**(BI)**

The ultimate goal of BI initiatives is to drive better business decisions that enable organizations to increase revenue, improve operational efficiency and gain competitive advantages over business rivals. To achieve that goal, BI incorporates a combination of analytics, data management and reporting tools, plus various methodologies for managing and analyzing data.

BI data can include historical information and real-time data gathered from source systems as it's generated, enabling BI tools to support both strategic and tactical decision-making processes. Before it's used in BI applications, raw data from different source systems generally must be integrated, consolidated and cleansed using data integration and data quality management tools to ensure that BI teams and business users are analyzing accurate and consistent information.

**7 REASONS WHY Peoples SHOULD ADOPT E-COMMERCE**

E-commerce refers to buy and selling of products via electronic systems like the internet and online payment gateway. In order to stand ahead of the competitors’ list appropriate [Ecommerce SEO services](https://www.estorefactory.com/) are imperative. The latest statistics from Statista have confirmed that global e-commerce retail online sales will touch $4.5 trillion in the next three-four years.

Most companies and sellers are making the best use of technology offering the most significant option for business firms to develop their outlets into a virtual retail store. Other interesting statistics from Statista B2B e-commerce sales are likely to touch $7.7 trillion soon.

In the United States alone, more than 60% of consumers purchase goods directly from online retail stores from the comfort of their residence. It clearly reflects the growing popularity of e-commerce stores in the US and other areas worldwide. People also love the idea of shopping necessary things 24x7x365 anytime and anywhere at the best and the most convincing price.

**Easy Doing of Business:** The listing services facilitate the entrepreneur to showcase their products one by one on the site itself.

**Product Offers and Datasheet:** Online product listing will enable retailers to display their products on the site properly. The ecommerce [**product listing services**](https://www.estorefactory.com/amazon-seo-ppc-services/) will help the entrepreneurs get good ranking on the site.

**Higher Search Engine Ranking and Visibility:** Online retailing largely depends on the number of traffic a site can generate.

**Warranty Disclosures:** One big advantage of e-commerce for retailers is that they appropriately disclose the warranty information with an apt description

**Less Inventory and Warehouse Cost:** In the last few years, e-commerce businesses have largely decreased the cost of inventory of goods through its automotive management inventory using web algorithm and other stockpiling techniques.

**Well-Researched and Stay Focused:** The ecommerce SEO provider offers an essential service of providing the right information relating to changing buying trends of the customers to the online retail owners. It helps the traders to stay vigil and fulfill customers’ needs and requirement first.

**Worldwide Sales of Products and Global Exposure:** The biggest advantage of online e-commerce business is its facilitation of the global sale of products. It also takes very less capital to start an e-commerce business than starting a traditional e-commerce business enterprise. Customers across the globe can easily buy these products from online e-commerce portals.

**Understanding eCommerce Digital Security**

If we have to put it into simple terms, we can say that eCommerce digital security is a set of guidelines.

These guidelines work towards ensuring that all the transactions happening through the internet are safe.

Users who engage in online selling and buying goods and services are protected by several protocols that are part of these guidelines.

Any eCommerce business must have basic security in place to win the customers' trust in the long run.

Such basic security includes - **Privacy, Integrity, Authentication, and Non-repudiation**. For an eCommerce business, taking care of these four pillars is as crucial as having a secure WiFi connection.

Prevention from all the activities that result in sharing customer data with unauthorized third parties is called Privacy. In the eCommerce business, you must ensure that customer data and account details stay between the retailer and the customer only, and no third party is included.

Most of the time, the sellers are responsible for the breach of confidentiality when they let others have access to private data. As an online business, it is your job to enable at least a bare minimum of firewall, anti-virus, encryption, or other data protection. It will help you in ensuring your customers that their card and payment details are safe with you.

This is also a vital concept of security in eCommerce. Integrity means ensuring that whatever information the customers have shared on the internet remains unchanged. According to this principle, the information shared by the customer should be used only for the reason it was needed.

If you make even the slightest of alterations in the data entered by the customer, they'll start to lose faith in the security and integrity of your business.

The authentication principle is there to ensure that both the buyer and the seller are genuine. They must be who they claim to be. Businesses selling a product have to prove the authenticity of their existence, their product, and whether they deliver on their promises.

The same goes for the other side. Customers should also prove their identity to make the seller feel secure about the transaction. Authentication and identification are something many eCommerce businesses are doing, so we know that it is a practical approach.

The word 'repudiation' means denial. And as the name suggests, the non-repudiation principle ensures that neither party can deny the actions they have performed throughout a transaction.

Both the seller and the customer should move forward with the transactions they have initiated. Many people, because of the virtual nature of transactions, feel eCommerce to be less secure. In this situation, the non-repudiation principle acts as a layer of protection.

**6 Reasons eCommerce Secure and Succesful**

**1. Reduces Customer Churn**

For any business, customer retention is one of the top priorities, and it is not easy as many people consider it to be.

To reduce the churn rate, it is essential to create a foundation of trust. To foster trust, you have to be very transparent and upfront with your data collection methods and procedures.

You can ask customers how they feel about the current privacy policy through various surveys and feedback forms.

2. Protects Corporate Assets

Your workforce must have skilled, responsible, and result-oriented individuals to manage the eCommerce business.

Suppose you wish to maintain a high level of efficiency and perform tasks optimally. In that case, you'll have to allow your employees to access a certain level of data from your customer database.

This can be data from support tickets, demographics, internal documents, financial statements, and much more.

However, you can't allow everyone to access this data. You must restrict its access from the ones who should not see it.

Balance out the risk associated with the misuse of your confidential and invaluable data, and ensure the database resources are used appropriately by asking users to verify their credentials.

3. Improves the User Experience

UX design and convenient navigation play an essential part in impressing a consumer and determining how they see your brand.

If your data collection notifications are not very clear, customers might not want to interact with your eCommerce site, which means you'll have a shortage in sales.

4. Boosts Employee Competence

Training employees to understand threats and determine their level of seriousness is very crucial for the success of any eCommerce business.

When your employees are adequately educated about the best practices, they can act as the front line to prevent hackers and viruses from entering the enterprise.

5. Optimizes Business Processes

Companies are updating their software to increase functionality and make systems capable of completing required tasks.

Most of the updates contain vital improvements in terms of security. It can clear out bugs, which results in speeding up the process.

6. Protects from Ransomware

Another digital security threat for eCommerce businesses is ransomware, a type of malware that encrypts a business's data.

The data or system can only be unlocked in exchange for a considerable sum of money. Any data that you have stored in your system can be at risk from ransomware.

You can do prepare by creating a backup of your important files in multiple places. This shouldn't be limited to cloud services, but also locally and on portable storage devices.

Biggest Security Threats to eCommerce Sites

There are numerous types of digital attacks you might face as an eCommerce business. And it is not possible to talk about even half of them in this blog post.

Phishing is a form of digital security threat that evolves the most. In eCommerce, this data privacy attack can cause devastating damage to both businesses and customers.

There are numerous types of phishing too, but let's not get into that here. If not identified properly, phishing can ruin the reputation of brands.

Malware and Ransomware

If your site is loaded with malware or ransomware, your customers might get their devices infected which can lock them out of their system and important data.

SQL Injection

This is a type of digital attack in which hackers use SQL (Structured Query Language) code to tamper with the database and gain access to valuable pieces of information through it.

This type of attack is one of the most prevalent ones on the internet, and attackers can potentially use it against any web application or website that has used an SQL-based database. Since SQL is used in most eCommerce sites, they are quite vulnerable to this attack.

Cross-Site Scripting (XSS)

In cross-site scripting (XSS), several malicious scripts are injected into benign and trusted websites.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end-user will never know what the script contains, and when executed, it will do the harm it was meant to do.