ETHICS IN CYBER SECURITY

Cybersecurity Ethics play a big part in any field of work, especially in professions that affect the lives of others. Physicians, attorneys, and other professionals have ethics that guide their conduct when they face issues peculiar to their professions.

Doctors can be penalized for violating codes of conduct, while lawyers can be disbarred for the same reason. Based on how important cybersecurity is today, it makes sense that people working in this industry have codes of conduct too.

Even though many will agree that cybersecurity experts need codes of conduct as they carry out their responsibilities, what is right and what is wrong in this field is not always clear. Cybersecurity professionals often have access to confidential data and knowledge about the networks of their clients, which gives them a great deal of power that can be abused.

However, there is an absence of well-defined ethics for cybersecurity professionals, both as IT security consultants and in-house security specialists, especially when compared to other professions. This doesn't in any way mean Cybersecurity ethics is a subject that can be overlooked.

Ethics Defined

Ethics refer to well-founded standards of what is right and wrong that prescribe what we ought to do when confronted with specific situations. The goal of ethics is not to dictate what professionals must do when faced with every ethical dilemma but to instill a strong sense of principles that govern behavior or conduct.

When applied to cybersecurity, ethics is very important as seemingly unimportant actions can lead to grave consequences for both the professionals and the organizations they work for. Hence, an understanding of the rules of ethical behavior can help practitioners figure out what is expected of them professionally.

Why Cybersecurity Ethics matter

Due to the rising number of Cybersecurity attacks, the demand for professionals has continued to climb as organizations struggle to ward off malicious attacks. This has made many organizations focus on developing the knowledge and talent of individuals and putting them on the frontline as quickly as possible. While this strategy has its advantages, the disadvantages can be weighty.

In the hunt for talents, many organizations often fail to consider that knowledge and skills are not enough, and that new recruits could potentially access the power they have from accessing sensitive data and the entire network.

It might not be so obvious, but the security of any network has a lot to do with ethics. Many security breaches and criminal behavior among IT experts have been traced to ethical lapses. For example, a United States Army soldier, Bradley Manning, was arrested and charged in 2010 for transferring classified data onto his personal computer and communicating national defense information to unauthorized persons. The leaked data included 250,000 U.S. diplomatic cables.

Another case to consider is that of Sergey Aleynikov, a former Goldman Sachs computer programmer, who was convicted of stealing proprietary source code that could spot tiny discrepancies in stick prices and. He exploited the code and earned hundreds of millions of dollars until he was arrested and convicted in 2009.

In 2020, two employees of General Electric were convicted and sentenced to prison time and $1.4 million in restitution to the company. This was the outcome of several years of investigation into the theft of sensitive data that the company used in calibrating turbines it manufactured as well as the marketing and pricing information used for promoting this service.

There are many other cases of data breaches caused by ethical lapses on the side of cybersecurity professionals. They show clear reasons cybersecurity matters today. Because ethical issues are a daily occurrence in cybersecurity, every organization that stores personal

and sensitive data must see to it that ethics are interwoven throughout the company and that their contractors are strictly guided by ethics.

Beyond the possibility of security breaches, cybersecurity ethics are important because they help to protect institutions and organizations. For instance, hospitals require the services of a cybersecurity professional to secure their hospital's network and critical data. In effect, this means the expert is closely involved in protecting sick patients even without medical training. The continued existence of the hospital and survival of the patients might be hinged on the success or failure of that professional.

In a similar way, ethics matter because cybersecurity experts don't just protect the sick but everyone since they have access to sensitive data.

Cybersecurity Ethical Issues

Ethical issues in this context refer to consequences, whether damages or benefits, that can come from the choices of cybersecurity professionals. For instance, it is not hard to understand how ethical issues in fields like engineering and aeronautics can have severe impacts on both individuals and companies alike. In the same vein, ethical issues exist in cybersecurity, and here are some of the key issues:

- Harm to privacy – For obvious reasons, ethics in cybersecurity determine data privacy to a large extent today. With individuals and companies generating tons of sensitive data like never before, cases of threats like identity thefts are increasing exponentially as hackers seek to steal and use the identity of victims for financial transactions or other forms of crime.

Since cybersecurity experts are the first line of defense against such attacks, they are trusted to guarantee privacy, but poor cybersecurity practices stemming from lax patching efforts and outdated encryption tools can increase the risks of a data breach. These practices are unethical and can cause significant privacy harm.

- Harm to property - Cybersecurity attacks predispose organizations to the destruction of both digital and physical property. When professionals fail to carry out their responsibilities ethically, it could lead to manipulation of the network and the exploitation of loopholes by profit-seeking criminal enterprises, politically motivated groups, and more. Professionals are expected to protect their organization's network at all times.
- Cybersecurity interests – Although the term hacking has a negative connotation, ethical hacking is now a thing today, even though there are many concerns about it. There have been debates in the 'hacking community' about the need for teaching students hacking skills. Opponents believe it encourages illegal activities, while proponents opine that it empowers students to identify and protect themselves from black hats.

There is a possibility that these skills could be wrongly used in the absence of education and emphasis on cybersecurity ethics.

Common Ethical challenges for Cybersecurity Professionals

Cybersecurity professionals face a wide range of challenges daily. It's important to know these challenges and take a stand on them to ensure ethical and effective cybersecurity practice.

- Ethical challenges in confidentiality – Confidentiality is a hot topic in cybersecurity. Professionals will be exposed to both private and proprietary data and must keep the information confidential. There might be pressure from time to time to divulge juicy information about a user or the company, but professionals must practice what is known as the 'butler's credo.' The butler never tells.
- Ethical challenges in threats - Response to threats and data breaches is part of the responsibility of cybersecurity professionals. How a Cybersecurity professional responds to threats counts. Most people can afford to leave their computer unattended to or ignore notifications, but for a cybersecurity expert, this could be a big lapse.
- Ethical challenges in balancing security with other values – There's a good chance that most cybersecurity professionals will stumble into the shady practices of a business unit. In such instances, it may seem like a good call to go public and shine a light on the wrongdoing but what determines if it's a good decision is the details of that particular decision. Cybersecurity professionals should explore ways of handling situations of this nature, and the first step is to report such to their supervisors.
- Ethical challenges in network monitoring and user privacy- Many professionals often find themselves in the dilemma of carrying out their responsibilities with regards to

network monitoring and user privacy without making unjustifiable intrusions on users and their privacy. This can be quite difficult, but it helps professionals to inform users of the network of active monitoring and also to what extent it will be done.

- Ethical challenges in data storage and encryption – Data storage and encryption are essential because they help to protect an organization's data and keep it safe. Cybersecurity professionals must continually identify the best ways of responsibly and safely storing and transmitting sensitive information. They must ensure that encryption practices are well-aligned with the industry's standards and that are storage methods are regularly improved or updated.
-

Key Notes

Cybersecurity professionals have an obligation to both their organizations and the general public to carry out their duties ethically. It's crucial to know where to draw the moral line and stay ethically sound while aiming to better the security of any network they are protecting.

The ethical practices of a cybersecurity professional are essential to maintaining trust, integrity, and security in the digital environment. Here are some key ethical practices that such a professional should adhere to:

1. Confidentiality:

- Data Protection: Ensuring that sensitive information is only accessible to those authorized to view it.
- Non-Disclosure: Avoiding the sharing of confidential information with unauthorized parties, both within and outside the organization.

2. Integrity:

- Honesty: Providing accurate and truthful information, whether in reporting security status or disclosing potential risks and incidents.
- Objectivity: Remaining unbiased and fair in all evaluations, decisions, and recommendations.

3. Accountability:

- Responsibility: Taking ownership of one's actions and their consequences, particularly in incident response and when dealing with data breaches.
- Transparency: Clearly communicating the rationale behind decisions and actions to stakeholders.

4. Respect for Privacy:

- Minimizing Intrusion: Only collecting and using personal data that is necessary for the specified purpose.
- User Consent: Ensuring that data collection and processing practices are transparent and that user consent is obtained when required.

5. Compliance:

- Legal Adherence: Following all relevant laws, regulations, and policies governing cybersecurity and data protection.
- Industry Standards: Adhering to best practices and standards set by professional organizations and industry bodies.

6. Professional Competence:

- Continuous Learning: Keeping up to date with the latest cybersecurity trends, threats, and technologies.
- Skill Development: Continuously improving one's skills and knowledge through training, certifications, and practical experience.

7. Non-Malfeasance:

- Avoiding Harm: Ensuring that actions do not intentionally or unintentionally cause harm to others, including individuals, organizations, and society.

- Ethical Hacking: Conducting penetration tests and vulnerability assessments responsibly and within legal and ethical boundaries.

8. Fostering Trust:

- Reliability: Being dependable and trustworthy in professional relationships and duties.
- Building Confidence: Promoting a security culture within the organization and among peers that emphasizes the importance of cybersecurity.

9. Equity and Fairness:

- Non-Discrimination: Treating all individuals fairly and without bias, ensuring equal access to security measures and protections.
- Fair Use: Ensuring that resources and tools are used fairly and only for their intended purposes.

10. Social Responsibility:

- Public Awareness: Educating the public and raising awareness about cybersecurity threats and best practices.
- Ethical Advocacy: Advocating for policies and practices that promote the overall good and protect the most vulnerable.

Adherence to these ethical practices helps ensure that cybersecurity professionals act in a manner that upholds the integrity of their profession, protects sensitive information, and fosters a secure and trustworthy digital environment.