate the networks. Use different SSIDs and different configurations for networks of varying security zones.
d. Also, refer to our Cyber Security Guidelines for Securing Home and Small Office Routers[18] for your routers and access points setup recommendations.

IoT Security

The hotel industry employs a number of IoT technologies such as Smart TV, Smart Mini Bars, Smart Light controls, Smart Doors etc. to enhance the comfort of its guests. The Smart Qatar Security Standard[19] covers in depth controls for IoT security.

[17] http://www.qcert.org/sites/default/files/public/documents/cs-csps_guidelines_for_public_wifi_eng_v1.0.pdf

[18] http://www.qcert.org/sites/default/files/public/documents/cs-csps_guidelines_home_office_routers_en_v1.0.pdf

[19] The Smart Qatar Security Standard can be made available on request.