Protecting Your Organisation from Data Breaches

What is a Data Breach?

A data breach, in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data. It also includes the loss of any storage medium or device, on which personal data is stored, in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

For organisations, the impact of data breaches can also be severe. It can result in a loss of trust or reputation for the organisations when restricted business information or customers' personal data is leaked or put up for sale online. In some cases, the data is held for ransom by cyber criminals, and may not be returned even if the ransom is paid.

As the number of reports of data breaches has increased globally, there is a need to be vigilant and take steps to prevent them. Organisations need to raise their defences against common data breach vectors to reduce the risk of a data breach and implement adequate measures to minimise the impact to their customers in the event of a compromise.

This advisory aims to provide guidance to organisations on the common causes of data breach, preventive measures to take, and how to respond to a data breach. It comprises the following sections:

Common Causes of Data Breach

Weak/Stolen Passwords

Weak password management facilitates threat actors' access into a system. This includes the use of weak passwords, such as those that comprise personal information or easy-to-guess passwords. Passwords are the keys to a lock and should be safeguarded in both the physical and cyber realms.

Unpatched Vulnerabilities

Vulnerabilities which are left unpatched could be exploited by threat actors to gain access into networks or systems to perform various malicious actions. These include modification of files, data exfiltration, and installation of malware or ransomware.

Social Engineering

Social engineering is the use of psychological manipulation to garnish sensitive credentials from victims. Phishing, the most common type of social engineering, is a technique used to obtain sensitive information such as login credentials or credit card details. A phishing email is an email disguised as being sent from a legitimate entity, with the motive of tricking victims into clicking on a phishing link. Clicking the link will lead to a phishing page which would request for the victims' confidential details or cause the victim's computer to be infected with malware. Phishing may also be conducted via SMS or social media.

Insider Threats

Insider threats may take the form of deliberate actions by disgruntled/rogue employees who knowingly leak data to competitors or sell them for financial gain. They may also take the form of unintended actions by careless employees who lose data-storage devices or send confidential emails to the wrong recipients.

Cybersecurity Measures for Organisations

To reduce the risk or impact of data breaches, organisations are recommended to adopt the following cybersecurity measures to secure their infrastructure and systems:

- Update systems, software and applications regularly to patch known vulnerabilities.
- Perform antivirus scans regularly and keep antivirus software updated with the latest malware signature files.
- Review user accounts periodically and remove accounts that are no longer needed.
- Install and use Virtual Private Network (VPN) for network infrastructure devices, endpoint devices, and other remote access systems.
- Encrypt important or sensitive data, both in storage and in transit (e.g., when sending over email) so that even if the encrypted data is stolen/leaked, the damage will be limited. Sensitive data should not be publicly accessible or left unencrypted.
- Limit privileged access to authorised personnel. This reduces the risk of privileged account abuse or compromise. For sensitive systems in particular, limit access to what is necessary.
- Restrict internet access such as through blacklisting or whitelisting, especially where there is direct access from endpoints to large amounts of personal or sensitive data.
- Review and only enable the necessary network ports and services that are required.
- Consider establishing a monitoring system or process to track the following:
    - Authentication logs for remote services and for suspicious account behaviour or activities across systems, e.g., if one account is logged into multiple systems simultaneously or if the login is occurring from an unexpected location.
    - Databases for suspicious activities, such as unauthorised copying or exfiltration of PII or important business data.
    - Outbound network traffic for unauthorised communications or data transmissions. For cloud-native applications, ensure proper configuration of security settings and access control.
- Maintain an updated backup of all the important data to facilitate restoration in the event of a ransomware attack or a data breach resulting in data loss. The backup should be stored offline and not connected to the enterprise network.
- Conduct security awareness training such as regular phishing simulation exercises for employees to learn and be aware of good cyber hygiene practices such as proper management of important data and identification of phishing emails and other forms of social engineering.

In addition to these cybersecurity measures, organisations should also develop a data security plan specific to the company's context that outlines how sensitive company data should be used and the destruction of data that is no longer needed.

For Organisations with an Online Presence

- Avoid requesting and storing PII, where possible. Review current data in the database and remove any unnecessary PII stored. If storing PII is necessary, encrypt the PII before saving the data in the database.
- Avoid storing credit card information on your website by using a good secure payment gateway that has robust checks and validation. Examples of such payment gateway services include those that are tested and approved by the Payment Card Industry (PCI) Council. If storing credit card information is necessary, organisations may wish to follow standards such as the PCI Data Security Standards.
- Enforce the need for customers to use a strong password for their online accounts. Where possible, organisations should implement a multi-factor authentication (MFA) as part of the customer login process.
- Install Transport Layer Security (TLS) certificates on your web server to secure and safeguard any data that is sent from the browser to the web server. This prevents threat actors from accessing or modifying any information transferred during a transaction, such as the customer's personal particulars or credit card details.
- Install web application firewalls and security plugins to block unauthorised traffic and malicious requests from accessing your network or system. This protects your web servers from common attacks such as SQL injection, cross-site scripting, and cross-site request forgery.
- Conduct regular code reviews and vulnerability assessments before and after deploying your web servers. Look out for possible code injections and ensure that third-party scripts or Application Programming Interfaces (API) will not compromise the servers' security.

Data Breach Response Plan

Besides preventive measures, organisations should also develop a data breach response plan that should encompass both administrative and containment/recovery actions if a data breach is detected.

<u>Administrative Actions</u>

- Lodge a police report if criminal activities (such as hacking or theft) is suspected.
- If you believe that PII was compromised, report the incident to the Personal Data Protection Commission (PDPC) at https://eservice.pdpc.gov.sg/case/db.
- Reach out to affected customers, if any, and take steps on securing their accounts.
- Develop a crisis communication plan for communicating how the company is managing the data breach.

<u>Containment/Recovery Actions</u>

- Conduct an internal investigation to determine how the data breach occurred. Organisations may wish to consider engaging professional services if the data breach occurred because of an intrusion into the company's system, to properly clean up and remediate the breach.
- Isolate the compromised system from the Internet or network by disconnecting all affected systems.
- Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts.

- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system.
- If necessary, restore your system to a clean backup, and/or rebuild the compromised system.
- Perform an antivirus scan to detect and remove any malware in the systems and patch all systems and software.
- Monitor the database and systems for any further suspicious activities.

References:

https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/how-to-guard-against-common-types-of-data-breaches-handbook.ashx
https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.ashx?la=en