The importance of cybersecurity

As we've discussed, security professionals protect many physical and digital assets. These skills are desired by organizations and government entities because risk needs to be managed. Let's continue to discuss why security matters.
Play video starting at ::17 and follow transcript0:17
Security is essential for ensuring an organization's business continuity and ethical standing. There are both legal implications and moral considerations to maintaining an organization's security. A data breach, for example, affects everyone that is associated with the organization. This is because data losses or leaks can affect an organization's reputation as well as the lives and reputations of their users, clients, and customers. By maintaining strong security measures, organizations can increase user trust. This may lead to financial growth and ongoing business referrals.

As previously mentioned, organizations are not the only ones that suffer during a data breach. Maintaining and securing user, customer, and vendor data is an important part of preventing incidents that may expose people's personally identifiable information.

Personally identifiable information, known as PII, is any information used to infer an individual's identity. PII includes someone's full name, date of birth, physical address, phone number, email address, internet protocol, or IP address and similar information.

Sensitive personally identifiable information, known as SPII, is a specific type of PII that falls under stricter handling guidelines and may include social security numbers, medical or financial information, and biometric data, such as facial recognition. If SPII is stolen, this has the potential to be significantly more damaging to an individual than if PII is stolen.

PII and SPII data are key assets that a threat actor will look for if an organization experiences a breach. When a person's identifiable information is compromised, leaked, or stolen, identity theft is the primary concern.

Identity theft is the act of stealing personal information to commit fraud while impersonating a victim. And the primary objective of identity theft is financial gain.

We've explored several reasons why security matters. Employers need security analysts like you to fill the current and future demand to protect data, products, and people while ensuring confidentiality, integrity, and safe access to information. This is why the U.S. Bureau of Labor Statistics expects the demand for security professionals to grow by more than 30% by the year 2030.

So keep learning, and eventually you'll be able to do your part to create a safer and more secure environment for organizations and people alike!

Revision #1
Created 30 May 2023 15:43:17 by naruzkurai
Updated 30 May 2023 21:56:57 by naruzkurai