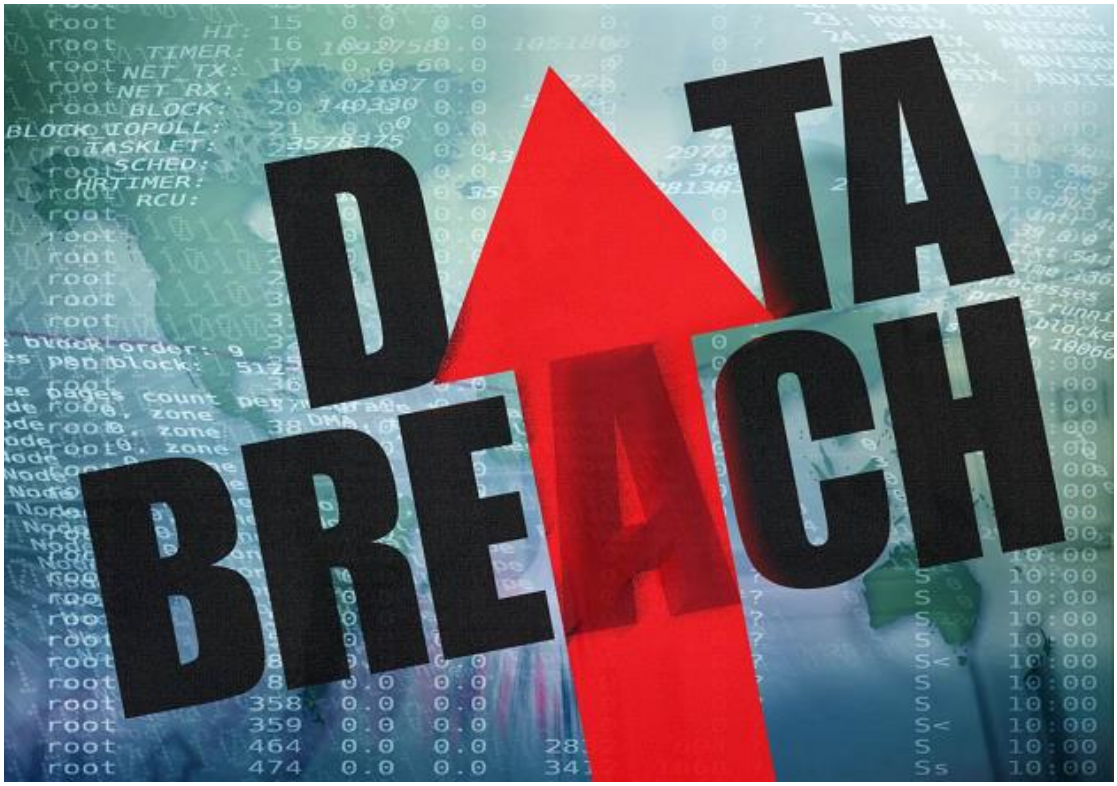
What Is The Difference Between

Data Loss Vs Data Leakage Vs Data Exfiltration?



We talk about data loss, data leakage and data exfiltration as if they are one of the same things. But, in fact, they are very different. And what makes it the difference is “**intention”**.

“Intention” is often defined as the purpose, aim, goal or objective to commit in carrying out action or actions in the future. It involves mental activities such as planning, rehearsal and forethought.

The difference between malicious and unintentional insider incidents is that the former has “intent” to commit a malicious act, whereas the latter, there is no “intent”.

Data Loss

Is the result of data that has been unintentionally or accidentally misplaced so that it is no longer accessible. Simply put, it is lost.

Here are some examples.

- One of the easiest ways to suffer data loss is by accidentally deleting the files without having any available backup.
- The computer disk drives may be physically damaged. They eventually break down over time.
- Power failures can ruin the effort and the time that you spent developing articles which were unfortunately not saved
- Water and fire damage on your expensive computers will definitely affect the electronics as well as the hard drive.

We often lose data simply because we haven’t got a proper workflow or procedure for data restoration.

Data Leakage

Is the result of the unauthorised and unintentional transmission of data within an organisation to an outside party. Be aware that data can be transferred electronically or physically.

Here are some examples.

- Someone taking a report home and accidentally misplaces it in the bus/taxi/train/plane. The leak occurs if someone takes that report.
- Sending an email with corporate information to the wrong recipient.
- Posting sensitive corporate information onto social media or public website with little security allowing the possibility of untrusted and unauthorised people to access information.

- Uploading work documents to unauthorised cloud storage to be able to access work from home.
- Unauthorised removal of physical equipment such as tapes, disks, or machines so that they can be worked on by a third party. How often have you seen a 2nd hand disk drive with someone else content on it?
- Storing sensitive information or programs on their laptops so that they could have full control over it.

Data Exfiltration

Is the result of unauthorised but intentionally copying, transferring or retrieval of data from within the organisation and taking it out. It is often referred to as "data theft".

Data exfiltration is primarily a "data breach" when the organisation data is illegally stolen. And the reason they steal it is usually for business advantage. They either take it with them to a new job, to start a new competing business or to take it to a foreign government or organisation.

Note, according to the insider threat division of CERT, nearly 75% of all data theft was carried out by insiders that had authorised access to the information.

What Can You Do Moving Forwards?

As the saying goes "data by itself" doesn't leave the organisation. It is essential that your organisation understand its information assets. Key questions that you must answer before you can move forward with a protection strategy needs to include the following.

- What types of data are processed? Is it medical information, personally identifiable information, credit card numbers, inventory records, etc.?
- What kind of devices process this data? Is it servers, workstations, laptops, mobile devices, etc.?

- Where is the data stored, processed and transmitted? Single location, multiple locations, foreign countries?
- How is this data being moved or transmitted? Does it involve only corporate channels or can it be moved using non-corporate channels like USBs, personal emails and cloud storage?
- What are the critical processes and systems that support the data?
- And who has access to these information assets?

Answering these questions will help your organisation to inventory your data and importantly develop the appropriate mitigation strategy whether it be data-loss, data-leakage or data-exfiltration.

How Can We Help You?

One of the best ways for your organisation to know its assets and protect them from the insider attacks effectively is to conduct a **data risk assessment**. The assessment purpose is to provide you with two key deliverables:

1. Who right now is placing your organisation at risk? Who right now may be putting your organisation in non-compliance? Is that the result of data leakage or data exfiltration?
2. What type of critical data does your business processes? Who has access to them and where it is stored? Is the data walking out the door without your knowledge?

Interested in gaining visibility? Reach us by leaving your details here - https://commsnet.com.au/contact-us .

Other Resources

Other similar articles

- ***Did You Know That All Data Theft Is An Insider Job***? You can find it here

- ***Why Data Loss Prevention Solutions Are Failing To Stop Insider Threat attacks.*** You can find it here

Take The Challenge

How resilient is your business from insider threat harm? Would you be interested in finding out how you compare to your industry peers? Would you be surprised to know that most organisations that have taken this assessment are somewhat vulnerable? To find out more, https://commsnet.com.au/contact-us

Contact Us

For more information, you can also send them an email at: info@commsnet.com.au Or give us a call at: +61 26282-5554.