Elements of a security plan

Security is all about people, processes, and technology.
It's a team effort, and I mean that literally.
Protecting assets extends well beyond one person or a group of people in an IT department.
The truth of the matter is that security is a culture.
It's a shared set of values that spans all levels of an organization.
These values touch everyone, from employees, to vendors, to customers.
Protecting digital and physical assets requires everyone to participate, which can be a challenge.

That's what security plans are for!
Plans come in many shapes and sizes, but they all share a common goal:
to be prepared for risks when they happen.
Placing the focus on people is what leads to the most effective security plans.
Considering the diverse backgrounds and perspectives of everyone involved ensures that no one is left out when something goes wrong.
We talked earlier about the risk as being anything that can impact the confidentiality, integrity, or availability of an asset.
Most security plans address risks by breaking them down according to categories and factors.

Some common risk categories might include, the damage, disclosure, or loss of information.
Any of these can be due to factors like the physical damage or malfunctions of a device.
There are also factors like attacks and human error.
For example, a new school teacher may be asked to sign a contract before their first day of class.
The agreement may warn against some common risks associated with human error, like using a personal email to send sensitive information.
A security plan may require that all new hires sign off on this agreement, effectively spreading the values that ensure everyone's in alignment.
This is just one example of the types and causes of risk that a plan might address.
These things vary widely depending on the company.
But how these plans are communicated is similar across industries.

Security plans consist of three basic elements: policies, standards, and procedures.
These three elements are how companies share their security plans.
These words tend to be used interchangeably outside of security, but you'll soon discover that they each have a very specific meaning and function in this context.

A policy in security is a set of rules that reduce risk and protects information.
Policies are the foundation of every security plan.
They give everyone in and out of an organization guidance by addressing questions like, what are we protecting and why?
Policies focus on the strategic side of things by identifying the scope, objectives, and limitations of a security plan.

For instance, newly hired employees at many companies are required to sign off on acceptable use policy, or AUP.
These provisions outline secure ways that an employee may access corporate systems.

Standards are the next part.
These have a tactical function, as they concern how well we're protecting assets.
In security, standards are references that inform how to set policies.
A good way to think of standards is that they create a point of reference.
For example, many companies use the password management standard identified in NIST Special Publication 800-63B to improve their security policies by specifying that employees' passwords must be at least eight characters long.

The last part of a plan is its procedures.
Procedures are step-by-step instructions to perform a specific security task.
Organizations usually keep multiple procedure documents that are used throughout the company, like how employees can choose secure passwords, or how they can securely reset a password if it's been locked.
Sharing clear and actionable procedures with everyone creates accountability, consistency, and efficiency across an organization.

Policies, standards, and procedures vary widely from one company to another because they are tailored to each organization's goals.
Simply understanding the structure of security plans is a great start.
For now, I hope you have a clearer picture of what policies, standards, and procedures are, and how they are essential to making security a team effort.

Revision #1
Created 2023-07-17 23:49:25 UTC by naruzkurai
Updated 2023-08-15 18:44:10 UTC by naruzkurai