Chandrawat & Partners

DATA SECURITY AND MANAGEMENT GUIDE

enquiries@chandrawatpartners.com| www.chandrawatpartners.co

Chandrawat & Partners

TABLE OF CONTENT

OVERVIEW

Two-and-a-half quintillion bytes of data are created daily. This could potentially rise due to better internet access. When it comes to the relationship between big data and safety, the impact is much more indirect. Insights drawn from big data are used to predict the places and blocks of time where crime is likely to be committed. Millions of individuals moving online have enabled industries to change the way they promote or provide services. Information security management is the process of protecting an organization's data and assets against potential threats. One of the primary goals of these processes is to protect data confidentiality, integrity, and availability.

According to the Ponemon Institute, the average cost of a data breach in terms of damage and resolution is a record-breaking $4.96 million per occurrence. While connected to internet services, digital transformation encourages recording everything done by a person or an application in great detail. A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information. This can be done physically by accessing a computer or network to steal local files or by bypassing network security remotely. The latter is often the method used to target companies.

Data security is the practice of safeguarding digital information from unauthorized access, accidental loss, disclosure and modification, manipulation, or corruption throughout its entire lifecycle, from creation to destruction. This practice is key to maintaining the confidentiality, integrity, and availability of an organization's data. Confidentiality refers to keeping data private, integrity to ensuring data is complete and trustworthy, and availability to providing access to authorized entities.

IMPORTANCE

Data is the lifeline of every organization. It helps in decision-making, finds solutions to problems, improves the efficiency and efficacy of operations, boosts customer service, informs marketing efforts, reduces risks, increases productivity, enhances collaboration, and is also instrumental in increasing revenue and profit. Data is often referred to as a company's crown jewels thus its protection must be taken seriously.

Much like Coca-Cola's secret recipe that is locked away in a vault, Hershey's secret lab that concocts its famous Kisses, and KFC's famous yet unknown 11 herbs and spices, it is crucial to keep certain data from prying eyes. It is not always as easy as putting something under lock and key, especially in a digital environment. Multiple employees, stakeholders, and partners need access to the data that enterprises value so highly. But more people having access means more chances for things to go wrong.

Data breaches, which occur when data is accessed in an unauthorized manner, are a major concern for organizations of all shapes, sizes, and industries. Data breaches are attributed to several cyber incidents, including accidental leaks or exposures, phishing attacks, distributed denial-of-service attacks, physical breaches, lack of access controls, and backdoors. Regulatory and legal fines may also be levied. In worst-case scenarios, companies can go bankrupt or out of business.

Data security is an important component in data compliance, the process that identifies governance and establishes policies and procedures to protect data. The process involves selecting applicable standards and implementing controls to achieve the criteria defined in those standards. Regulatory compliance, which refers to organizations following local, state, federal, international, and industry laws, policies, and regulations is related to data compliance.

TYPES OF DATA SECURITY

ACCESS CONTROLS

This type of data security measure includes limiting both physical and digital access to critical systems and data. This includes making sure all computers are protected with mandatory login entry, and that physical spaces can only be entered by authorized personnel.

AUTHENTICATION

Similar to access controls, authentication refers specifically to accurately identifying users before they have access to data that is present. This usually includes things like passwords, PINs, security tokens, swipe cards, or biometrics.

BACKUPS & RECOVERY

Good data security means one has a plan to securely access data in the event of system failure, disaster, data corruption, or breach. One will need a backup data copy, stored on a separate format such as a physical disk, local network, or cloud to recover if needed.

DATA MASKING

Comprehensive data security means that the systems can endure or recover from failures. Building resiliency into hardware and software means that events like power outages or natural disasters will not compromise security.

DATA RESILIENCY

By using data masking software, information is hidden by obscuring letters and numbers with proxy characters. This effectively masks key information even though unauthorized party gains access to it. The data changes to the original form when an authorized user receives it.

ENCRYPTION

A computer algorithm transforms text characters into an unreadable format via encryption keys. Only authorized users with the proper corresponding keys can unlock and access the information. Everything from files and a database to email communications can — and should — be encrypted to some extent.

ELEMENTS AND PRACTICES

MAIN ELEMENTS OF DATA SECURITY

There are three core elements of data security that all organizations should adhere to: Confidentiality(C), Integrity(I), and Availability(A). These concepts are also referred to as the CIA Triad, functioning as a security model and framework for top-notch data security.

- Confidentiality- Ensures that data is accessed only by authorized users with the proper credentials.

- Integrity- Ensure that all data stored is reliable, accurate, and not subject to unwarranted changes.

- Availability- Ensures that data is readily — and safely — accessible and available for ongoing business needs.

BEST PRACTICES FOR ENSURING DATA SECURITY

There is no silver bullet that will guarantee 100 percent security of the data. However, there are several steps, tactics, and best practices that can help minimize the chances of a data breach, loss, and exposure.

- Quarantine sensitive files: One common data management mistake is placing sensitive files on a shared or open drive accessible to the entire company. One would want to eliminate this practice, placing sensitive data into safely quarantined areas. Gain control of the data by using data security software that continually classifies sensitive data and moves it to a secure location.

- Behavior-based permissions: Overly permissive behavior is another common misstep, where more people have access to data than is necessary. A convoluted web of temporary access and permissions quickly arises, with individuals having access to data that they should have not.

- Prepare for cyber threats: Good data security is all about thinking ahead. One would want to have a solid cybersecurity policy that encompasses current and potential future threats to the data. This includes both external hackers and insider threats. Aside from the policy, employ software that provides real-time monitoring and alerts of suspicious activities.

- Delete unused data: Storing stale data for longer than necessary presents a significant liability in terms of data security. One will want to have processes and technologies in place to eliminate sensitive data that's no longer necessary for ongoing business activities.

CYBER CRIME COMPLAINT

HOW TO REGISTER CYBER CRIME COMPLAINT

The crime investigation team has been establishing many cyber crime cells in different cities of India, taking care of the reports and investigations of cyber crimes. At present, most cities in India have a dedicated cyber crime cell. You can make a complaint anytime to the cyber police or crime investigation department either offline or online. To give punishment for cybercrime, the first and foremost step is to lodge complaints against the crime. One needs to file a written complaint with the cyber crime cell of any jurisdiction.

In the written complaint, one needs to provide name, contact details, and address for mailing. One needs to address the written complaint to the Head of the cyber crime cell of the city where a cyber crime complaint is filed. According to the Information and Technology Act, a cyber crime comes under the purview of global jurisdiction which means that a cyber crime complaint can be registered with any of the cyber cells in India, irrespective of the place where it was originally committed or the place where the victim is currently residing/ staying.

HOW TO REPORT AN FIR FOR A CYBER CRIME

If one does not have access to any of the cyber cells in India, one can file a First Information Report (FIR) at the local police station. In case the complaint is not accepted there, the approach can be made to the Commissioner or the city's Judicial Magistrate. Certain cybercrime offenses come under the Indian Penal Code. One can register a cyber crime FIR at the nearest local police station to report them. It is mandatory under Section 154 of the Criminal Procedure Code, for every police officer to record the information/complaint of an offense, irrespective of the jurisdiction in which the crime was committed.

HOW TO FILE CYBER CRIME COMPLAINT ONLINE

The online portal where a victim can file a cyber crime complaint is https://cybercrime.gov.in/Accept.aspx, an initiative of the government of India that caters to complaints about online child pornography, child sexual abuse material, or sexually explicit content such as rape/gang rape content, and other cyber crimes such as social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes, and online cyber trafficking. The portal also provides an option of reporting an anonymous complaint about reporting the same.

HOW TO FILE A COMPLAINT AGAINST CYBER STALKING AND CYBER BULLYING

Cyber Stalking is the persistent use of the internet, e-mail, social networks, instant messaging, or related digital devices to irritate, badger, or threaten people. Before the February 2013 amendment, there was no specific law against it, now it falls under the purview of the Criminal Law Amendment Act, 2013. Under Section 354(d), if any person follows a woman and tries to contact her to foster personal interaction despite the woman's disinclination towards it, then he is committing stalking and can be charged with it. Also, if a person monitors the use by a woman of the internet, email, or any other form of electronic communication, he commits the offense of stalking. Steps to file a complaint against Cyber Stalking are as follows:

1. Register a written complaint to your immediate cyber cell in the city.
2. File an F.I.R. at the local police station. In case of non-acceptance of a complaint, one can always refer the complaint to the commissioner or judicial magistrate of the city.
3. Legal counsel/assistance to help to file a case will be provided.

Cyberbullying is bullying executed through digital devices like computers, laptops, smartphones, and tablets leading to humiliation. It also comprises posting, sending, or sharing negative, nasty, or false information about another individual for causing humiliation and what is popularly known as character assassination.

1. Most social media platforms such as Facebook, WhatsApp, Instagram, Twitter, etc. have clear guidelines concerning reporting and curbing cyberbullying. Such platforms can help in having the offensive post removed.
2. Further, one can report cyberbullying in India by mailing a complaint to complain **info@cybercert.in** describing the details.
3. One can also complain about your nearest cyber cell unit.

CYBER CRIME AGAINST WOMEN AND CHILDREN

The rise of cybercrime has resulted in targeting the most vulnerable segment of society, women and children. The most common and frequently reported sorts of cyber crimes against women include cyberstalking, pornography, morphing, online harassment, trolling and bullying, threat and intimidation, and email spoofing.

The Ministry of Home Affairs introduced the scheme for cyber crime Prevention against Women and Children (CCWC) to handle cyber crimes against women and children effectively in the country with an estimated outlay of Rs. 223.198 crores (approximately), for formulating:

1. Online cybercrime reporting unit,
2. Forensic unit,
3. Capacity building unit,
4. Research and development unit and
5. Awareness creation unit.

DOCUMENTS REQUIRED TO FILE A COMPLAINT

For email-based complaints:

- A written complaint explaining the complete incidence and offense,
- copy of the alleged email taken from the original receiver.
- full header of the alleged e-mail.
- copy of email and header should be in both hard & soft forms (in CD-R only).

For mobile app-based complaints:

- a screenshot of the alleged app,
- the location from where it was downloaded,
- the victim's bank statements in case any transactions were made after/before/during the incident,
- soft copies of all the above-mentioned documents.

For business email-based complaints:

- a written brief about the offense and the incident,
- originating name (as in the email or offender) and location,
- originating bank name and account number (as per the email),
- recipient's name (as in bank records), bank account,
- date and amount of transaction as done,
- SWIFT number.

For data theft complaints:

- a copy of the stolen data and brief,
- the copyright certificate of the allegedly stolen data,
- details of the suspected employee/(s),

For ransomware/malware complaints:

- email id /phone number (or any details) or any other means of communication through which ransom has been demanded,
- if malware was sent in the attachment of the mail, screenshots of the mail with a full header of the first receiver be provided.

For internet banking/online transactions/lottery scam/fake call-related complaints:

- bank statement of the concerned bank for the last six months,
- a copy of the SMS/(s) received related to the suspected transactions,
- copy of the victim's ID & address proof as per the bank record.

For net banking/ATM complaints:

- a printout of the alleged emails with their complete header as received by the original receiver (forwarded emails should be avoided),
- victim's bank statement,
- details of the suspected transactions,
- soft copies of all the aforesaid documents.

DATA SECURITY STRATEGIES

A comprehensive data security strategy incorporates people, processes, and technologies. Establishing appropriate controls and policies is as much a question of organizational culture as it is of deploying the right toolset. This means making information security a priority across all areas of the enterprise.

- **Physical security of servers and user devices**

Regardless of whether the data is stored on-premises, in a corporate data center, or the public cloud, one needs to ensure that facilities are secured against intruders and have adequate fire suppression measures and climate controls in place. A cloud provider will assume responsibility for these protective measures.

- **Access management and controls**

The principle of "least-privilege access" should be followed throughout the IT environment. This means granting database, network, and administrative account access to as few people as possible, and only those who need it to get their jobs done.

- **Application security and patching**

All software should be updated to the latest version as soon as possible after patches or new versions are released.

- **Backups**

Maintaining usable, thoroughly tested backup copies of all critical data is a core component of any robust data security strategy. In addition, all backups should be subject to the same physical and logical security controls that govern access to the primary databases and core systems.

- **Employee education**

Training employees in the importance of good security practices and password hygiene and teaching them to recognize social engineering attacks transforms them into a human firewall that can play a critical role in safeguarding the data.

DATA SECURITY MANAGEMENT

Data security management is a way to maintain the integrity of data and to make sure that the data is not accessible to unauthorized parties or susceptible persons to corrupt it. Data security is put in place to ensure privacy in addition or protecting this data. Data itself is a raw form of information that is stored on network servers, possibly personal computers, and in the form of columns and rows. This data can be anything from personal files to intellectual property and even top-secret information. Because of the growing use of the internet, there is an emphasis on protecting personal or company data and this protection is known as data security which can be acquired by using specific software solutions or hardware mechanisms.

Information can be encrypted or unreadable to a person with no access. When encrypting this data, mathematical sequences and algorithms are used to scramble information. Encryption allows only an approved party to decode this unreadable text with a key. Only those that have this key can access any information. Authentication is another form of data security to be used for more daily access. A sign-on to an email account, bank account, etc., only allows the user with the proper key or password.

The most used method of keeping data protected is with data security software. This software keeps unauthorized parties from accessing private data and offers a variety of different options. Data can also be protected with IP security. Data security tends to be necessary for large businesses, but the small ones usually have fewer infrastructures in place, making the information not a great loss if breached. Depending on the services and content that is to be protected, there can be preventative measures to further protect the information.

DATA PROTECTION TRENDS

Data Portability and Data Sovereignty

Mobile Data Protection

Ransomware

Copy Data Management ("CDM")

Disaster Recovery as a Service

DATA PORTABILITY

Data portability is an important requirement for many modern IT organizations. It means the ability to move data between different environments and software applications. Very often, data portability means the ability to move data between on-premises data centers and the public cloud, and between different cloud providers. Data portability also has legal implications—when data is stored in different countries, it is subject to different laws and regulations. This is known as data sovereignty.

Traditionally, data was not portable and it required huge efforts to migrate large datasets to another environment. Cloud data migration was also extremely difficult, in the early days of cloud computing. New technical methods are developing to make migration easier, and thus make data more portable.

A related issue is the portability of data within clouds. Cloud service providers tend to have proprietary data formats, templates, and storage engines. This makes it difficult to move data from one cloud to another and creates vendor lock-in. Increasingly, organizations are looking for standardized ways of storing and managing data, to make it portable across clouds.

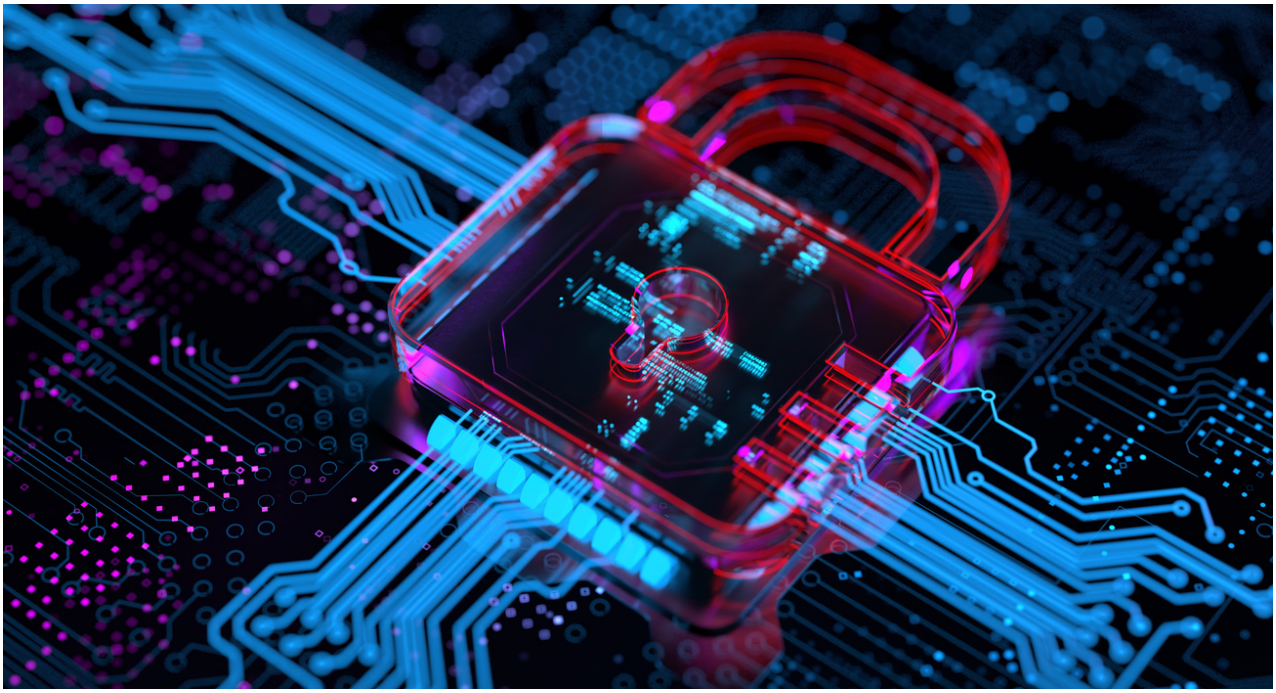
MOBILE DATA PROTECTION

Mobile device protection refers to measures designed to protect sensitive information stored on laptops, smartphones, tablets, wearables, and other portable devices. A fundamental aspect of mobile device security is preventing unauthorized users from accessing the corporate network. In the modern IT environment, this is a critical aspect of network security.
There are many mobile data security tools, designed to protect mobile devices and data by identifying threats, creating backups, and preventing threats on the endpoint from reaching the corporate network. IT staff use mobile data security software to enable secure mobile access to networks and systems.

Common capabilities of mobile data security solutions include:

- enforcing communication via secure channels;
- performing strong identity verification to ensure devices are not compromised;
- limiting the use of third-party software and browsing to unsafe websites;
- monitoring for threats on the device;
- encrypting data on the device to protect against device compromise and theft;
- perform regular audits of endpoints to discover threats and security issues.

RANSOMWARE



Ransomware is a rising cybersecurity threat, which is a top security priority for almost all organizations. Ransomware is a type of malware that encrypts user data and demands a ransom to release it. New types of ransomware send the data to attackers before encrypting it, allowing the attackers to extort the organization, threatening to make its sensitive information public.

Backups are an effective defense against ransomware—if an organization has a recent copy of its data, it can restore it and regain access to the data. However, ransomware can spread across a network over a long period, without encrypting files yet. At this stage, ransomware can infect any connected system, including backups.

There are multiple strategies for preventing ransomware and in particular, preventing it from spreading to backups:

- The simplest strategy is to use the old 3-2-1 backup rule, keeping three copies of the data on two storage media, one of which is off-premises.
- Security vendors have advanced technologies that can detect ransomware at its early stages, or in the worst case, block encryption processes as they begin.
- Storage vendors are offering immutable storage, which ensures that data cannot be modified after it is stored.

COPY DATA MANAGEMENT AND DISASTER RECOVERY

Copy Data Management (CDM)

Large organizations have multiple datasets stored in different locations, and many of them may duplicate data between them. Duplicate data creates multiple problems—it increases storage costs, creates inconsistencies and operational issues, and can also result in security and compliance challenges. Typically, not all copies of the data will be secured in the same way. It is no use securing a dataset and ensuring it is compliant when the data is duplicated in another unknown location. CDM is a type of solution that detects duplicate data and helps manage it, comparing similar data and allowing administrators to delete unused copies.

Disaster Recovery as a Service

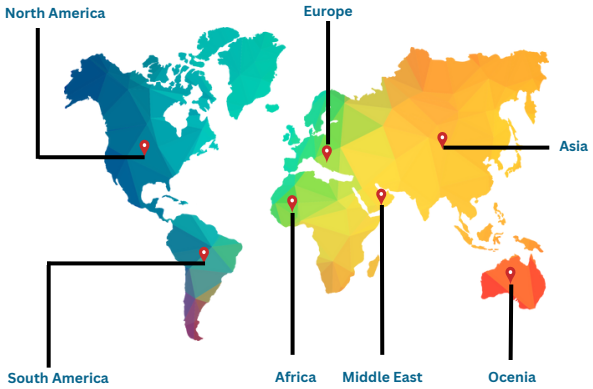
Disaster recovery as a service (DRaaS) is a managed service that gives an organization a cloud-based remote disaster recovery site. Traditionally, setting up a secondary data center was extremely complex and involved massive costs, and was only relevant for large enterprises. With DRaaS, any size organization can replicate its local systems to the cloud, and easily restore operations in case of a disaster.

HOW WE CAN HELP?

Our team has significant experience in advising clients across the entire spectrum of privacy and data protection concerns, ranging from advice on general regulatory compliance, transaction-related advice, drafting or review of policies, data processing agreements and other associated documents, cross-border data transfers and disclosures, government access requests, data security and breach notification, data retention, use of new age technologies, defense against investigations and proceedings regarding privacy/data protection violations or security failures.

- We help and advise our clients throughout the entire process, making sure to stay with them every step of the way.
- We also advise on data protection matters in certain niche sectors such as blockchain, cloud, artificial intelligence, etc.
- We counsel international clients on issues related to data protection and privacy across major jurisdictions and sectors such as banking and insurance, financial institutions, luxury goods, consumer goods, health care, payroll processing companies, pharmaceuticals, telecommunications, and internet service providers, credit research agencies, employee screening companies, etc.
- In addition to providing regular advice on issues involving data protection and privacy, we also assist several international companies with global privacy law projects.
- Our experts regularly assist a variety of businesses with several complicated transactions, thereby attaining in-depth knowledge about how different industries function, the specific concerns concerning data and information management, and the practical aspects.

SERVING CLIENTS WORLDWIDE



Key Contact

Surendra Singh Chandrawat

Managing Partner

surendra@chandrawatpartners.com

Connect Surendra on

LinkedIn WhatsApp

Chandrawat & Partners is a leading and rapidly growing full-service law firm in India providing high quality professional, legal and corporate services to foreign and local clients, representing worldwide companies and individuals in a wide range of practice areas and sectors.

Follow us on: LinkedIn twitter facebook Instagram