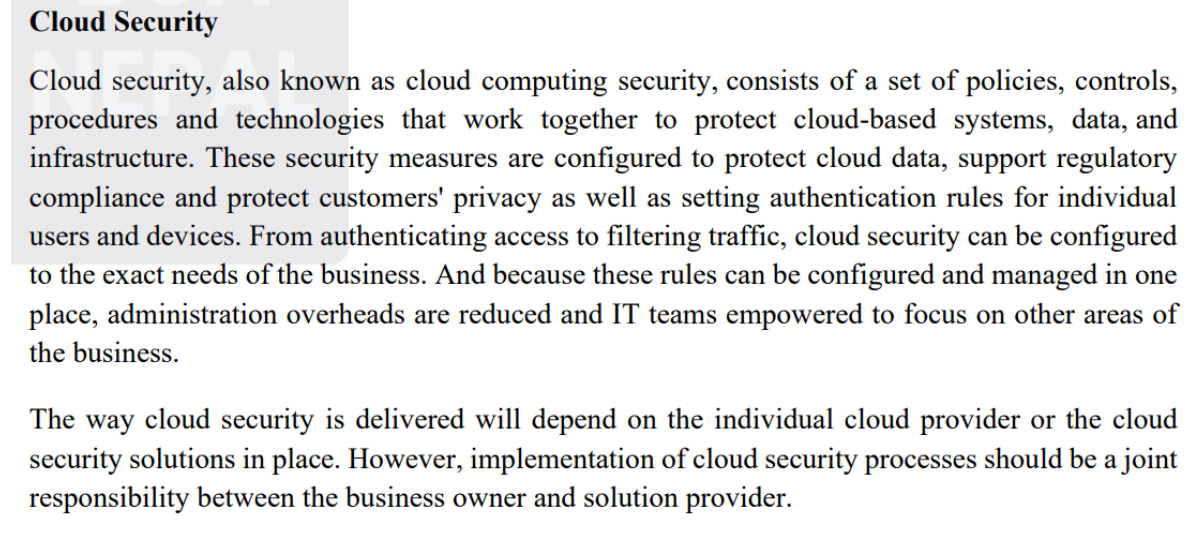
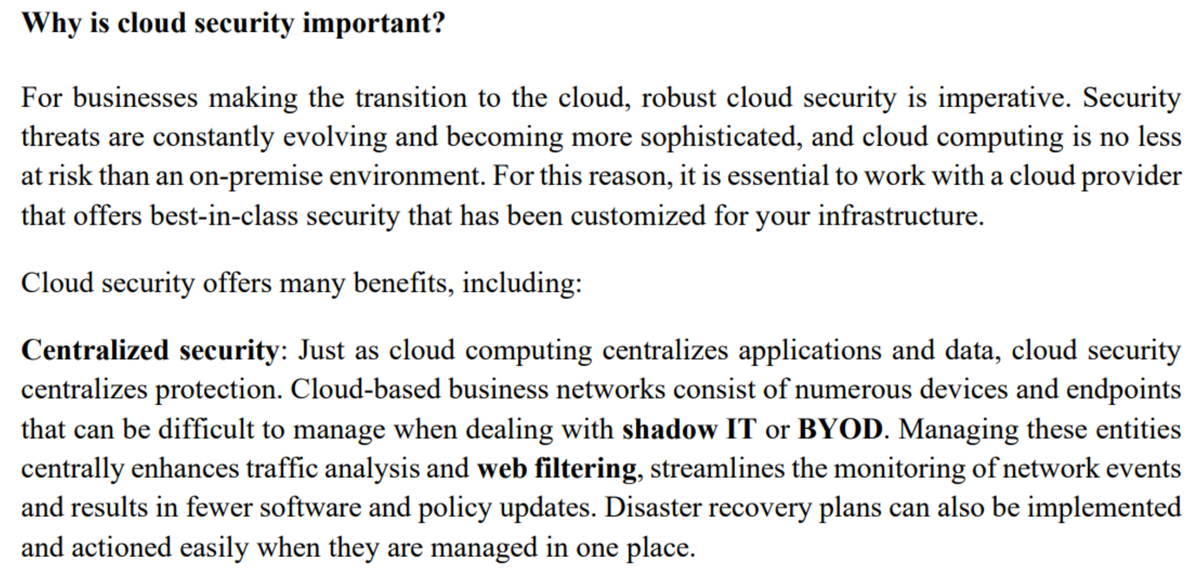


Cloud Security

Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data, and infrastructure. These security measures are configured to protect cloud data, support regulatory compliance and protect customers' privacy as well as setting authentication rules for individual users and devices. From authenticating access to filtering traffic, cloud security can be configured to the exact needs of the business. And because these rules can be configured and managed in one place, administration overheads are reduced and IT teams empowered to focus on other areas of the business.

The way cloud security is delivered will depend on the individual cloud provider or the cloud security solutions in place. However, implementation of cloud security processes should be a joint responsibility between the business owner and solution provider.

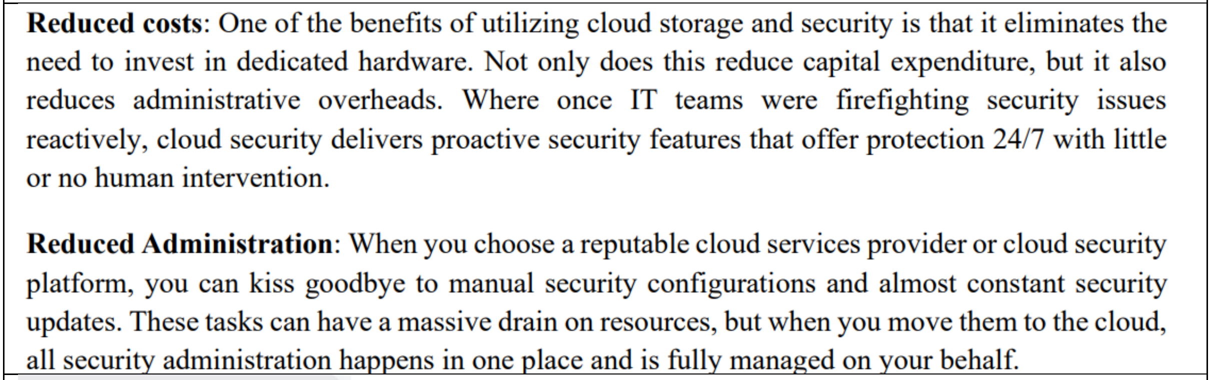


Why is cloud security important?

For businesses making the transition to the cloud, robust cloud security is imperative. Security threats are constantly evolving and becoming more sophisticated, and cloud computing is no less at risk than an on-premise environment. For this reason, it is essential to work with a cloud provider that offers best-in-class security that has been customized for your infrastructure.

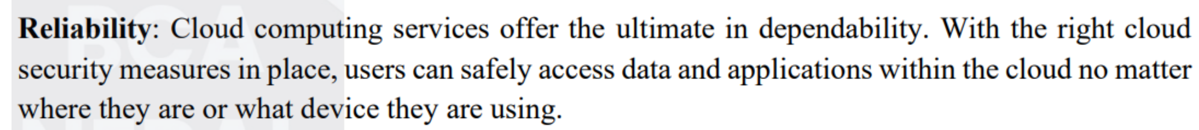
Cloud security offers many benefits, including:

Centralized security: Just as cloud computing centralizes applications and data, cloud security centralizes protection. Cloud-based business networks consist of numerous devices and endpoints that can be difficult to manage when dealing with **shadow IT** or **BYOD**. Managing these entities centrally enhances traffic analysis and **web filtering**, streamlines the monitoring of network events and results in fewer software and policy updates. Disaster recovery plans can also be implemented and actioned easily when they are managed in one place.



Reduced costs: One of the benefits of utilizing cloud storage and security is that it eliminates the need to invest in dedicated hardware. Not only does this reduce capital expenditure, but it also reduces administrative overheads. Where once IT teams were firefighting security issues reactively, cloud security delivers proactive security features that offer protection 24/7 with little or no human intervention.

Reduced Administration: When you choose a reputable cloud services provider or cloud security platform, you can kiss goodbye to manual security configurations and almost constant security updates. These tasks can have a massive drain on resources, but when you move them to the cloud, all security administration happens in one place and is fully managed on your behalf.



Reliability: Cloud computing services offer the ultimate in dependability. With the right cloud security measures in place, users can safely access data and applications within the cloud no matter where they are or what device they are using.

What are the Security Risks of Cloud Computing

Cloud computing provides various advantages, such as improved collaboration, excellent accessibility, Mobility, Storage capacity, etc. But there are also security risks in cloud computing.

Some most common Security Risks of Cloud Computing are given below-

Data Loss

Data loss is the most common cloud security risks of cloud computing. It is also known as data leakage. Data loss is the process in which data is being deleted, corrupted, and unreadable by a user, software, or application. In a cloud computing environment, data loss occurs when our sensitive data is somebody else's hands, one or more data elements can not be utilized by the data owner, hard disk is not working properly, and software is not updated.

Hacked Interfaces and Insecure APIs

As we all know, cloud computing is completely depends on Internet, so it is compulsory to protect interfaces and APIs that are used by external users. APIs are the easiest way to communicate with most of the cloud services. In cloud computing, few services are available in the public domain. These services can be accessed by third parties, so there may be a chance that these services easily harmed and hacked by hackers.

Data Breach

Data Breach is the process in which the confidential data is viewed, accessed, or stolen by the third party without any authorization, so organization's data is hacked by the hackers.

Vendor lock-in

Vendor lock-in is the of the biggest security risks in cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving one cloud to another.

Increased complexity strains IT staff

Migrating, integrating, and operating the cloud services is complex for the IT staff. IT staff must require the extra capability and skills to manage, integrate, and maintain the data to the cloud.

Spectre & Meltdown

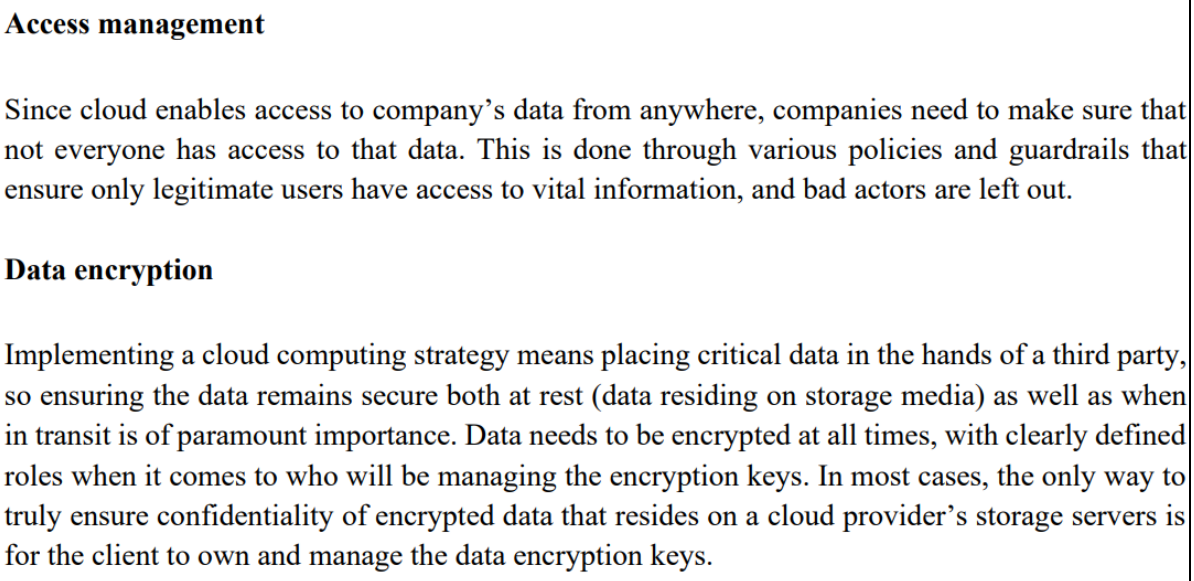
Spectre & Meltdown allows programs to view and steal data which is currently processed on computer. It can run on personal computers, mobile devices, and in the cloud. It can store the password, your personal information such as images, emails, and business documents in the memory of other running programs.

Denial of Service (DoS) attacks

Denial of service (DoS) attacks occur when the system receives too much traffic to buffer the server. Mostly, DoS attackers target web servers of large organizations such as banking sectors, media companies, and government organizations. To recover the lost data, DoS attackers charge a great deal of time and money to handle the data.

Account hijacking

Account hijacking is a serious security risk in cloud computing. It is the process in which individual user's or organization's cloud account (bank account, e-mail account, and social media account) is stolen by hackers. The hackers use the stolen account to perform unauthorized activities.



Access management

Since cloud enables access to company’s data from anywhere, companies need to make sure that not everyone has access to that data. This is done through various policies and guardrails that ensure only legitimate users have access to vital information, and bad actors are left out.

Data encryption

Implementing a cloud computing strategy means placing critical data in the hands of a third party, so ensuring the data remains secure both at rest (data residing on storage media) as well as when in transit is of paramount importance. Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys. In most cases, the only way to truly ensure confidentiality of encrypted data that resides on a cloud provider’s storage servers is for the client to own and manage the data encryption keys.

Cloud security risks and solutions

Cloud computing is continually transforming the way companies store, use, and share data, workloads, and software. The volume of cloud utilization around the globe is increasing, leading to a greater mass of sensitive material that is potentially at risk.

The market for worldwide cloud computing is projected to grow to $191 billion in two years. There are many pros of cloud computing, which are driving more firms and individuals to the cloud. The benefits include low costs, improved employee productivity, and faster to market, among many more.

Regardless of the great advantages, saving a firm's workloads to a cloud service that is publicly hosted exposes the organization to new data security risks which cause unease for some firms' IT departments and clients.

With more and more data and software moving to the cloud, unique info-security challenges crop up. Here are the top cloud computing security risks that every firm faces.

Cloud security risks

1. Theft or loss of intellectual property

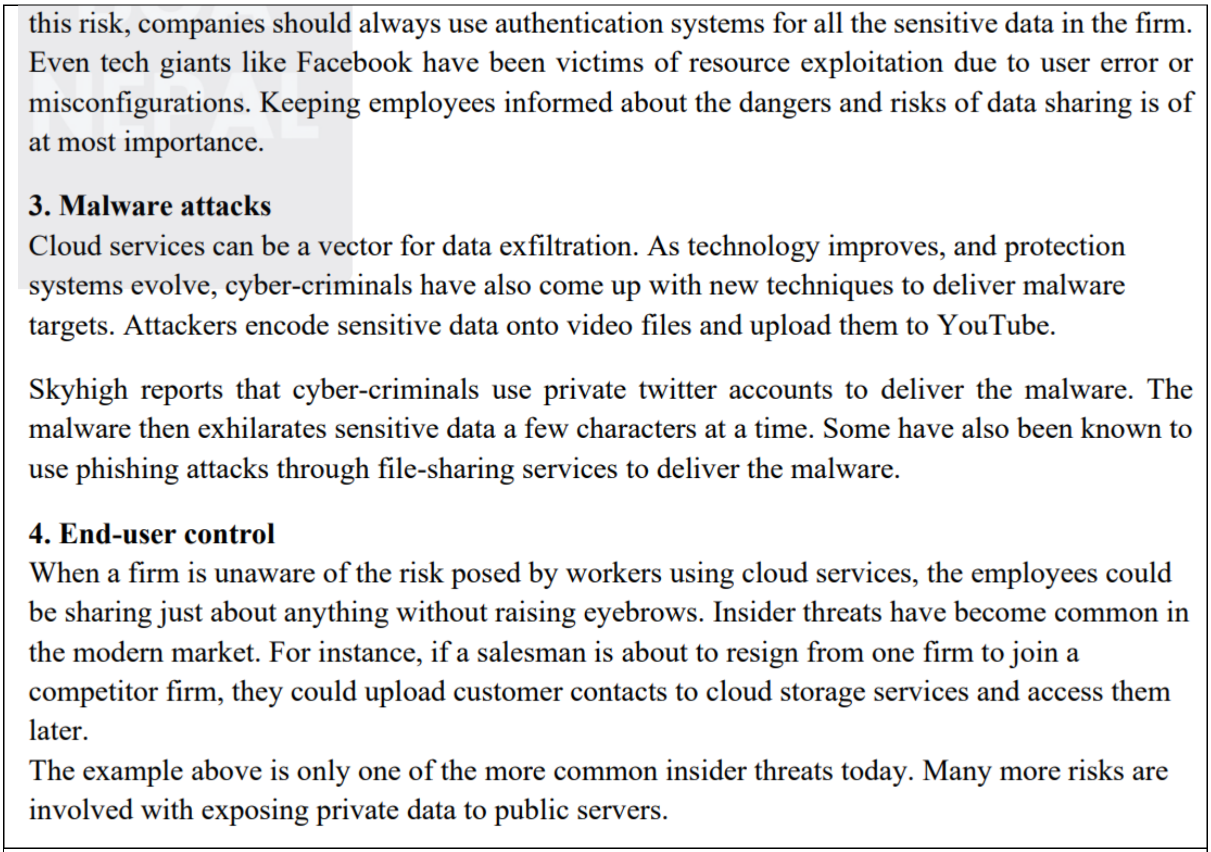
An outstanding 21% of data uploaded by companies to cloud-based file management services contain sensitive data. The analysis that was done by Skyhigh found that companies face the risk of having their intellectual property stolen.

The Ponemon Institute and Surveying 409 IT investigated the risk posed by BYOC (bring your own cloud). The analysis revealed that most of the interviewees had no idea of the threat posed by bringing their own cloud storage devices to their organization. Employees unwittingly help cyber-criminals access sensitive data stored in their cloud accounts.

Weak cloud security measures within an organization include storing data without encryption or failing to install multi-factor authentication to gain access to the service.

2. Compliance violations

Organizations can quickly go into a state of non-compliance, which puts them in the risk of serious repercussions. BYOC is one of the ways companies often violate one of the tenets and regulations instituted by the government or Industrial Corporation. Whether it is FERPA for confidential student documents or HIPAA for private patient records, most firms operate under a regulatory body.



this risk, companies should always use authentication systems for all the sensitive data in the firm. Even tech giants like Facebook have been victims of resource exploitation due to user error or misconfigurations. Keeping employees informed about the dangers and risks of data sharing is of at most importance.

3. Malware attacks

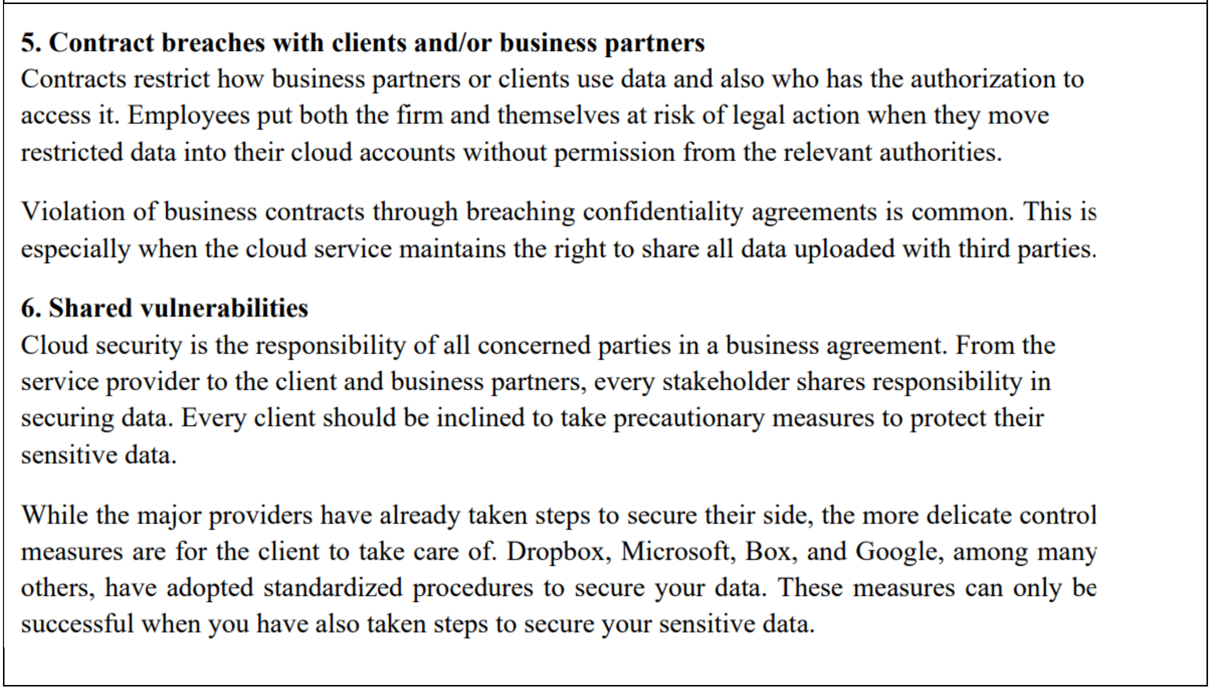
Cloud services can be a vector for data exfiltration. As technology improves, and protection systems evolve, cyber-criminals have also come up with new techniques to deliver malware targets. Attackers encode sensitive data onto video files and upload them to YouTube.

Skyhigh reports that cyber-criminals use private twitter accounts to deliver the malware. The malware then exhilarates sensitive data a few characters at a time. Some have also been known to use phishing attacks through file-sharing services to deliver the malware.

4. End-user control

When a firm is unaware of the risk posed by workers using cloud services, the employees could be sharing just about anything without raising eyebrows. Insider threats have become common in the modern market. For instance, if a salesman is about to resign from one firm to join a competitor firm, they could upload customer contacts to cloud storage services and access them later.

The example above is only one of the more common insider threats today. Many more risks are involved with exposing private data to public servers.



5. Contract breaches with clients and/or business partners

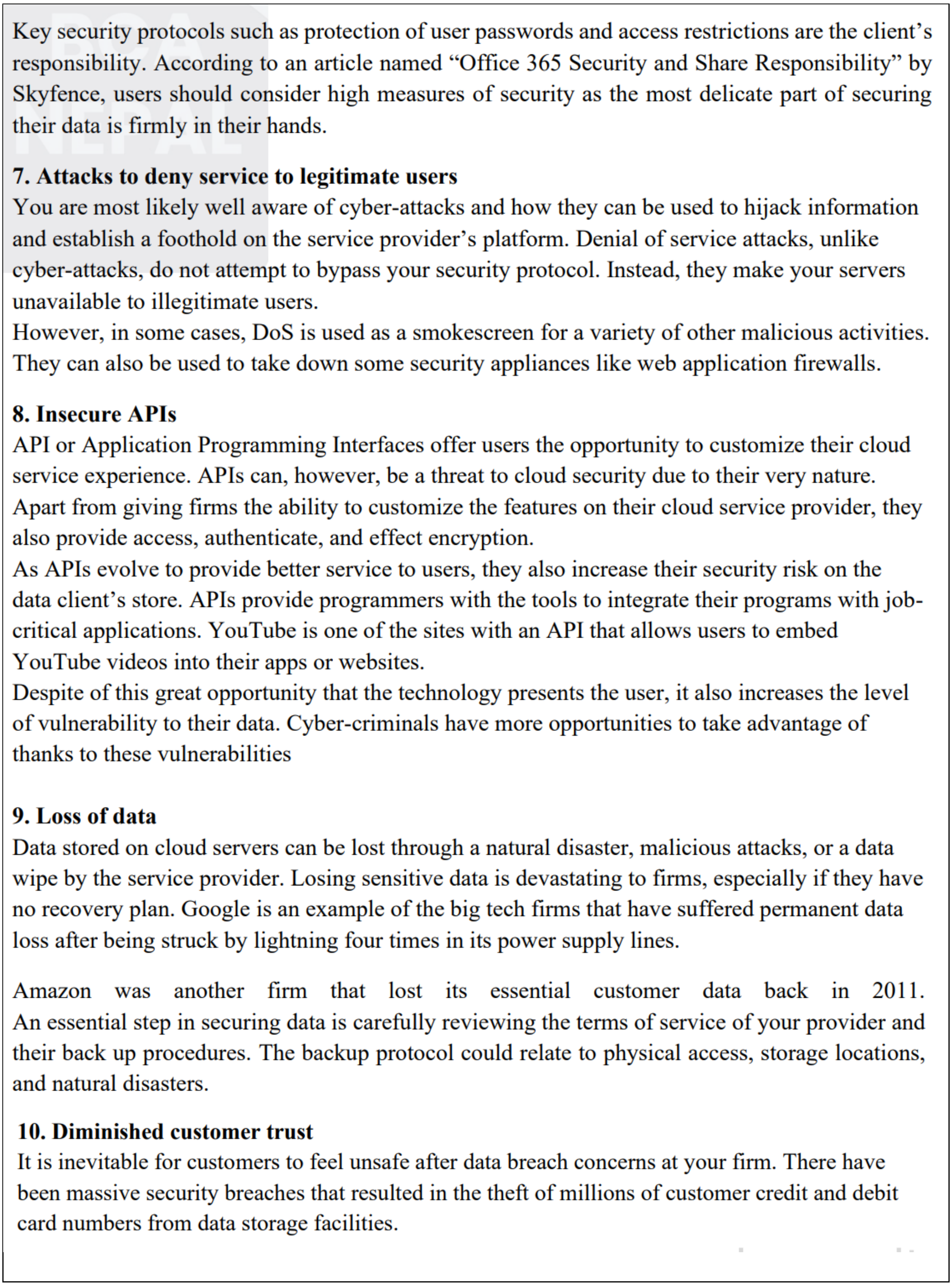
Contracts restrict how business partners or clients use data and also who has the authorization to access it. Employees put both the firm and themselves at risk of legal action when they move restricted data into their cloud accounts without permission from the relevant authorities.

Violation of business contracts through breaching confidentiality agreements is common. This is especially when the cloud service maintains the right to share all data uploaded with third parties.

6. Shared vulnerabilities

Cloud security is the responsibility of all concerned parties in a business agreement. From the service provider to the client and business partners, every stakeholder shares responsibility in securing data. Every client should be inclined to take precautionary measures to protect their sensitive data.

While the major providers have already taken steps to secure their side, the more delicate control measures are for the client to take care of. Dropbox, Microsoft, Box, and Google, among many others, have adopted standardized procedures to secure your data. These measures can only be successful when you have also taken steps to secure your sensitive data.



Key security protocols such as protection of user passwords and access restrictions are the client's responsibility. According to an article named "Office 365 Security and Share Responsibility" by Skyfence, users should consider high measures of security as the most delicate part of securing their data is firmly in their hands.

7. Attacks to deny service to legitimate users

You are most likely well aware of cyber-attacks and how they can be used to hijack information and establish a foothold on the service provider's platform. Denial of service attacks, unlike cyber-attacks, do not attempt to bypass your security protocol. Instead, they make your servers unavailable to illegitimate users.

However, in some cases, DoS is used as a smokescreen for a variety of other malicious activities. They can also be used to take down some security appliances like web application firewalls.

8. Insecure APIs

API or Application Programming Interfaces offer users the opportunity to customize their cloud service experience. APIs can, however, be a threat to cloud security due to their very nature.

Apart from giving firms the ability to customize the features on their cloud service provider, they also provide access, authenticate, and effect encryption.

As APIs evolve to provide better service to users, they also increase their security risk on the data client's store. APIs provide programmers with the tools to integrate their programs with job-critical applications. YouTube is one of the sites with an API that allows users to embed YouTube videos into their apps or websites.

Despite of this great opportunity that the technology presents the user, it also increases the level of vulnerability to their data. Cyber-criminals have more opportunities to take advantage of thanks to these vulnerabilities

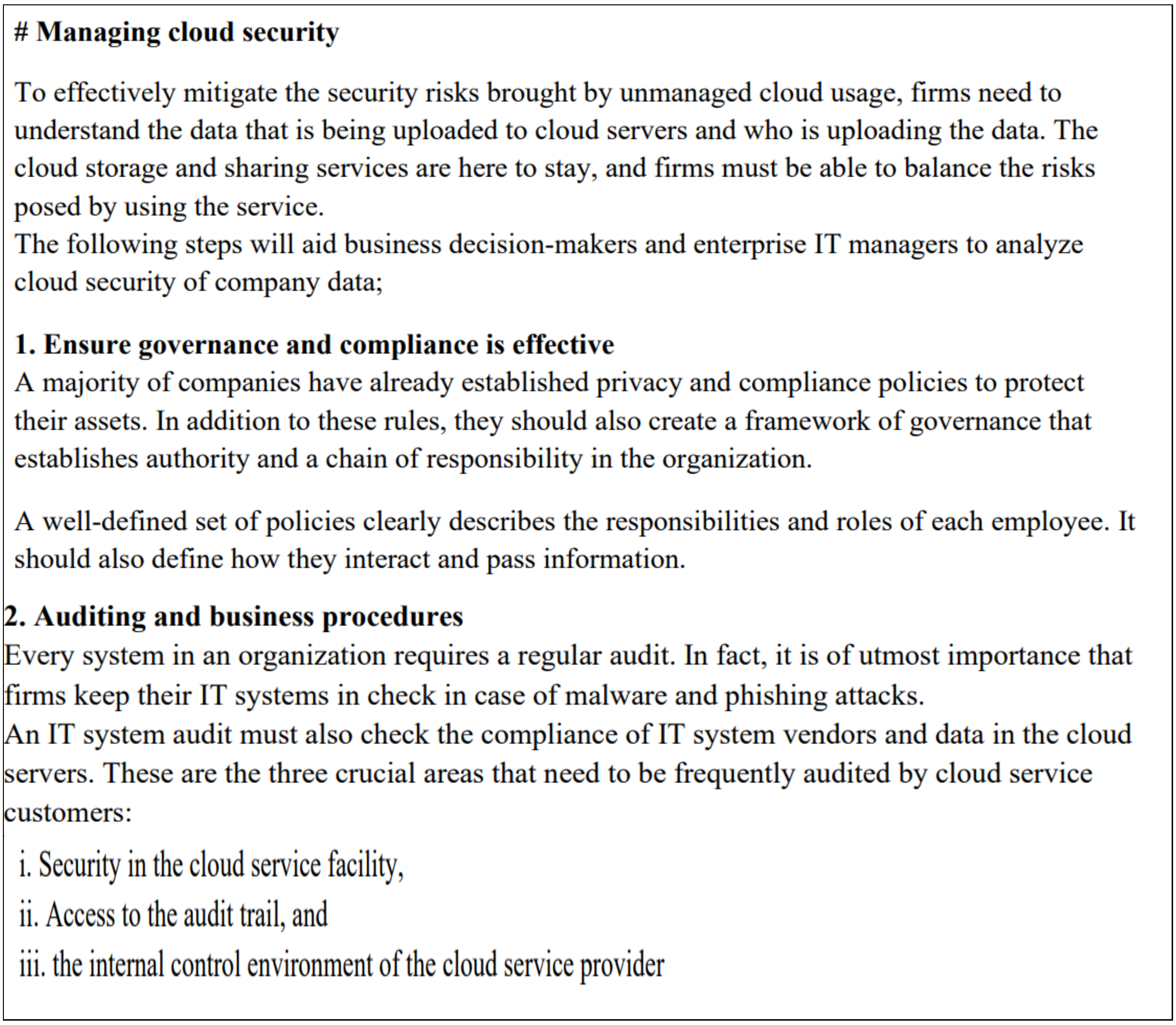
9. Loss of data

Data stored on cloud servers can be lost through a natural disaster, malicious attacks, or a data wipe by the service provider. Losing sensitive data is devastating to firms, especially if they have no recovery plan. Google is an example of the big tech firms that have suffered permanent data loss after being struck by lightning four times in its power supply lines.

Amazon was another firm that lost its essential customer data back in 2011. An essential step in securing data is carefully reviewing the terms of service of your provider and their back up procedures. The backup protocol could relate to physical access, storage locations, and natural disasters.

10. Diminished customer trust

It is inevitable for customers to feel unsafe after data breach concerns at your firm. There have been massive security breaches that resulted in the theft of millions of customer credit and debit card numbers from data storage facilities.



# Managing cloud security

To effectively mitigate the security risks brought by unmanaged cloud usage, firms need to understand the data that is being uploaded to cloud servers and who is uploading the data. The cloud storage and sharing services are here to stay, and firms must be able to balance the risks posed by using the service.
The following steps will aid business decision-makers and enterprise IT managers to analyze cloud security of company data;

1. Ensure governance and compliance is effective
A majority of companies have already established privacy and compliance policies to protect their assets. In addition to these rules, they should also create a framework of governance that establishes authority and a chain of responsibility in the organization.

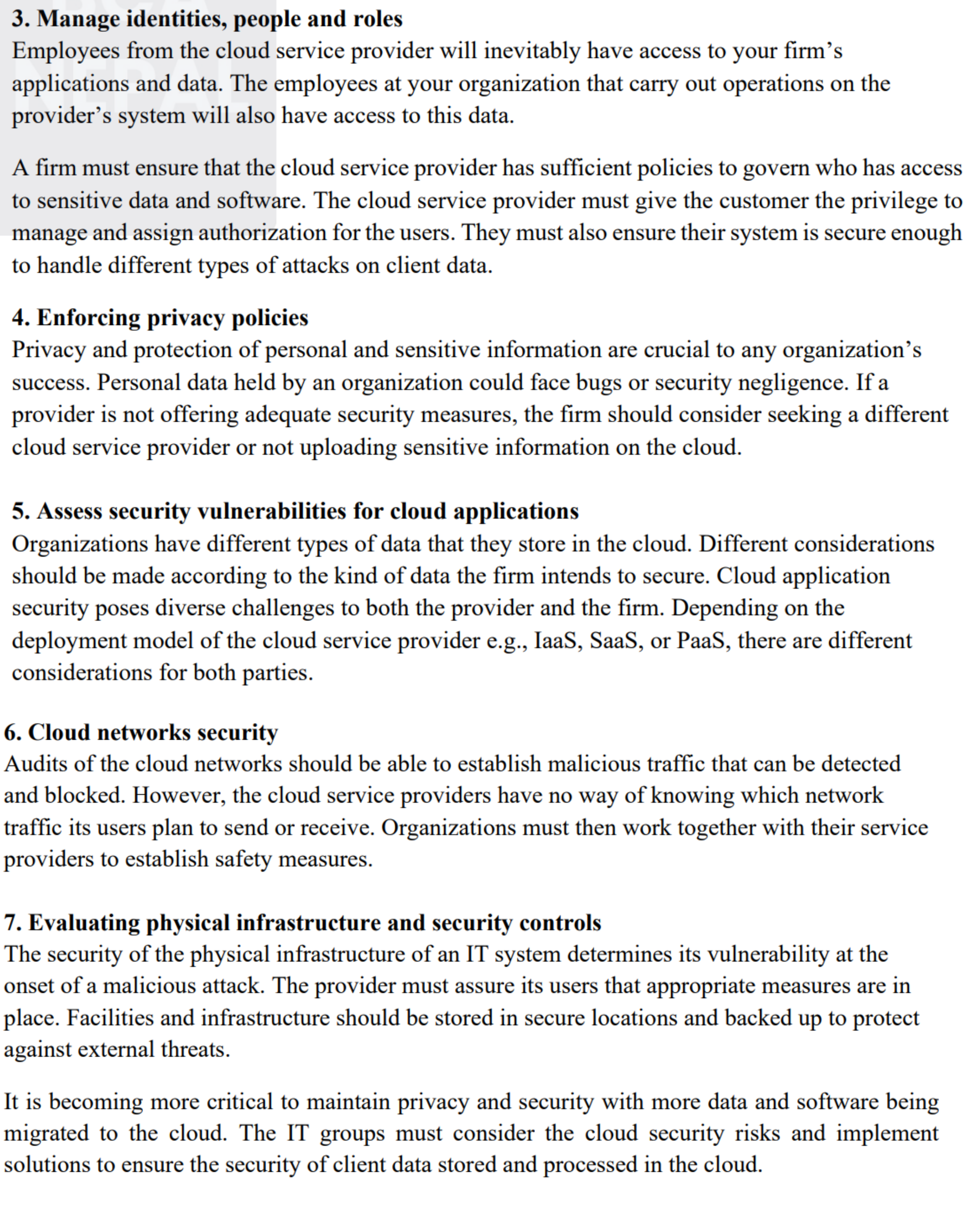
A well-defined set of policies clearly describes the responsibilities and roles of each employee. It should also define how they interact and pass information.

2. Auditing and business procedures
Every system in an organization requires a regular audit. In fact, it is of utmost importance that firms keep their IT systems in check in case of malware and phishing attacks.
An IT system audit must also check the compliance of IT system vendors and data in the cloud servers. These are the three crucial areas that need to be frequently audited by cloud service customers:

i. Security in the cloud service facility,

ii. Access to the audit trail, and

iii. the internal control environment of the cloud service provider



3. Manage identities, people and roles

Employees from the cloud service provider will inevitably have access to your firm's applications and data. The employees at your organization that carry out operations on the provider's system will also have access to this data.

A firm must ensure that the cloud service provider has sufficient policies to govern who has access to sensitive data and software. The cloud service provider must give the customer the privilege to manage and assign authorization for the users. They must also ensure their system is secure enough to handle different types of attacks on client data.

4. Enforcing privacy policies

Privacy and protection of personal and sensitive information are crucial to any organization's success. Personal data held by an organization could face bugs or security negligence. If a provider is not offering adequate security measures, the firm should consider seeking a different cloud service provider or not uploading sensitive information on the cloud.

5. Assess security vulnerabilities for cloud applications

Organizations have different types of data that they store in the cloud. Different considerations should be made according to the kind of data the firm intends to secure. Cloud application security poses diverse challenges to both the provider and the firm. Depending on the deployment model of the cloud service provider e.g., IaaS, SaaS, or PaaS, there are different considerations for both parties.

6. Cloud networks security

Audits of the cloud networks should be able to establish malicious traffic that can be detected and blocked. However, the cloud service providers have no way of knowing which network traffic its users plan to send or receive. Organizations must then work together with their service providers to establish safety measures.

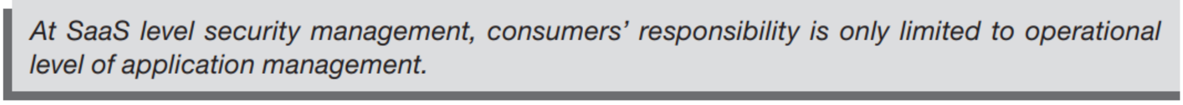
7. Evaluating physical infrastructure and security controls

The security of the physical infrastructure of an IT system determines its vulnerability at the onset of a malicious attack. The provider must assure its users that appropriate measures are in place. Facilities and infrastructure should be stored in secure locations and backed up to protect against external threats.

It is becoming more critical to maintain privacy and security with more data and software being migrated to the cloud. The IT groups must consider the cloud security risks and implement solutions to ensure the security of client data stored and processed in the cloud.

Software as a service security (SaaS)

In SaaS model, it is the responsibility of the provider to manage the complete set of applications they deliver to consumers. Therefore, the SaaS providers must take suitable measures to make their offering secure so that consumers with ill intention cannot cause harm to them. From the consumer's viewpoint, the use of SaaS reduces lots of tensions. At the SaaS level, consumers are only responsible for the operational security management of the applications which includes user authentication and access control management.



At SaaS level security management, consumers' responsibility is only limited to operational level of application management.

Figure 16.1 summarizes the whole discussion by showing consumers' responsibility in security management at different levels of cloud applications. Here, the horizontal axis represents three cloud services and the vertical axis represents consumers' responsibility in cloud application security management. It can be seen from Figure 16.1 that consumers' responsibility for application level security management decreases as they move from IaaS towards SaaS. As discussed earlier, at the SaaS level, consumers' responsibility becomes very limited

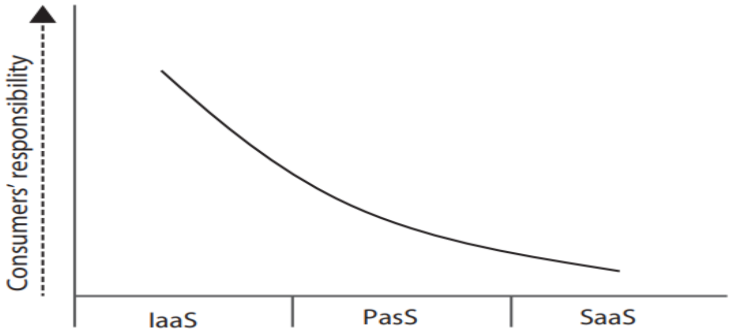


FIG 16.1: Application security responsibility of consumers

SaaS security is the managing, monitoring, and safeguarding of sensitive data from cyber-attacks. With the increase in efficiency and scalability of cloud-based IT infrastructures, organizations are also more vulnerable.

SaaS maintenance measures such as SaaS security posture management ensure privacy and safety of user data. From customer payment information to inter-departmental exchange of information, strengthening the security of SaaS applications is vital to your success.

To help this cause, regulatory bodies worldwide have issued security guidelines such as GDPR (General Data Protection Regulation of EU), EU-US and the Swiss-US Privacy Shield Frameworks.

Every SaaS business must adopt these guidelines to offer safe and secure services. Whether you are starting anew or adding an aspect to your IT arsenal, SaaS security is essential for successful ventures.

The Anatomy of SaaS Security

Every organization offering a cloud-based service can leverage preventive measures such as SaaS security posture management to continuously monitor and protect sensitive information.

Let us understand the anatomy of SaaS security in cloud computing environments. If we look at an ideal SaaS product technology stack from a bird's eye view, it forms a three-layer cake where each part represents different environments.

Three layers of SaaS security:

Infrastructure (server-side)

Network (the internet)

Application and Software (client-side)

Infrastructure

The server-side of your technology stack refers to the internal exchange of information. For instance, if your SaaS business is using AWS, you must secure every point of information exchange between the cloud storage provider and your software platform.

Every IoP initiated from the client-side starts at this level. Moreover, depending upon the kind of storage you purchase (shared, dedicated, or individual server), you must enhance your SaaS security measures.

Network

The exchange of information between the server-side and client-side is done over the internet. This is by far the most vulnerable layer of every SaaS business. Hackers are well versed in finding back-doors through weak encryptions of data packets exchanged over the internet.

The effectiveness of SaaS security is directly proportional to the integrity of data encryption methods and the ability for real-time monitoring of information exchange over the internet. With the advent of digital payments and online KYCs, businesses are constantly sending and receiving sensitive information. Hence it becomes even more important to install network security measures.

Application and Software

Application and software are the final layers of SaaS security. As mentioned above, a single data breach could very well be the cause of unparalleled user attrition. Therefore, to ensure the safety of user data, we must deploy impenetrable SaaS security measures.

We must ensure that all the 3rd party applications and software that you use are continuously monitored. Further, the unpredictability of the client-side environment demands higher standards of security measures than conventional methods.

SaaS Security Best Practices for Secure Products

The competition in every market is such that companies must necessarily evolve and introduce new features/tools in existing SaaS products. Whether you are removing bugs or adding new features, it is crucial to have security processes for such events. Let’s take a look at SaaS security best practices that you can follow for your organization:

Encryption is a must

Data encryption ensures that every piece of information is protected from cyberattacks at all times. From internal communication to customer service conversations, your data must be encrypted at all times. Here are a few encryption types that you can employ in **your SaaS product:**

Data Encryption Standard (DES)

RSA

All of these encryption types enhance the security of your SaaS products through their innate mathematically secure algorithms made by the brightest minds in data encryption.

Back-up User Data in Multiple Locations

Effective customer data management is essential for offering satisfactory services. Backing up user data in multiple locations, i.e., disaster recovery ensures that one system’s failure does not compromise the ability of the entire infrastructure. Many cloud platforms offer backup functionality. However, you must be diligent with timely backups.

Customer Education

A Gartner’s report suggests that over 95% of all cloud security failures will happen from the consumer end. When onboarding a new user, it is essential to educate them about the best practices for data safety. Ensure that your customers know the standard operating procedures of your SaaS platforms. Vigilant subscribers will serve as additional security layers for your organization.

Compulsory Strong Passwords

The virtual world is all about passwords, from email to banking; passwords primarily protect everything. Hackers these days are becoming intelligent at cracking passwords based on the public information available on the internet. Therefore, you must have strong password policies that ensure users set strong passwords that cannot be cracked easily.

. Vulnerability testing

You can expect SaaS providers to make high claims regarding SaaS security. But the onus to verify these claims can end up with the clients. If the SaaS provider has tools or checks, they should be reliable and meets all standards. Apart from these, you should also ensure that intensive checks are done on the SaaS systems.

There are multiple ways to assess SaaS security, such as automated tools or manually by security experts. A comprehensive SaaS security check should meet both automated and manual checks since it would also consider real-world scenarios and the latest threats. A number of quality SaaS security solutions are available to help you with the security testing process.

Policies for data deletion

Data deletion policies play an important role in customers' data safe. SaaS providers should be clear in declaring their data deletion policies to their clients. These policies are mentioned in the service agreement and should include what would happen after the customer's data retention timeline ends. When applicable, client data should be programmatically deleted from the server and respective logs should be generated.

Data security at the user level

Multiple levels of SaaS security can limit the damage from cyber-attacks. At the user level, security protocols such as role-based permissions and access, and enforced distribution of tasks, will protect your system from attacks that leverage internal security gaps.

Virtual Private Network/Virtual Private Cloud

VPN and VPC provide a safe environment for clients for their operation and data storage. These are better options and more secure than multi-tenant systems. These also enable users to log in and use SaaS applications from anywhere by securing endpoints and protecting the infrastructure.

Virtual Machine Management

Your virtual machine needs to be updated regularly to maintain a secure infrastructure. Keep up with the latest threats and patches on the market and deploy them timely to protect your VM.

Consult a SaaS Security Firm

When in doubt, consult an expert. SaaS security firms such as Cloudlytics employ the brightest minds in data encryption, software monitoring, and AI-based vigilance. You can leverage our testing protocols and monitoring systems to build a safe and secure SaaS platform.

How can Cloudlytics help?

Cloudlytics is a cloud-driven security provider for modern enterprises that offer compliance solutions, security analytics, and asset monitoring. Over the years, we have had the good fortune of working with enterprises from various industries such as OTT platforms. We offer an extensive range of future-proof SaaS security solutions such as:

Compliance Manager

An all-inclusive compliance manager maintains an unwavering security posture by identifying, prioritizing, and remediating compliance. The platform offers actionable insights on the well-being of your SaaS platform and user information.

Event Analytics

Driven by machine learning and big-data analysis, event analytics solutions from Cloudlytics present a secure environment for developing resolute applications of the future.

AWS Architecture Review

AWS architecture review offers a detailed analysis of your AWS environment. It employs a structured framework of testing operational excellence, security, cost optimization, and performance of your hosting environment.

Cloud Intelligence Engine

Record resource configurations and capture changes with cloud intelligence engines. The SMART engine helps organizations retain configurations long after the resources have been deleted.

These are a few of the many ways that Cloudlytics can help you build SaaS security measures for successful future platforms. We are passionate about security because we believe that the world would be a better place if our data is secure against malicious forces of the internet.

Why is SaaS Security important?

SaaS (Software as a Service) has become increasingly popular in recent years due to its flexibility, cost-effectiveness, and scalability. However, this popularity also means that SaaS providers and their customers face significant security challenges.

SaaS Security is important because:

- Sensitive data would be well-protected and not compromised by hackers, malicious insiders or other cyber threats.
- SaaS security helps avoid severe consequences such as legal liabilities, damage to reputation and loss of customers.

- Aids in increasing the trust of the SaaS provider to the customers.

Aids in compliance with security standards and regulations.

- Ensures the security and protection of applications and data hosted from cyber threats, minimizing the chance,s of data breaches and other security incidents.

Challenges in SaaS security

Some of the most significant challenges in SaaS security include:

1. Lack of Control

SaaS providers typically host applications and data in the cloud, meaning that customers have less direct control over their security. This can make it challenging for customers to monitor and manage security effectively.

2. Access Management

SaaS applications typically require users to log in and authenticate their identity. However, managing user access can be challenging, particularly if the provider is hosting applications for multiple customers with different access requirements.

3. Data Privacy

SaaS providers may be subject to data privacy regulations, which can vary by jurisdiction. This can make it challenging to ensure compliance with all relevant laws and regulations, particularly if the provider hosts data for customers in multiple countries.

4. Third-party integration

SaaS providers may integrate with third-party applications, such as payment processors or marketing platforms. However, this can increase the risk of security incidents, as vulnerabilities in third-party software can potentially affect the entire system.

5. Continuous monitoring

SaaS providers must continuously monitor their systems for security threats and vulnerabilities. This requires a high level of expertise and resources to detect and respond to security incidents effectively.

Security monitoring

Monitoring is a critical component of cloud security and management. Typically relying on automated solutions, cloud security monitoring supervises virtual and physical servers to continuously assess and measure data, application, or infrastructure behaviors for potential security threats. This assures that the cloud infrastructure and platform function optimally while minimizing the risk of costly data breaches.

Cloud security monitoring allows you to:

- **Maintain compliance** – most major regulations, such as PCI DSS and HIPAA, require monitoring. Organizations using cloud platforms should leverage observation tools to comply with these regulations and avoid penalties.
- **Discover vulnerabilities** – it is important to maintain visibility over your cloud environments to identify vulnerabilities. You can use an automated observation tool to quickly send alerts to your IT and security teams and help them identify suspicious behavior patterns and indicators of compromise (IoCs).
- **Avoid business disruptions** – security incidents can disrupt business operations or force you to shut them down altogether. Disruptions and data breaches can impact customer trust and satisfaction, so it is important to monitor your cloud environments to maintain business continuity and data security and business continuity.
- **Protect sensitive data** – you can use a cloud security monitoring solution to perform regular audits and keep your data secure. You can monitor the health status of your security systems and receive recommendations for implementing security measures.
- **Leverage continuous monitoring and support** – A cloud security management service can monitor your system 24/7. While maintaining security on-premises requires physical monitoring at regular intervals, cloud-based services allow you to implement continuous monitoring, significantly decreasing the risk of letting threats slip unnoticed.

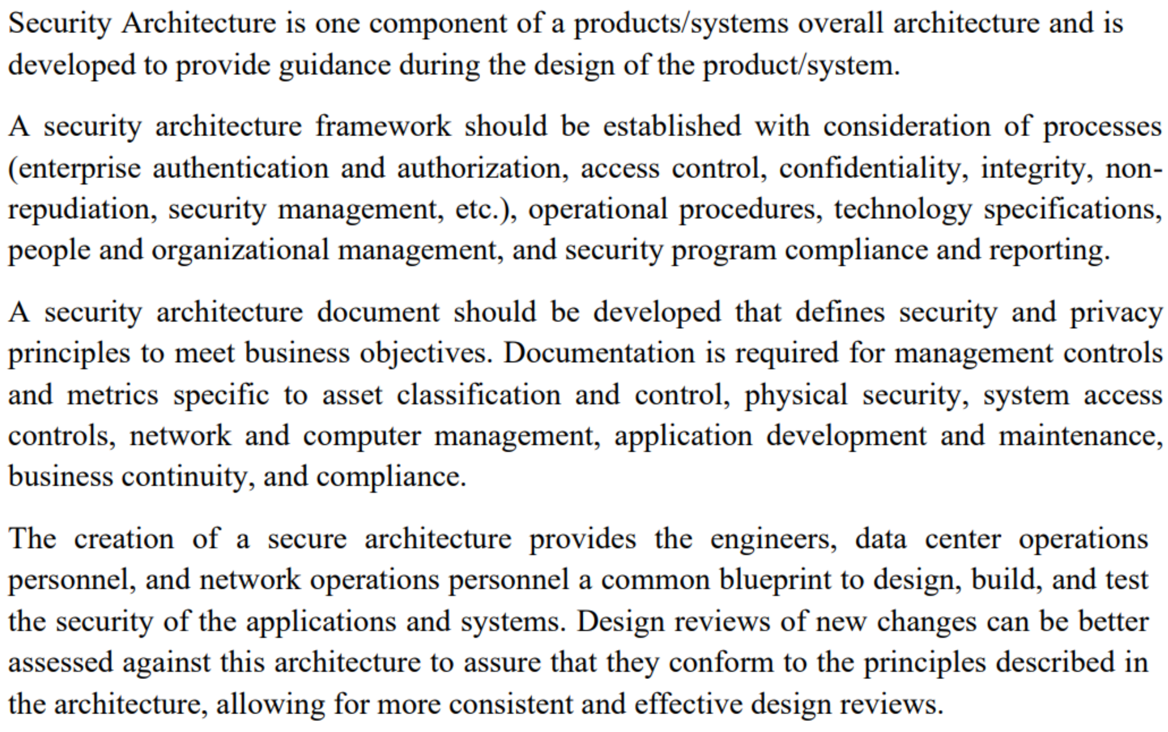
.

Below are some key benefits of cloud security monitoring:

- **Customizability:** Cloud security monitoring solutions will allow companies to replace or integrate their cloud solution into their existing infrastructure. The ability of cloud security tools to fit into any local compliance measures makes cloud security monitoring a safe and flexible option.

- **Promptness of response to threat/issues:** Because cloud security monitoring tools rely on real-time assessment and scanning, organizations can expect a prompt and timely threat-response process.
- **Automation:** The ability to automate scanning and monitoring processes will save time and costs for your team by freeing up space so you can focus on other important tasks.
- **Knowledge and informed decision-making:** Automated, real-time assessments mean your team will always have the most accurate and up-to-date information to inform their decision-making capabilities.

Security architecture design:



Security Architecture is one component of a products/systems overall architecture and is developed to provide guidance during the design of the product/system.

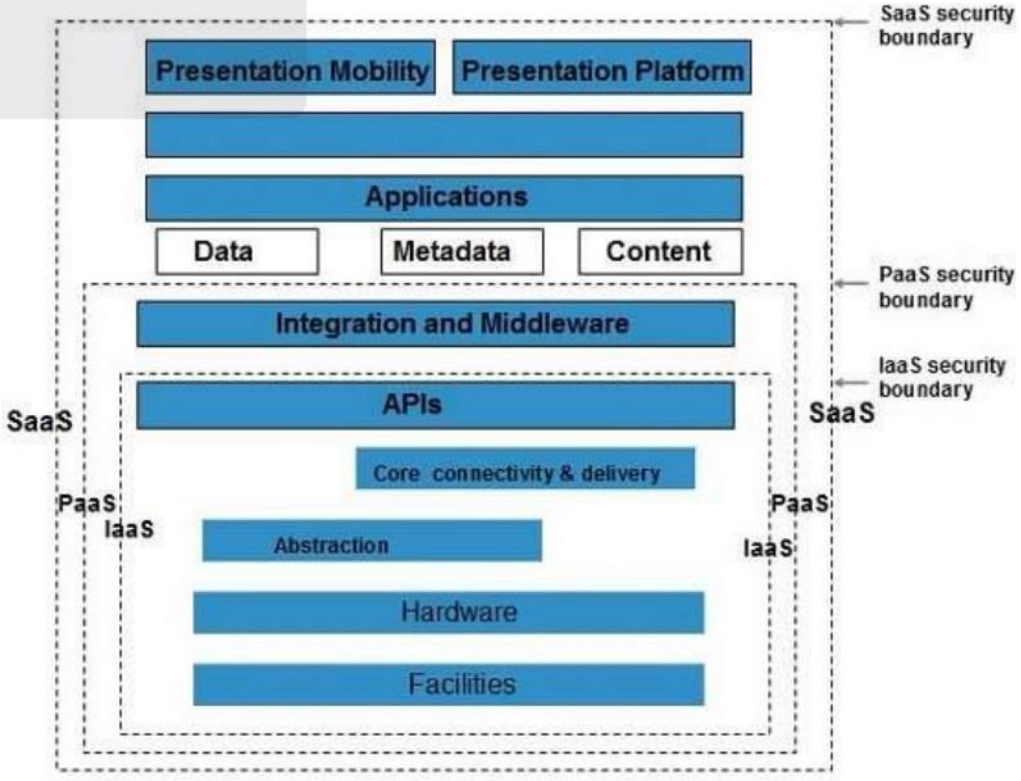
A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, non-repudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting.

A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance.

The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and customer. **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the **CSA stack model:**



Data security

Cloud data security is the practice of protecting data and other digital information assets from security threats, human error, and insider threats. It leverages technology, policies, and processes to keep your data confidential and still accessible to those who need it in cloud-based environments.

Cloud computing delivers many benefits, allowing you to access data from any device via an internet connection to reduce the chance of data loss during outages or incidents and improve scalability and agility. At the same time, many organizations remain hesitant to migrate sensitive data to the cloud as they struggle to understand their security options and meet regulatory demands.

Understanding how to secure cloud data remains one of the biggest obstacles to overcome as organizations transition from building and managing on-premises data centers. So, what is data security in the cloud? How is your data protected? And what cloud data security best practices should you follow to ensure cloud-based data assets are secure and protected?

Cloud data security protects data that is stored (at rest) or moving in and out of the cloud (in motion) from security threats, unauthorized access, theft, and corruption. It relies on physical security, technology tools, access management and controls, and organizational policies.

Data privacy, integrity, and accessibility
Cloud data security best practices follow the same guiding principles of information security and data governance:

- **Data confidentiality:** Data can only be accessed or modified by authorized people or processes. In other words, you need to ensure your organization's data is kept private.
- **Data integrity:** Data is trustworthy—in other words, it is accurate, authentic, and reliable. The key here is to implement policies or measures that prevent your data from being tampered with or deleted.
- **Data availability:** While you want to stop unauthorized access, data still needs to be available and accessible to authorized people and processes when it's needed. You'll need to ensure continuous uptime and keep systems, networks, and devices running smoothly.

What are the challenges of cloud data security?

As more data and applications move out of a central data center and away from traditional security mechanisms and infrastructure, the higher the risk of exposure becomes. While many of the foundational elements of on-premises data security remain, they must be adapted to the cloud.

Common challenges with data protection in cloud or hybrid environments include:

- **Lack of visibility.** Companies don’t know where all their data and applications live and what assets are in their inventory.
- **Less control.** Since data and apps are hosted on third-party infrastructure, they have less control over how data is accessed and shared.
- **Confusion over shared responsibility.** Companies and cloud providers share cloud security responsibilities, which can lead to gaps in coverage if duties and tasks are not well understood or defined.
- **Inconsistent coverage.** Many businesses are finding multicloud and hybrid cloud to better suit their business needs, but different providers offer varying levels of coverage and capabilities that can deliver inconsistent protection.
- **Growing cybersecurity threats.** Cloud databases and cloud data storage make ideal targets for online criminals looking for a big payday, especially as companies are still educating themselves about data handling and management in the cloud.
- **Strict compliance requirements.** Organizations are under pressure to comply with stringent data protection and privacy regulations, which require enforcing security policies across multiple environments and demonstrating strong data governance.
- **Distributed data storage.** Storing data on international servers can deliver lower latency and more flexibility. Still, it can also raise data sovereignty issues that might not be problematic if you were operating in your own data center.

Application security:

Cloud application security is the process of securing cloud-based software applications throughout the development lifecycle. It includes application-level policies, tools, technologies and rules to maintain visibility into all cloud-based assets, protect cloud-based applications from cyberattacks and limit access only to authorized users.

Cloud application security is crucially important for organizations that are operating in a multi-cloud environment hosted by a third-party cloud provider such as Amazon, Microsoft or Google, as well as those that use collaborative web applications such as Slack, Microsoft Teams or Box. These services or applications, while transformational in nature to the business and its workforce, dramatically increase the attack surface, providing many new points of access for adversaries to enter the network and unleash attacks.

Cloud Application Security Threats

Cloud applications are vulnerable to a wide range of threats that may exploit system misconfigurations, weak identity management measures, insecure APIs or unpatched software. Here we review some of the most common threats organizations should consider when developing their cloud application security strategy and solution.

Misconfigurations

Misconfigurations are the single largest threat to both cloud and app security. These errors can include misconfigured S3 buckets, which leave ports open to the public, or the use of insecure accounts or an application programming interface (API). These errors transform cloud workloads into obvious targets that can be easily discovered with a simple web crawler. In the cloud, the absence of perimeter security can make those mistakes very costly. Multiple publicly reported breaches started with misconfigured S3 buckets that were used as the entry point.

Because many application security tools require manual configuration, this process can be rife with errors and take considerable time to set up and update. To that end, organizations should adopt security tooling and technologies and automate the configuration process.

Unsecured APIs

APIs are often the only organizational asset with a public IP address. This can make them an easy target for attackers, especially if they are insecure due to lackluster access controls or encryption methods.

Insufficient Visibility and Threat Detection

The shift to the cloud is a relatively recent phenomenon for many organizations. This means that many companies may not have the security maturity needed to operate safely in a multi-cloud environment.

For example, some vulnerability scanners may not scan all assets, such as containers within a dynamic cluster. Others cannot distinguish real risk from normal operations, which produces a number of false alarms for the IT team to investigate.

As such, organizations must develop the tools, technologies and systems to inventory and monitor all cloud applications, workloads and other assets. They should also remove any assets not needed by the business in order to limit the attack surface.

Misunderstanding the “Shared Responsibility Model”(i.e., Runtime Threats)

Cloud networks adhere to what is known as the “shared responsibility model.” This means that much of the underlying infrastructure is secured by the cloud service provider. However, the organization is responsible for everything else, including the operating system, applications and data. Unfortunately, this point can be misunderstood, leading to the assumption that cloud workloads are fully protected by the cloud provider. This results in users unknowingly running workloads in a public cloud that are not fully protected, meaning adversaries can target the operating system and the applications to obtain access. Even securely configured workloads can become a target at runtime, as they are vulnerable to zero-day exploits.

Shadow IT

Shadow IT, which describes applications and infrastructure that are managed and utilized without the knowledge of the enterprise’s IT department, is another major issue in cloud environments. In many instances, DevOps often contributes to this challenge as the barrier to entering and using an asset in the cloud — whether it is a workload or a container — is extremely low. Developers can easily spawn workloads using their personal accounts. These unauthorized assets are a threat to the environment, as they often are not properly secured and are accessible via default passwords and configurations, which can be easily compromised.

Lack of a Comprehensive Cloud Security Strategy

As workloads move to the cloud, administrators continue to try and secure these assets the same way they secure servers in a private or an on-premises data center. Unfortunately, traditional data center security models are not suitable for the cloud. With today’s sophisticated, automated attacks, only advanced, integrated security can prevent successful breaches. It must secure the entire IT environment, including multi-cloud environments as well as the organization’s data centers and mobile users. A consistent, integrated approach that provides complete visibility and granular control across the entire organization will reduce friction, minimize business disruption and enable organizations to safely, confidently embrace the cloud.

Types of application security

Different types of application security features include authentication, authorization, encryption, logging, and application security testing. Developers can also code applications to reduce security vulnerabilities.

- **Authentication**: When software developers build procedures into an application to ensure that only authorized users gain access to it. Authentication procedures ensure that a user is who they say they are. This can be accomplished by requiring the user to provide a user name and password when logging in to an application. Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).
- **Authorization**: After a user has been authenticated, the user may be authorized to access and use the application. The system can validate that a user has permission to access the application by comparing the user's identity with a list of authorized users. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.
- **Encryption**: After a user has been authenticated and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal. In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be encrypted to keep the data safe.
- **Logging**: If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.
- **Application security testing**: A necessary process to ensure that all of these security controls work properly.

Virtual machine security :

The term **"Virtualized Security,"** sometimes known as "security virtualization," describes security solutions that are software-based and created to operate in a virtualized IT environment. This is distinct from conventional hardware-based network security, which is static and is supported by equipment like conventional switches, routers, and firewalls. Virtualized security is flexible and adaptive, in contrast to hardware-based security. It can be deployed anywhere on the network and is frequently cloud-based so it is not bound to a specific device.

In Cloud Computing**,** where operators construct workloads and applications on-demand, virtualized security enables security services and functions to move around with those on-demand-created workloads. This is crucial for virtual machine security. It's crucial to protect virtualized security in cloud computing technologies such as isolating multitenant setups in public cloud settings. Because data and workloads move around a complex ecosystem including several providers, virtualized security's flexibility is useful for securing hybrid and multi-cloud settings.

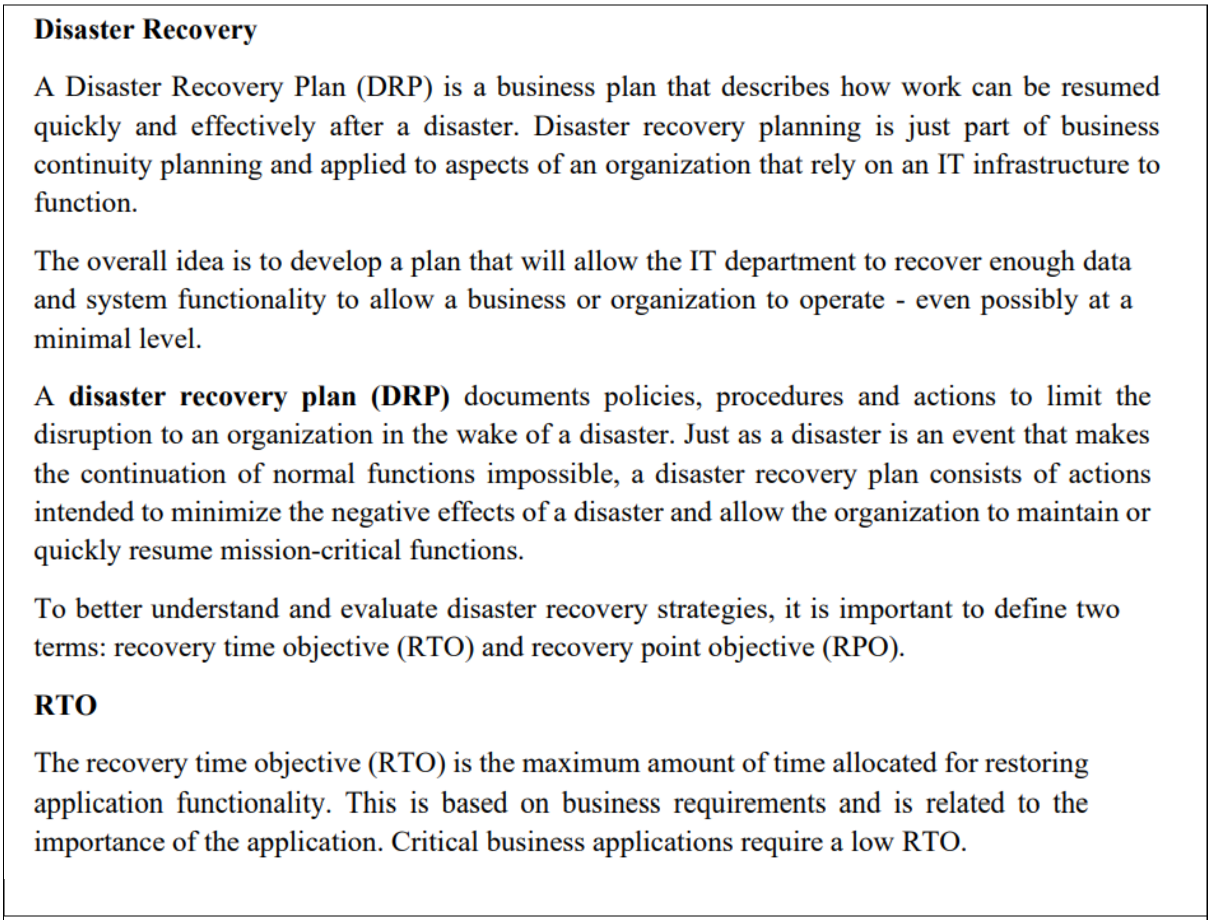
Virtual Machine Security

The administrator must set up a program or application that prevents virtual machines from consuming additional resources without permission. Additionally, a lightweight process that gathers logs from the VMs and monitors them in real-time to repair any **VM tampering must operate on a Virtual Machine**. Best security procedures must be used to harden the guest OS and any running applications. These procedures include setting up firewalls, host intrusion prevention systems (HIPS), anti-virus and anti-spyware programmers, online application protection, and log monitoring in guest operating systems.

Benefits of Virtualized Security

Virtualized security is now practically required to meet the intricate security requirements of a virtualized network, and it is also more adaptable and effective than traditional physical security.

- **Cost-Effectiveness:** Cloud computing's virtual machine security enables businesses to keep their networks secure without having to significantly raise their expenditures on pricey proprietary hardware. Usage-based pricing for cloud-based virtualized security services can result in significant savings for businesses that manage their resources effectively.
- **Flexibility:** It is essential in a virtualized environment that security operations can follow workloads wherever they go. A company is able to profit fully from virtualization while simultaneously maintaining data security thanks to the protection it offers across various data centers, in multi-cloud, and hybrid-cloud environments.
- **Operational Efficiency:** Virtualized security can be deployed more quickly and easily than hardware-based security because it doesn't require IT, teams, to set up and configure several hardware appliances. Instead, they may quickly scale security systems by setting them up using centralized software. Security-related duties can be automated when security technology is used, which frees up more time for IT employees.
- **Regulatory Compliance:** Virtual machine security in cloud computing is a requirement for enterprises that need to maintain regulatory compliance because traditional hardware-based security is static and unable to keep up with the demands of a virtualized network.



Disaster Recovery

A Disaster Recovery Plan (DRP) is a business plan that describes how work can be resumed quickly and effectively after a disaster. Disaster recovery planning is just part of business continuity planning and applied to aspects of an organization that rely on an IT infrastructure to function.

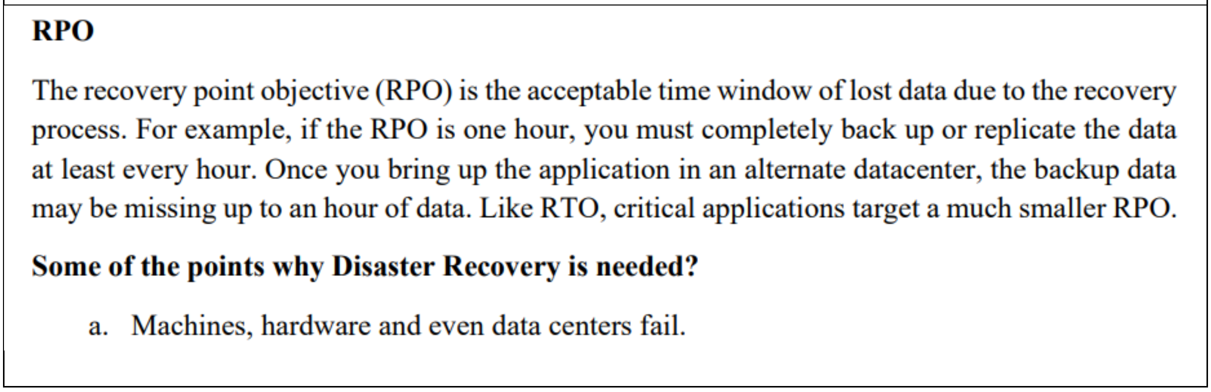
The overall idea is to develop a plan that will allow the IT department to recover enough data and system functionality to allow a business or organization to operate - even possibly at a minimal level.

A **disaster recovery plan (DRP)** documents policies, procedures and actions to limit the disruption to an organization in the wake of a disaster. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of actions intended to minimize the negative effects of a disaster and allow the organization to maintain or quickly resume mission-critical functions.

To better understand and evaluate disaster recovery strategies, it is important to define two terms: recovery time objective (RTO) and recovery point objective (RPO).

RTO

The recovery time objective (RTO) is the maximum amount of time allocated for restoring application functionality. This is based on business requirements and is related to the importance of the application. Critical business applications require a low RTO.

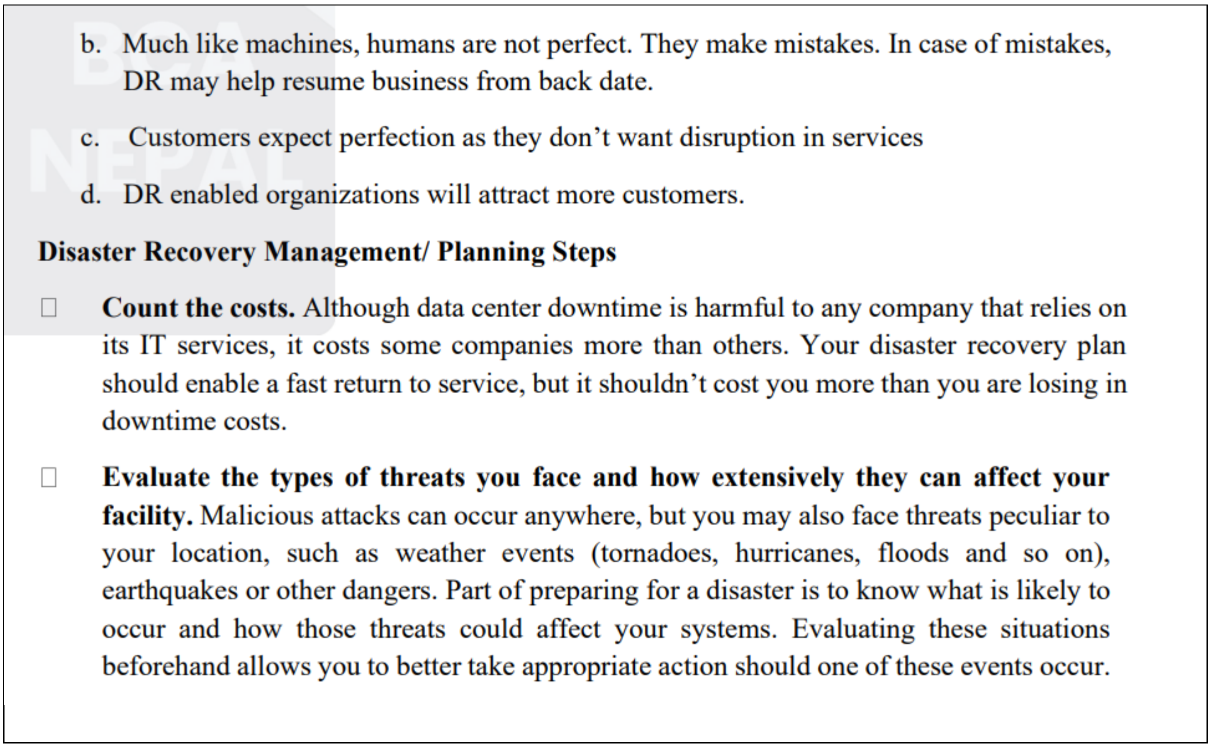


RPO

The recovery point objective (RPO) is the acceptable time window of lost data due to the recovery process. For example, if the RPO is one hour, you must completely back up or replicate the data at least every hour. Once you bring up the application in an alternate datacenter, the backup data may be missing up to an hour of data. Like RTO, critical applications target a much smaller RPO.

Some of the points why Disaster Recovery is needed?

a. Machines, hardware and even data centers fail.



b. Much like machines, humans are not perfect. They make mistakes. In case of mistakes, DR may help resume business from back date.

c. Customers expect perfection as they don't want disruption in services

d. DR enabled organizations will attract more customers.

Disaster Recovery Management/ Planning Steps

- **Count the costs.** Although data center downtime is harmful to any company that relies on its IT services, it costs some companies more than others. Your disaster recovery plan should enable a fast return to service, but it shouldn't cost you more than you are losing in downtime costs.

- **Evaluate the types of threats you face and how extensively they can affect your facility.** Malicious attacks can occur anywhere, but you may also face threats peculiar to your location, such as weather events (tornadoes, hurricanes, floods and so on), earthquakes or other dangers. Part of preparing for a disaster is to know what is likely to occur and how those threats could affect your systems. Evaluating these situations beforehand allows you to better take appropriate action should one of these events occur.

- **Know what you have and how critical it is to operations.** Responding to a disaster in your data center is similar to doing so in medicine: you need to treat the more serious problems first, then the more minor ones. By determining which systems are most critical to your data center, you enable your IT staff to prioritize and make the best use of the precious minutes and hours immediately following an outage. Not every system need be functional immediately following a disaster.
- **Identify critical personnel and gather their contact information.** Who do you most want to be present in the data center following an outage? Who has the most expertise in a given area and the greatest ability to oversee some part of the recovery effort? Being able to get in touch with these people is crucial to a fast recovery. Collect their contact information and, just as importantly, keep it up to date. If it's been a year or more since you last checked, some of that contact information is likely out of date. Every minute you spend trying to find important personnel is time not spent on recovery.
- **Train your employees.** Knowledge of how to implement disaster recovery procedures is obviously important when an outage occurs. To this end, prepare by training personnel and not just in their respective areas of expertise. Everyone should have some broad- based knowledge of the recovery process so that it can be at least started even if not everyone is present.
- **Practice.** Needless to say, this is perhaps the most critical part of preparation for a downtime event. The difference between knowing your role and being able to execute it well is simply practice. You may not be able to shut down your data center to simulate precisely all of the conditions you will face in an outage, but you can go through many of the procedures nevertheless. Some recommendations prescribe semiannual drills, at a minimum, to practice implementing the disaster recovery plan. If there's one thing you take from this article, it's that you should practice your disaster recovery plan—don't expect it to unfold smoothly when you need it (regardless of how well laid-out a plan it is) if you haven't given it a trial run or two.
- **Automate where possible.** Your staff is limited, so it can only do so much. The more that your systems can do on their own in a recovery situation, the faster the recovery will generally be. This also leaves less room for human error—particularly in the kind of stressful atmosphere that exists following a disaster.
- **Follow up after a disaster.** When a downtime event does occur, evaluate the performance of the personnel and the plan to determine if any improvements can be made. Update your plan accordingly to enable a better response in the future. Furthermore, investigate the cause of the outage. If it's an internal problem, take necessary measures to correct equipment issues to avoid the same problem occurring again.

Identity management and access control :

Identity and access management (IAM or IdAM for short) is a way to tell who a user is and what they are allowed to do. IAM is like the bouncer at the door of a nightclub with a list of who is allowed in, who isn't allowed in, and who is able to access the VIP area. IAM is also called identity management (IdM).

In more technical terms, IAM is a means of managing a given set of users' digital identities, and the privileges associated with each identity. It is an umbrella term that covers a number of different products that all do this same basic function. Within an organization, IAM may be a single product, or it may be a combination of processes, software products, cloud services, and hardware that give administrators visibility and control over the organizational data that individual users can access.

What is identity in the context of computing?

A person's entire identity cannot be uploaded and stored in a computer, so "identity" in a computing context means a certain set of properties that can be conveniently measured and recorded digitally. Think of an ID card or a passport: not every fact about a person is recorded in an ID card, but it contains enough personal characteristics that a person's identity can quickly be matched to the ID card.

To verify identity, a computer system will assess a user for characteristics that are specific to them. If they match, the user's identity is confirmed. These characteristics are also known as "authentication factors," because they help authenticate that a user is who they say they are.

The three most widely used authentication factors are:

John logs in by entering his email, *john@company.com*, and the password that only he knows – for example, *"5jt*2)f12?y"*. Presumably, no one else besides John knows this password, so the email system recognizes John and lets him access his email account. If someone else tried to impersonate John by entering their email address as *"john@company.com,"* they wouldn't be successful without knowing to type *"5jt*2)f12?y"* as the password.

Something the user has: This factor refers to possession of a physical token that is issued to authorized users. The most basic example of this authentication factor is the use of a physical house key to enter one's home. The assumption is that only someone who owns, rents, or otherwise is allowed into the house will have a key.

In a computing context, the physical object could be a key fob, a USB device, or even a smartphone. Suppose that John's organization wanted to be extra sure that all users really were who they said they were by checking two authentication factors instead of one. Now, instead of just entering his secret password – the something the user knows factor – John has to show the email system that he possesses an object that no one else has. John is the only person in the world who possesses his personal smartphone, so the email system texts him a one-time code, and John types in the code to demonstrate his possession of the phone.

Something the user is: This refers to a physical property of one's body. A common example of this authentication factor in action is Face ID, the feature offered by many modern smartphones. Fingerprint scanning is another example. Less common methods used by some high-security organizations include retina scans and blood tests.

Imagine John's organization decides to tighten security even more by making users verify three factors instead of two (this is rare). Now John has to enter his password, verify possession of his smartphone, and scan his fingerprint before the email system confirms that he really is John.

To summarize: In the real world, one's identity is a complex mix of personal characteristics, history, location, and other factors. In the digital world, a user's identity is made up of some or all of the three authentication factors, stored digitally in an identity database. To prevent impostors from impersonating real users, computer systems will check a user's identity against the identity database.

What is access management?

"Access" refers to what data a user can see and what actions they can perform once they log in. Once John logs into his email, he can see all the emails he has sent and received. However, he should not be able to see the emails sent and received by Tracy, his coworker.

In other words, just because a user's identity is verified, that doesn't mean they should be able to access whatever they want within a system or a network. For instance, a low-level employee within a company should be able to access their corporate email account, but they should not be able to access payroll records or confidential HR information.

Access management is the process of controlling and tracking access. Each user within a system will have different privileges within that system based on their individual needs. An accountant does indeed need to access and edit payroll records, so once they verify their identity, they should be able to view and update those records as well as access their email account.