Ethics in Cybersecurity

In security, new technologies present new challenges. For every new security incident or risk, the right or wrong decision isn't always clear.

For example, imagine that you're working as an entry-level security analyst and you have received a high risk alert. You investigate the alert and discover data has been transferred without authorization.

You work diligently to identify who made the transfer and discover it is one of your friends from work. What do you do?

Ethically, as a security professional, your job is to remain unbiased and maintain security and confidentiality.

While it's normal to want to protect a friend, regardless of who the user in question may be, your responsibility and obligation is to adhere to the policies and protocols you've been trained to follow. In many cases, security teams are entrusted with greater access to data and information than other employees. Security professionals must respect that privilege and act ethically at all times.

Security ethics are guidelines for making appropriate decisions as a security professional. As another example, if you as an analyst have the ability to grant yourself access to payroll data and can give yourself a raise, just because you have access to do so, does that mean you should? The answer is no. You should never abuse the access you've been granted and entrusted with.

Let's discuss ethical principles that may raise questions as you navigate solutions for mitigating risks. These are confidentiality, privacy protections, and laws.

Let's begin with the first ethical principle, confidentiality. Earlier we discussed confidentiality as part of the CIA triad. Now let's discuss how confidentiality can be applied to ethics. As a security professional, you'll encounter proprietary or private information, such as PII. It's your ethical duty to keep that information confidential and safe. For example, you may want to help out a coworker by providing computer system access outside of properly documented channels. However, this ethical violation can result in serious consequences, including reprimands, the loss of your professional reputation, and legal repercussions for both you and your friend.
\
The second ethical principle to consider is privacy protections. Privacy protection means safeguarding personal information from unauthorized use. For example, imagine you receive a personal email after hours from your manager requesting a colleague's home phone number. Your manager explains that they can't access the employee database at the moment, but they need to discuss an urgent matter with that person.

As a security analyst, your role is to follow the policies and procedures of your company, which in this example, state that employee information is stored in a secure database and should never be accessed or shared in any other format. So, accessing and sharing the employee's personal information would be unethical. In situations like this, it can be difficult to know what to do. So, the best response is to adhere to the policies and procedures set by your organization.

A third important ethical principle we must discuss is the law. Laws are rules that are recognized by a community and enforced by a governing entity.

For example, consider a staff member at a hospital who has been trained to handle PII, and SPII for compliance. The staff member has files with confidential data that should never be left unsupervised, but the staff member is late for a meeting. Instead of locking the files in a designated area, the files are left on the staff member's desk, unsupervised. Upon the employee's return, the files are missing. The staff member has just violated multiple compliance regulations, and their actions were unethical and illegal, since their negligence has likely resulted in the loss of private patient and hospital data.

As you enter the security field, remember that technology is constantly evolving, and so are attackers' tactics and techniques. Because of this, security professionals must continue to think critically about how to respond to attacks.

Having a strong sense of ethics can guide your decisions to ensure that the proper processes and procedures are followed to mitigate these continually evolving risks.

Revision #2
Created 2 June 2023 21:11:06 by naruzkurai
Updated 3 June 2023 04:51:01 by naruzkurai