Cybersecurity

Keeping safe in the digital world

BWAMBALE JORAM

MSC. CYBERSECURITY

Objectives

This aims to provide a comprehensive understanding of cybersecurity, its importance, and practical tips for staying safe online.

explore the need for online safety in everyday digital interactions.

What is Cybersecurity

Cybersecurity is the ongoing effort to protect individuals, organizations, and governments from digital attacks by protecting networked systems and data from unauthorized use or harm.

- ***Personal:*** *safeguard your identity, your data, and your computing devices.*
- ***Organizational:*** *protect the organization's reputation, data, and customers.*
- ***Government:*** *national security, economic stability, and the safety and wellbeing of citizens are at stake.*

1.1 Personal Data

Protecting Your Personal Data

Personal data is any information that can be used to identify you, and it can exist both offline and online.

Offline identity

As a result, family and friends know details about your personal life, including your full name, age, and address.

Online identity

Username, social identity, online presence

You should take care to limit the amount of personal information you reveal through your online identity.

Consider the impact of sharing personal details on social media platforms among Ugandan youth, emphasizing the risks of identity theft and scams.

Your Data

- Personal data describes any information about you (name, social security number, driver's license number, date and place of birth, your mother’s maiden name, pictures, or messages exchanged with others).
- Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy, and potentially causing serious damage to your reputation.
- ***Hackers can get their hands on your personal data through records including:***
- Medical, educational, employment and financial records.

Where Is Your Data?

- Imagine that yesterday you shared a couple of photos of your first day on the job with a few of your close friends. But that should be OK, right? Let's see…

- You took some photos at work on your mobile phone.
- Copies of these photos are now available on your mobile device.
- You shared these with five close friends, who live in various locations across the world.
- All of your friends downloaded the photos and now have copies of your photos on their devices.
- One of your friends was so proud that they decided to post and share your photos online.
- The photos are no longer just on your device.
- They have in fact ended up on servers located in different parts of the world and people whom you don't even know now have access to your photos.

What's More?

- This is just one example that reminds us that every time we collect or share personal data, we should consider our security.
- There are different laws that protect your privacy and data in your country.
- **Do you know where your data is?**
  - Following an appointment, the doctor will update your medical record.
    - For billing purposes, this information may be shared with the insurance company.
    - In such cases, your medical record, or part of it, is now accessible at the insurance company.
  - Store loyalty cards may be a convenient way to save money on your purchases.
    - However, the store is using this card to build a profile of your purchasing behavior, which it can then use to target you with special offers from its marketing partners.

Smart Devices

Consider how often you use your computing devices to access your personal data.

Unless you have chosen to receive paper statements, you probably access digital copies of bank account statements via your bank's website.

And when paying a bill, it's highly likely that you've transferred the required funds via a mobile banking app.

But besides allowing you to access your information, computing devices can now also generate information about you.

- Wearable technologies such as smartwatches and activity trackers collect your data for clinical research, patient health monitoring, and fitness and wellbeing tracking.

Identity Theft

- Not content with stealing your money for short-term financial gain, cybercriminals are invested in the long-term gain of identity theft.

- **Medical theft**
  - Rising medical costs have led to an increase in medical identity theft, with cybercriminals stealing medical insurance to use the benefits for themselves.
  - Where this happens, any medical procedures carried out in your name will then be saved in your medical records.

- **Banking**
  - Stealing private data can help cybercriminals access bank accounts, credit cards, social profiles, and other online accounts.
  - Armed with this information, an identity thief could file a fake tax return and collect the refund.
  - They could even take out loans in your name and ruin your credit rating (and your life as well).

Who Else Wants My Data?

- It's not just criminals who seek your personal data.
- The table describes other entities interested in your online identity and why.

Your Internet Service Provider	Your ISP tracks your online activity, and in some countries, they can sell this data to advertisers for a profit. In certain circumstances, ISPs may be legally required to share your information with government surveillance agencies or authorities.
Advertisers	Targeted advertising is part of the internet experience. Advertisers monitor and track your online activities such as shopping habits and personal preferences and send targeted ads your way.
Search engines and social media platforms	These platforms gather information about your gender, geolocation, phone number, and political and religious ideologies based on your search histories and online identity. This information is then sold to advertisers for a profit.
Websites you visit	Websites use cookies to track your activities to provide a more personalized experience. But this leaves a data trail that is linked to your online identity that can often end up in the hands of advertisers!

Protect yourself

- **Use Strong Passwords or PINs:**
  - Set a strong password or PIN to unlock your phone.
  - Avoid easily guessable passwords, such as "1234" or "password."
- **Enable Biometric Authentication:**
  - Use fingerprint or facial recognition if your phone supports these features.
- **Regular Software Updates:**
  - Keep your phone's operating system, apps, and security software up to date. Updates often include security patches

Protect yourself

- **Install Apps from Trusted Sources:**
  - Only download apps from official app stores like Google Play (Android) or the App Store (iOS).
- **Review App Permissions:**
  - Be cautious about granting unnecessary permissions to apps. Only provide the permissions they need to function.
- **Use a VPN (Virtual Private Network):**
  - Consider using a reputable VPN to encrypt your internet connection, especially when using public Wi-Fi networks.

Protect yourself

- **Beware of Phishing:**
  - Avoid clicking on suspicious links in emails, text messages, or social media. Verify the legitimacy of requests before providing personal information.
- **Secure Your Wi-Fi Connection:**
  - Set a strong password for your home Wi-Fi network to prevent unauthorized access.
- **Enable Two-Factor Authentication (2FA):**
  - Whenever possible, enable 2FA for your accounts to add an extra layer of security.

Protect yourself

- **Regularly Backup Your Data:**
  - Backup your phone's data regularly to protect against loss or ransomware attacks.
- **Be Mindful of Bluetooth and NFC:**
  - Disable Bluetooth and NFC when not in use to prevent unauthorized connections.
- **Review and Adjust Privacy Settings:**
  - Regularly check and adjust privacy settings on your apps and devices to control the information they collect.
- **Remote Wipe/Find My Phone Feature:**
  - Activate the remote wipe and "Find My Phone" features in case your phone is lost or stolen.

Protect yourself

- **Use a Reputable Antivirus App:**
  - Install a reliable antivirus app to help protect against malware and other security threats.
- **Educate Yourself:**
  - Stay informed about common cybersecurity threats and best practices for staying safe online.

1.2 Organizational Data

Types of Organizational Data

- **Traditional data** is typically generated and maintained by all organizations, big and small.

- It includes the following:
  - **Transactional data** such as details relating to buying and selling etc
  - **Intellectual property** such as patents, trademarks, and new product plans
  - **Financial data** such as income statements, balance sheets, and cash flow statements,

Types of Organizational Data (Cont.)

Internet of Things (IoT) and Big Data

- **IoT** is a large network of physical objects, such as sensors, software, and other equipment.
- All of these ‘things’ are connected to the Internet, with the ability to collect and share data.
- Data storage options are expanding through the cloud and virtualization.
- The emergence of IoT has led to exponential growth in data, creating a new area of interest in technology and business called 'Big Data.'

The Cube

CIA

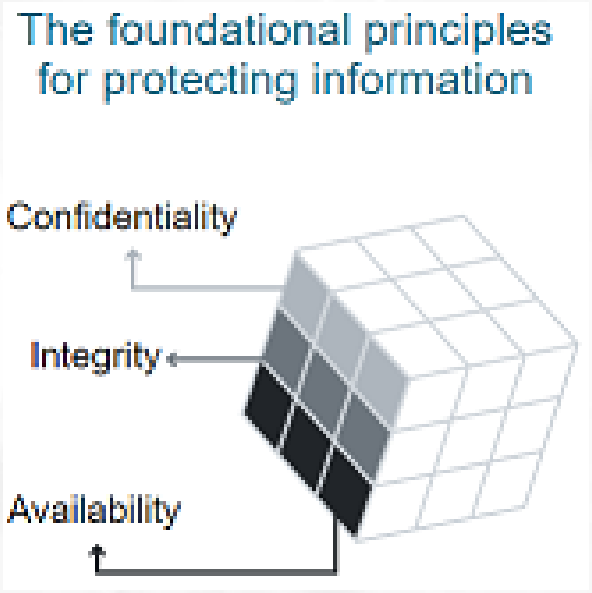
This security model has three dimensions:

1. **The foundational principles for protecting information systems**

   - **Confidentiality** is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources, and processes. Methods to ensure it includes **data encryption**, **identity proofing,** and **two factor authentication**.

   - **Integrity** ensures that system information or processes are protected from intentional or accidental modification. One way to ensure it is to use a **hash function** or **checksum**.

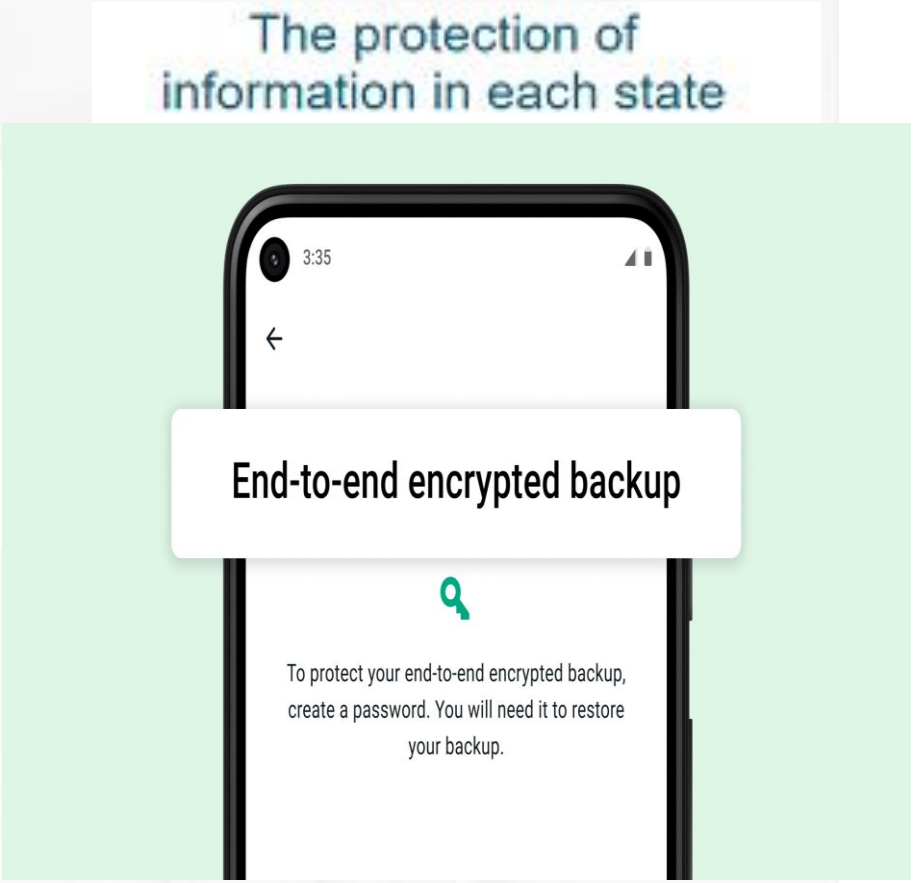
   - **Availability** means that authorized users are able to access systems and data when and where needed and those that do not meet established conditions, are not. This can be achieved by **maintaining equipment**, **performing hardware repairs**, **keeping operating systems and software up to date**, and **creating backups**.



The Cube (Cont.)

2. **The protection of information in each of its possible states**

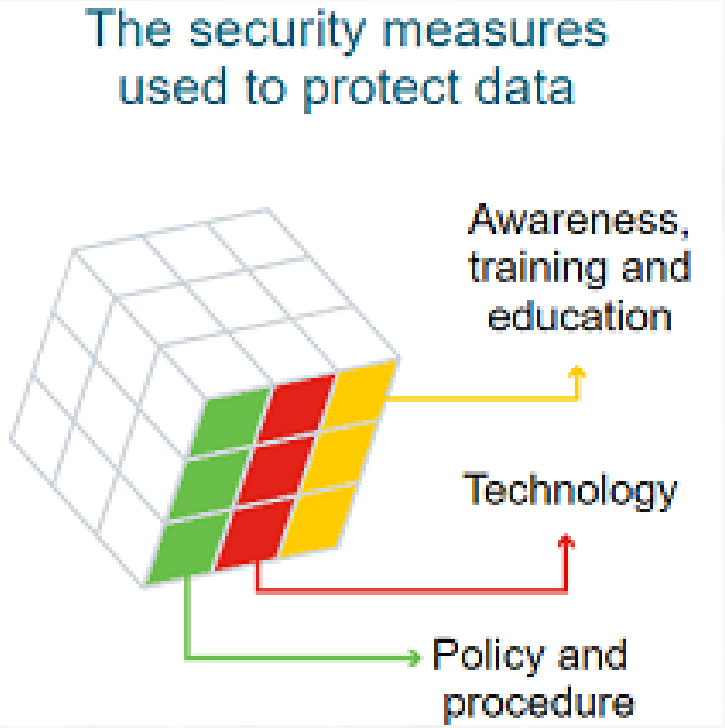
- **Processing** refers to data that is being used to perform an operation such as updating a database record (data in process).
- **Storage** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive, or USB drive (data at rest).
- **Transmission** refers to data traveling between information systems (data in transit).



The Cube (Cont.)

3. **The security measures used to protect data**

- **Awareness, training and education** are the measures put in place by an organization to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems.
- **Technology** refers to the software- and hardware-based solutions designed to protect information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents.
- **Policy and procedure** refers to the administrative controls that provide a foundation for how an organization implements information assurance, such as incident response plans and best practice guidelines.



Is This For Real?

- Phishing is very common and often works.
- For example, in August 2020, elite gaming brand Razer experienced a data breach which exposed the personal information of approximately 100,000 customers.
- A security consultant discovered that a cloud cluster (a group of linked servers providing data storage, databases, networking, and software through the Internet), was misconfigured and exposed a segment of Razer's infrastructure to the public Internet, resulting in a data leak.
- It took Razer more than three weeks to secure the cloud instance from public access, during which time cybercriminals had access to customer information that could have been used in social engineering and fraud attacks.
- Organizations, therefore, need to take a proactive approach to cloud security to ensure that sensitive data is secured.

Data Security Breaches

- Data security breaches are becoming all too common, and the implications are severe.
- The IoT is connecting more and more devices, creating more opportunities for cybercriminals to attack.
- Two well-known data security breaches include:

    - **The Persirai botnet**
        - In 2017, an Internet of Things (IoT) botnet, Persirai, targeted over 1,000 different models of IP cameras, accessing open ports to inject a command that forced the cameras to connect to a site which installed malware on them.
        - Once the malware was downloaded and executed, it deleted itself and was therefore able to run in memory to avoid detection.
        - Over 122,000 of these cameras from several different manufacturers were hijacked and used to carry out DDoS attacks, without the knowledge of their owners.
        - A DDoS attack occurs when multiple devices infected with malware flood the resources of a targeted system.

Data Security Breaches (Cont.)

- **Equifax Inc.**
  - In September 2017, Equifax, a consumer credit reporting agency in the US, publicly announced a data breach event: attackers had been able to exploit a vulnerability in its web application software to gain access to the sensitive personal data of millions of customers.
  - In response to this breach, Equifax established a dedicated website that allowed Equifax customers to determine if their information was compromised.
  - However, instead of using a subdomain of equifax.com, the company set up a new domain name, which allowed cybercriminals to create unauthorized websites with similar names.
  - These websites were used to try and trick customers into providing personal information.
  - Attackers could use this information to assume a customer's identity.
  - In such cases, it would be very difficult for the customer to prove otherwise, given that the hacker is also privy to their personal information.

1. **Marriott International (2018):**

   Marriott disclosed a data breach that exposed the personal information of up to 500 million guests. The breach involved unauthorized access to the Starwood guest reservation database.

2. **Capital One (2019):**

   Capital One experienced a data breach that affected approximately 100 million individuals. The breach involved the theft of personal information, including names, addresses, credit scores, and social security numbers.

3. **Target (2013):**

   Target suffered a significant data breach during the holiday shopping season, affecting about 40 million credit and debit card accounts. The breach was attributed to malware installed on point-of-sale systems.

Home Depot (2014):

Home Depot experienced a data breach that compromised payment card information of around 56 million customers. The breach resulted from a cyberattack on the company's point-of-sale registers.

eBay (2014):

1. eBay announced a data breach that affected approximately 145 million users. The breach involved unauthorized access to a database containing user information, including names, email addresses, and encrypted passwords.

Sony PlayStation Network (2011):

1. Sony's PlayStation Network suffered a data breach that exposed the personal information, including names, addresses, and login credentials, of millions of users.

Anthem (2015):

1. Anthem, one of the largest health insurance companies in the U.S., experienced a data breach that exposed the personal information of nearly 78.8 million individuals.

Consequences of a Security Breach

These examples show that the potential consequences of a security breach can be severe.

Reputational damage	A security breach can have a negative long-term impact on an organization's reputation that has taken years to build. Customers, particularly those who have been adversely affected by the breach, will need to be notified and may seek compensation and/or turn to a reliable and secure competitor. Employees may also choose to leave in light of a scandal. Depending on the severity of a breach, it can take a long time to repair an organization's reputation.
Vandalism	A hacker or hacking group may vandalize an organization's website by posting untrue information. They might even just make a few minor edits to your organization's phone number or address, which can be trickier to detect. In either case, online vandalism can portray unprofessionalism and have a negative impact on your organization's reputation and credibility.
Theft	A data breach often involves an incident where sensitive personal data has been stolen. Cybercriminals can make this information public or exploit it to steal an individual's money and/or identity.
Loss of revenue	The financial impact of a security breach can be devastating. For example, hackers can take down an organization's website, preventing it from doing business online. A loss of customer information may impede company growth and expansion. It may demand further investment in an organization's security infrastructure. And let's not forget that organizations may face large fines or penalties if they do not protect online data.
Damaged intellectual property	A security breach could also have a devastating impact on the competitiveness of an organization, particularly if hackers are able to get their hands on confidential documents, trade secrets and intellectual property.

1.3 What Was Taken?

Scenario 1

- Security breaches today are all too common, with attackers constantly finding new and innovative ways of infiltrating organizations in search of valuable information.
- Consider the following two fictional scenarios.

Scenario 1:

- According to our sources, a well-known hotel chain that operates across the world has reported a massive data breach, with the personal information of over three million guests exposed to hackers.
- The hotel discovered that hackers gained access to its customer database by using the login details of one of its employees.
- At this point, the hotel doesn’t believe that the hackers were able to access any account passwords or financial information.
- Recent guests are encouraged to check the hotel chain’s web portal to see if they have been impacted by this breach.

Scenario 2

Scenario 2:

- The team at @Apollo is concerned because eLearning platforms are becoming prime targets for attackers as more and more organizations make the move to digital learning.
- A popular online training platform admitted leaving the personal data of millions of its students (many of them minors) exposed on a publicly accessible cloud database.
- Hackers were able to directly access students' full names, email addresses, phone numbers, and school enrollment details from the Internet!
- While it's unclear what the hackers have done with this acquired information, it's safe to say that they have everything they need to carry out widespread phishing or malware attacks.

Key Takeaways

- A security breach is an incident that results in unauthorized access to data, applications, services or devices, exposing private information that attackers can use for financial gain or other advantages.
- There are many ways to protect yourself and your organization.
- It’s important to be aware of common cyber threats and remain vigilant so that you don’t become the next victim.

Find out More

Search for a few additional examples of recent security breaches.

- In each case, can you identify:
    - what was taken?
    - what exploits the attackers used?
    - what actions could be taken to prevent the breach from occurring again in the future?

1.4 Cyber Attackers

Types of Attackers

- Cyber attackers range from amateur to organized and will try anything to get their hands on personal information.
- They are often categorized as white hat, gray hat, or black hat attackers.

Amateur Hackers

- The term 'script kiddies' emerged in the 1990s and refers to amateur or inexperienced hackers who use existing tools or instructions found on the Internet to launch attacks.
- Some script kiddies are just curious, others are trying to demonstrate their skills and cause harm.

Types of Attackers (Cont.)

Hackers

- This group of attackers break into computer systems or networks to gain access.
- Depending on the intent of their break-in, they can be classified as the following:
  - **White hat attackers** break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done with prior permission and any results are reported back to the owner.
  - **Gray hat attackers** may set out to find vulnerabilities in a system, but they will only report their findings to the owners of a system if doing so coincides with their agenda. They might even publish details about the vulnerability on the internet so that other attackers can exploit it.
  - **Black hat attackers** take advantage of any vulnerability for illegal personal, financial, or political gain.

Types of Attackers (Cont.)

Organized Hackers

- These attackers include organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers.
- They are usually highly sophisticated and organized and may even provide cybercrime as a service to other criminals.
- Hacktivists make political statements to create awareness about issues that are important to them.
- State-sponsored attackers gather intelligence or commit sabotage on behalf of their government.
- They are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.

Internal and External Threats

- Cyber attacks can originate from within an organization as well as from outside of it.

- **Internal**
  - Employees, contract staff, or trusted partners can accidentally or intentionally:
    - mishandle confidential data
    - facilitate outside attacks by connecting infected USB media into the organization's computer system
    - invite malware onto the organization's network by clicking on malicious emails or websites
    - threaten the operations of internal servers or network infrastructure devices

- **External**
  - Amateurs or skilled attackers outside of the organization can:
    - exploit vulnerabilities in the network
    - gain unauthorized access to computing devices
    - use social engineering to gain unauthorized access to organizational data

1.5 Cyberwarfare

Sign of the times (Stuxnet)

- One example of a state-sponsored attack involved the Stuxnet malware that was designed not just to hijack targeted computers but to actually cause physical damage to equipment controlled by computers!

- Watch a short video on the case of Stuxnet and discover the impact this malware had on Iran’s nuclear enrichment plant.

The Purpose of Cyberwarfare

- The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.
- Cyberwarfare is used in the following ways:

- **To gather compromised information and/or defense secrets**
  - A nation or international organization can engage in cyberwarfare to steal defense secrets and gather information about technology that will help narrow the gaps in its industries and military capabilities.
  - Furthermore, compromised sensitive data can give attackers leverage to blackmail personnel within a foreign government.

The Purpose of Cyberwarfare (Cont.)

- **To impact another nation's infrastructure**
  - Besides industrial and military espionage, a nation can continuously invade another nation's infrastructure to cause disruption and chaos.
  - For example, a cyber attack could shut down the power grid of a major city.
  - Consider the consequences if this were to happen; roads would be congested, the exchange of goods and services would be halted, patients would not be able to get the care they would need if an emergency occurred, access to the internet would be interrupted.
  - By shutting down a power grid, a cyber attack could have a huge impact on the everyday life of ordinary citizens.

Thank you