Straive™

Connecting the dots

The Emerging Data Landscape Calls For A New Take On Data Security

WHITEPAPER

1. Introduction

A growing number of businesses are coming to the realization that their data is their most important asset. However, not even the most established companies are always successful in providing the highest level of data security. Devastating data breaches have been known to result in immediate loss of customer trust along with financial, reputational, and legal consequences. Additionally, it is extremely crucial to effectively safeguard company data from malware (malicious software), ransomware, and other risks as data protection requirements become more stringent.

Businesses risk exposing both their clients and themselves to data breaches as they collect more information on their readers online through e-commerce, email campaigns, and online subscriptions. According to the Cost of a Data Breach Report 2021, the average cost of a data breach worldwide grew by an alarming 10% in 2021. In light of this, it is evident that businesses must strengthen their security protocols.

The majority of database security breaches involve compromised credentials or malicious users. Software cannot prevent malicious users from causing harm or address the problem of persons intentionally or unintentionally losing or leaking credentials. Software, on the other hand, can evaluate a database's security concerns, profile user accounts, find sensitive data in a database and even disguise it, and audit database activities. To enable database security, data protection, and data governance, it is essential to have actionable intelligence about database users, database setup, database content, and database activities.

A growing number of businesses are beginning to take this threat seriously. Securing important assets and gaining a competitive edge is important, but so is adhering to consumer demands and industry regulations like the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and the General Data Protection Regulation (GDPR) of the European Union. Data breaches continue to be a real and ongoing threat, as evidenced by the education behemoth Cengage Group's agreement to purchase cybersecurity education provider Infosec for $190.8 million in January 2022.

2. What is Data Security and why is it important

Data security is the process of protecting digital assets from unauthorized access, unintentional loss, disclosure and alteration, manipulation, or corruption across all stages of its existence - from creation to destruction. This approach is essential for protecting the confidentiality, availability, and integrity of a company's data. Collectively referred to as the "CIA triad," businesses may suffer reputational and financial harm if any one of the three elements is compromised.

Implementing tools and technology that improve the organization's visibility into where its crucial data is located and how it is used is a key component of data security. These solutions should ideally be able to implement security measures like encryption, data masking, and redaction of sensitive information, as well as automate reporting to speed up audits and ensure compliance with legal standards.

2.1.Why Data Security Matters

Legally, businesses must take precautions to prevent user and customer data from being lost or stolen and getting into the wrong hands. For instance, the California Consumer Privacy Act (CCPA), the GDPR of the European Union, the HIPAA, and the PCI DSS are examples of industry and state rules that specify an organization's legal responsibility to secure data.

Data security is also essential for preventing the reputational damage associated with a data breach. A high-profile data breach or hack might cause customers to lose trust in an organization and switch to a competitor. In the event that sensitive data is lost, there is a danger of substantial financial loss, in addition to fines, legal fees, and restoration costs.

Today, organizations are placing more and more emphasis on data security. Here are the top reasons:

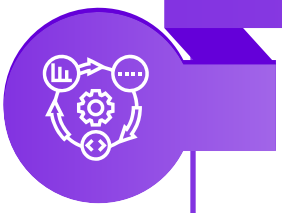
Data breaches:

A data breach, also referred to as a data leak, is a security incident that occurs when sensitive data is accessed by or made available to unauthorized viewers. Data breaches can lead to significant financial repercussions. It can disrupt business operations, which can have a negative impact on revenue. A breach may also result in legal penalties, and the regulatory body may impose fines or other penalties if it includes a violation of a compliance requirement or industry mandate.

Meeting compliance requirements:

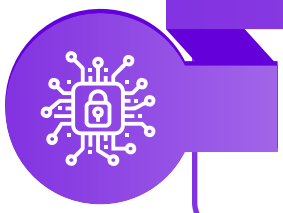
A robust data security plan must adhere to compliance regulations, but simply checking the appropriate boxes during compliance audits is not enough. Regulations frequently only address certain facets of data security, such data privacy, while real-world security risks advance more quickly than new laws. The protection of sensitive data should beconsidered as an ongoing, long-term endeavor. Businesses that disregard the need to protect sensitive data run the danger of paying significant fines and losing important client relationships.

Ensuring business continuity:



An organization must take necessary precautions to protect all information stored, including contact information of clients as well as financial and payment information. As consumers are increasingly more concerned about their privacy, businesses must make a commitment to safeguarding consumer data in order to preserve and enhance their brand value, demonstrate transparency and reliability, as well as to support and expand their operations. Companies can significantly lower the likelihood that a business continuity threat would disrupt the organization if they are aware of the risks and take adequate preparations.

Lack of cybersecurity talent:



Companies have resorted to a variety of stopgap strategies in an effort tohalt the onslaught of attacks as a result of the talent crisis, which has shown little sign of abating. Companies that are desperate for prevention against cyber-attacks leave themselves open to being taken advantage of by unscrupulous vendors that sell solutions that are only partially developed. Many firms still view security as an optional component rather than integrating it with business operations.

Cloud security:

Since the onset of the Covid-19 pandemic, cloud adoption has skyrocketed, as businesses have created opportunities for employees to work from home. Cloud data security was suddenly on everyone's radar. Historically, data protection solutions focused primarily on preventing malevolent attackers from entering systems containing sensitive data. However, with cloud computing, data is kept in systems that are outside the conventional boundary and is free to move anywhere. Consequently, businesses require a data-centric security policy that prioritizes the rotection of their most sensitive data.

The vast majority of businesses constantly acquire, sell, and transfer packets of high-value intellectual property online. It is obvious that people with criminal tendencies would be motivated to take advantage of such a high level of activity. Additionally, businesses are gathering an increasing amount of consumer data through social networking and online focused marketing initiatives in order to grow their communities, which makes it even more crucial to have effective data security protocols in place. There is no single approach that offers a comprehensive data security solution. Therefore, it's critical for companies to recognize their vulnerabilities and take appropriate precautions.

3. Components of Data Security

The 'CIA triad': The 'CIA triad' serves as the cornerstone of every data security strategy. This strategy must include policies, controls, technologies, and processes that safeguard data created, collected, stored, received, and transferred by an organization. Confidentiality, integrity, and availability comprise the "CIA triad" of Data Security requirements that all businesses must comply to.

01 Confidentiality entails limiting unauthorized access to sensitive information so that it does not reach the wrong hands. Organizations should employ security mechanisms including encryption, multi-factor authentication, secure configuration management, monitoring, and alerting, as well as access control lists (ACLs) based on the least privilege principle, to secure confidential information.

Integrity involves protecting data from unauthorized deletion or change. The widespread use of digital signatures by government and healthcare institutions to authenticate content validity and protect transactions is one way to maintain data integrity. **02**

03 Availability necessitates ensuring that security controls, computer systems, and software all function effectively so that services and information systems are always accessible when required. For instance, your accounting team won't be able to send, pay, or process anything until they have access to your financial database.

Data Privacy: Data privacy is an area of data protection that involves proper handling of sensitive data including personal data and other confidential data, such as financial and intellectual property data. Businesses make the mistake of assuming that by protecting sensitive and personal data from hackers, they are immediately in compliance with data privacy laws. However, this is not the case. Data privacy regulates how the data is gathered, shared, and used, whereas data security safeguards against data compromise by hostile insiders and external intruders.

4. Data Breach and Its Consequences

Millions of records and sensitive data could be lost as a result of a data breach, harming not just the organization that experienced the breach but also everyone whose personal information had been registered with the company. Detecting and preventing data loss has become one of the most serious organizational security challenges as the volume of data continues to expand dramatically and data breaches occur more frequently than ever before. In spite of the numerous research efforts that have been put into preventing the disclosure of confidential information, the issue continues to be a topic of current investigation.

There have been numerous high-profile cases of data loss over the past few years that have cost businesses millions of dollars. In 2016, Yahoo revealed that a data breach that appeared to have been "state-sponsored" in 2014 had resulted in the theft of at least 500 million accounts. In the digital era, where data volume is rising constantly, data leaks are occurring more frequently than ever. Because of this, ensuring that sensitive information is not shared with unauthorized parties has become one of the most critical security challenges for businesses

Internal and external information breaches can lead to data leakage, either on purpose or by accident. Managing and analyzing massive volumes of data gives businesses a huge competitive advantage. However, this also puts sensitive and important business data at danger of being lost or stolen, which poses substantial security concerns for businesses.

In the aftermath of a data breach, businesses can face an array of immediate financial repercussions. The Payment Card Industry Security Standards Council may assess sanctions for a data breach. Regulatory agencies and card network companies may levy an additional penalty, depending on the circumstances.

A company's responsibility to perform a forensic investigation to determine the cause of a data breach is one of the repercussions of a data breach. These investigations usually result in information and proof that can be used to stop such data breaches in the future.

4.1.Types of data breaches

We have witnessed numerous attacks over the last few years that have compromised the privacy of millions of individuals. The list is endless, ranging from intrusions that have compromised hospital patient information to breaches that have impacted universities and their students. Corporate security is not improving quickly enough, the security of vital infrastructure is in jeopardy, and state-sponsored hackers from around the world are becoming bolder and more competent. Let's examine the most common types of data breaches and their effects on businesses.

Malware or Virus:

Malware or viruses can be delivered to individuals with the intention of destructing information on their computers. Any business could suffer from this, but companies that rely heavily on data may be particularly affected. For instance, if a hospital received a malware, it might erase the data of it’s patients. This could lead to a very grave situation, which could also result in being fatal for some patients. To prevent these types of attacks, do not click on anything for which you are unsure of the source. Some businesses that request that customers or potential customers email them information may instruct them to include it in the body of the email rather than attach anything.

Ransomware:

Ransomware is when you receive an unexpected notification informing you that your computer or phone has been compromised. In this situation, the individual will inform you that if you pay a price in exchange. This might range from being negligible to costing hundreds of thousands of dollars. Many businesses employ risk management solution providers to prevent the release or deletion of sensitive or compromising data.

Stolen Information:

Humans are quite prone to making mistakes. mistakes could end up costing their business hundreds of thousands, if not millions, of dollars. It is extremely common for an employee's computer, phone, or file to be taken after being left in an unauthorized location. Such negligence can jeopardize client data in addition to newly developed prototypes that have not yet been made public.

Cracking Passwords:

Password theft is another highly widespread issue. This occurs more frequently than one would expect. There is a risk that snooping employees will access the information elsewhere if businesses leave computer passwords on notes that are accessible to anyone. If someone knows your password, it goes without saying that they can access your files and locate any type of confidential information on your organization that they want to see.

Phishing:

Attacks such as "phishing" include delivering false communications that seem to be from a reliable source. It is generally done via email. The intention is to steal personal information like credit card numbers and login credentials or to infect the victim's computer with malware. Phishing begins with a deceptive email or other communication designed to trick a target into divulging sensitive information. The communication is designed to appear to have originated from a reliable source. The victim is persuaded to divulge sensitive information, typically on a fraudulent website. Phishing is frequently the first step in cybercrime assaults like ransomware and advanced persistent threats (APTs). No single cybersecurity solution is capable of preventing phishing assaults. Instead, enterprises must employ a multi-layered strategy to lower the severity of any attacks that do happen and cut down on their frequency. Access control, malware prevention, email and online security, and user behavior monitoring are all network security technologies that need to be implemented. User education is another method of protecting your firm from phishing. Targets frequently include senior executives. It is therefore important to instruct them on how to identify phishing emails and what to do if they get one.

5. Securing your data is important, but how?

Data loss prevention (DLP) is rapidly transitioning from a nice-to-have to a must-have as more and more companies are empowering workers to work from anywhere, on any device. After realizing the threat that cybercriminals with malevolent intent pose to their data subjects, several nations have joined the data protection bandwagon over the years. This is a war that nobody wants to fight, but we must all be prepared for it. Several fundamental defensive measures should be used in such a situation where those with both good and bad intentions are aggressively chasing the data of individuals and organizations.

Establish a data protection strategy:

Every organization must create, implement, and maintain a robust data security plan. This strategy should include a list of the many categories of data that the company collects, stores, processes, or communicates. Clearly articulating security policies and procedures for each category of data is essential. Additionally, the data security plan should specify the steps to be followed in the event of a real or hypothetical security breach. Responses to data requests and demands made by government bodies should also be addressed in the data security plan. The organization's sole point of contact for handling government data requests should be identified in the plan.

Data Encryption:

For sensitive data, data security plans should mandate the use of strong encryption. Data should be transmitted and kept in encrypted form. Even if the third party can provide encryption services themselves, it is still best practice to encrypt the data before transmitting it. This is necessary when employing external parties for the purpose of data storage. The NSA and law enforcement agencies often demand encryption keys and other information from data storage and communications companies. In this context, it is essential to utilize your own encryption technologies to secure the data more completely, rather than depending on service provider encryption that government authorities can easily decrypt.

Use firewalls & access controls:

Usage firewalls and access controls: Data security strategies should mandate the use of access controls. Passwords, authentication requirements, and biometric systems should be implemented as part of these controls. It is recommended to use several authentication methods. Data security policies and procedures should take into account the fact that all authorized users' behavior affects how well user authentication mechanisms like passwords work. For instance, the entire network and all of the data it manages could be compromised if one person loses control of their password. When managing access to the core data network from mobile devices and the internet, it is important to implement access control measures such as firewalls.

Manage your own data:

Data security plans should specify which information is deemed to be so sensitive that it should not be kept on devices connected to untrusted networks. Some extremely sensitive information might not be maintained on machines that can be accessed through the Internet for security reasons. It is crucial that every organization carefully assess all the many types of data it manages to determine whether part of it ought to be kept off computers that can be accessed remotely.

Use external service providers with caution:

Data security plans must include policies and processes for the usage of external parties for data storage, communications, and processing. The plan should specify the circumstances in which such external data service providers may be employed and the types of data that may be processed by these service providers. In order to comply with the organization's data security plan and all relevant legal and regulatory obligations related to the data, it is crucial to ensure that the service providers' data security procedures are adequate. All data service providers' past performance and service offers must be thoroughly evaluated in advance. Key data security clauses that are legally enforceable should be included in terms of service and service agreements with data service providers.

Malicious parties, inadvertent events, and governments all around the world pose a threat to critical data held by all organizations. Data security breaches can have disastrous effects on any business. In light of this, an organization's entire strategic planning and risk management analysis should include a key component on data security. Planning and analysis with legal counsel are essential.

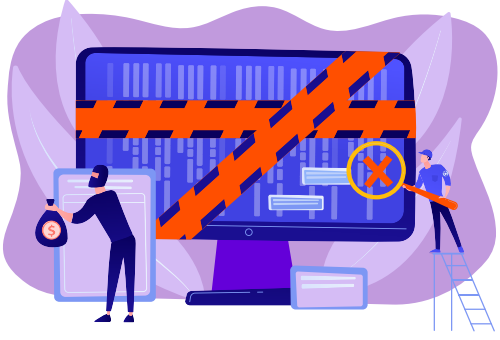
6. Supply Chain Attacks - the new go-to tactic for hackers

A Supply Chain Attack happens when someone gains access to an organization’s systems and data through an external partner or provider. A supply chain attack aims to compromise and disrupt a system within the organization's supply chain with the objective of doing harm. Attacking a third-party supplier or vendor with ties to the actual target is a common method of accomplishing this.

6.1. Detecting a Supply Chain Attack

An enterprise should first have a systematic verification mechanism in place for all the potential entry points into a system in order to efficiently detect supply chain attacks. Taking stock of all of the assets and data paths contained within a supply chain should be done, as this will make it easier to identify any potential security flaws that may exist within a system.

The subsequent action would be to construct a threat model of the environment the organization operates in. Assigning assets to various kinds of adversaries is one aspect of threat models. The categories can then be ranked to determine an attack's severity. It is important to update these scores frequently and organize assets in terms of their level of exposure to risk.



It is imperative that each and every new update be tested as soon as it is released. Tests designed to detect supply chain attacks should be able to locate malicious file activity, registry keys, and mutual exclusion (mutex) files.

6.2. Best Practices against Supply Chain Attacks

Attackers constantly search for the weakest link when it comes to supply chain attacks. Therefore, even sophisticated corporate defences may not be sufficient to safeguard vital assets. The fact that these applications come from a trustworthy third party implies that they are frequently exempt from the same level of examination. This presents an opportunity for attackers. If they go deep enough back along the supply chain, there is a good chance they will locate an exploitable flaw and begin their ascent to vital applications.

Security best practices are essential for minimizing the risk of supply chain attacks. These include:

1. Third-party risk management - Businesses are required to carry out a comprehensive review of the safety procedures followed by their suppliers. To ensure that all departments are on the same page in terms of security, they must eliminate internal operational silos.
2. Authentication and encryption - Enterprises can mitigate the impact of supply chain attacksby identifying and encrypting highly sensitive data in their ecosystem. Even if hostile actors get access, they will not be able to access protected assets.
3. Evaluating existing strategies - Improved supply chain security begins with existing strategies: Do they successfully mitigate supply chain threats? Are they compliant with regulatory requirements? Can they adapt to a changing risk landscape?
4. Continuous testing - Conducting penetration tests and vulnerability scans on a regular basis could assist in locating potential vulnerabilities in supply chain security. Potential entry points can be eliminated from that point.
5. Zero trust frameworks - Enterprises can establish a viable front line of defence by adopting an"always validate, never trust" paradigm. Zero trust necessitates that even well-known applications and services undergo security checks before receiving network access.

Supply chain attack risk can also be mitigated by employing proper security measures. Solutions that use blockchain for safe transactions, artificial intelligence for better threat detection, and cloud-based threat analysis for quick risk assessment are frequently the ones that benefit businesses the most in this situation.

6.3. Preventing Supply Chain Attacks

Supply chain applications are required for organizations to provide scalable services. Nevertheless, trust is a factor that can minimize complexity; yet, it also contributes to an increase in total risk. Businesses must take control of third-party links using both tools and strategies designed to identify unexpected behaviors, find malicious code, and limit access to possible dangers in order to lessen the impact of supply chain attacks.

7. Investing in the right data security procedures

Investing in the right data security procedures is essential to ensure business continuity. Here's a quick look at some tips for protecting your data.

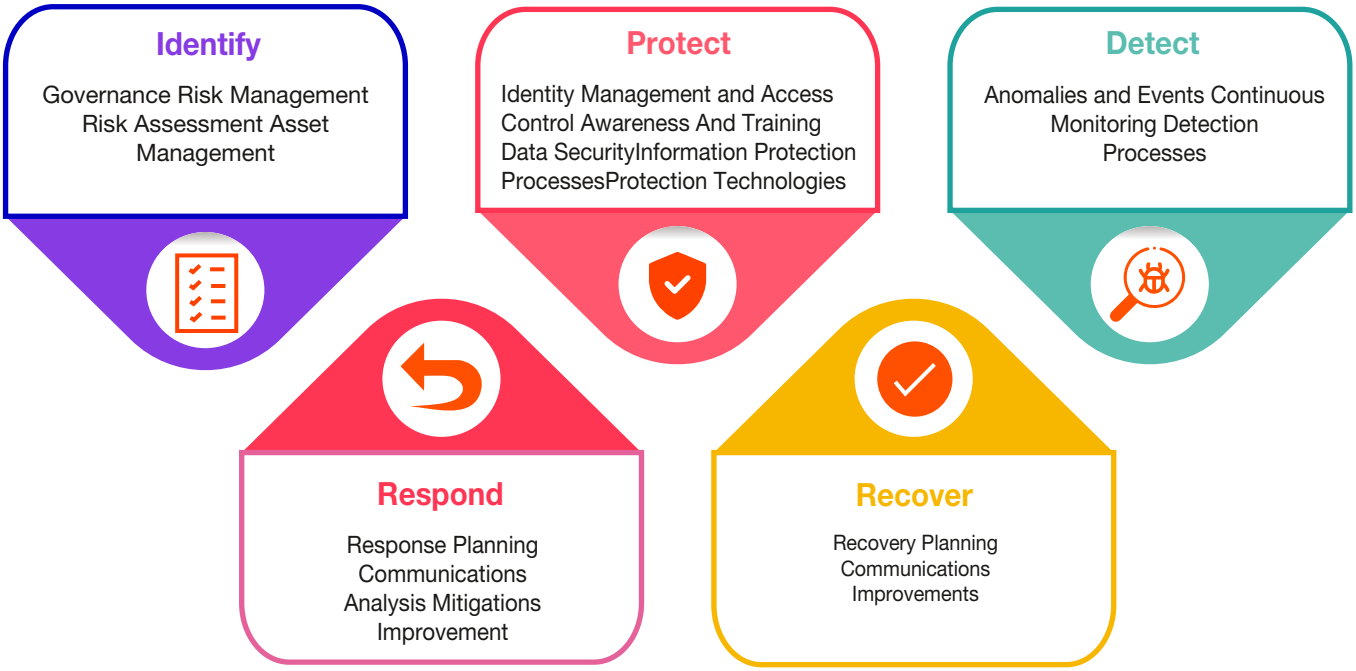
A) Information Security Culture

Human connection is vital for the success of information security operations. Employee volunteers, who are passionate about learning, teaching, and educating peers about how to prevent information security breaches and other cybercrimes and attacks, can become the elite guardians and representatives of data privacy and security across the company. Monthly engagements can include monthly networking and training activities, as well as awards and recognitions. Every aspect of an organization should be empowered by a people-led information security culture, which also constantly fosters new ideas.

B) Information Security Practices – Based on CIS Controls

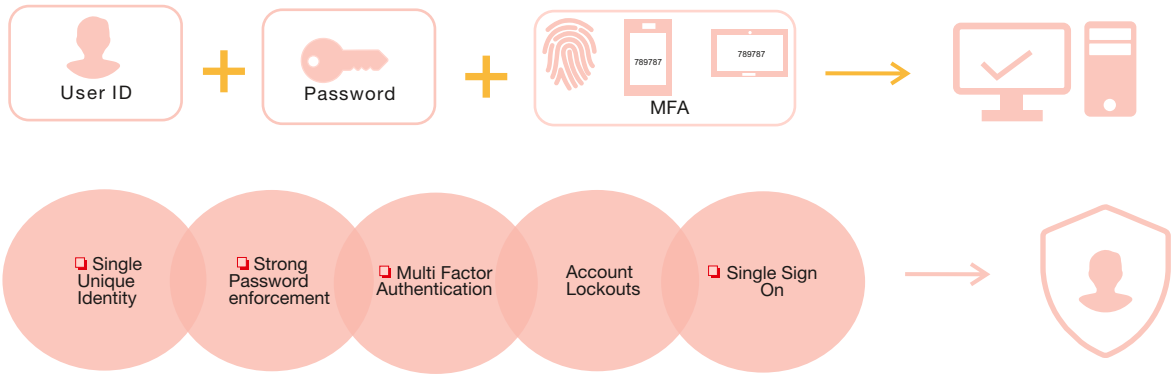
The Center for Internet Security (CIS) Controls, which offer a prioritized way to increase business security, are the foundation of an organization's information security practices. A framework approach offers a number of essential advantages, including:

- A prioritized list of security measures to reduce the most common cyber-attacks on systems and networks.
- Several legal, regulatory, and policy frameworks have systems mapped to them and use them as references.
- Enhancements to maintain compatibility with modern systems and software
- Capability to support both cloud-exclusive and hybrid setups.



C) Robust Identity Management

Given the increasing volume of threats that enterprises must contend with, strong identity authentication is more crucial than ever. This is exacerbated by the increasing growth of remote work and digital contacts across many channels, which presents significant issues for security and IT teams tasked with protecting the identities of their employees and consumers. Organizations today need a high-confidence, automated means of controlling access and verifying the identity of every user on their network.



D) Secure Configuration and Vulnerability Management

Identification, assessment, remediation, and reporting of security vulnerabilities in systems and the software that runs on them are all elements of vulnerability management. Implementing this alongside other security measures is essential for organizations to prioritize potential risks and reduce their "attack surface."

E) IT Infrastructure

It is essential for organizations to include a collection of IT and Administrative Controls to ensure the protection of sensitive data. EDRs can monitor for warnings using a cloud-based UI. A Zero Trust virtual private network (VPN) with multi factor authentication (MFA) may also be imposed.

8. Conclusion

The objective of most, if not all, cyberattacks is to access sensitive data. Databases and other information stores are a common target for hackers since they house the majority of sensitive and important data. The majority of businesses are wise enough to forbid access from unrestricted personal devices, but managing compliance is often challenging when data is held in siloed systems across many apps, in a web of accounts, files, and assets. Given the opportunity, end users frequently alter control file settings, set up their own user groups, install third-party software, and other actions that frequently result in unpleasant data breach headlines.

Companies must prevent end users from gaining access to more resources than they need to perform their jobs. Role-based permissions can be applied to data to limit end users' access to only the information that is appropriate for them to see. Additionally, everyone within the organization should receive training on fundamental cybersecurity concepts, best practices for protecting sensitive data, and attack avoidance. This includes training staff members to avoid clicking on dubious links, making sure the operating system, antivirus software, and other applications are current, and avoiding sending confidential business data through unsecure channels.

Data security doesn't really involve completely eradicating risks - that is not possible. Organizations can, at the very least, significantly reduce risks by implementing proper security measures.

About Straive (formerly SPi Global)

Straive is a market leading content technology enterprise that provides data services, subject matter expertise (SME) and technology solutions to multiple domains such as research content, e-Learning / EdTech and data/information providers. With a client-base scoping 30 countries worldwide, Straive's multi-geographical resource pool is strategically located in eight countries - Philippines, India, USA, China, Nicaragua, Vietnam, United Kingdom and the company headquarters in Singapore.

www.straive.com
straiveteam@straive.com

Reference

Tips for protecting your organization's data
Data Intelligence: Safely Protecting Cloud……
Enterprise data breach: causes, challenges, prevention…
Data Security in the Publishing Industry
Data Security Explained: Challenges and Solutions
7 Most common types of data breaches…..
Supply chain attack
Supply Chain Attack: What It…