Ethics in Computing

Cybersecurity is a field evolving rapidly owing to the pace at which hackers create new ways to attack us. When I started to work in Cybersecurity in 2004, cybersecurity focused on protecting systems using firewalls and antivirus, and now the focus has shifted to protecting users. The entire profession is usually reactive, but ethics is always proactive. We cannot practice ethics 75% of the time and claim to be compliant (www.isc2.org, n.d.). I have always liked this definition of ethics: “Do what is right even when no one is watching”.

An ethical code is a moral code by which a person lives. For businesses, ethics can also refer to the framework you create for what is and isn't acceptable behaviour within your organization. Cyber-ethics is what distinguishes security employees from hackers in computer security. It is the understanding of right and wrong and the ability to follow ethical ideals while working. Simply said, technically, compliance acts may not be in the best interests of the consumer or the organization, and security experts must be able to appraise these concerns appropriately.

Cybersecurity experts have access to the sensitive personal data they were recruited to secure. As a result, it is critical that staff in these sectors have a

strong sense of ethics and respect for your customers' privacy. The information technology sector also expands and evolves so rapidly that navigating it requires a strong ethical foundation. It is critical that your personnel assess what is best for your consumers and the organization. Specific scenarios that your employees may face are sometimes impossible to predict. Therefore, a strong ethical basis can serve as the foundation that allows employees to behave in their best interests even in challenging, unforeseen circumstances (Reciprocity, 2021).

For those who work with computer systems, the Association for Computing Machinery (ACM) has developed a Code of Ethics and Professional Conduct. This code contains:

1) General Ethical Principles: These foundation rules include honesty, respect for privacy and intellectual property rights, and avoiding discrimination and other forms of harm.
2) Professional Responsibilities: This section of the code refers to a professional's responsibility to the field, which includes executing work to the best of one's capacity while maintaining a high degree of competence. This category also highlights increased public knowledge of their work as well as the ability to accept reviews when necessary.

3) Professional Leadership Principles: Computer science professionals must strive for the greater good, enhance their colleagues' working conditions, and encourage other field members to learn and flourish (Association for Computing Machinery, 2018).

These principles are only guidelines, but they serve as an excellent starting point for discussions about ethics in the area.

Depending on the field, ethical violations may also result in fines and other financial consequences. Banking and healthcare are particularly vulnerable, so being aware of the risks and emphasizing the importance of ethics to the employees is of utmost importance. We can achieve this by doing the following:

- Personal codes of ethics can differ greatly from person to person, and no two employees will have the same ideas about poor behaviour. As a result, firms must specify the ethical behaviour they demand from their employees and hire only those who can uphold those basic moral standards. This is especially true for the Chief Information Security Officer, who must lead the rest of his or her staff with integrity.

- Creating a code of conduct for the staff might help instill ethics in the organization. Regular training sessions and company meetings can also assist staff to develop a strong sense of ethics and a strong sense of community.
- Some organizations try to standardize cybersecurity ethics. While organizations such as ISSA and SANS give ethical accreditations for computer ethics, these programs are not universally recognized. Employees who have completed these courses should still be scrutinized before being employed.
- Ethics in the workplace begin at the top. C-suite executives and board members must set an example of ethical behaviour. By leading by example, high-level personnel can ensure that employees in all departments understand what is expected of them.
- Penalties for moral violations should be communicated throughout the organization and enforced when ethical issues arise.
- It is also critical to maintain an open and honest relationship with investors and customers. If something goes wrong—and something will sooner or later—your organization should notify affected parties as soon as possible, along with a thorough plan for reducing the effects and ensuring it does not happen again.

As an information security expert, navigating the complexity of ethics can be a difficult undertaking. As someone who possess several security certifications like CISSP, CISA, CISM, CRISC and CCSP on the other hand, have proven and verified my dedication to upholding ethical norms. When a business requires specific security capabilities, persons with these qualifications can provide a broad range of knowledge and expertise that is not restricted to information security.

References:

Association for Computing Machinery (2018). ACM Code of Ethics and Professional Conduct. [online] Acm.org. Available at: https://www.acm.org/code-of-ethics.

Reciprocity (2021). The Importance of Ethics in Information Security. [online] Reciprocity. Available at: https://reciprocity.com/the-importance-of-ethics-in-information-security/.

www.isc2.org. (n.d.). CISSP: What Do You Do When No One Is Watching? | (ISC)2 Article. [online] Available at: https://www.isc2.org/Articles/What-Do-You-Do-When-No-One-is-Watching# [Accessed 6 Oct. 2022].