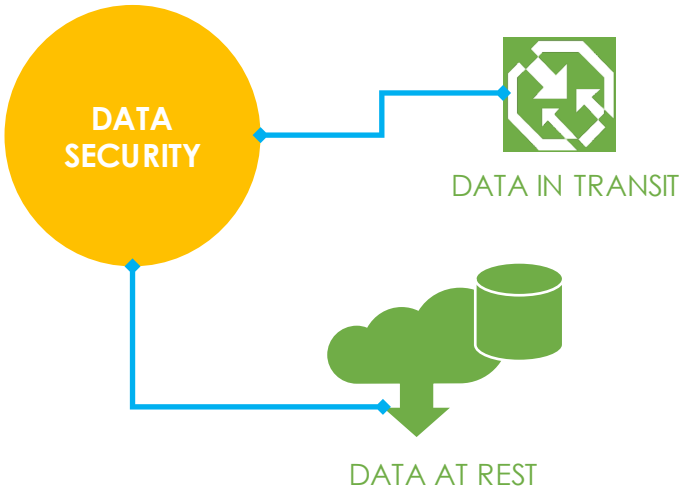
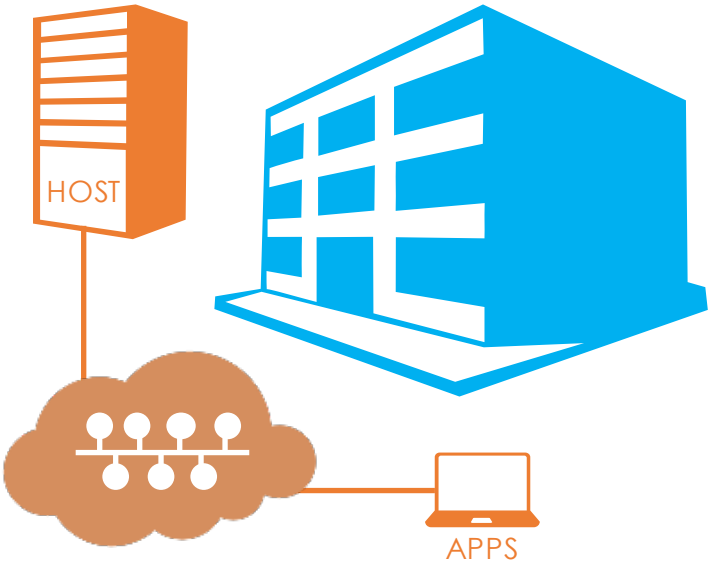
Secure Your Data
A Best Practices Guide

With significant rise in cyber attacks, managing security for organisations has been an indispensable task. The greater dependence on inherently distributed computing resources has made the process of cyber-defense complex and difficult.

However, there has been rapid progress to counter cyber-threats, and organisations can avail expertise and solutions to keep their data secured both at rest (storage) and in transit (transfer).





The complexity of the scope of data security can be understood from the fact that we have to ensure that it remains safe (cannot be accessed without appropriate authentication) on the networks and hosts we have control, and also on those we do not have control, yet we use those to transfer our data through and store some information about or even the data itself. Thus data security pervades physical domain, technology and administrative processes too.

In this guide, we propose a five step method, a framework, to ensure appropriate security measures for your data.

1. Evaluation

Before adopting any security framework for your organisation, it is imperative to understand the specific requirements that your business pose in regard to security.

During business operations and customer relationship management, the sensitive data of your customers are exposed to people who directly handle such operations, and business associates and subcontractors who support such activities.

The evaluation will also have to be done towards adopting available technologies, established standard practices, and imparting training to the people involved in the whole process.

While **SSL** certificate has been a de facto standard for encryption and validation of data in transit, **PIC-DSS** and **HIPPA** have become standards to store and manage sensitive data. Similarly, **OWASP** guidelines are the most accepted list to adhere to for the software apps on web and cloud. Also, **ISO 27001** enforces best practices in the organisational processes and facilitates implementation of security frameworks within organisation and in the associated supply chain.

2. Preparation

Once we have the list of requirements, those specific to the industry concerned or just standard procedures, we should then move forward with a set of goals and the timelines in which these goals can be achieved. This of course includes strategy of managing threats.

Preparation for implementing a security framework in an organisation involves skill upgrades (more than just awareness), choice of right technologies and using those, refinements or modifications to the existing operational processes, and strategy to manage IT resources.

This step also includes a decision to adopt one or more security standards as the situation demands. In fact, it is the level of trust you would like to instill in your customers towards the security of their data that reside under your control.

It is imperative to engage all stakeholders of product and service deliveries in an organisation so that they understand and share the same security objective. There should also be an awareness drive among business associates and subcontractors to retain the integrity control in the whole process of security implementation.

Facility Access Control	Information System Activity	Accountability
PHYSICAL	TECHNICAL	ADMINISTRATIVE
Restricted access to facility Guidelines for workstation use, and handling devices and media	Network, Host and application hardening Security Information and Event Management (SIEM) system enforcement	Agreements with people who handle sensitive data Breach Notification Rule Audit Reporting and Documentation

3. Implementation

Implementation is critical, and is the most intricate part of any security framework. We must segregate the components that we use and have control over, and that we don't have control. The things we control is our own private network, onsite servers, workstations. We can also have a fair understanding over the level of security measures that are in place on the networks and servers in public clouds. Moreover, we may have an SLA to back such an assurance.

But then our data may be scattered on the Intranet and emails. These use network territories that we are not aware of. We do not also control such users directly who use our data on these networks. And here lies our security framework, which will ensure protection of data in different situations.

Apart from physical safeguards (an integral part of any security framework), we need to have requisite measures to handle user sensitive data, payments and operation over both trusted and untrusted networks.

With regard to process implementation, we must address privacy of data during saving, accessing and sharing. The issue of data integrity control needs to be tackled by managing unique user identification, emergency access procedures, authentication and validation of data in disk and databases.

The network and host must be hardened and application should adhere to standard security guidelines of OWASP. Encryption and decryption mechanism should be implemented as required for both data in storage and data in transit. SSL implementation is also an essential part thereof. VPN may be used for data access and management. Regular scanning service should be activated to prevent attacks from either internal or external vectors.

4. Management

Managing a security framework within an organisation entails continual monitoring and taking corrective steps. It is always an advantage if we have a Security Information and Event Management (SIEM) system in place for the purpose. Of course, assigning appropriate privileges to the users of the Information System must be done within the scope of RBAC (Role-Based Access Control) scheme.

The process can be more expansive if we have any of the standards like HIPAA, PCI-DSS, etc. implemented within the organisation. The technical aspects of such standard demand specific server and network setup, and would escalate the IT budget accordingly. But it is then the effective cost of operation that matters; and such cost escalation can be covered by better customer loyalty and the protection your organisation would enjoy due to this.

While physical and administrative aspects are rather straight-forward, managing information system would require extensive system administration and software management activities. You may opt for a right Cloud vendor to manage your data security at the central level as that is the most complicated constituent of the whole framework.

Evaluate the general requirements of your industry, and specific requirements.

Prepare your people and process to handle the transition.

Implement physical infrastructure, Information System and administrative process.

Manage your security within an information and event management framework

Audit your security framework and performance against the evolving cyber threats, and make changes as needed.

Capitalise on the opportunity to incorporate security solutions for your organisation

5. Audit

The cyber threats are evolving, and so also the solutions. On the other hand, an organisation has to protect itself from attacks and intrusions with their limited budget.

The audit requires up-to-date knowledge about the evolving security conditions, and clear understanding of appropriate solutions.

The audit may be done by internal experts or may be outsourced to an external vendor having such specialisation. The process will require to compare the performance of the existing security framework against the goals, and investigating the current and future security risks and vulnerabilities within the system. This will enable you to take appropriate actions to remain safe and secured with your data, and consequently, with your business.

Do not go at it alone!

Let Us Manage Your Security

www.batoi.com/solutions/security

BATOI®