INFOSEC REPORT

MOHAMMAD IDREES

BITM-F19-096
December 7, 2022

Twitter

With 100 million daily active users and 500 million tweets sent each day, Twitter, a social networking website make to known in 2006, is without a doubt one of the most well-known social media platforms existing today. Twitter can be used to follow prominent celebrities, remain in touch with former high school pals, and get news. But its popularity might be scary, Twitter is thankfully quite simple to use. We'll go over what Twitter is, who uses it, and how to start using it right away in this article.

WHAT IS TWITTER

Co-founder of Twitter Jack Dorsey had an idea in 2006: he would build an SMS-based messaging system that allowed friends to stay in touch by posting statuses. Twitter was originally conceived as a concept very comparable to texting. The concept altered, in large part as a result of suggesting meetings with Evan Williams, Dorsey's co-founder. Jack made the first tweet on March 21, 2006, with the message of "just setting up my twttr...". More than 60,000 tweets were exchanged during the 2007 South by Southwest Interactive conference, which witnessed Twitter's exponential rise.

The Twitter team used the conference as an opportunity to start expanding their user base. The 140 character limit was first set by cell carriers, not Twitter, as Twitter started as an SMS-based site. Since Twitter is a platform that aims to provide highly skimmable material

for our tech-heavy, attention-deficit modern world, they decided to keep the limit as Twitter developed into a web platform.

Over the last ten years, Twitter has experienced exponential progress. Its ultimate goal is to quickly disseminate information, some of which may be serious (like when Iranian protesters used Twitter to assemble marches). In many respects, Twitter is a platform with boundless potential and purpose. It can introduce you to your neighbor as rapidly as it can connect you with someone in Thailand. You can choose to follow news sources, celebrities, comics, business influential, or friends in your feed. Twitter has effectively developed a very addictive platform by allowing each user to customize their content to their individual preferences and interests.

USE OF TWITTER?

Twitter is a social media platform with the main goal of connecting users and enabling them to express their ideas to a large audience.

Users can follow people or businesses who post content they enjoy reading, learn about the greatest news and events happening right now, or just use Twitter to connect with pals. PR groups and marketers can also use Twitter to engage their audience and raise brand awareness

Twitter for Marketers

Twitter can be a very useful channel for expanding your audience and giving them insightful stuff to read before becoming consumers. The character limit can also assist you in coming up with succinct and intriguing adverts, such as a mention of a webinar your company is hosting or a link to a free e-book.

Twitter can also be used to establish genuine and intimate connections with your audience. You can "like" or "retweet" a comment if it makes reference to one of your goods or services. Alternately, if a client expresses dissatisfaction with your services on Twitter, you can get in touch to address the issue right away. Twitter is a social media platform with the main goal of connecting users and enabling them to express their ideas to a large audience. Users can follow people or businesses who post content they enjoy reading, learn about the greatest news and events happening right now, or just use Twitter to connect with pals. PR groups and marketers can also use Twitter to engage their audience and raise brand awareness.

Twitter as a News Source:

Twitter is sometimes even faster than traditional media channels at breaking news dissemination, hence it is frequently used for this purpose. For instance, before many media outlets had learned about the US Airways plane crash-landing in the Hudson River in 2009, Janis Krum's was one of the first to share the news on Twitter: As a reporter, you may build a sizable audience by tweeting succinct summaries to inform your audience of everyday occurrences. Twitter is frequently a good resource when

looking for insider information or direct quotes to utilize for an article because many celebrities, athletes, and politicians choose to post on their rather than via media sources when they want to share information with their supporters.

PHYSICAL SECURITY:

What is Physical Security?

Physical security is the safeguarding of people, equipment, networks, and data from physical acts and events that could result in significant financial loss or other harm to a business, government agency, or academic institution. This covers defense against burglary, theft, vandalism, terrorism, fire, flood, and other natural catastrophes. While most of these are insured, physical security prioritizes damage prevention in order to prevent the time, money, and resources lost as a result of these catastrophes. The three essential parts of the physical security framework are access control, surveillance, and testing. How successfully each of these elements is implemented, enhanced, and maintained frequently has an impact on how effective a physical security program is for an organization.

Physical security and digital security are increasingly entwining, when traditionally they were two distinct fields. Access control and monitoring systems preserve digital logs, surveillance systems are becoming more and more internet-connected, and use cases for AI in physical security are becoming more and more

prevalent. For instance, CCTV-based image recognition can notify you when individuals or cars are approaching. In more advanced systems, facial or even walk recognition across entire facilities is conceivable and can alert you to the presence of an unauthorized visitor or a worker who is in a restricted area. Access restrictions integrated with behavioral analytics can notify you of unexpected behavior. Drone manufacturers are increasingly striving to incorporate automated, unmanned capabilities as businesses start using drones to monitor their operations. Over the next five years, investments in physical security might "dominate" AI-based video analytics, according to Memoori study.

PHYSCIAL SECURITY OF TWITTER

Twitter data centers are built with security in mind. Twitter claims to never sell or distribute their custom-built servers outside of their own data centers. In addition, Twitter facilities are among the safest places for user data to reside thanks to the 24/7 worldwide efforts of industry-leading security staff. Twitter business continuity and catastrophe recovery plans are also quite strong. For instance, they instantly and easily switch data access to a different data centre in the case of a fire or any other disturbance to ensure that users can continue working without interruption. Even in the case of a power outage, data centers are kept running by emergency backup generators. Twitter data centers' ISO 22301:2019 certification serves as evidence of their continued dedication to business continuity. Instead of keeping each user's data on a single

computer or group of computers, Twitter disperse all data, including their own, over numerous computers in various places.

The data is then split up and replicated across several systems to prevent a single point of failure. As an additional security safeguard, they give these data chunks random names that are unintelligible to the naked eye. Twitter servers automatically backup important data while users are working. You can therefore resume using your computer right away if an accident occurs, such as a computer breakdown or theft. Last but not least, Twitter carefully monitor each hard drive's location and condition in data centers. To stop unauthorized access to the data on hard drives that have reached the end of their useful lives, they destroy them thoroughly or in several steps.

Multiple security measures are in place to protect Twitter's user's data centers and guard against unwanted access to information. They claim to make use of biometric authentication, extensive camera coverage, secure perimeter defense systems, and a security force on duty around-the-clock. At Twitter data centers, they also implement a tight access and security policy and make sure that every employee has received security awareness training. Additionally, they have regional and local security operations centers that cover complete fleet of data centers. These SOCs continuously track local and worldwide events that can have an impact on how twitter's data centers operate and monitor alerts at all of our locations. To make sure they're always ready to respond to any crisis, the teams also conduct a strong enterprise risk management program in addition to routine testing to proactively identify and reduce

any hazards to the data centers. Twitter started providing phishing-resistant security keys to its staff and demanding that their teams utilize them as an additional security measure. With tremendous success, Twitter two step authentication is applied to place in 2017. All new hires at Twitter were obliged to complete security, privacy, and data protection trainings. In addition, mandatory training courses on how to avoid becoming phishing targets for attackers were required for those with access to non-public data. The business added that it has been enhancing its internal detection and monitoring capabilities, which warn it of potential unwanted access.

PERSONAL SECURITY:

The methods and best practices used to safeguard your privacy, data, and gadgets against unwanted access and harmful cyberattacks called personal security. The three pillars that make up personal security may come to mind:

i. Online Privacy
ii. Data protection
iii. Device Security

Online Privacy:

You may imagine that one of the key components of the most exquisite personal cybersecurity dessert is your online privacy. Hackers may ruin the credit history you worked so hard to earn if they gained access to details like credit card and banking information stored online. They might even sell this information to other cybercriminals on the dark web. Additionally, everyone should be aware of how to safeguard themselves against these cybersecurity threats given that almost 10 million people have their identities stolen annually.

Former or current workers, contractors, or business partners are the sources of insider threats. They might abuse their access or inside information to hurt our customers, employees, property, or reputation. The goal of personnel security is to lower the risks brought on by insider threats. Any person who intentionally or unintentionally undermines the security of their organization or New Zealand by engaging in espionage, terrorism, the unauthorized disclosure of information, or the loss or depletion of a resource is considered an "insider threat" or "insider" (or capability).

Common insider acts are:

Fraud or procedural corruption brought on by the unauthorized revelation of public, private, or proprietary information. Theft, assault, or physical harm to others. Unauthorized access to ICT systems. Economic or industrial espionage. Many security lapses are inadvertent and happen because people are unaware of or pay little attention

to security procedures, are preoccupied, or are tricked into unintentionally helping a third party.

Personal Security of Twitter:

Protects your account from phishing

Every day, Twitter stops more than 100 million phishing attempts. However, even the savviest users might be duped by sophisticated phishing techniques into providing their sign-in information to hackers. When using Advanced Protection, user must sign in to your Twitter Account using a security key to confirm your identity. Without your username and password, unauthorized users cannot sign in.

Provides extra protection from harmful Content:

Twitter's Safe Browsing shields 4 billion devices from dangerous links, while Advanced Protection does even more thorough checks before each Tweet. It alerts you to potentially hazardous files and may even stop you from accessing them.

Keeps your personal information secure

You are frequently prompted to grant access to your Twitter Account data, such as your contacts, location, or Gallery, when you join up for new apps or services ,instead of giving

all information Twitter ask the users which information they want to give to particular application for signup. Twitter Accounts have built-in security features that verify more than 40 million saved passwords daily for breaches. However, some attackers have the ability to pose as an authorized third party in order to access information.

Twitter provides these services to safeguard the personal security:

1: Never reveal your password to anyone!

No one from Twitter will ever request your password. To assist you, they don't require it.

2: Please review your privacy settings.

To control who can send you messages, access your Stories, or view your location on Map, check your privacy settings.

3: Pick a Secure Password

Don't use personal information in your password, such as your name, username, phone number, or birthdate, and choose a password that is at least 8 characters long. Your password should be a combination of numbers, symbols, capital, and lowercase letters. Don't divulge your password to anyone and refrain from using it on other websites or apps.

Verify both your email and phone number:

Check the Twitter settings to make sure the email address and mobile number linked to your account are correct.

Configure Two-Factor Authentication.

For added security, you can use two-factor authentication to confirm that you are the one logging into your Twitter account. This increases the security of your account.

OPERATION SECURITY:

WHAT IS OPERATION SECURITY?

Operational security (OPSEC) is a security and risk management procedure that guards against the unauthorized access to critical data. Another definition of OPSEC is a method for spotting seemingly innocent behaviors that can unintentionally give away sensitive information to a hacker. OPSEC encourages IT and security professionals to look at their operations and systems from the standpoint of a possible attacker. It is both a process and a strategy. It covers analytical tasks and procedures including social media and behavior monitoring as well as security best practices. The use of risk management to identify potential risks and weaknesses in business operations, operational procedures,

and the software and hardware that employees utilize is a vital component of OPSEC. OPSEC teams can identify problems they may have overlooked by viewing systems and operations from a different angle, which can be essential to putting the right countermeasures in place to protect their most sensitive data.

How OPSEC came into picture

During the Vietnam War, a U.S. military unit called Purple Dragon played a key role in the development of OPSEC. Without being able to decrypt their communications or have intelligence assets to steal their data, the U.S.'s opponents might predict the counterintelligence team's strategies and tactics. They came to the conclusion that the American military personnel were actually providing their adversary with information. The initial OPSEC definition was created by Purple Dragon, who stated that it was "the capacity to keep information of our strengths and weaknesses hidden from hostile forces." Other government organizations, including the Department of Defense, have now adopted this OPSEC procedure in their initiatives to safeguard trade secrets and national security.

Additionally, it aids businesses in addressing corporate espionage, information security, and risk management by helping them handle the need to protect consumer data.

OPERATION SECURITY IN TWITTER

Vulnerability management:

Through a combination of commercially available and custom-built internal tools, intense automated and manual penetration attempts, quality assurance procedures, software security reviews, and external audits, Twitter's vulnerability management methodology actively checks for security threats.

When a vulnerability that needs to be fixed is found, the vulnerability team logs it, assigns it to an owner, and prioritizes it based on severity. The staff monitors every issue and does repeated follow-ups until they can confirm that it has been resolved. In order to follow reported problems with Twitter services and open-source tools, Twitter also keeps in touch with the security research community and engages in frequent communication with them.

Malware prevention:

A successful malware attack may result in account breach, data theft, and potentially more network access. Twitter employs a range of techniques to prevent, detect, and get rid of malware because it takes these risks to its networks and users very seriously.

Malicious software is installed on users' computers via malicious websites or email attachments in order to steal personal data, commit identity theft, or attack other systems. These websites download hijacking software onto users' computers without their knowledge when they visit them. Twitter's anti-malware strategy starts with infection prevention by scouring its search index for websites that might be used as delivery systems for malware or phishing. Our attachment malware scanner, which scans more than 900 million Tweets a week to block malicious content, is another one of our major defenses. The 63% of harmful documents that we block change daily. We recently incorporated a new generation of document scanners that use deep learning to enhance our detection abilities in order to keep ahead of this continuously changing danger.

Twitter's Safe Browsing technology shields more than 100 million devices every day. Thousands of new hazardous links are found every day by Safe Browsing, many of which are genuine websites that have been compromised. We display alerts on Twitter's Search and in web browsers when we find hazardous sites.

Monitoring

The main sources of data for Twitter's security monitoring software include internal network traffic, user actions on systems, and external awareness of vulnerabilities. At many places in our global network, internal traffic is examined for suspicious activity,

such as the existence of traffic that could suggest connections to botnets, using a combination of open-source and for-profit technologies for traffic capture and parsing. By using a customized correlation system based on Twitter technology and by looking through system logs to spot odd behavior, such as attempts to access consumer data, we further this network analysis.

Twitter security engineers actively examine incoming security reports, keep an eye on public mailing lists, blogs, and wikis, and establish standing search alerts on public data repositories to seek for security issues that could harm the company's infrastructure. Automated system log analysis is used in conjunction with automated network analysis to identify potential unknown threats and escalate them to Twitter security staff.

Incident management:

A crucial component of Twitter's comprehensive security and privacy program is incident response. They have a strict procedure in place to handle data incidents. This procedure outlines actions, escalations, mitigation, resolution, and notification for any potential issues that may affect the privacy, accuracy, or accessibility of client data.

Teams of experienced incident responders from several specialized fields oversee Twitter's incident response program to make sure each response is properly targeted to the problems posed by each occurrence.

Teams of experienced incident responders from various specialized fields oversee Twitter's incident response program to make sure each response is properly tailored to the problems presented by each incident. These teams' subject-matter specialists participate in various ways. For instance, incident commanders evaluate the incident's nature and coordinate the incident response, which includes finishing the incident's triage assessment, modifying its severity as needed, and activating the necessary incident response team with the necessary operational/technical leads who review the facts and pinpoint key areas that need investigation. The digital forensics team detects ongoing attacks and conducts forensic investigations as part of the resolution process. Product engineers strive to minimize the negative effects on customers and offer fixes for the faulty product (s). The legal team interacts with law enforcement and government authorities, provides legal advice, and works with members of the relevant security and privacy team to implement Twitter's plan for evidence collecting. Support staff members monitor customer notifications and respond to customer questions, concerns, and requests for further information and support.

Communication Security:

The prevention of unwanted access to telecommunications traffic or to any written material that is transmitted or transferred is known as communications security (COMSEC). Its objective is to protect the transfer of classified and unclassified DoD

information that has not been authorized for public release while preserving its availability, secrecy, and integrity. It is utilized for analogue and digital applications, wired and wireless lines, and secures voice, video, and data transmission on military communications networks. COMSEC consists of:

- Crypto security
- Transmission Security (TRANSEC)
- Emission security
- Physical security of COMSEC material

Objectives of COMSEC

1: Information sent by the DOD must be safeguarded using COMSEC procedures.

2: The techniques that have been approved must be used for the development, acquisition, operation, maintenance, and disposal of COMSEC materials.

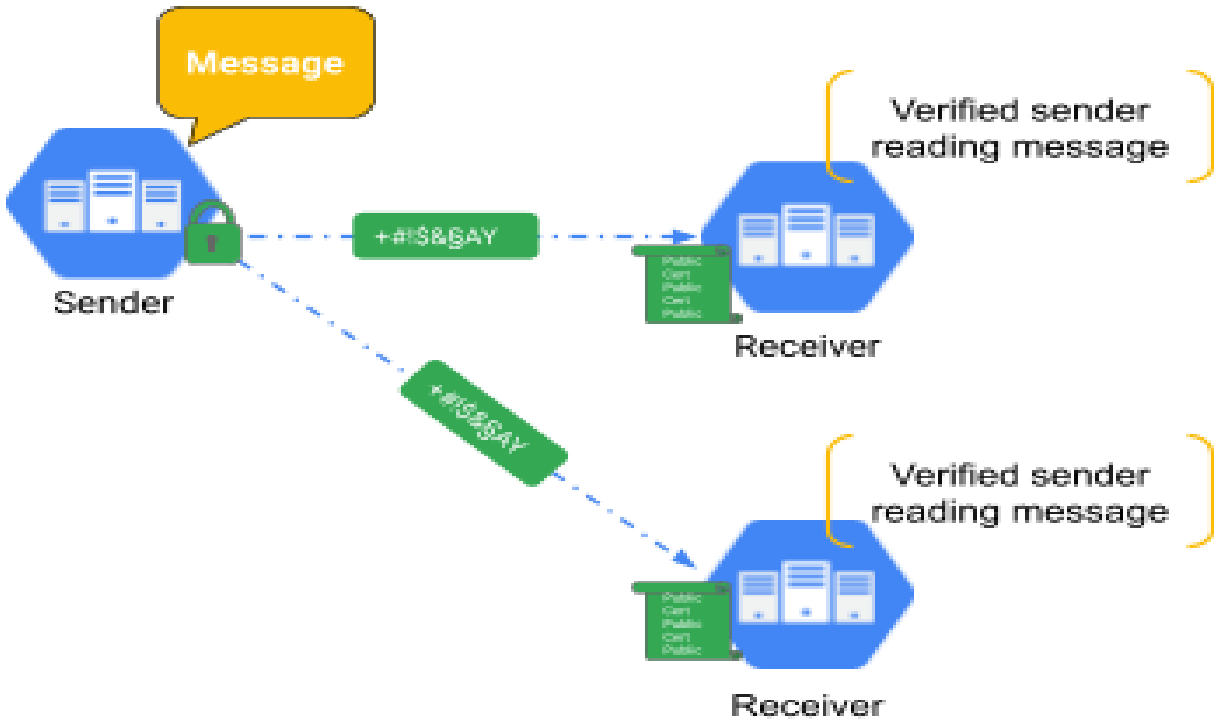
3: It is necessary to design and maintain a program to guarantee the operational readiness of frequently used COMSEC equipment during emergencies or disasters.

4: COMSEC hardware must be interoperable with key management systems that have received DOD approval. The COMSEC Material Control System (CMCS), a comparable

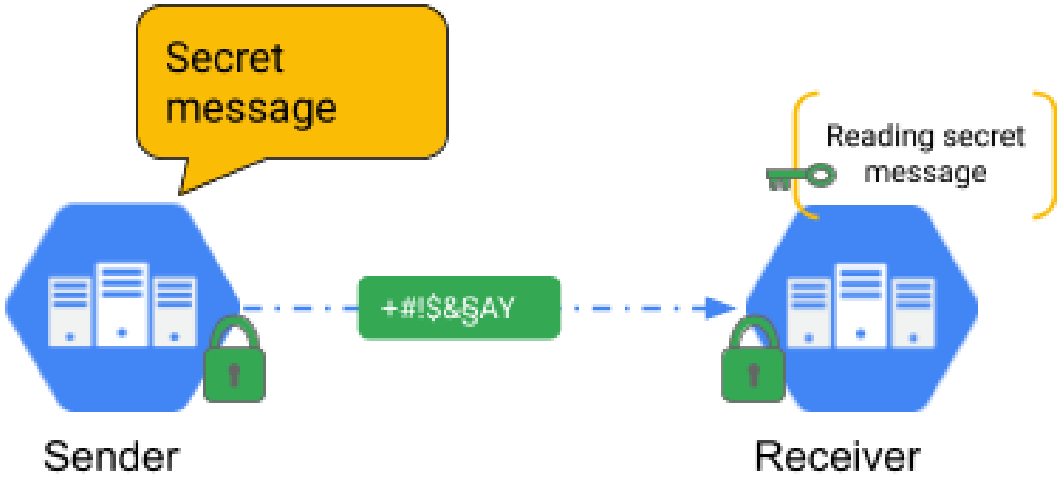
material control system, or a combination of the two must be used to track controlled cryptographic items (CCI) in a way that ensures responsibility and visibility.

COMSEC in Twitter:

Chat capabilities allow you to share files and high-resolution photographs, send messages over mobile data and Wi-Fi, see when someone is typing, and see when messages have been read. When you use chat features, the Rich Communication Service (RCS) protocol, a carrier communications industry standard, is used to send your messages. Everyone involved in a conversation must have chat features enabled before messages can be sent via RCS. If not, SMS or MMS can be used to send messages. Chat services may be offered by your RCS service provider, such as your cell carrier, or Jibe Mobile from Twitter.



One to One Messages:



Network Security

Network security is essential for safeguarding client data and information, maintaining the security of shared data, guaranteeing dependable network performance, and protecting against online threats. An effective network security solution lowers overhead costs and protects businesses from significant losses brought on by a data breach or other security incident. Ensuring appropriate access to systems, applications, and data facilitates company operations and customer service.

How does network security work?

When addressing network security across an enterprise, there are numerous layers to take into account. The network security layers concept allows for attacks to occur at any

tier, thus your network security hardware, software, and rules must be developed to target each area. Physical, technical, and administrative measures are commonly used to secure networks. The various methods of network security and how each control operates are briefly described below.

Physical Network Security:

Physical security measures are intended to keep unauthorized employees from physically accessing network equipment like routers and cable cabinets. In any organization, controlled access via locks, biometric authentication, and other technologies is crucial.

Technical Network Security:

Data that is stored on the network or that is in transit across, into, or out of the network is protected by technical security mechanisms. Data and systems must be protected from unauthorized persons as well as from malevolent employee behavior. Protection is required on both fronts.

Administrative Network Security:

Security procedures and rules that regulate user behavior, such as how users are verified, what level of access they have, and how IT staff members update the infrastructure, make up administrative security controls.

Network Security of Twitter:

Twitter Cloud has enhanced its Private Service Connect product, which connects groups, projects, and other organizations over encrypted links, on the networking front. PSC now has routing, telemetry, and security based on Layer 7 to guarantee uniform policy control throughout the service. According to Sambi, it also supports connecting on-premises sites to other PSC endpoints via Twitter Cloud's highly available, low-latency connection service, Cloud Interconnect. Confluent, Data bricks, DataStax, Grafana, and Neo4J all offer managed data and analytical services that are integrated with PSC. According to Sambi, PSC prevents customer network traffic from accessing the open internet by routing it only through Twitter's backbone network. Customers use PSC endpoints with private IP addresses on Twitter Virtual Private Cloud (VPC) networks to connect to Twitter Cloud. Twitter has expanded its centralized Network Intelligence Center to include network management. The platform's Network Analyzer, which learns and keeps track of customer networks to find errors and alterations in network topology, firewall rules, routes, load balancers, and connectivity to services and applications, the business claimed, is now available. Performance Dashboard, one of the new features of Network Intelligence Center, offers visibility into latency measures for Twitter Cloud-to-internet traffic at the project and global levels. According to Sambi, this aids in the planning of the overall network architecture and the placement of customer Twitter Cloud resources. Cloud Firewall Essentials and Cloud Firewall Standard, two tiers of the company's Cloud Firewall service, were on display.

Expanded policy objects for firewall rules are provided by Cloud Firewall Standard, which is intended to make configuration and micro-segmentation easier. The new entry-level firewall capability is called Cloud Firewall Essentials. It has built-in IAM [identification and access management] controls that can be applied across VPCs and supports batch-rule updates. It also has global and regional network firewall policies. Scalable micro-segmentation policies that follow workloads wherever they are placed are made possible by new IAM-governed Tags.

Information Security:

The methods and techniques that businesses employ to safeguard information are referred to as information security (or InfoSec). This includes setting up security measures to prohibit unauthorized users from accessing sensitive data. Network and infrastructure security, testing, and auditing are just a few of the many topics covered by the expanding and changing field of information security (InfoSec). Sensitive data is protected by information security from unauthorized actions such as inspection, modification, recording, interruption, or destruction. The objective is to guarantee the security and privacy of sensitive data, including financial information, intellectual property, and account information for customers. Data loss, data manipulation, and

theft of confidential information are all effects of security events. Attacks can cause delays in business operations, harm a company's reputation, and cost money. Organizations need to set aside money for security and make sure they are prepared to stop attacks like phishing, malware, viruses, malicious insiders, and ransomware in their tracks.

Three Principals of InfoSec

Confidentiality:

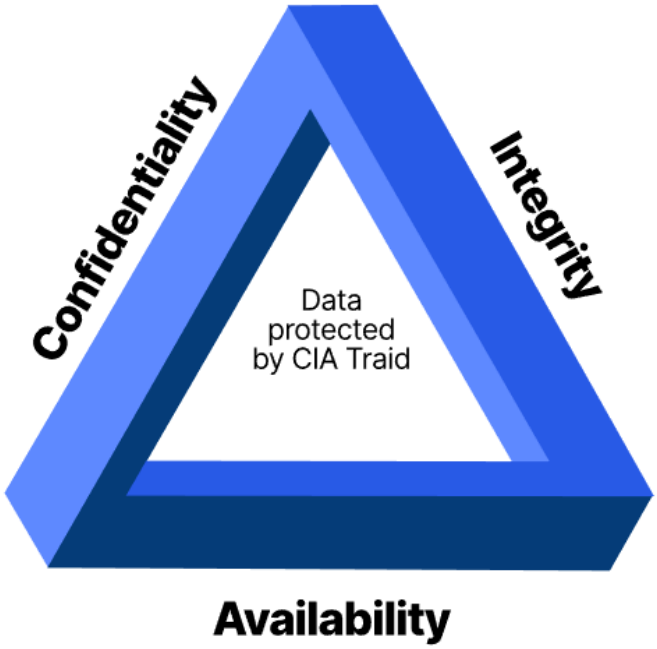
Measures to maintain confidentiality are intended to stop unlawful information dissemination. The confidentiality principle's goals are to maintain the privacy of personal information and guarantee that only the people who require it to carry out their organizational duties can see it and access it.

Integrity:

Protection from unwanted data changes (additions, deletions, revisions, etc.) is a component of consistency. The integrity principle guarantees that data is accurate and trustworthy and is not improperly manipulated, whether intentionally or unintentionally.

Availability:

The protection of a system's capacity to make data and software completely accessible when a user needs them is known as availability. The goal of availability is to make the technological foundation, the applications, and the data accessible when they are required by a business process or by its clients.



Information Security in Twitter:

While in transit, encryption keeps data private and secure. Twitter services are more secure and private thanks to encryption. The data user generate moves between user device, Twitter services, and Twitter's data centers. When user send tweet, share videos, browse the web, or store photos. We use multiple security layers to protect this data, including cutting-edge encryption methods like HTTPS and Transport Layer Security.

If we notice anything that we believe you should be aware of, such as a strange login or a harmful website, file, or program, Twitter will alert you right away. They'll also provide you advice on how to improve your security.

For instance, on Twitter it will alert you if someone signs into your account from a device that isn't connected to you or before you download an attachment that might compromise your security. You may secure your account with just one click by receiving a notification when we find something suspect in your account in your inbox or on your phone. Ads that include malware, block the content you are attempting to see, advertise phony goods, or otherwise violate our advertising policy may have an adverse effect on your online experience and risk your security, we treat this issue seriously.

Through a combination of real reviewers and advanced automation, we successfully block billions of undesirable ads annually - approximately 100 each second. We also provide you with the means to block certain types of adverts and report objectionable ones. And we actively share our knowledge and best practices to help everyone use the internet safely. We run one of the most secure and dependable cloud infrastructures in the world, with everything from private undersea cables that carry data between continents to custom-designed data centers. It is constantly watched over to keep your data safe and accessible.

Additionally, platform services can be automatically and instantaneously switched from one facility to another in the case of a disturbance, allowing them to continue uninterrupted. Online accounts

offer useful, customized services, but logging in to them also poses the biggest security risk in existence right now. Every day, data breaches reveal millions of passwords, putting your personal information at danger. You can quickly and securely sign in to the apps and services you love with the help of our built-in authentication tools and services.

Security and Risk Management

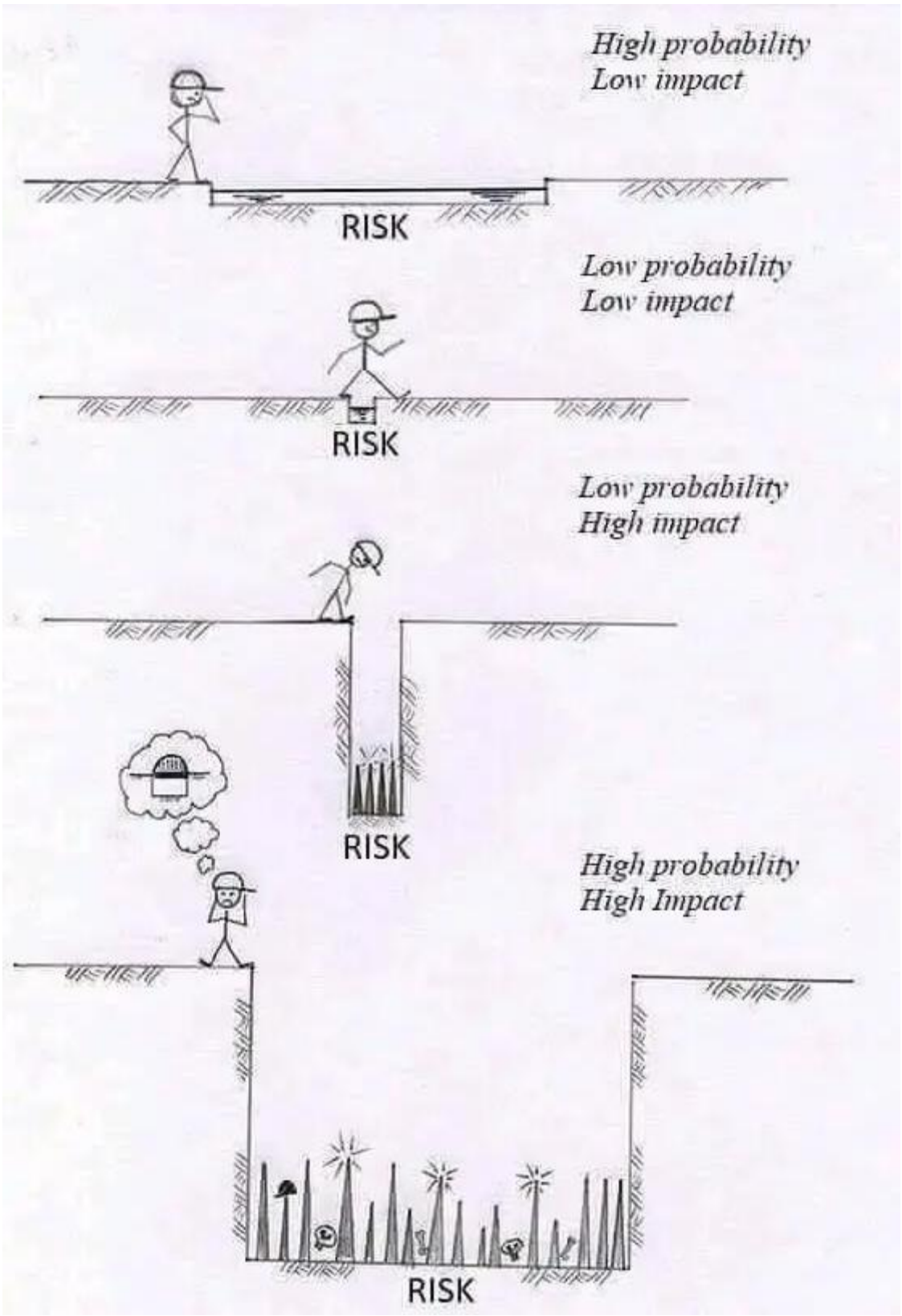
To reduce misconfigurations, reduce risk, and improve security readiness, Twitter's Risk Manager Tool scans your workloads on Twitter Cloud and offers proactive security recommendations. Risk Manager generates a report that serves as an indicator of your security baseline and assists you in continuously understanding your security risk posture so you can decide where to direct your security investments. Obtain a Risk Manager report with identified risks against the CIS Benchmark, which is the industry standard. The report can be sent directly from the UI to the insurance companies Allianz Global Corporate & Specialty (AGCS) and Munich Re in order to ascertain their underwriting eligibility for Cloud Protection +, a cyber-insurance plan created just for users of Twitter Cloud.

How to manage risks on Twitter?

1 Understand what information they have on you.

2 Do not use Facebook to sign into other accounts

3 Avoid the suspicious link


High probability
Low impact
RISK
Low probability
Low impact
RISK
Low probability
High impact
RISK
High probability
High Impact
RISK

Security Architecture

Security architecture is a comprehensive security design that takes into account both the requirements and potential hazards present in a certain situation or environment. Additionally, it details where and when to implement security controls. In general, the design process is repeatable. Clear design principles are reported in security architecture, and detailed security control specifications are typically recorded in separate documents. A design that includes a structure and addresses the connection between its components is referred to as system architecture.

- Risk management
- Benchmarking and good practice
- Financial
- Legal and regulatory

Twitter uses the widely used SHA-256 secure hashing algorithm, which is a standard in fields like online banking. Twitter uses a secure way which is called Hashing, A "hashing algorithm" is a one-way mathematical operation that yields a text's non-reversible, fixed-length fingerprint. The "message digest"—basically a fingerprint of the original data—is always produced when the same hashing technique is applied to a text string. It is not possible to reverse this fingerprint back to its original value using any mathematical operation or "key."

Every Twitter user's "hash" values are already calculated by Twitter. Your list of hashes is compared to previously computed hashes when your data is sent to the servers. The Twitter user is added to a custom audience that is kept in advertisements account if a matching hash is discovered. They just disregard a specified hash if there is no match for it. Twitter is aware that you wish to target the users who have been matched with advertising, but it is unaware of your relationship with these users (such as whether they are prospects or customers).