

Cybersecurity Introduction





Introduction

Introduction



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.

Introduction



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.



On a personal level, you need to safeguard your identity, your data, and your computing devices.

Introduction



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.



At an organizational level, it is everyone's responsibility to protect the organization's reputation, data and customers.

Introduction



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.



As more digital information is being gathered and shared, its protection becomes even more vital at the government level, where national security, economic stability and the safety and wellbeing of citizens are at stake.

Data Protection



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

What is the difference between your offline and online identity.





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

What is the difference between your offline and online identity.



Your offline identity is the real-life person that you present in daily basis at home, at school or at work. As a result, family and friends know details about your personal life, including your full name, your age and address. It's important to overlook the importance of securing your offline identity. Identity thieves can easily steal your data from right under your nose when you are not looking.



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

What is the difference between your offline and online identity.



Your online identity is not just a name. It's who you are and how you present yourself to others online. It includes the username or alias you use for your online accounts, as well as the social identity you establish and portray on online communities and websites.

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



Many people think that if they don't have any social media or online accounts set up, then they don't have an online identity. This is not the case. If you use the web, you have an online identity.



It's your first day on the job, and it's time to choose a username for your online identity. Which of the following options would you choose?

- A. Mouaad.Mohy**
- B. M.Moh12**
- C. MMohy.IT**
- D. MMoh**
- E. MMohy1990**

Your Data

Your Data



Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends. Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.

Your Data



Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends. Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.



Medical records

Every time you visit the doctor, personal information regarding your physical and mental health and wellbeing is added to your electronic health records (EHRs). Since the majority of these records are saved online, you need to be aware of the medical information that you share.

And these records go beyond the bounds of the doctor's office. For example, many fitness trackers collect large amounts of clinical data such as your heart rate, blood pressure and blood sugar levels, which is transferred, stored and displayed via the cloud. Therefore, you should consider this data to be part of your medical records.

Your Data



Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends. Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.



Education records

Educational records contain information about your academic qualifications and achievements. However, these records may also include your contact information, attendance records, disciplinary reports, health and immunization records as well as any special education records including individualized education programs (IEPs).

Your Data



Personal data describes any information about you, including your name, social security number, driver license number, date and place of birth, your mother's maiden name, and even pictures or messages that you exchange with family and friends. Cybercriminals can use this sensitive information to identify and impersonate you, infringing on your privacy and potentially causing serious damage to your reputation.



Employment and financial records

Employment data can be valuable to hackers if they can gather information on your past employment, or even your current performance reviews.

Your financial records may include information about your income and expenditure. Your tax records may include paychecks, credit card statements, your credit rating and your bank account details. All of this data, if not safeguarded properly, can compromise your privacy and enable cybercriminals to use your information for their own gain.

**Where is
Your Data?**

Where is Your Data?



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

Where is Your Data?



Only yesterday, you shared a couple of photos of your first day on school 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.

Where is Your Data?



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

You shared these with five close friends, who live in various locations across the world.



Where is Your Data?



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



All of your friends downloaded the photos and now have copies of your photos on their devices.

Where is Your Data?



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

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.



There is
more ...

There is 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. But do you know where your data is?

Here are more examples which may not be so obvious.

There is 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. But do you know where your data is?

Here are more examples which may not be so obvious.



There is 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. But do you know where your data is?

Here are more examples which may not be so obvious.



Following an appointment, the doctor will update your medical record. For billing purposes, this information may be shared with the insurance company. In such case, your medical record, or part of it, is now accessible at the insurance company.

There is 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. But do you know where your data is?

Here are more examples which may not be so obvious.

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 behaviour, 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. As the global fitness tracker market grows, so also does the risk to your personal data.





It might seem that information available online is free. But is privacy the price we pay for this digital convenience?

For example, social media companies generate the majority of their income by selling targeted advertising based on customer data that has been mined using algorithms or formulas. Of course, these companies will argue that they are not 'selling' customer data, but 'sharing' customer data with their marketing partners.

**What Do
Hackers
Want?**

What Do Hackers Want?



So, with all this information about you available online, what do hackers want?

What Do Hackers Want?



Cybercriminals are certainly very imaginative when it comes to gaining access to your money. But that's not all they are after — they could also steal your identity and ruin your life.

Identity Theft



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

Identity Theft



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



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.

Identity Theft



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

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.

Who Else Wants My Data?



It's not just criminals who seek your personal data.

Your Internet Service Provider (ISP).

Advertisers.

Search engine and social media platforms.

Websites you visit.

Who Else Wants My Data?



It's not just criminals who seek your personal data.

Your Internet Service Provider (ISP).

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.

Search engine and social media platforms.

Websites you visit.

Who Else Wants My Data?



It's not just criminals who seek your personal data.

Your Internet Service Provider (ISP).

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 engine and social media platforms.

Websites you visit.

Who Else Wants My Data?



It's not just criminals who seek your personal data.

Your Internet Service Provider (ISP).

Advertisers.

Search engine 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.

Who Else Wants My Data?



It's not just criminals who seek your personal data.

Your Internet Service Provider (ISP).

Advertisers.

Search engine and social media platforms.

Websites you visit.

Websites use cookies to track your activities in order 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!

Organizational Data



It's obvious that cybercriminals are becoming more sophisticated in their pursuit of valuable personal data. But they also pose a huge threat to organizational data.



Traditional 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, production activities and basic organizational operations such as any information used to make employment decisions.
- **Intellectual property** such as patents, trademarks and new product plans, which allows an organization to gain economic advantage over its competitors. This information is often considered a trade secret and losing it could prove disastrous for the future of a company.
- **Financial data** such as income statements, balance sheets and cash flow statements, which provide insight into the health of a company.





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. And given that storage options are expanding through the cloud and virtualization, it's no surprise that the emergence of IoT has led to an exponential growth in data, creating a new area of interest in technology and business called 'Big Data.'



The Cube



The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security initiatives by considering all of the related factors that impact them. This security model has three dimensions:

- 1.The foundational principles for protecting information systems.
- 2.The protection of information in each of its possible states.
- 3.The security measures used to protect data.

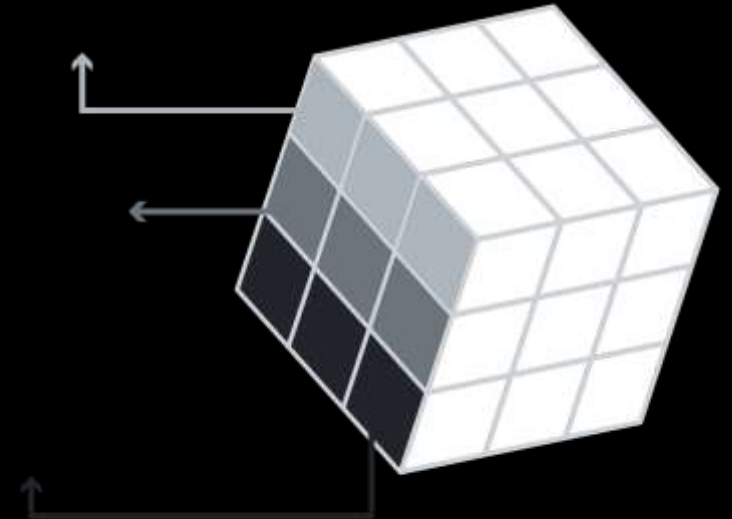
The Cube



The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security initiatives by considering all of the related factors that impact them. This security model has three dimensions:

- 1.The foundational principles for protecting information systems.
- 2.The protection of information in each of its possible states.
- 3.The security measures used to protect data.

The foundational principles
for protecting information

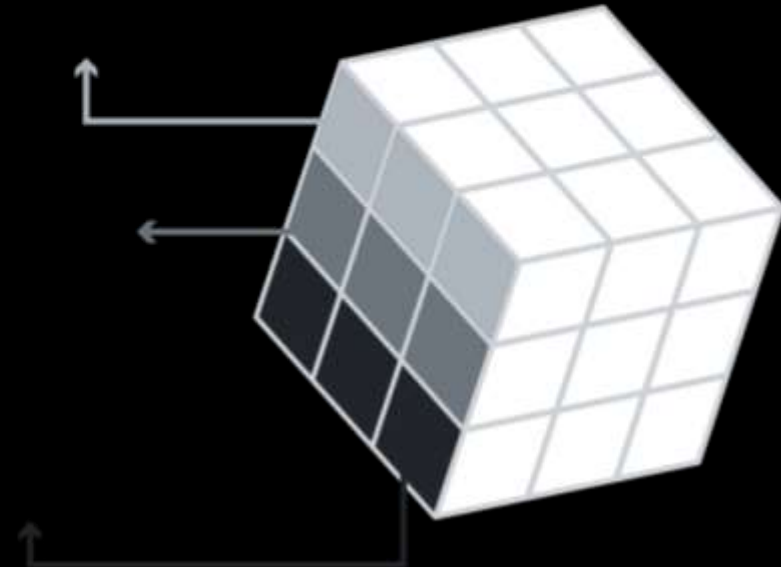


The Cube



- **Confidentiality** is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include **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 integrity 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 foundational principles
for protecting information

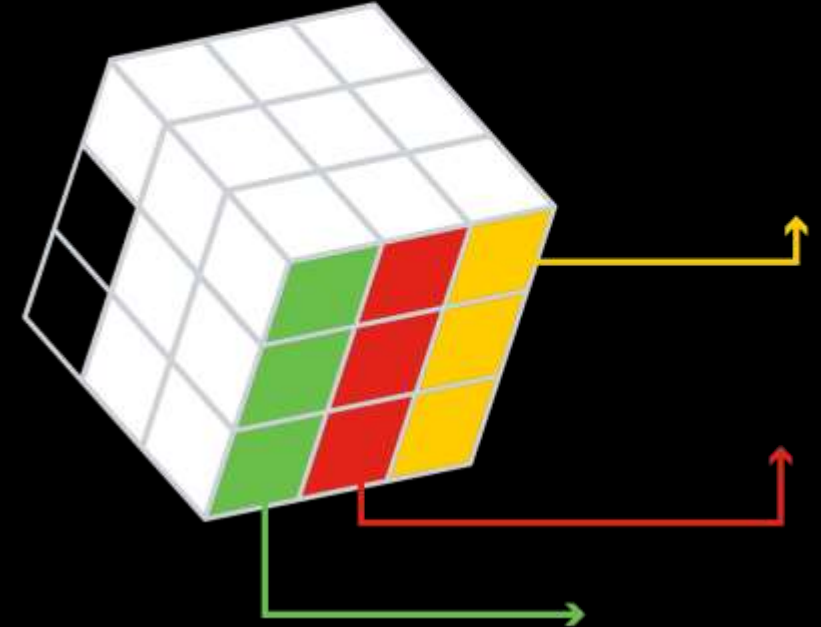


The Cube



- **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.

The security measures
used to protect data

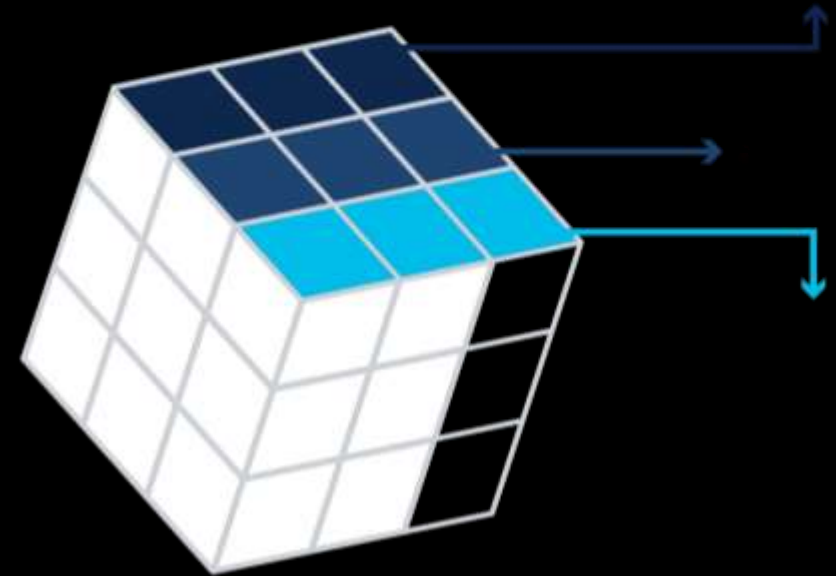


The Cube



The protection of
information in each state

- **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).



What do you think?



A concerned customer has forwarded on what they believe to be a fraudulent email. It looks as if it has been sent by @Apollo but something appears a little 'phish-y.'

What do you think?



A concerned customer has forwarded on what they believe to be a fraudulent email. It looks as if it has been sent by @Apollo but something appears a little 'phish-y.'

Security Notice



POLLO <service@@polo.com>

Tue 01/02/2021 14:00

To: You



Dear Ms Patel

As a precautionary measure we restricted access to your Account until you validate has been changed. To prevent further irregular activity, you will be unable to access your account until this issue has been resolved

To fix security info, click below to reactivate your account.

<http://123contactform.com/contact-form-@apollo.234.54674.html>


@pollo Support Team


What do you think?



Which of the following indicates that it is in fact a phishing email?

Security Notice

 POLLO <service@@polo.com>
Tue 01/02/2021 14:00
To: You



Dear Ms Patel

As a precautionary measure we restricted access to your Account until you validate has been changed. To prevent further irregular activity, you will be unable to access your account until this issue has been resolved

To fix security info, click below to reactivate your account.
<http://123contactform.com/contact-form-@apollo.234.54674.html>

@pollo Support Team

1. Link URL
2. Customer Name
3. Graphics
4. The language, spelling and grammar
5. Email address

Data Security Breaches

Data Security Breaches



The implications of a data security breach are severe, but they are becoming all too common.

Data Security Breaches



The implications of a data security breach are severe, but they are becoming all too common.



EQUIFAX®



The implications of a data security breach are severe, but they are becoming all too common.



The Persirai Botnet

In 2017, an Internet of Things (IoT) botnet, Persirai, targeted over 1,000 different models of Internet Protocol (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 distributed denial-of-service (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.

The IoT is connecting more and more devices, creating more opportunities for cybercriminals to attack.

Data Security Breaches



The implications of a data security breach are severe, but they are becoming all too common.

Equifax Inc.

In September 2017, Equifax, a consumer credit reporting agency in the United States, 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.

The Equifax logo, featuring the word "EQUIFAX" in a bold, white, sans-serif font with a registered trademark symbol (®) to the upper right. The logo is set against a solid blue rectangular background.

Consequences of Security Breach



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

Reputational damage.

Vandalism.

Theft.

Loss of revenue.

Damaged intellectual property.

Consequences of 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.

Theft.

Loss of revenue.

Damaged intellectual property.

Consequences of Security Breach



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

Reputational damage.

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.

Loss of revenue.

Damaged intellectual property.

Consequences of Security Breach



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

Reputational damage.

Vandalism.

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.

Damaged intellectual property.

Consequences of Security Breach



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

Reputational damage.

Vandalism.

Theft.

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.

Consequences of Security Breach



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

Reputational damage.

Vandalism.

Theft.

Loss of revenue.

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.

Consequences of Security Breach



Despite the best of intentions and all the safeguards you can put in place, protecting organizations from every cyberattack is not feasible.

Cybercriminals are constantly finding new ways to attack and, eventually, they will succeed.

When they do, it will be up to cybersecurity professionals, like you, to respond quickly to minimize its impact.



Security breaches can have devastating consequences for an organization. Therefore, it is crucial to take appropriate steps and implement measures to protect against cyber attacks.