Data Breaches are the New Normal –
Detect, remediate, and prevent Oracle data breaches

SafePaaS™

Data breaches are on the rise and the number of data breaches we have already seen in 2020 is alarming. The COVID-19 pandemic has heightened the vulnerability organisations face with potentially devastating consequences. Customers are losing trust in businesses as the data breaches become part and parcel of a modern society.

The majority of sensitive data such as customer credit details, supplier bank information and employee national ID's are stored in ERP systems. However, the fine-grained security measures required to protect this data have been overlooked for many years. As organizations have exposed ERP systems to the internet that provides continuous online access, the data stored in ERP systems has become vulnerable to cyber-attacks.

In response to the COVID-19 pandemic, IT Managers have rapidly enabled new capabilities to support an entirely remote workforce, which has created an opportunity for cyber criminals to access sensitive data making ERP attacks especially lucrative. With an increased number of employees using unmanaged devices to access confidential data, organisations need to be better prepared to face the threat of cyber leaks and the likelihood of a data breach. An increased number of connected devices providing access from anywhere increases attack surface. In addition to the exposed ERP systems, as organizations accelerate digital transformation enabled by Cloud, Big Data, and Internet of Things, the attack surface for enterprise data will continue to grow.

Proliferating breaches and the public demand for privacy and control of their own data have led governments to adopt new regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in that US state. Many others are following suit. These regulations require organizations to comply in the way they collect, store, share, and delete data. Failure to comply could result in steep fines, potentially costing a company millions for a data breach.

Oracle users can prevent data breaches by implementing data governance best practices for the overall management of data availability, relevancy, usability, integrity and security in an enterprise. Organizations that adopt data governance principals can manage their information knowledge and answer compliance questions, such as:

- What do we know about our data?
- Where did this data come from?
- Does this data adhere to company policies and rules?

Data governance practices provide a holistic approach to managing, improving, and leveraging information to help an enterprise's overall data management efficiency.

Protecting data stored in Oracle requires data rules logic that can detect violations of data elements identified as sensitive and governed by company policies or regulatory principals. Data violations must be remediated by applying corrective actions such as anonymization and pseudonymization of data. Continuous monitoring of sensitive data can prevent and mitigate the risk of accidental or intentional data disclosure.

SafePaaS™

Emerging Data Breaches

On April 1st, 2020 Marriott announced a security breach that may have exposed the personal information of 5.2 million guests. This marks Marriott's second data breach in recent years, following a breach in 2018. Personal information such as names, birthdates, and phone numbers may have been taken in the breach, along with language preferences and loyalty account numbers, Marriott said.

EasyJet, the low-cost European Airline is facing a legal claim brought by thousands of its customers after the airline announced in May of 2020 that the personal details of about nine million passengers were breached by a cyberattack.

T-Mobile, Nintendo, Estée Lauder have also been victims of attacks in 2020.

The work from home model has created an opportunity for cyber criminals to access sensitive data. With an increased number of employees using unmanaged devices to access confidential resources and remote working here to stay, organisations need to be better prepared to face the threat of cyber leaks and the likelihood of a data breach.

The International Association of IT Asset Managers (IATAM) is warning that at-home work due to the COVID-19 pandemic is leading to a spike in data breaches that's greater than anticipated.

"One example would involve removing admin permissions so that employees can complete the task without administrator oversight. Another would be allowing the use of "unpatched" business computers that allow hackers to load malicious files with admin privileges. In some cases, companies with high-end virtual private networks (VPNs) pre-loaded on business computers are allowing people to work from home on personal devices either with no VPN or with a lower-end virtual private network that may be less hacker resistant," IATAM said in a statement.

Assets on home networks are fundamentally less secure. Many businesses reacted quickly to stay-at-home orders. If unprepared, their technology has no chance to adapt as quickly, leaving many people working from home under less-than-ideal security conditions.

"Many company devices were deployed into a work-from-home situation quickly, leaving little time to ensure that they would be secure via a virtual private network or other means," IATAM said.

SafePaaS™

Data Protection Regulations

Privacy regulations such as GDPR, implemented in Europe in May 2018, gives consumers more choices and protections about how their data is used. For companies, the GDPR requires meaningful changes in the way they collect, store, share, and delete data. Failure to comply could result in steep fines, potentially costing a company up to 4 percent of its global revenue.

In the United States, the California Consumer Privacy Act (CCPA) went into effect in the state in January 2020. It gives residents the right to know which data is collected about them and to prevent the sale of their data. CCPA is a broad measure, applying to for-profit organizations that do business in California and meet one of the following criteria: earning more than half of their annual revenues from selling consumers' personal information; earning gross revenues of more than $50 million; or holding personal information on more than 100,000 consumers, households, or devices.

Organizations should develop clear, standardized procedures to govern requests for the removal or transfer of data by adopting a data protection framework to comply with privacy principles. For example, start by assessing your existing data management practices and processes against the following GDPR principles to identify the gaps:

Principle 1: **LAWFULNESS, FAIRNESS, AND TRANSPARENCY**

Consumer consent is critical: Core to the GDPR is the idea of consent—any EU resident must give explicit consent before their personal data can be captured, processed, and stored. GDPR narrows the scope of the EU Data Protection Directive's 'opt-in' system that states, personal data must be collected for a very specific, pre-defined purpose clearly communicated to each individual.

Shifting data control back to the individual: The 'fairness' element of the principle instructs that all EU individuals have the 'right to be forgotten' or request that their personal data be deleted from all data stores within the organization (and from those of its third-party suppliers). In addition, ' transparency' gives individuals the 'right to access' all personal data currently being held by the organization. Individuals can request a copy of all data held in a structured, digital, and commonly used format—a request that must be fulfilled within a month of receipt. In essence, the 'lawfulness, fairness, and transparency principle' shifts the control of personal data back into the hands of the individual.

Principle 2 & 3: **ACCURACY AND PURPOSE LIMITATION**

Data authenticity is a must: Closely linked to the principle of transparency is that of accuracy. The 'accuracy principle' mandates that all personal data must be accurate and kept up to date. It gives individuals the right to request that inaccurate information be corrected. The 'purpose limitation principle' instructs that personal data can only be processed for its initial intended purpose; further processing of the collected data is prohibited without renewed consent from the individual.

SafePaaS™

Principle 4 & 5: **DATA MINIMISATION AND STORAGE LIMITATION**

Limiting the scope of data collection and storage: The GDPR introduces the concept of 'Privacy by Design and by Default'—integrating data protection and privacy controls into the development lifecycle of new business processes, applications, and services that touch personal data. The 'data minimization principle' states that only the personal data that is absolutely necessary should be collected. Further, the 'storage limitation principle' mandates that personal data must be stored for no longer than is required and that individuals must be informed about the planned retention period for their personal data.

Principle 6: **INTEGRITY AND CONFIDENTIALITY**

Limiting the scope of data collection and storage: Encryption is the cornerstones of protection: Personal data should be protected appropriately according to the 'integrity & confidentiality principle'. Building on 'privacy by design', the GDPR states that personal data should be rendered anonymous where possible. This anonymization ensures that EU residents can no longer be identified by the data. As such, restrictions on processing the data are circumvented. In addition, Article 25 of the GDPR mandates that controllers implement appropriate technical and organizational controls to safeguard the processing of any personal data that cannot be made anonymous. The effectiveness of implemented controls must be measured and documented on a regular basis.

Principle 7: **ACCOUNTABILITY**

Data Protection Officers govern adherence to regulation: The final principle, the 'accountability principle', instructs that all organizations processing personal data of EU residents must be able to give evidence to demonstrate compliance with all other principles. As such, organizations that systematically collect and process personal data must appoint a data protection officer (DPO). This role will be pivotal in governing the implementation of controls necessary to comply with the GDPR rules. Data breach notification becomes mandatory: All controllers and processors of personal data must designate a supervisory authority—a country DPA who, in addition to the DPO, maintains primary oversight of all data-processing activities. Each organization must implement a data-breach notification scheme that ensures all known breaches are reported to the appropriate DPA within 72 hours and records of these data breaches are stored.

Heightened requirements for processors: The onus is on organizations to continuously monitor, review, and enhance controls to limit and secure the processing of personal data. And for the first time, the responsibility doesn't fall fully on controllers. Under the regulation, data processors are also responsible for the maintaining the privacy and confidentiality of personal data. They must ensure adequate technical and administrative controls to protect personal data. Data must also be processed solely according to any contracts laid out between the controller and the processor. Notably, the gap between controllers and processors in terms of risk and liability has shrunk.

SafePaaS™

Data Governance Best Practices

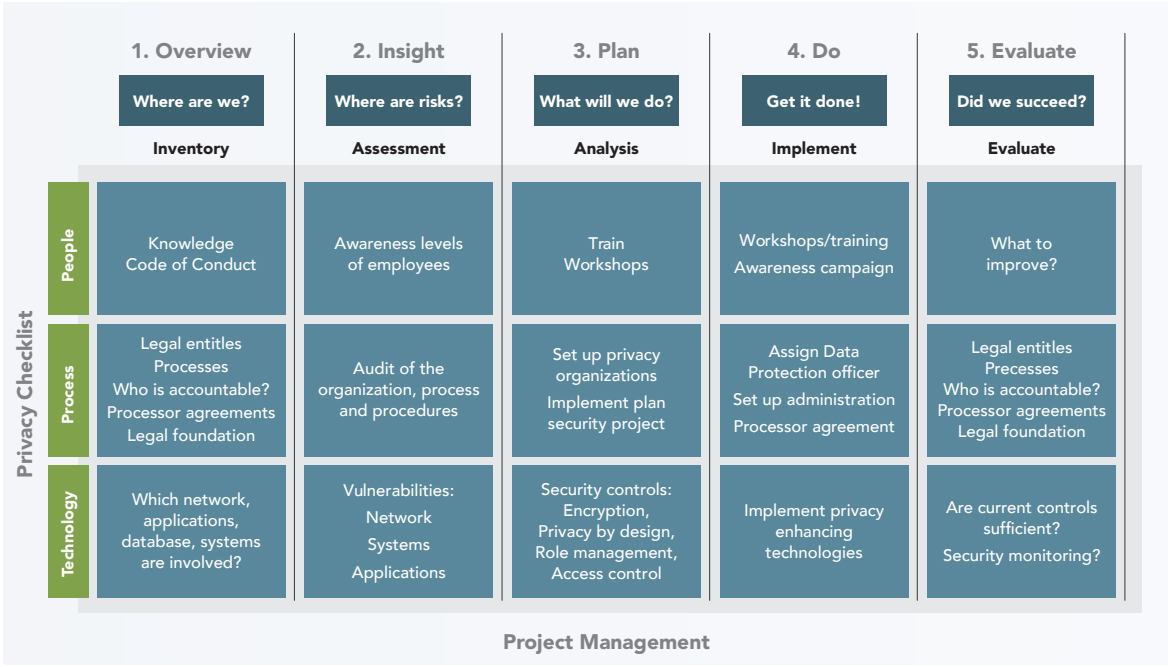
Data Governance best practices have emerged for organizations that seek to address enhanced data-protection requirements. These span the life cycle of enterprise data, and include steps in operations, infrastructure, and customer-facing practices, and are enabled by data mapping.

Data governance requires a combination of a data protection project team, a defined process, and technology tools.

Establish a Data Protection project team that includes members trained on the data management process and technology. Ideally team members should be well versed in data privacy management requirements and best practices. The team will be responsible for conducting the tasks and provide necessary requirements for a comprehensive assessment.

Design and document the process workflow of gathering data protection requirements and identify gaps against the requirements. Prepare survey templates to gather requirements to build efficiency in the process. Multiple template may be required based on data source, data types and compliance mandate.

Implement the data protection platform to ensure collaboration and sustainability. A minimum viable data protection platform should support built-in digital data discovery, data inventory, DPIA / PIA and assessment templates enabled by workflows, and analytics that will enable the team to collaborate, guide the workflow process, serve as the central repository of compliance evidence, and facilitate ongoing periodic audits that reflect business changes.



This chart shows a high-level plan that can be used to develop a sustainable data governance plan:

SafePaaS™

Detect, Remediate and Prevent Oracle Data Breaches

Oracle is the most widely used database for business-critical applications such as Oracle E-Business Suite, SAP, PeopleSoft, J D Edwards, Hyperion, as well as Oracle Fusion Cloud. A data breach in these ERP business applications or other industry solutions such as Retek Retail Solution, Higher Ed Campus Solution, Telecom Billing Solution, etc that store information on customers, employees and suppliers can lead to increased compliance risks, loss of customer trust and reputational damage.

Oracle data protection requires continuous data access monitoring to safeguard Oracle database and applications against threats such as:

- Stolen credentials obtained from social engineering, key-loggers, and other mechanisms to get access to privileged accounts in your database.
- Insiders that misuse privileged accounts to access sensitive data, or to create new accounts, and grant additional roles and privileges for future exploits as well as bypass the organization's usage policies.
- Unintended mistakes from junior DBAs who might use unauthorized SQL commands that change the database configuration and put the database in a vulnerable state.
- Sensitive data leaks during maintenance window from the application administrators.
- Weaknesses in the application access controls resulting in escalated privileges that create the surface area for attack on the underlying database.

Oracle customers should take a risk-based approach to detect, remediate, and prevent data breaches in business-critical Oracle systems. First and foremost, establish data access policies, and detect access policy violations by scanning data access privileges. Next, remediate the risks by removing user access where possible and anonymize or pseudonymize sensitive data where access must be granted. Finally, prevent future data breach risks, by adding approval workflows to control privileged user accounts as well as control application and system configurations.

Establishing access policies requires control over full application functions and schema or around specific transactions and tables with sensitive data. These security policies, when applied to an access rules engine, identify application data which is a potential risk of unauthorized privileged users access. The same polices can also be used to provide real-time preventive controls that prevent ad hoc changes to application security and data structures.

Remediation requires corrective actions that remove user access and privileges to data that is marked for protection under the established access polices. User accounts are commonplace in all applications and databases and are used by privileges users and DBAs for daily tasks such as user management, performance tuning, testing functionality, patching, backup and recovery, and space management, etc. Many Oracle predefined system users such as SYSTEM and roles such as DBA role can

SafePaaS™

access any application data in the database. Due to their wide-ranging access, most organizations enforce strict processes and internal rules on who can be granted privileged access or DBA access to the databases. These accounts and roles, however, have also been a prime target of hackers because of their unimpeded access inside the database. They have also been misused by insiders to gain access to confidential information. Therefore, remediation should include limiting the use of system accounts as well. Additionally, anonymization and pseudonymization of data can also reduce the risk of accidental or intentional data disclosure by making the information unidentifiable to an individual even with access to system accounts.

Prevent future data breach risks by controlling user access requests to applications and data using multi-level workflows that provide fine-grained data access risks within the approval request. High risk application and database configuration controls can also be enforced using approval workflows to prevent system changes that could lead to an insecure database configuration, prevent configuration drift, reduce the possibility of audit findings, and improve compliance. Changes to database structures such as application tables and roles, privileged role grants, and ad hoc creation of new database accounts are just a few examples of configuration drift that can have serious consequences. For example, Oracle Database Vault allows customers to prevent configuration drift by controlling the use of commands such as ALTER SYSTEM, ALTER USER, CREATE USER, DROP USER, etc. It can also establish an additional layer of database controls over Privilege Users such as DBA account to further improve security by creating a highly restricted application environment ("Realm") inside the Oracle database that prevents access to application data from privileged accounts while continuing to allow the regular authorized administrative activities on the database. Realms can be placed around all or specific application tables and schemas to protect them from unauthorized access while continuing to allow access to owners of those tables and schemas, including those who have been granted direct access to those objects.

To learn more contact:

Emma.kelly@safepaas.com
https://www.safepaas.com/contact
https://www.safepaas.com/

SafePaaS™