Discussion-1 Security Breaches

Discussion Topic:

Have you personally (or your organization) experienced a cybersecurity breach - stolen identity, credit card fraud, computer virus infestation, malware attack, social engineering, etc.? If yes, describe how the attack progressed and the related damages you experienced. If no, then are you (or your organization) generally fearful of such attacks, and how is protection ensured?

Describe the kind of cybersecurity problems that either you or your company have experienced. What were the root causes of these problems? Based on what you know so far about cyber security, how should these have been addressed?

My Post:

Hello Class,

In the context of an organization that I am part of, like my place of employment, I do not deal directly with security issues, so I am not aware of how they deal with or if they have experienced cybersecurity breaches.
As an individual, on my own devices, I implement security systems such as antivirus software. So far, I have not really experienced a major cybersecurity breach, that I am aware of …, I suspect that my systems/devices have been compromised at some point, but I didn't find out. Anyhow, I am fearful of security breaches that will result in my personal information (e.g., Amazon account info, credit card info) being compromised/stolen. To protect against such risks, I take the following measures/precautions:

I install antivirus software on all my systems, including my cell phones, which helps detect and remove known viruses and malware. I use a combination of VPNs, software firewalls, and physical firewalls (routers) for my home network and on my devices. This helps to protect my network and my devices from being accessed by unauthorized actors. I also enable two-step/three-step authentication for my various online accounts whenever possible. This adds an extra layer of security, making it harder for unauthorized individuals/entities to access my accounts even if they have my username/email and password. I also use different email accounts, usernames, and strong passwords for each of my online accounts. This helps to minimize the risk of my account credentials being stolen, and if they are, it prevents them from being used to access all or several of my other online accounts. Finally, I use common sense and prudence when opening and replying to unknown email addresses, texts & phone calls from unknown phone numbers and email addresses. This protects against the risk of 'social engineering' attacks, which trick users/victims into revealing information or self-infecting their computers by installing or using malicious software.

In the context of organizations and as described by our course study guide, "$(ISC)^2$ SSCP Certification Training Guide" (uCertify, n.d.), the various cybersecurity issues mentioned in the previous paragraph can be addressed by applying the Confidentiality, Integrity, Availability (CIA) model for information security, where:
Confidentiality involves preventing unauthorized access to information. This means that organizations need to implement access controls, encryption, and policies regarding privileged information and communications.

Integrity involves ensuring that the information the organization provides is reliable, whole, and complete. This allows the organization's processes of communication, data storage, and user/access/business logic implementation to be trustworthy (authorized and controlled). Availability involves providing access only when and where it is needed, in a usable and secure format.

In addition to CIA, to keep their information secure, organizations need to implement the concept of authenticity, that is, providing a system that confirms that a person or entity is who they claim to be; and the concept of non-repudiation, ensuring that data does not change as it moves between locations.

-Alex

References:

uCertify (n.d). (ISC)² SSCP Certification Training Guide. uCertify. ISBN: 976164493776.