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 be severe. It can result in a loss of trust or reputation when restricted business information or customers' personal data is leaked or sold online. In some cases, the data that is held for ransom by cybercriminals 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 are urged to raise against common data breach vectors to reduce the risk of a data breach and implement adequate measures to minimise the impact to your customers in the event of a compromise.

This advisory provides guidance to organisations on the following:

- Common Causes of Data Breaches
- Cybersecurity Measures for Organisations
- Data Breach Response Plan

Common Causes of Data Breaches

<u>Weak/Stolen Passwords</u>

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

<u>Unpatched Vulnerabilities</u>

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

<u>Social Engineering</u>

Social engineering is the use of psychological manipulation to get victims to perform certain actions or reveal sensitive credentials. Phishing, the most common type of

social engineering, is a technique used by threat actors to obtain sensitive information such as login credentials or credit card details. Phishing can be conducted via email, messaging platforms such as WhatsApp and SMS or social media, with the message disguised as being sent from a legitimate entity. The motive is to trick victims into clicking on a phishing link which could either lead to a phishing page requesting for confidential details, or cause the victim's device to be infected with malware.

Insider Threats

Insider threats may originate from deliberate actions by disgruntled/rogue employees who knowingly leak data to competitors or sell them for financial gain. It may also arise from careless employees who lose data-storage devices or send confidential emails to the wrong recipients.

Security Misconfiguration and Inadequate Access Controls

Improperly configured cloud storage services, databases and application programming interfaces (APIs) may inadvertently expose sensitive information to unauthorised parties. Excessive access privileges, publicly accessible cloud storage and compromised access credentials may also allow threat actors to access or exfiltrate sensitive data.

Cybersecurity Measures for Organisations

Organisations should adopt the following measures to secure their infrastructure and systems:

Maintain Good Cyber Hygiene

- 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.
- Install and use Virtual Private Network (VPN) for network infrastructure devices, endpoint devices, and other remote access systems.
- Review and only enable the necessary network ports and services that are required.
- Restrict internet access through blacklisting or whitelisting, especially where there is direct access from endpoints to large volumes of personal or sensitive data.
- Maintain an updated backup of all important data to facilitate restoration in the event of a ransomware attack or a data breach. 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 apply good cyber hygiene practices such as

proper management of important data and identification of phishing emails and other forms of social engineering.
- Conduct regular configuration reviews, vulnerability assessments, access reviews and incident-response exercises.

Strengthen Access Controls and Authentication

- Review user accounts periodically and remove accounts that are no longer needed.
- 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.
- Enable Multi-Factor Authentication (MFA), particularly for privileged accounts, remote access services and systems containing sensitive information.
- Apply granular access controls based on the principle of least privilege, restricting access to sensitive databases, tables, columns or individual records according to operational needs.
- Where applicable, segregate database administration and system administration privileges to reduce the risk of excessive access being misused or compromised.
- Enforce strong password policies by requiring users to use passwords of at least 12 characters, comprising a combination of uppercase and lowercase letters, numbers and special characters. Passwords should not contain personal information, such as names, dates of birth or NRIC numbers.

Monitoring for Anomalous Activity

- 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 Personally Identifiable Information (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 controls.
  - Unusual database queries, large-volume downloads and unexpected access to sensitive information from unfamiliar accounts or locations.
  - Maintain visibility across all AI tools deployed across the organisation and track for any unusual traffic outside of its intended purpose, data flow and intended users.

Protect Sensitive Data

- 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.
- Implement appropriate encryption key management practices to protect sensitive data and prevent unauthorised access to encryption keys.
- Consider implementing Data Loss Prevention (DLP) controls to detect and restrict unauthorised transfers of sensitive information, particularly large-volume transfers.

In addition, 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

Secure Internet-Facing Systems

- 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.
- Restrict unnecessary exposure of administrative interfaces, databases and other sensitive services to the internet.
- Avoid requesting and storing PII where possible. Review current data in the database and remove any unnecessary PII. 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 strong passwords for their online accounts. Where possible, organisations should implement 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

helps prevent threat actors from accessing or modifying information transferred during a transaction, such as the customer's personal particulars or credit card details.

Secure Cloud Environments

- Ensure that cloud storage services, databases and associated APIs are securely configured, with access restricted to authorised users and services. Cloud resources should be configured to be private by default to prevent unintended public access.
- Conduct regular reviews of cloud security configurations, access permissions and security settings to identify and remediate misconfigurations.
- Secure cloud access keys and credentials. Avoid embedding credentials in application source code or storing them in publicly accessible repositories.
- Rotate or revoke compromised or unnecessary credentials and access keys promptly.

Additional measures:

- Maintain appropriate system, application, database and cloud audit logs to support the detection and investigation of potential data breaches.
- Establish appropriate alerts for suspicious activities, including unusual or large-volume transfers of sensitive information, to facilitate timely detection and investigation.
- Investigate suspicious data access or transfers promptly, even when there are no visible signs of ransomware encryption or system disruption.

Data Breach Response Plan

Organisations should also develop a data breach response plan that should include administrative, containment, investigation and recovery actions if a data breach is detected.

Administrative Actions

- Activate your organisation's incident response plan and notify relevant internal stakeholders, including management, IT security personnel and the Data Protection Officer (DPO).
- Lodge a police report if criminal activities (such as hacking or theft) are 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 to secure their accounts.
- Develop a crisis communication plan to inform and assure stakeholders how your organisation is managing the data breach.

Containment and Investigation

- Conduct an internal investigation to determine how the data breach occurred. Organisations may wish to engage professional services if there has been an intrusion into internal systems, to contain and remediate the breach.
- Isolate the compromised system from the Internet or other networks by disconnecting all affected systems. Where practicable, preserve relevant evidence before taking containment actions that may affect the investigation.
- 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.
- Revoke compromised access credentials and keys to prevent further unauthorised access to the system.
- Determine the period of compromise, the systems and accounts affected, personnel who reported the incident and the types and volume of data potentially accessed or exfiltrated.

Recovery and Prevention

- 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 system for any further suspicious activities.
- Review and strengthen security measures based on weaknesses identified during the investigation.
- Conduct a post-incident review to identify gaps in existing processes, improve security controls, and prevent similar incidents from recurring.

References

1. Personal Data Protection Commission (PDPC) – Good Practices to Secure Personal Data in the Cloud Platform: https://www.pdpc.gov.sg/assets/37d76636-a8ad-4903-af1d-d4503bda7d0d
2. Personal Data Protection Commission (PDPC) – Guide to Data Protection Practices for ICT Systems: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/tech-omnibus/guide-to-data-protection-practices-for-ict-systems.pdf
3. Personal Data Protection Commission (PDPC) – Guide on Managing and Notifying Data Breaches under the PDPA: 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.pdf

4. Joint Advisory against using NRIC Numbers for Authentication by the Personal Data Protection Commission (PDPC) and Cyber Security Agency of Singapore (CSA): https://www.pdpc.gov.sg/media-events/joint-advisory-against-using-nric-numbers-for-authentication-by-the-personal-data-protection-commission-pdpc-and-cyber-security-agency-of-singapore-csa
5. Advisory for Data Protection Risks When Using Unauthorised AI Tools For the Development of Software or Scripts: https://www.pdpc.gov.sg/media-events/advisory-for-data-protection-risks-when-using-unauthorised-ai-tools-for-the-development-of-software-or-scripts