SecurityAwarenessNews

the security awareness newsletter for security aware people

Confidentiality, Integrity, and Availability

The Three Pillars of Security
Multi-Factor Authentication Security
Data Lifecycle Management

The Three Pillars of Security

Confidentiality, integrity, and availability represent the three pillars of information security. They work together to create a foundational model that helps organizations protect people, data, and assets. Here's a general overview of what each pillar symbolizes.

Confidentiality:

Keeping information private

This one is the most straightforward of the three: ensuring private information remains private. That means not only preventing attackers from stealing data, but also preventing mistakes that lead to data leaks.

Integrity:

Keeping information accurate

The concept behind integrity refers to securely maintaining data so it's always accurate and never tampered with by unauthorized parties. This includes preventing it from being harmfully modified or deleted, whether accidentally or intentionally, and protecting data throughout its lifecycle.

Availability:

Keeping information accessible

When authorized people can't access assets or information, it impacts entire operations. Ransomware is a prime example of this scenario. It's a form of malicious software (malware) that encrypts systems or data, blocking access until a ransom is paid.

The idea behind this model is that security requires a balanced approach, with each pillar receiving equal priority. This helps organizations develop effective policies aimed at reducing risk and maintaining privacy.

The Three Pillars and You

Confidentiality, integrity, and availability are three of the most important concepts of information security. Let's put these concepts into practice through a few security awareness action items.

Stay alert for scams that aim to steal data. You can identify them by remaining aware of common warning signs, such as threatening language and urgent requests.

Use strong, unique passwords for every account. A strong password is long, hard to guess, and adheres to organizational guidelines.

Never install unapproved software. Most organizations have policies that control what software people use and when it gets updated. Be sure to always follow those policies.

Lastly, remember that you are the last line of defense. It's your commitment to security awareness that helps keep people and data safe.

Multi-Factor Authentication Explained

Password management plays a major role in protecting the confidentiality, integrity, and availability of information. Unfortunately, even the strongest passwords can be leaked or stolen when major security breaches occur.

That's why multi-factor authentication (MFA) is so important. It's a security feature that adds extra steps to your basic login procedure by combining two or more of the following common types of factors:

- **Knowledge** – something you know, such as your password
- **Possession** – something you have, such as your smartphone
- **Biometrics** – something unique to you, such as your fingerprints

MFA works by prompting you to input the additional factors after you enter your login credentials. They can be delivered in a few different ways, including the following examples:

- **Text message** - The additional factor is sent via text to your phone
- **Email** - Similar to a text message but delivered to your inbox
- **Software token** - This option uses applications, such as a mobile authenticator application, that create one-time passwords, which expire and regenerate in short time intervals
- **Hardware token** - Instead of manually entering the additional factor, a hardware token is inserted into a USB port or tapped on a device

While each of these types of MFA are better than using none at all, it's worth noting that some are considered much less secure than others. Both text messages and emails, for example, can be intercepted by cybercriminals. This means they might be able to steal the additional authentication factors.

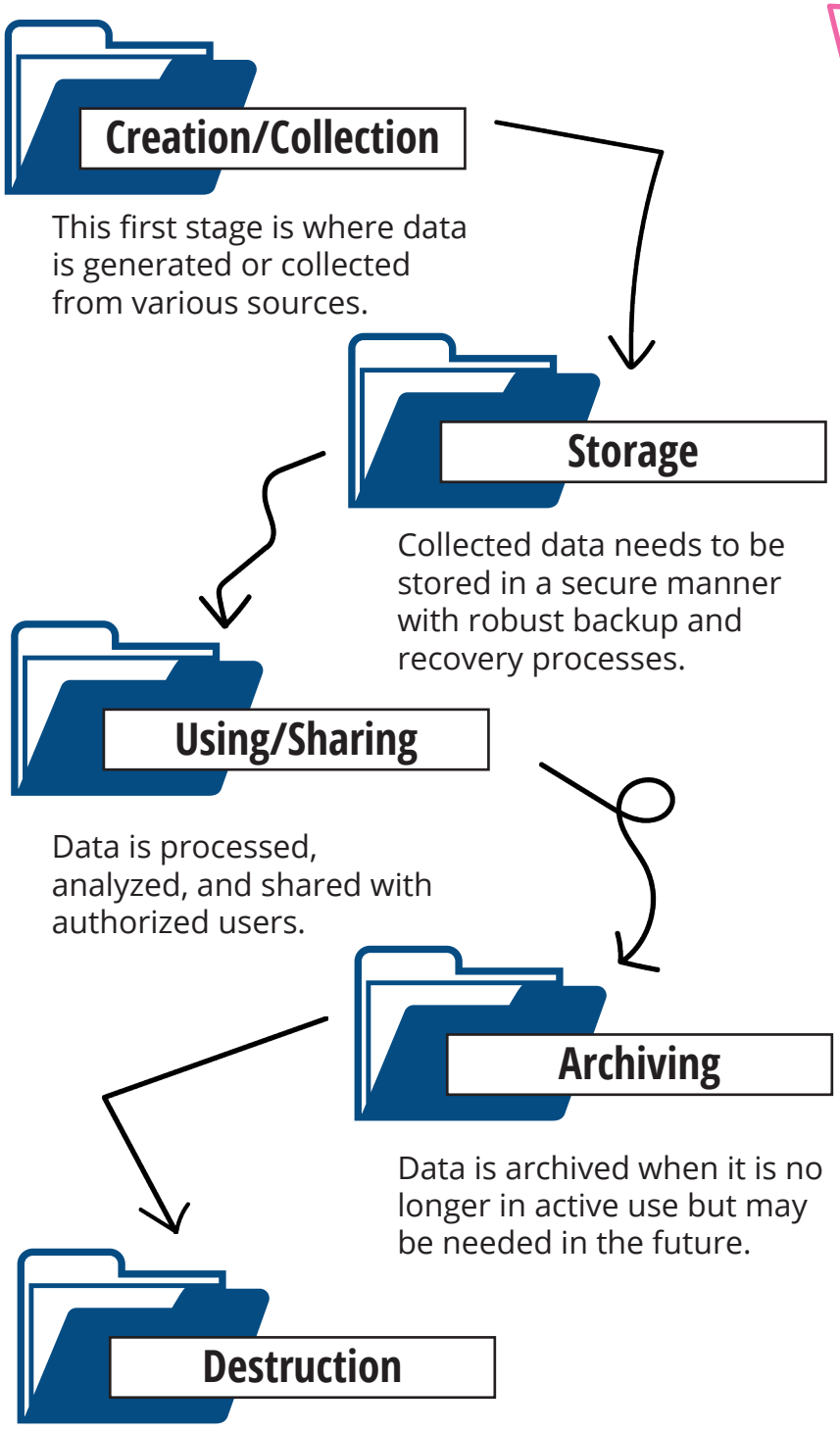
Conversely, software and hardware tokens require physical possession of your smartphone or the hardware token. This makes them a much better option for security purposes.

MFA and You

Here at work, it's your responsibility to always follow password policies, including when and how to use MFA. In your personal life, consider implementing MFA wherever it's available, and ensure your passwords are long and unique.

Data Lifecycle Management

Data lifecycle management refers to the process of managing data via a tiered approach. While the terminology for each tier can vary, here's what the life cycle of data generally involves:



This approach helps organizations gain insights into what data they have, how it's being stored, who should have access, and when data should be archived or deleted. It's a crucial process for ensuring security and privacy of the entire organization.

Data Lifecycle and You

Even if you're not in a position to impact the actual process of data management, you are in a position to protect any confidential information you have access to.

Take it personally.

Imagine what could happen if your personal information got leaked or stolen. Use that mindset when handling others' sensitive information.

Verify before sharing.

Whenever someone requests confidential information, take time to verify that they are legitimate and trustworthy. Never assume someone is who they claim to be.

Follow policy.

Policies exist to ensure confidential information remains confidential. By always following those policies, you can help maintain data privacy.