Issued@2024 By Information Security Group

STAFF HANDBOOK FOR OASIS TRAVEL AGENCY

Table of Contents

Document Status

Document Name	Staff Handbook of information Security
Document Code	001
Authored by	Lo Wing Yin(23464267), Ke Hengqi (23439335)
Approved by	Head of Information Technology Department
Version Number	1.0
Date Approved	April 2024
Revision History	Nil

Purpose

The Staff Handbook of Information Security has been prepared to remind all staff of their roles and responsibilities in protecting the company's information when using its IT resources.

Please read and understand this handbook to facilitate responsible use of the company’s IT resources.

Information Security Roles and Responsibilities

1. Staff:

Information security is the responsibility of all employees of the company. All staff members requiring access to the information systems are responsible for ensuring its security.

All staff members shall familiarize themselves with policies and ensure their adherence. It must be the endeavour of every staff member to ensure the security of information systems, to help maintain the confidentiality, integrity, and availability of those systems, and to promptly report any actual or suspected security weaknesses or breaches to the appropriate authority.

2. Head of the Department:

The head of the department at all levels is responsible for ensuring that their staff members are aware of and adhere to the security requirements of the division.

They are also responsible for monitoring the implementation of the security plan and ensuring that the security requirements are met.

3. Information Security Steering Committee:

The Information Security Steering Committee, which may comprise the Additional Commissioner, Chief Technology Officer, and Director of IT, will be responsible for approving all policy matters relating to information security and exceptions on a case-by-case basis.

The Information Security Steering Committee will also be responsible for providing direction and advice to all employees regarding updates and breaches on Information Security policies.

General Principles of Information Security Policy

The objectives of Information System Security are to ensure:

1. **Confidentiality**: Protect data from unauthorized access and disclosure.

2. **Integrity**: Ensure data is complete and accurate from its original form.

3. **Availability**: Maintain the ability to access resources when needed, even under natural disasters or after suffering from cyberattacks. Availability of information to the right people at the right time.

4. **Authentication**: Restrict access to resources such as printers, servers, databases, directories, or drives in a computer system to specific users. The most common form of authentication is a login and password combination that verifies user information. Multifactor authentication is highly recommended for access control of our IT access in the company.

Critical Measure taken for ensuring data Confidentiality, Integrity, and Availability			
	Confidentiality	**Integrity**	**Availability**
1	**Access Control based on the principle of least privilege**		**Deploy distributed system instead of single system to ensure data available when system fail**
2	**Sensitive data masking and encryption**	**Data encryption in transit and in rest**	**Regularly Backup information**
3	**Strong User Authentication by using multifactor authentication**	**Checksums and Hashing for verify the integrity of data**	**Regularly test system to identify potential risk and weakness**

General Principles of Information Security Policy

For All Information Systems Users, Please **Understand the Following:**

The Information Systems Users will play a major role in ensuring that all information security requirements are met.

Users will be responsible for:

1. Ensuring that they are aware of and understand the information security policy.
2. Taking all reasonable precautions to protect information systems against unauthorized access, use, disclosure, modification, duplication, or destruction.
3. Assisting and cooperating in the protection of the systems they use.
4. Ensuring that information and data are used solely for business purposes.
5. Using information systems only as appropriate for their job responsibilities.
6. Reporting security problems or issues to the relevant Division Head and IT Department as appropriate.

Guidelines for information Classification

Classification and Handling of Information

In an information management system, it's imperative to classify information appropriately to ensure its protection and integrity. Following the framework provided by ISO 27001:2022 and ISO 27002:2022, information can be categorized into four levels of confidentiality: Confidential, Restricted, Internal, and Public. Each classification level dictates the extent of access and the potential risks associated with the disclosure of that information.

Confidential Information

Access: Only senior management has granted access.

Description: Confidential information constitutes the highest level of sensitivity within an organization. Access to such data should be strictly controlled and limited to authorized personnel only. Any breach of confidentiality could have significant legal, financial, and reputational consequences for the company.

Examples: Legal documents, HR records, customer personal information, or customer financial information

Restricted Information

Access: Most staffs have access.

Description: While not as critical as confidential information, restricted information still demands careful handling. It's essential to restrict access to only those staffs who require it for their duties. Unauthorized disclosure of such information could lead to competitive disadvantages or breaches of privacy, impacting the organization's operations and trust.

Examples: Business plans, security plans, staff personal information.

Internal Information

Access: All staffs have access.

Description: Internal information forms the backbone of organizational culture and operations. While less sensitive than confidential or restricted information, it still requires protection from unauthorized access. Open access within the organization fosters transparency and collaboration, but precautions must be taken to prevent leakage to external parties, which could still harm the company's interests.

Examples: Internal news, training material, staff handbook.

Public Information

Access: Everyone has access.

Description: Public information represents the least sensitive category, as its disclosure does not pose any direct threat to the organization's interests. However, even though it's intended for public consumption, ensuring accuracy and consistency in public-facing materials remains crucial for maintaining the company's reputation and credibility.

Examples: Tour promotional materials, publicly available travel packages and prices, official announcements.

Guidelines for information Handling

Staff should handle the CONFIDENTIAL/RESTRICTED information in the database and server according to well-defined handling procedures to ensure its security and integrity:

- **Access Control on the Database System and Server**
  1. Every staff member shall only have access to the system and the server necessary for their job on the basis of the principle of least privilege.
  2. Log in to the system and the server using a user account name and password followed by a time-sensitive one-time passcode (two-factor authentication (2FA)).
  3. Every staff member will be issued a unique pair of a user account name and initial password to access. • Staff members have to keep their login credentials secure, and each password is not to be shared with any other staff member within the institution.
  4. Upon first-time access, the user will be required to change their password to a new one, where each password is a complex combination including strings, integers, and special characters.
  5. Each staff member will be required to change their password regularly and set a password for access every three months.
  6. For security reasons, if a staff member forgets or inputs the wrong password three times, the account in the system is locked. Please follow the procedures to reset the password and get approval from the authorized person.
     - **Persons Responsible For:**
       - The Database Administrator of Information Technology is responsible for issuing the user account and initial password for all employees.
       - The head of each department is responsible for authorizing staff to access the database and authenticate the identity of staff in his/her department for the matter of reissuing passwords.
       - The Manager of Information Technology is responsible for answering questions from all staff related to database operations.

Guideline for Data Protection Principles and Handling

According to the six Data Protection Principles (DPP) in Hong Kong, staff shall have an understanding of them and ensure their handling of customer's personal data complies with the ordinance.

- **DPP1: Aims and Manner of Collection of Personal Data** The data collected must be sufficient and critical but not excessive for the intended purpose. For example, the collection of identity card numbers and copies.
- **DPP2: Accuracy and Duration of Retention of Personal Data** Data users must ensure that the data is accurate, and the retention period is reasonable and related to the purpose of the event. For instance, business transactions should be kept for not less than seven years.
- **DPP3: Use of Personal Data** The use of personal data must be related to the original purpose of collection. For example, any illegal purpose of data use is prohibited.
- **DPP4: Security of Personal Data** Data users are responsible for protecting the personal data they hold against unauthorized or accidental access, modification, loss, or use. For instance, any breach in the security of personal data can have severe consequences, including penalties for data leakage.
- **DPP5: Openness and Transparency of Policies** Data users must take all practicable steps to ensure the openness of their personal data policies, the type of data, and the purpose of holding it. For example, information technology policy.
- **DPP6: Access and Correction** Data subjects have the right to request access to and rectify their own personal data.

Guideline for Data Handling

The database administrator is responsible for inserting, modifying, and disposing of data in the database and server after receiving requests and approval from the head of each department. Authorized database users are only allowed to view and download permissioned data for business use.

Data Masking

1. Staff must adhere to data masking policies and guidelines established by the organization.
2. Staff should have a clear understanding of what constitutes sensitive data within the organization.
3. Staff involved in data handling and management shall mask data aligned with business requirements and regulatory standards.

Data Integrity

1. Use checksums or hashing algorithms to verify the integrity of data during transmission or storage.
2. Implement an audit trail to track changes.

Data Storage

1. All data should be stored securely on company-approved systems.
2. Protect confidential information by encryption and by enforcing a password on files.
3. Avoid storing customer data on personal devices or external drives.
4. It is not recommended to store confidential/restricted information on portable media unless staff have approval from their head of department.
5. Confidential information stored on portable media must be encrypted and securely handled.

Data Backup

1. Ensure that all files and email boxes are backed up regularly and timely in designated directories and cloud systems.
2. Ensure that backups are done before your computer is repaired or has new software installed or has software/hardware upgrades.
3. Ensure your auto-backup schedule on the system is turned on.

Guideline for Data Handling

Data Transfer

1. Do not transmit sensitive information to unauthorized people or to authorized people without appropriate security (i.e., encryption).
2. When transferring customer data electronically, use secure methods such as encrypted emails or file transfer protocols offered by the IT department.
3. Double-check recipient details to avoid sending data to the wrong recipient.

Data Disposal

1. Properly dispose of any physical documents or electronic files containing customer data that are no longer needed.
2. Shred paper documents and securely wipe electronic storage devices before disposal.

Information Security

1. Ensure using an encrypted channel for transmitting information such as SSL/TLS (Secure Sockets Layer/Transport Layer Security) to establish a secure connection over the Internet.
2. Staff who are remote working from home are responsible for ensuring the use of IPsec (Internet Protocol Security) to secure internet protocol (IP) communications by encrypting and authenticating data packets.
3. Ensure that your workstation is equipped with up-to-date antivirus software and firewalls.
4. Avoid accessing customer data over public Wi-Fi networks or unsecured connections.
5. Be cautious of phishing emails and never click on suspicious links or download attachments from unknown sources.

Usage of Information Resources

Understand and follow the regulations in using the agency information and IT resources.

Important general usage guidelines

1. IT resources are primarily intended for operation, administrative work, and provision of social or community services.
2. Employees must not ignore or refuse legitimate requests for data under applicable laws, such as court orders or compliance with regulatory investigations.
3. Attend the safety lecture the company's IT staff hold if you have not heard of it before.
4. Safety lectures should be organized for all staff periodically to enhance awareness of safety.

Use information legally and ethically

The following actions should be PROHIBITED:

For CONFIDENTIAL information:

1. Using sensitive or confidential information for personal gain or to harm others. This includes trading, selling, or sharing customer data without consent.
2. Disclosure of confidential or restricted information to unauthorized individuals inside and outside the organization. This includes discussing sensitive information in public areas where it can be overheard.
3. Verdict against some or all relevant data privacy laws and regulations, such as DPP, CAP486, or others applicable in your jurisdiction.
4. Anonymous the personal information when sending it to the company that helps us develop the AI services.

For ALL information:

5. Accessing or attempting to access data for which the employee has no authorization. This includes using another employee's login credentials to access information.
6. Unauthorized alteration, deletion, or manipulation of any data within company systems. This ensures data integrity and trustworthiness.
7. Using company resources to conduct or promote illegal activities, including copyright infringement, fraud, or other crimes.
8. Using information to discriminate against individuals based on race, gender, religion, ethnicity, disability, sexual orientation, or any other protected characteristic.
9. Do actions and decisions involving company data that might conflict with the company's best interests or benefit a third party inappropriately.

Usage of Information Resources

Use computing machines responsibly and efficiently

Computing equipment is fundamental of the company. The use of computer equipment (such as server clusters, office computers, mobile devices, etc.) must adhere to the following principles:

1. All access to sensitive areas, such as server rooms and file storage facilities, is restricted to authorized personnel only.
2. Do not move the machines to a place where surveillance cameras cannot observe them.
3. Keep equipment clean and in good working condition to extend its lifespan and functionality.
4. Report any suspicious activities or individuals near computing machines.

Safeguarding the company's Information System (IS) and Account

To ensure the regular operation of internal and external services within the company, the use of the Information system of the company must adhere to the following principles:

For All staff:

1. Use strong passwords for all systems and change the password regularly.
2. Locking your workstations when leaving your desks and not leaving sensitive information unattended.
3. Enable the password-protected screen saver on computing machines and set the timeout not to exceed 30 minutes.
4. ALWAYS keep the antivirus software and firewall alive.
5. Consider TWICE before clicking hyperlinks or opening email attachments.
6. Do not download any software or files from unknown, untrusted, or unconfirmed sources.
7. Do not use email accounts for internal use only to register in the public network.
8. Strictly follow the regulation of setting passwords in the company as follows:

Item	**Rule**
Complexity	It should contain the following types of characters: 1. Upper Case Character 2. Lower Case Character 3. Number 4. Special Character
Length	8-16 characters
Change frequency	At least every year
Password history	Disallow reuse of the password for at least one year.

For IT staff:

Usage of Information Resources

9. Keep operating systems, software applications, antivirus, and firewall programs updated with the latest security patches and updates confirmed by IT security staff.
10. Back up the system and file regularly, and at least have three copies for every piece of data.
11. Report the safety conditions of IS periodically.

Using the IT service of the company responsibly

Responsible usage of IT services can enhance the productivity and safety of the company. To realize this, the following principles should be adhered to:

1. Be aware of ransomware, malware infections, data leakage, and other Internet access hazards.
2. Use ONLY the services the company provides (e.g., Remote Access, Document Edit, Email Services) when dealing with the data related to the company.
3. Do NOT send email or instant messages containing CONFIDENTIAL information without proper authorization AND data encryption.
4. Do NOT install, turn on, or share any wireless routers or network devices on campus without proper authorization.
5. Do NOT share your remote-access login credentials with any outside parties.

Using portable storage and mobile devices safely and securely

Improper portable storage and mobile device use could cause leakage and financial loss. To avoid the situation, it is essential that:

For All staff:

1. All data stored on portable devices should be encrypted to ensure that data remains protected, even if the device is lost or stolen.
2. Use the VPN if the mobile device wants to access the company's network through WAN.
3. Prohibit the storage of sensitive or critical business data on portable storage devices unless essential and approved by Managerial AND IT staff.
4. Never leave the portable devices unattended.
5. Use ONLY the portable devices approved by Managerial AND IT staff.
6. Ensure that all the CONFIDENTIAL or RESTRICTED data are erased from the portable devices after use or before disposal.
7. Report to the Managerial AND IT staff as soon as possible if a device containing CONFIDENTIAL or RESTRICTED information is lost or stolen.

For IT staff:

8. Continuously Update and Ensure that the encryption software uses the latest encryption method in all platforms to provide the encryption service to all staff.

9. Ensure the VPN service is always accessible to all staff.

Safeguard the AI Services

The company introduced AI services to enhance customers' experience and accelerate the company's operation. We need to use AI services with these principles:

For All Staff

1. Attending ongoing training and education programs that help ensure the understanding of the technology implications and how to use it responsibly.
2. Mandate strict adherence to established ethical guidelines for AI use. This includes respecting user privacy, ensuring fairness, and avoiding discrimination.
3. Report any ethical concerns related to AI applications and involve them in discussions on ethical AI use.
4. Express concerns or suggestions regarding AI services.

For IT Staff

5. Implement awareness programs about potential risks associated with AI, including biases, misuse, and data security issues.
6. Report the situation on the disposal of AI services periodically.
7. Monitor AI systems for any signs of malfunction, bias, or security issues.
8. Conduct regular risk assessments of AI systems to identify vulnerabilities and implement appropriate security measures.

Incidence Response

In this section, several types of attacks will be displayed, along with examples. And for every attack, the book will introduce the response to them.

1. **Ransomware Attack**

   Case 1: TravelEx (2020)

   TravelEx was hit by a ransomware attack that led to significant operational disruption and forced the company to turn off its systems [1].

   Case 2: Carnival Corporation (2020)

   Carnival Corporation, a major cruise line operator, disclosed a ransomware attack where the personal data of guests and employees might have been accessed [1].

   Response:

   1. Immediate Containment

   - **Isolate Affected Systems**: Quickly isolate infected computers from the network to prevent the spread of ransomware. Disconnect Wi-Fi, LAN cables, and other network connections.
   - **Power Down Devices**: If the scope of infection is unclear, power down potentially affected devices to minimize data encryption.
   - **Secure Backup Data**: Ensure backups are offline and secure from encryption. Check the integrity of backup data before proceeding with any other steps.

   2. Assessment and Analysis

   - **Identify the Ransomware Variant**: Determine the strain of ransomware to understand its behavior, encryption, and possible decryption tools available. Use online resources or consult with cybersecurity experts.
   - **Assess the Impact**: Determine the extent of the damage, including which systems, data, and services are affected. Assess operational impact and report to relevant stakeholders.

   3. Notification and Communication

   - **Notify Internal Teams**: Immediately inform your IT team and Managerial staff. Communicate with the legal, public relations, and compliance teams to prepare for broader communications.
   - **Legal and Regulatory Compliance**: Contact legal counsel to discuss obligations under data protection laws and consider notifying law enforcement and regulatory agencies.
   - **Communicate with Stakeholders**: Keep employees, customers, and partners informed as appropriate, maintaining transparency about the incident's impact and recovery efforts.

   4. Engage with Professionals

   - **Cybersecurity Experts**: If in-house expertise is insufficient, promptly engage with external cybersecurity professionals specializing in ransomware mitigation and data recovery.

Incidence Response

- **Forensic Analysis**: Consider hiring a forensic team to trace the attack vector, understand how the security breach occurred, and identify system vulnerabilities that must be addressed.

5. Decision on Ransom Payment

- **Evaluate the Necessity**: Assess the necessity of paying the ransom based on the ability to recover data from backups and the critical nature of the encrypted data.
- **Consult and Deliberate**: Discuss with law enforcement and cybersecurity experts to understand the risks and potential consequences of paying the ransom.
- **Consider the Implications**: Understand that paying the ransom does not guarantee data recovery and may encourage future attacks.

6. Recovery and Restoration

- **Clean and Restore**: Use trusted antivirus and anti-malware software to clean the infection from all affected systems. Begin restoration from backups after ensuring no traces of the infection remain.
- **Phased Restoration**: Restore critical services first to minimize business impact. Gradually restore other systems and data, monitoring for stability and signs of lingering issues.

7. Post-incident review and Strengthening

- **Conduct a Post-Incident Review**: Analyze the attack to determine its cause, the effectiveness of the response, and areas for improvement.
- **Update Security Policies and Procedures**: Revise your cybersecurity strategies based on insights gained from the incident. Improve training programs to enhance awareness and readiness against future attacks.
- **Implement Robust Defenses**: Strengthen defenses by implementing recommended security measures such as endpoint protection, email filtering, and network segmentation.

8. Continuous Monitoring

- **Monitor Systems**: Closely watch network traffic and system logs for unusual activities that might indicate a recurrence or a failed attempt to clear the ransomware fully.

2. **Data Breach**

Case 1: British Airways (2019)

This breach involved stealing customer data from approximately 500,000 customers due to a sophisticated cyber-attack. British Airways faced a significant fine due to this incident [2].

Case 2: SITA Passenger Service System (2021)

A data breach at SITA, which provides services to several major airlines, led to the leakage of frequent flyer data from multiple carriers [1].

Response:

1. Detection and Identification

- **Detect the Breach**: Use security systems and monitoring tools to detect unusual activity that may indicate a breach. Ensure that breach detection capabilities are up-to-date and active.
- **Identify the Breach**: Once detected, promptly identify the scope, nature, and extent of the breach. Determine which data types, systems, and information have been compromised.

2. Containment and Eradication

- **Short-term Containment**: Immediately isolate affected systems to prevent further data loss. This may involve taking certain servers offline, restricting network access, or disabling compromised accounts.
- **Long-term Containment**: Look for root causes and other security weaknesses that could lead to future breaches. Secure these vulnerabilities to prevent recurrence.
- **Eradicate the Threat**: Remove malicious content, malware, or unauthorized access points from the environment. Ensure that the threat is completely eradicated with the help of cybersecurity experts.

3. Assessment

- **Impact Assessment**: Evaluate the implications of the breach on business operations, customer relations, and legal compliance. Understand who is affected and the potential consequences for those individuals.
- **Regulatory Assessment**: Determine your obligations under applicable data protection laws (like GDPR, HIPAA) to report the breach to authorities and affected individuals.

4. Notification

- **Notify Authorities**: Report the breach to relevant authorities as required by law, typically within 72 hours of discovery.
- **Notify Affected Parties**: Inform individuals whose data has been compromised, providing details about what was involved, the possible risks, and how they can protect themselves.

- **Internal Communication**: Communicate with internal teams to coordinate the response and manage the situation. Keep key stakeholders informed about the breach and the steps being taken.

5. Recovery

- **Restore Systems**: Once the threat is contained and eradicated, begin restoring data from backups and bringing systems back online cautiously.
- **Monitor Systems**: After recovery, closely monitor systems for signs of new security issues or indications that the breach wasn't fully contained.

6. Post-Incident Analysis

- **Conduct a Post-Mortem**: Analyze how the breach happened, what response measures were effective, and where improvements are needed. This should involve all relevant stakeholders.
- **Document the Breach**: Keep detailed records of the breach, its impact, how it was handled, and the lessons learned. This documentation will be valuable for regulatory compliance and future security planning.

7. Prevent Future Breaches

- **Revise Security Policies**: Update security policies, practices, and technologies based on lessons learned from the incident.
- **Enhance Security Measures**: Implement stronger security measures such as better encryption, more rigorous access controls, and advanced threat detection capabilities.
- **Staff Training**: Enhance training programs to include the latest cybersecurity practices and lessons learned from the incident. Ensure all employees understand their role in maintaining security.

8. Ongoing Monitoring and Improvement

- **Continuous Monitoring**: Implement an ongoing monitoring strategy to detect future incidents early.
- **Regular Security Audits**: Schedule regular security audits to assess the effectiveness of new security measures.

3. **Unauthorized Access**

Case 1: Sabre Hospitality Solutions (2017)

Sabre's booking system was breached, impacting the data of multiple hotels and their guests. The breach included unauthorized access to payment information [1].

Case 2: Cathay Pacific (2018)

Cathay Pacific was fined for failing to protect customers' data, resulting in unauthorized access to the personal information of approximately 9.4 million passengers [1].

Response:

1. Detection and Confirmation

- **Identify the Incident**: Quickly detect and confirm the unauthorized access through system alerts, user reports, or irregular system behavior.
- **Assess the Initial Impact**: Determine what data, systems, or services have been accessed or compromised.

2. Containment

- **Isolate Affected Systems**: Immediately isolate affected systems to prevent further unauthorized access or damage. This might include disconnecting from the network, changing passwords, or temporarily disabling affected accounts.
- **Maintain Evidence**: Preserve logs, metadata, and other digital evidence to help forensic analysis. Be sure to maintain the integrity of this data securely.

3. Eradication

- **Remove Access**: Ensure the unauthorized access is cut off once isolated. This might involve removing remote access tools, malware, or any backdoors the attacker leaves.
- **Secure Vulnerabilities**: Patch the exploited vulnerabilities that allowed unauthorized access. Update and strengthen firewall rules, intrusion detection systems, and other security measures.

4. Recovery

- **Restore Systems**: Gradually restore the isolated systems to regular operation once you are confident that the threat is fully neutralized. Ensure systems are clean and monitored closely during the recovery phase.
- **Reinforce Security**: Enhance security measures to fortify systems against similar or new types of attacks. This might include updating passwords, implementing multi-factor authentication, and improving access controls.

5. Investigation

- **Determine the Cause**: Conduct a thorough investigation to determine how the unauthorized access occurred. This could involve IT forensic

analysis to trace the attacker's movements and uncover how security defenses were breached.
- **Assess Full Impact**: Evaluate the complete impact of the unauthorized access, considering potential data loss, system compromise, and related consequences.

6. Notification

- **Regulatory Compliance**: Notify relevant authorities if required by law, such as under GDPR or HIPAA, where there's an obligation to report security breaches.
- **Notify Affected Parties**: Inform individuals whose data or privacy may have been compromised, advising them on steps to protect themselves from potential harm.

7. Review and Improvement

- **Lessons Learned**: Review the incident to learn lessons about vulnerabilities and the effectiveness of your security posture.
- **Update Incident Response Plan**: Refine your incident response strategy based on what was learned to improve future responses to similar incidents.
- **Continuous Monitoring and Training**: Enhance ongoing monitoring systems to detect unusual activities early. Regularly train staff on security awareness and procedures for detecting and responding to security incidents.

8. Documentation

- **Document the Incident**: Keep detailed records of the incident's timeline, management, and recovery process. Documentation is crucial for legal reasons and for improving response strategies.

4. **Critical Vulnerability**

Case 1: Lastminute.com (No time)

This booking site was found to have a critical vulnerability that could potentially allow attackers to hijack user session cookies [2].

Response:

1. Vulnerability Identification

- **Regular Scanning**: Conduct regular scans using vulnerability assessment tools to identify potential security weaknesses in your systems.
- **Stay Informed**: Subscribe to security advisories from vendors, industry groups, and cybersecurity organizations to receive timely alerts about newly discovered vulnerabilities.

2. Assessment

- **Severity Assessment**: Evaluate the criticality of the identified vulnerability based on its potential impact and the likelihood of exploitation.
- **Asset Inventory**: Identify which systems, applications, or data are affected by the vulnerability to understand the scope of potential impact.

3. Prioritization

- **Risk-Based Prioritization**: Prioritize remediation efforts based on the risk level of the vulnerability and the value and sensitivity of the affected assets.
- **Regulatory Requirements**: Consider compliance requirements that may dictate the urgency of addressing specific vulnerabilities, especially those impacting protected or regulated data.

4. Containment

- **Temporary Measures**: Implement temporary countermeasures or workarounds to reduce risk if immediate remediation isn't feasible. This might include disabling affected systems, restricting access, or applying interim security controls.

5. Remediation

- **Patch Management**: Apply patches or updates vendors provide as soon as they are available and tested.
- **Configuration Changes**: If no patch is available, make necessary configuration changes recommended by security advisories to mitigate the risk.
- **Custom Fixes**: For vulnerabilities in custom-developed software, develop and deploy a fix as quickly as possible.

6. Verification

- **Testing**: After applying patches or other fixes, test the system to ensure that the vulnerability has been effectively mitigated and that the fix hasn't adversely affected system functionality.
- **Re-scan**: Conduct follow-up scans to confirm that the vulnerability no longer exists in the environment.

7. Communication

- **Internal Notification**: Keep relevant stakeholders within the organization informed about the vulnerability and steps being taken to address it.
- **External Communication**: If necessary, communicate with customers or partners about the vulnerability, particularly if their data or operations could be impacted.

8. Review and Learn

- **Post-Remediation Review**: After remediation, review the incident to understand how the vulnerability occurred, whether it was exploited, and the effectiveness of the response.
- **Process Improvement**: Update your vulnerability management processes based on lessons learned to improve future responses to similar situations.

9. Documentation

- **Record Keeping**: Document all actions taken from detection to resolution. This documentation is crucial for compliance, auditing, and historical reference.

10. Continuous Improvement

- **Security Posture Enhancement**: Use the incident to strengthen your overall security posture. Enhance your vulnerability management program and invest in more robust cybersecurity tools and training.

5. **Phishing Attack**

Case 1: Booking.com (2023)

Booking.com confirmed a phishing campaign targeting its users and trying to steal their credit card information [3].

Response:

1. Immediate Assessment

- **Confirm the Attack**: Verify that the phishing attack is indeed occurring and gather examples of the phishing attempts, such as emails or websites that misuse your agency's name.
- **Understand the Scope**: Determine how widespread the phishing attack is and which customers or potential customers are being targeted.

2. Incident Response Team Activation

- **Assemble a Response Team**: This team should include members from IT security, legal, customer service, and public relations departments to handle the different aspects of the incident.

3. Communication and Notification

- **Notify Customers**: Alert your customers immediately about the phishing attack. Inform them that your agency's name is being used fraudulently and advise them on how to recognize and avoid phishing attempts.
    - **Clear Instructions**: Provide specific examples of the phishing attempts and clear instructions on what to do if they receive a suspicious email or communication.
- **Public Announcement**: Consider making a public announcement if the attack is widespread. This could be through your website, social media channels, or a press release to reach a broader audience.
- **Regulatory Reporting**: Report the incident to relevant authorities. This could include law enforcement, cybercrime units, or data protection regulators, depending on the nature of the phishing attack and the jurisdiction.

4. Enhance Security Measures

- **Monitor and Block**: Work with your IT team or an external cybersecurity firm to monitor for new phishing attempts and try to block malicious activities related to the attack.
- **Strengthen Email Security**: Implement advanced email filtering technologies that can help detect and block phishing emails before they reach your customers.
- **Customer Verification Processes**: Strengthen and reinforce processes for verifying customer identities over the phone or via email to prevent data breaches.

5. Customer Education

- **Educational Campaigns**: Launch a campaign to educate your customers about phishing attacks and how to protect themselves.

Include tips on how to identify legitimate communications from your agency.
- **Regular Updates**: Regularly update your customers on new types of scams and what measures your agency is taking to protect them.

6. Legal Actions
- **Cease and Desist**: Through your legal department, issue a cease and desist letter to the perpetrators if they are identifiable.
- **Domain Takedowns**: Work with domain registrars to take down fraudulent websites that use your brand name or likeness.

7. Ongoing Monitoring and Review
- **Incident Review**: After the initial crisis is managed, conduct a thorough review of how the incident was handled and what could be improved.
- **Continuous Monitoring**: Keep an eye on new phishing trends and potential threats by setting up alerts for your brand name and related keywords.

8. Reputation Management
- **Manage Online Presence**: Actively manage your online presence to reassure current and potential customers of your legitimacy and ongoing efforts to protect their interests.
- **Customer Support**: Enhance customer support to handle increased inquiries and provide reassurance to concerned customers.

References

[1] How Dangerous Is the Cyber Attack Risk to Transportation? (securityintelligence.com)
[2] In Spite Experiencing Some of the Biggest Data Breaches in Recent Years, the Travel Industry Is Still Full of Security Holes - CPO Magazine
[3] Catches of the Month: Phishing Scams for November 2023 - IT Governance UK Blog
[4] https://www.goodaccess.com/blog/remote-access-control-what-is-it-and-how-does-it-work#how-access-control-work
[5] https://www.microsoft.com/en-us/security/business/security-101/what-is-two-factor-authentication-2fa
[6] https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf
[7] https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html