Security controls

These days, information is in so many places at once.
As a result, organizations are under a lot of pressure to implement effective security controls that protects everyone's information from being stolen or exposed.
Security controls are safeguards designed to reduce specific security risks.
They include a wide range of tools that protect assets before, during, and after an event.

Security controls can be organized into three types:
technical, **operational**, and **managerial**.

Technical control types include the many technologies used to protect assets.
This includes encryption, authentication systems, and others.

Operational controls relate to maintaining the day-to-day security environment.
Generally, people perform these controls like awareness training and incident response.

Managerial controls are centered around how the other two reduce risk.
Examples of management controls include policies, standards, and procedures.

Typically, organization's security policy outlines the controls needed to achieve their goals.
Information privacy plays a key role in these decisions.
Information privacy is the protection of unauthorized access and distribution of data.
Information privacy is about the right to choose.
People and organizations alike deserve the right to decide when, how, and to what extent private information about them is shared.
Security controls are the technologies used to regulate information privacy.

For example, imagine using a travel app to book a flight.
You might browse through a list of flights and find one at a good price.
To reserve a seat, you enter some personal information, like your name, email, and credit card number for payment.
The transaction goes through successfully, and you booked your flight.
Now, you reasonably expect the airline company to access this information you enter when signing up to complete the reservation.

However, should everyone at the company have access to your information?
A person working in the marketing department shouldn't need access to your credit card information.
It makes sense to share that information with a customer support agent.
Except, they should only need to access it while helping with your reservation.
To maintain privacy,
security controls are intended to limit access based on the user and situation.
This is known as the principle of least privilege.

Security controls should be designed with the principle of least privilege in mind.
When they are, they rely on differentiating between data owners and
data custodians.

A data owner is a person who decides who can access, edit, use, or
destroy their information.
The idea is very straightforward except in cases where there are multiple owners.
For example, the intellectual property of an organization can have
multiple data owners.

A data custodian is anyone or anything that's responsible for
the safe handling, transport, and storage of information.
Did you notice that I mentioned, "anything?"
That's because, aside from people, organizations and
their systems are also custodians of people's information.

There are other considerations besides these when implementing security controls.
Remember that data is an asset.
Like any other asset, information privacy requires proper classification and
handling.
As we progress in this section,
we'll continue exploring other security controls that make this possible.
(Required)

Revision #1
Created 2023-07-19 08:22:16 UTC by naruzkurai
Updated 2023-08-15 18:44:10 UTC by naruzkurai