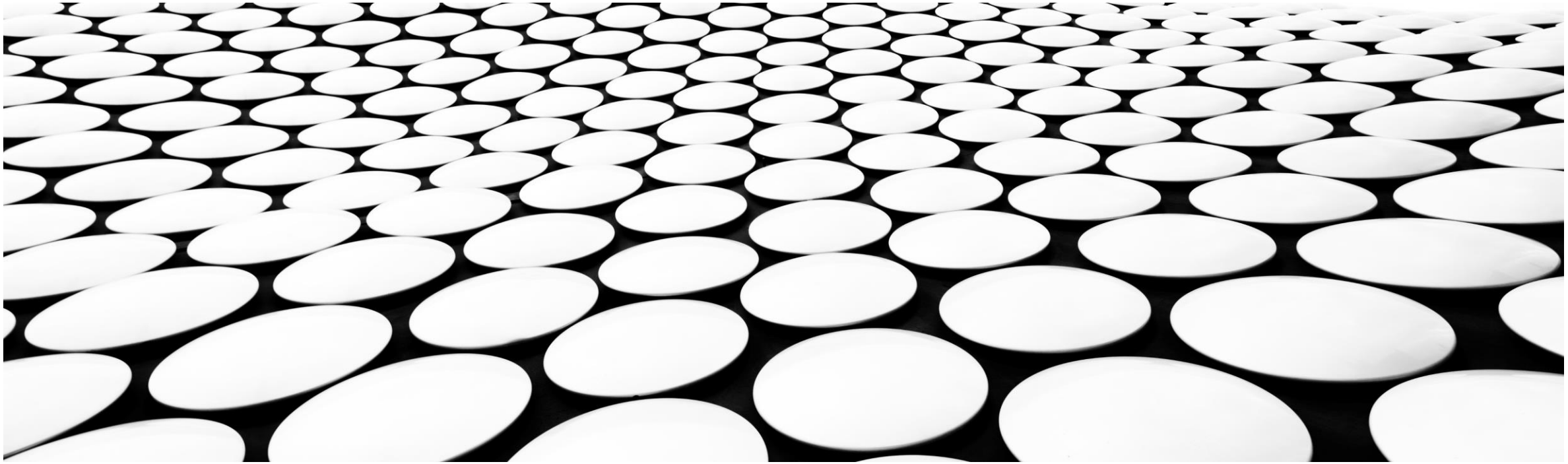
CYBERSECURITY ESSENTIALS

MOHAMMED FADHIL MAHDI



MODULE
INTRODUCTION TO CYBERSECURITY

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.
Select the pin icons to find out more about the three levels of protection.

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

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

Government
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.

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

Your offline identity is the real-life persona that you present on a 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, age and address.

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.

PROTECTING YOUR PERSONAL DATA

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.

Your Online Identity

That's not quite right.

When choosing a username, it's important not to reveal any personal information.

Some other useful tips to help you generate your username:

- Don't use your full name or parts of your address or phone number.
- Don't use your email username.
- Don't use the same username and password combination, especially on financial accounts.
- Don't choose a super-odd username and then reuse it again and again — it makes you easier to track.
- Don't choose a username that gives clues to your passwords such as a series of numbers/letters, the first part of a two-part phrase, such as knock-knock or starlight, or the department in which you work, such as IT.
- Do choose a username that's appropriate for the type of account, i.e., business, social or personal.

Go back, reset and have another try.

YOUR DATA

Image with selectable areas. Select each button to show more information.
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

Education records

Employment and financial records

WHERE IS YOUR DATA?

This has got you thinking. Only 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.

This is just one example that reminds us that every time we collect or share personal data, we should consider our security.

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.

WHO ELSE WANTS MY DATA?

It’s not just criminals who seek your personal data.
Select the headings below to find out what other entities are interested in your online identity and why.

- ❑ **Your Internet service provider (ISP)**
- ❑ **Advertisers**
- ❑ **Search engines and social media platforms**
- ❑ **Websites you visit**

TYPES OF 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.

TYPES OF ORGANIZATIONAL DATA

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

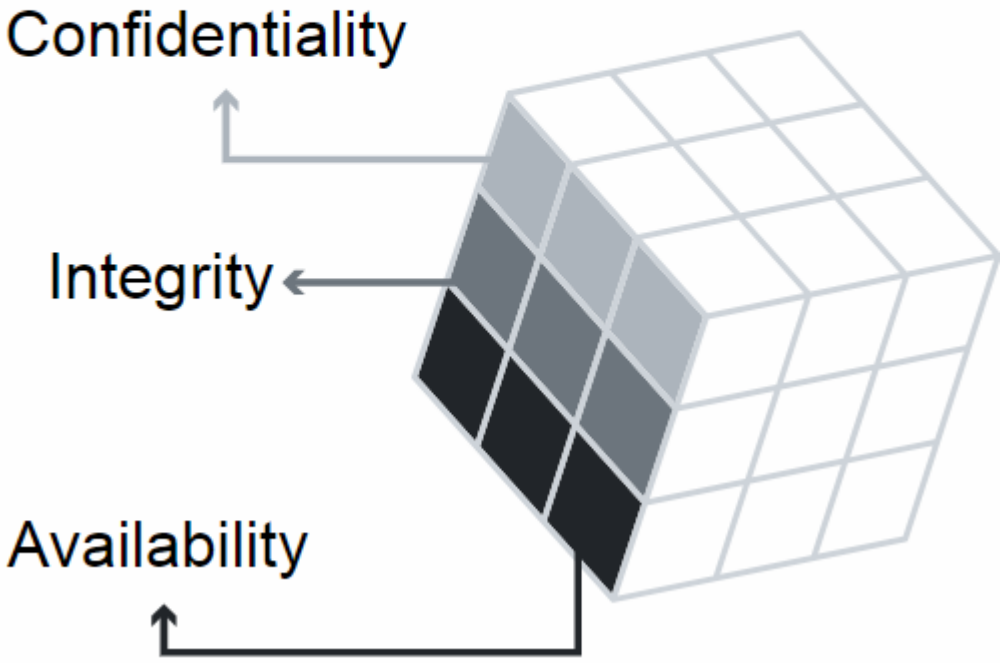
The McCumber Cube is a model framework created by John McCumber in 1991 to help organizations establish and evaluate information security initiatives by considering all of the related factors that impact them. This security model has three dimensions:

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 foundational principles for protecting information

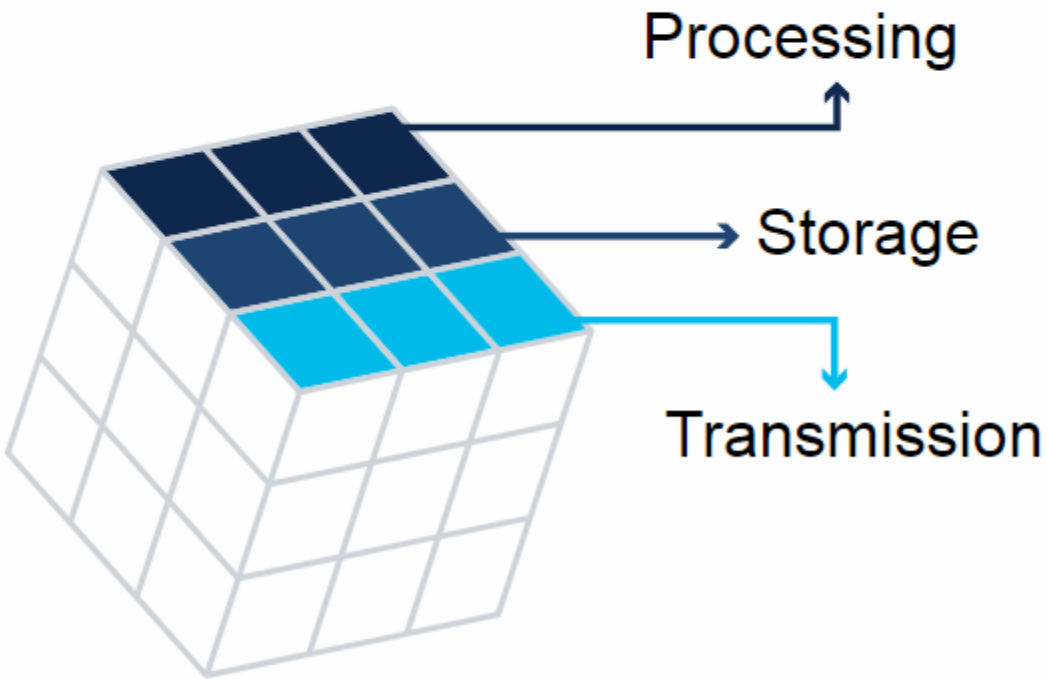


Confidentiality is a set of rules that prevents sensitive information from being disclosed to unauthorized people, resources and processes. Methods to ensure confidentiality include **data encryption**, **identity proofing** and **two factor authentication**.

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**.

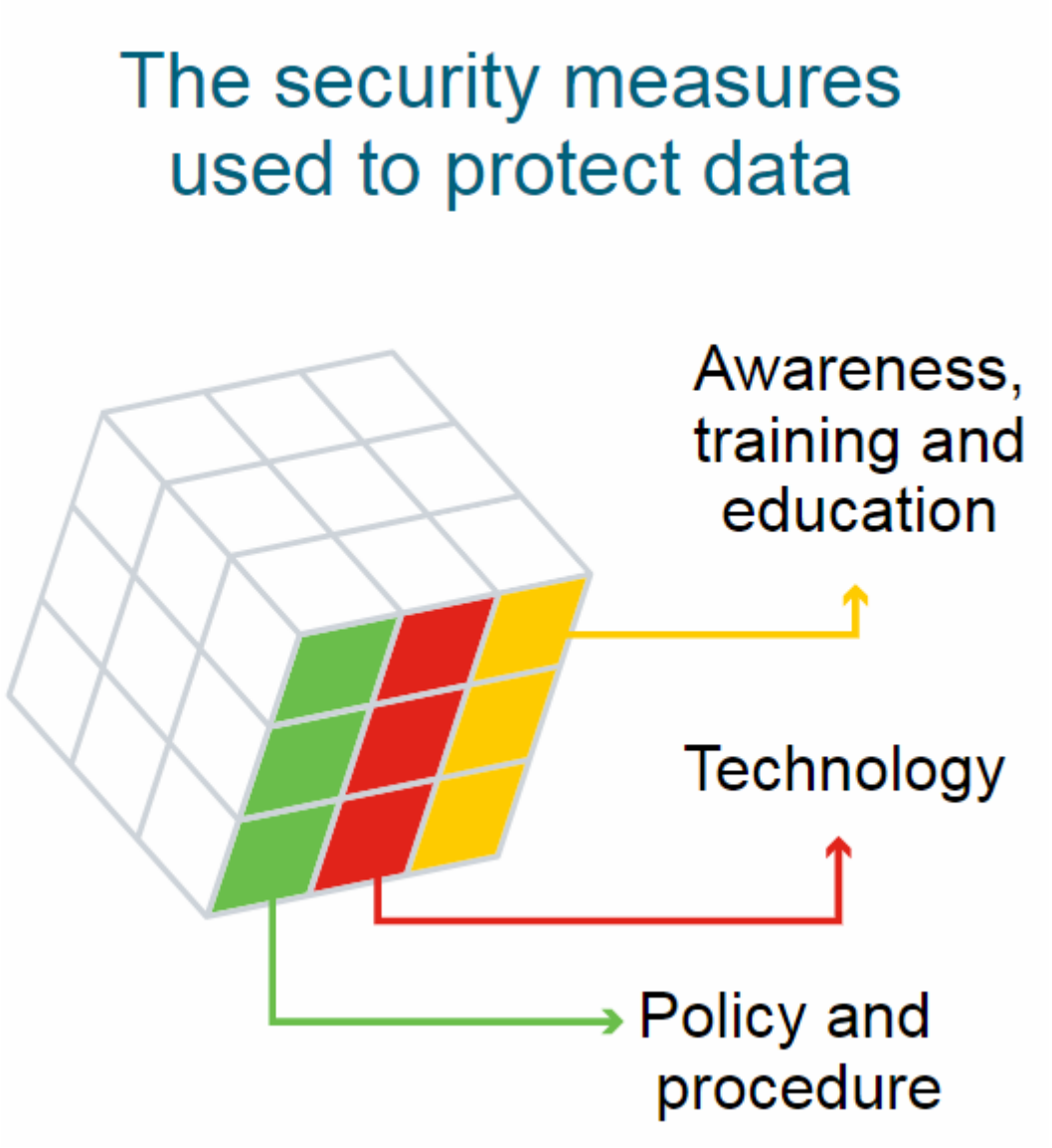
The protection of information in each state



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).

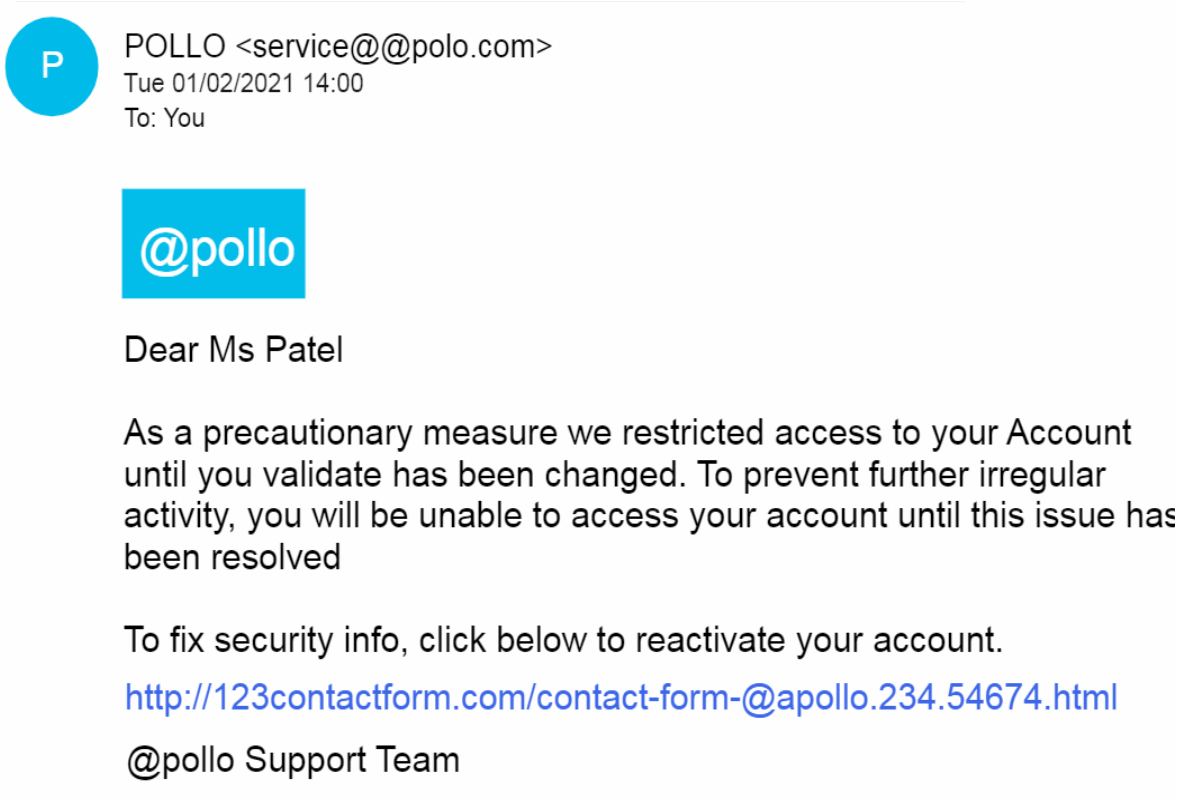


Awareness, training and education are the measures put in place by an organization to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems.

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.

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.'



P

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

@pollo

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

Take a look at the email. Which of the following indicates that it is in fact a phishing email? Don't forget, you have a chance to earn valuable defender points if you answer this correctly.
Select four correct answers, then Submit

- ❑ Graphics
- ❑ Email address
- ❑ Link URL
- ❑ Customer name
- ❑ The language, spelling and grammar

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.'

That’s right! You know exactly what to look out for and have earned yourself some defender points — well done!

Closer inspection reveals:

•that the sender's email domain is spelled incorrectly
•that the link URL is not pointing to @Apollo's website
•poor language, spelling and grammar
•low quality, pixelated graphics

Phishing emails can be hard to detect. For example, they will often address you by name to appear legitimate, but hackers can easily find this information on the Internet. So, it’s important to stay alert and think before you click.

Consequences of a Security Breach

Reputational damage : A security breach can have a negative long-term impact on an organization's reputation that has taken years to build. 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.

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.

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.

Types of Attackers

Amateurs

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. While script kiddies may use basic tools, their attacks can still have devastating consequences.

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 white, gray or black hat hackers.

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. Or 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

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.

What Color Is My Hat?

After hacking into ATM systems remotely using a laptop, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities.

Gray hat

This attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings.

Black hat

This attacker's job is to identify weaknesses in a company's computer system.

White hat

This attacker used malware to compromise a company's system and steal credit card information that was then sold to the highest bidder.

Black hat

While carrying out some research, this attacker stumbled across a security vulnerability on an organization's network that they are authorized to access.

White hat

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.

Cyberwarfare

Cyberwarfare, as its name suggests, is the use of technology to penetrate and attack another nation's computer systems and networks in an effort to cause damage or disrupt services, such as shutting down a power grid.

Sign of the times (Stuxnet)

One example of a state-sponsored attack involves the Stuxnet malware that is designed to not only hijack target computers but also cause physical damage to equipment controlled by the computers!

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.

Cyberwarfare can destabilize a nation, disrupt its commerce, and cause its citizens to lose faith and confidence in their government without the attacker ever physically setting foot in the targeted country.