



DATA SECURITY

A COMPREHENSIVE GUIDE FOR BEGINNERS



Contents

1. Introduction to Data Security	03
2. What is Personally Identifiable Information?	04
3. Why is it important to protect PII?	05
4. What is Data Security?	07
5. Importance of Data Security	08
6. Advantages of Data Security	10
7. Three Stages of Digital Data	02
• Data at Rest	
• Data in Transit	
• Data in Use	
8. Protecting the Data: Stage by Stage	13
9. To Conclude	19
10. References	20

Introduction to Data Security

According to Wikipedia, Data is anything that denotes “characteristics or information, usually numerical, that are collected through observation.” In short, our names, addresses, email ids, phone numbers, social security numbers, and any other similar information can be classified or identified as data.

Even weights, prices, costs, numbers of items sold, product names, tax codes, registration marks, etc. are all data. Images, sounds, multimedia, and animated pictures are visual representations of data.

Many a time, the terms "data" and "information" are often used interchangeably, however, these have distinct meanings. Data is sometimes said to be transformed into information when it is viewed in context or post-analysis. While in the academic treatment of data, it is treated as units of information, the use of data can be varied including for scientific research, business management, finance, governance, and virtually in every other form of human organizational activity.

To be precise, we are surrounded by data. But this data is extremely delicate in nature and requires complete protection from falling into wrong hands. The need for data security is immense.



When talking about data security, it is the process of protecting data. Though not the only process of protecting data, data security is identified as one of the top ways of keeping the data safe.

Used by all organizations, both big and small, private and public, data security is a topic of high importance. This whitepaper makes an effort to delve deeper into the concept of data security by taking into consideration some of the basics about it. By clearing the basic concept of data security, we aim to create more awareness around both organizations and their employees.

In this whitepaper, you will learn about:

- *What is data security?*
- *Why is it important?*
- *What is Personal Identifiable Information?*
- *The different stages of data security and how to protect data in each stage*



Personal Identifiable Information or commonly known as PII has been the topic of discussion for many years now. The term has been doing its rounds in the industry, yet, the cloud of confusion surrounding it is immense.

National Institute of Standards and Technology Special Publication 800 defines Personally Identifiable Information as *"any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."*

What is Personal Identifiable Information?

“

To simplify this definition, PII is any data that helps you identify yourself.

”

PII covers a wide list of information that can be used to identify a person. Primarily some of these include:

- Name
- Postal address
- Email IDS
- Phone numbers
- Date of birth
- Social Security Numbers
- Credit card numbers
- Passport number
- Driver's License number, and much more.

However, with the expansion of technology, the scope of PII has increased as well.

Login ids, digital images, IP addresses, biometric, geolocation, and even social media posts can be considered PII.

Now, it is essential to understand that PII is the American version of Personal Data, which is highly prevalent in the European Union.

Most organizations collect PII of their customers for various reasons, including:

- To improve the quality of services provided
- To re-sale products or services
- To market their products and services, and much more

Different countries have different sets of rules when it comes to protecting all the personal data that is collected. While Australia has the Privacy Act 1988, the EU has put into action GDPR. HIPAA is commonly followed in the United States of America.



Why is it important to protect PII?

Personal Identifiable Information is unique to each person and can be used to identify individuals.

This automatically renders PII as intricate data. In the wrong hands, PII can be used for fraud and scams. And that is a good enough reason to ensure that your data should be protected!

This type of personal information can often be used to steal someone's identity. Depending on the thief's intention, such delicate data can be used to commit a myriad of crimes.

Often cases are heard where cybercriminals have accessed an individual's PII as means to malicious intent.

Various studies have shown that in 2016, cyber-criminals reached its peak of committing identity theft. Up to \$16 billion were lost in identity theft and fraud.

You must be thinking of how identity theft occurs?

And when it happens what is done with the data?

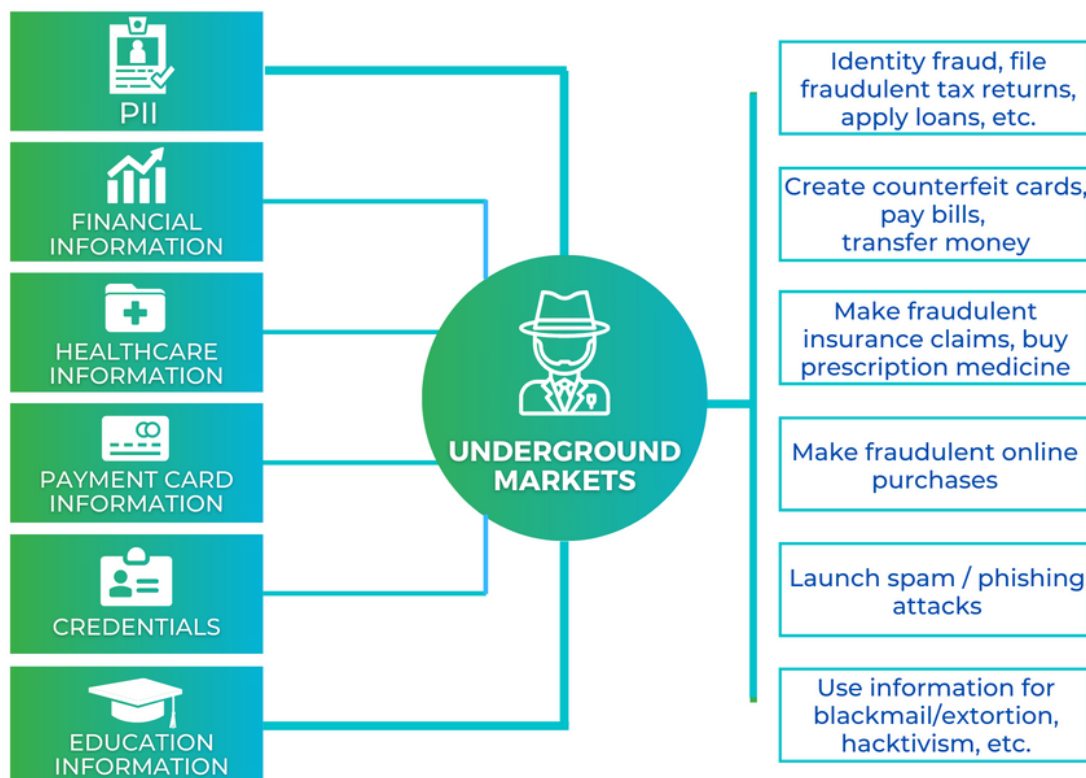
Well, let's delve deeper into the same.

The general public has a misconception that identity theft occurs primarily due to hacking. However, studies show a picture that is quite different.

Between the years 2005 to 2015,

- 41% of identity theft occurred due to loss or theft of a device
- 25% of identity theft happened due to hacking or malware
- 17.38% of identity theft as a result of unintended disclosure
- 12.01% of identity theft occurred due to insider leak
- 1.43% of identity theft as a result of payment card fraud
- 3.16% remains unknown

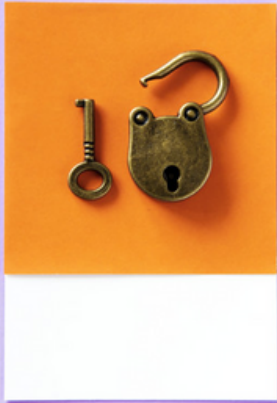
Now the question stands, what happens to all the information that is stolen? Here is a diagram to help you comprehend the situation better.



Source : <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity>

No doubt safeguarding all that personal data is a responsibility that lies with us, both individuals and organizations. Thus, the introduction of data security.

What is Data Security?



In simple terms, data security is both the practice and the technology of protecting valuable and sensitive company and customer data, such as personal or financial information. As mentioned earlier, every organization collects personal data for reasons that can be varied. And each of these data collected is extremely valuable. Sensitive too. This makes it pivotal for organizations to secure the data. Hence, data security.

Data security can be applied using a range of techniques and technologies. This can include administrative controls, logical controls, physical security, organizational standards, and other safeguarding techniques. The idea here is to limit access to unauthorized or malicious users.

The process of securing data for each organization can be different.

Several considerations are taken into account when securing data. Some of these may include:

? *Where is the sensitive data located?*

The first step to protect your data is to know where it is located. Without knowing where the data is stored, it is impossible to take the right measures.

? *Who has access to the data?*

When users have unchecked access to the data or have infrequent permission reviews, it puts the organization's data at the risk of theft or misuse. It is thus pivotal to know who has access to the company's data at all times. This step is most vital when making data security considerations.

? *Has real-time monitoring of data been implemented?*

Continuous monitoring and real-time alerting are essential not only to meet compliance regulations but also to detect unusual activities and suspicious accounts. This consideration is important before it is too late.

While these considerations are integral to securing your organization data, there are three core elements of data security. Often known as CIA Triad, this is a security model and guide that allows organizations to keep their sensitive information protected from unauthorized access and data exfiltration.

These elements can be identified as:

- *Confidentiality ensures that the data is accessed only by authorized personnel*
- *Integrity ensures that the information is reliable and accurate*
- *Availability ensures that the data is available and accessible for various business needs*



By creating a security system that includes both the considerations and the elements, a robust result can be achieved.

Importance of Data Security

When it comes to the importance of data security, many organizations still appear to be in doubt.

It is often assumed that only big organizations should worry about securing their data, but in reality, regardless of the size of your company, data security is a necessity.

Here are three compelling reasons why data security is important.

Ensure the Continuity of Your Business



The industry today is data-driven. Data forms the primary asset of all organizations in today's landscape. From running operations to making decisions, much relies on the data acquired and available.

Now imagine, one morning you walk into your office and find that all the data you have collected over a period has disappeared. This will render your business unable to function. Data security ensures that routine backups are made and all of it is available in its original form, ensuring business continuity takes place.

Avoid Data Breaches



Every organization is responsible to perform its due diligence when it comes to client information or employee records. Data breaches can severely impact an organization and have negative consequences including:

- Financial loss
- Loss of public trust
- Damage to brand reputation
- Legal or regulatory consequences associated with breaches of private information

Every year, small and medium businesses (SMEs) lose almost \$120,000 per cyber incident. A cumulative total will be huge. Thus, data security is a topic that no organizations can ignore.

Prevent Unauthorized Access to Private Information



Over the years, hackers have updated themselves with the latest technologies. They have become savvy when it comes to evading security measures. Companies that do not pay heed to security can be compared with us leaving our front door open at night.

Every business has vulnerabilities, and some of these include:

- Computers, laptops and other electronic devices
- Website
- Network
- Peripheral equipment

By adding walls of security, access to this vulnerable information can be prevented.

Reading these points only affirm the idea that data security is of paramount importance and should be considered by all.





Now that we have already established the background to data security and why it is important, let us look into the advantages of offering security.

Protecting valuable information

Any information that you collect from your clients or employees is sensitive. This goes without saying. No matter what product you develop, until you can protect valuable information, the process is not complete. You just make your life easier by integrating data security measures.

Staying ahead of competitors

Security is often not considered by many. By keeping your security system updated, you can stay ahead of your competitors.

Advantages of Data Security

Given the industry security standards, if you consider it from the beginning, you just add to your list of benefits.

Caring about clients

If clients know that you provide robust data security, their trust in you increases tenfold. And let's be honest, trust drives sales. By having your data security in place, you just show clients that you care about them and that can be essential in increasing sales.

Reducing the costs of development

Plugging security into your application beforehand reduces cost development and support time. The necessity of adding security features to your solution is a mandate. The further you delay the process, the more codes you will have to modify. Inadvertent data loss caused by insecure software may cost you significant money and time. So having data security in place from the get-go will save you both time and money.

Increasing software interoperability

By adding security, you only increase software interoperability.

When updates are to be made, developers usually look at data storage and faster ways of implementation.

With data security in place, the exchange of software and its use becomes easier. And you just make your organization a reliable entity in the industry.



Stages of Digital Data

Now before you go onto selecting the right process for securing your data, it is essential to understand the different stages that data undergoes.

The process of securing data depends on the stage it is in.

There are three basic stages of data:



Data at Rest



File Servers & Network Shares



Document Management Systems



External Storage



Databases



Endpoint, Laptop, PCs



Mobile Devices



Cloud Storage

This term refers to data that is stored in a device or backup medium of any form. From hard drives to backup tapes, from offsite cloud backup to even mobile devices, any data that is stored and currently not in use is categorized under this term.

The data in this case is inactive yet stable. To simplify this, the data is not traveling within the system or network, and it is not being acted upon by any application.

When the data is at rest, it has already reached a destination (even if temporarily). Additional layers of security can be added to the data at rest to keep it protected.

It is pivotal to remember that data at rest should always be encrypted.

Data in Transit

Data in transit or data in motion is the second stage where the data is moving. It is the data that is currently traveling across a network or is ready to be processed.

The data in motion includes any data that is moving across both cable and wireless transmission. Emails and files transferred over FTP or SSH are often categorized under this.

The sensitive nature of communication makes it imperative that all data in motion should be encrypted. Adding encryption guarantees that it cannot be read or manipulated by hackers, cyber-criminals, or anyone who doesn't have access.



Email



Downloads, Uploads



LAN Transfers



File Sync Apps



Cloud



Collaboration tools

Data in Use



Office Apps, PDFs, etc



Databases, Corporate Apps



Cloud Apps



Mobile Apps

Data in use refers to the data that is being processed by one or more applications. This is the data that is currently in the process of being generated, updated, appended, and/or erased.

The data is often classified under this stage when it is being viewed by users accessing through various endpoints.

Data in use is the most susceptible to being hacked and thus, requires multiple layers of security. It is often challenging as multiple users access this mainframe data at the same time from various devices (which can also include personal devices).

Strong user authentication, identity management, profile permissions are primary to securing the data in use. As you identify these data in different stages, the process to secure them changes as well.



Protecting the Data: Stage by Stage



Protecting Data at Rest

Data at rest is usually considered to be secure when it is encrypted. With a proper encryption key at work, it will require an unworkable amount of time in a brute-force attack to decrypt the data.

Since the encryption key is not present in the same storage medium, is considerably lengthy, and is random, the data becomes immune to the attacks of the hackers. Different data protecting technology can be implemented here, which may include:



	Full Disk Encryption Device Encryption	File / Folder level Encryption	Database Encryption	IRM (Information Rights Management)	DLP (Data Leak Prevention)	MDM (Mobile Device Management)	Cloud Access Security Broker (CASB)
 File Servers & Network Shares	✓	✓		✓	✓		
 Document Management Systems				✓	✓		
 External Storage	✓	✓		✓	✓		
 Databases			✓				
 Endpoint, Laptop, PCs	✓	✓		✓	✓		
 Mobile Devices				✓		✓	
 Cloud Storage				✓			✓

01 Full disk encryption:

When the hard disk is encrypted, it cannot be accessed even if mounted to another device (in case you lose your device). The data will be transparent only to the correctly logged in user, regardless of the encryption. However, if the data is extracted from the disk, it wouldn't be secure any longer.

02 File encryption:

Under this process, not the entire disk, but only concerned files are encrypted. Files can also be encrypted when in transit to prevent unauthorized access. Only the people with the key to the file can access it. However, if the key is made public, accessing the data stored becomes easy.

03 Database encryption:

Database systems such as SQL Server or Oracle use Transparent Data Encryption (TDE) to protect data stored in databases. These technologies perform encryption and decryption operations on files in real-time. It also allows application developers to work with encrypted data using AES without needing to modify existing applications. However, once the data is extracted, it is no longer safe.

04 Digital Rights Management (IRM):

Using Digital Rights Management technologies documents can be encrypted and be accessible to only those with the rights. Unlike the other methods of encryption, the files can be read but not completely accessed or decrypted.

05 Mobile Device Management (MDM):

MDM tools protect data stored in mobile devices. They allow limited access to certain applications. They can also completely block applications. But if the data is sent outside the device, it can be easily decrypted.

06 Data Leak Prevention (DLP):

DLPs enable the location-sensitive data on an endpoint or network repository. When in the repository, the data can be deleted or blocked for certain users who have violated any security policy. But this is only applicable if the data is inside the organization. Once it leaves, no control can be maintained whatsoever.

07 Cloud Access Security Broker (CASB):

CASB allows us to apply security policies to documents we have in cloud systems such as Office 365, Salesforce, etc..

CASBs are capable of detecting sensitive data in certain cloud repositories and applying protection policies to these documents. However, like DLP, CASBs are applicable only when the data is still stored in the cloud. Nothing can be done once it has left the cloud.

Challenges of Data at Rest Protection

- The data can be stored in different media and equipment
- The data can be scattered across various mobile devices
- The data stored in the cloud can be difficult to manage
- It becomes difficult to comply with different data protection regulations



✓ Protecting Data in Transit

We are living in the age of digitalization and there can be different methods of sharing data with different people. Emails are the biggest source of sharing data. Over 3.9 billion people use emails daily and by 2023, the number can reach as high as 4.3 billion people.

Other collaborative platforms such as Slack or Microsoft Teams are also used widely to share data.

To protect such data that is in transit, the following methods can be used:

	Email Encryption	MFT (Managed File Transfer)	IRM (Information Rights Management)	DLP (Data Leak Prevention)	Cloud Access Security Broker (CASB)
 Email	✓		✓	✓	
 Downloads, Uploads		✓	✓	✓	
 LAN Transfers			✓	✓	
 File Sync Apps			✓		
 Cloud			✓		✓
 Collaboration tools			✓		✓

01 Email Encryption:

This provides end-to-end protection for all messages and attachments shared through emails. Public Key Infrastructure (PKI) is often used to encrypt the contents of an email. This is a combination of a private key (known to the sender) and a public key (known to the recipient). The former can be used to encrypt the email and can be decrypted only with the private key of the recipient. Once the email has been decrypted, it can be forwarded or copied.

02 Managed File Transfer (MFT):

This is used when transferring files through FTP. The file is uploaded to a platform and a link is generated to

download it. This link can then be shared with the recipient, who can download the same via HTTPS. Expiration date and time, or even a password can be set for the link. However, once the download is complete, there is no control over the security of the data.

03 Data Leak Prevention (DLP):

DLP technologies provide similar kind of protection to data in transit as it does to the data at rest. It can detect if any attempt is being made to share confidential data. Additionally, they can block of making copies can also be practiced. But these can be prone to false positives and block valid submissions.

04 Cloud Access Security Brokers (CASB):

Regarding data in transit, they can detect if any user is trying to make an unauthorized download of sensitive data or has violated any security policy.

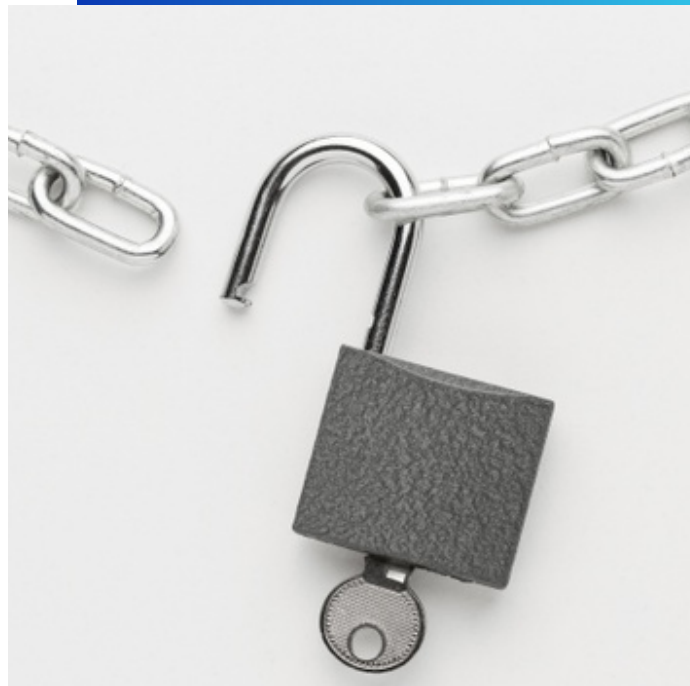
But once the data is downloaded, no security can be guaranteed whatsoever.

05 Digital Rights Protection:

The recipient can only view the data but not make any changes to it or download it. This method is often amalgamated with the DLPs and CASBs for additional data security, especially if the data being shared is confidential.

Challenges of Data in Transit Protection:

- There can be infinite channels and means of communication
- CASBs are available for a very limited number of applications
- It is impossible to maintain control at the receiving end
- It is difficult to determine what should be protected and what should be not



Protecting Data in use

As established earlier, it is extremely difficult to maintain the security of data that is in use. This type of data is extremely vulnerable as many have access to it and has to be decrypted in most cases. To protect such types of data, certain methods can be applied. These are:

01 Identity Management Tool:

Such tools check the identity of the person trying to access a particular file. These tools are designed to examine the background of the users. Two-factor authentication is often considered to be a part of this process.

		IdM (Identity & Access Management)	RBAC & Conditional Access (Role Based Access)	IRM (Information Rights Management)
	Office Apps, PDFs, etc			
	Databases, Corporate Apps			
	Cloud Apps			
	Mobile Apps			

02 Role-Based Access Control (RBAC):

Under this process, certain parameters are allocated to the users like their IP location to provide access. The idea is to limit access to only certain people. However, once accessed, the data can be easily obtained.

03 Digital Rights Protection:

This process limits the functions of all users. So even if you have complete authority to view the data, you might not have access to download it. For instance, editing or downloading the data can be controlled. There are cloud management systems or document managers that can be used to perform similar actions. This is one of

the most preferred methods of data security.

Challenges in Data in Use Protection:

- Tools only control access to data before allowing access. Once given access, there is no going back
- Users can take pictures of the data even if they do not have access to download it

There might be challenges to keeping the data secured, however, by limiting access and by adding layers of encryption, security can be achieved.

Most organizations thus combine 2 or 3 processes for each step to keep their data security game at the top.

To Conclude



Protecting the data in your organization is of utmost importance. Not only does it contain personal information of both clients and employees, but it can also contain sensitive information integral for the function of your business as well.

At MoveInSync, we deal with the data of thousands of employees and clients, adding data security to our priority thus. We understand the sensitivity of the data we collect to provide seamless commute services to our clients and their employees. Therefore, without a question, data security is a priority for us.

In each stage of data, we use top-level encryption, sometimes 2 or 3 processes, to ensure that the data cannot be breached.

Data security is becoming a major topic of discussion due to its rising importance in today's landscape.

With data security in place, we can prevent crime from happening. As it is often said, "It takes 20 years to build your reputation, and just a minute for a cyber incident to ruin it."

Let's protect our data.
Let's protect our people.

References

- <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity>
- <https://www.sealpath.com/protecting-the-three-states-of-data/>
- <http://aspg.com/three-states-digital-data/#.XzDUzCgzY2z>
- https://www.datamotion.com/best_practices_-securing_data_at_rest_in-use_and_in_motion/
- <https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest>
- <https://www.ccsegarra.com/advantages-of-offering-data-security/>
- <https://www.sales-i.com/the-importance-of-data-security>
- <https://www.infomaxoffice.com/importance-of-data-security-for-businesses/#:~:text=Data%20security%20is%20when%20protective,data%20from%20loss%20or%20corruption.>



MoveInSync Technology Solutions Pvt Ltd,
HSR Layout, Bengaluru, India 560 102

<https://www.Workinsync.io/>
hello@workinsync.io

