5.1.1 Legal Issues in Cybersecurity

protect against attacks, cybersecurity professionals must have the same skills as the attackers.However, cybersecurity professionals use their skills within the bounds of the law.

Personal legal issues : Most hacks leave tracks, which can be traced back to you. Cybersecurity professionals develop many skills, which can be used positively or illegally. There is always a huge demand for those who choose to put their cyber skills to good use within legal bounds.

Corporate legal issues : Most countries have cybersecurity laws in place, which businesses and organizations must abide by. In some cases, if you break laws while doing your job, the organization may be punished and you could lose your job. In other cases, you could be prosecuted, fined and possibly sentenced. In general, if you are unsure whether an action or behavior might be illegal, assume that it is illegal and do not do it. Always check with the legal or HR department in the organization.

International law and cybersecurity : International cybersecurity law is a constantly evolving field. Cyber attacks take place in cyberspace, an electronic space created, maintained and owned by both the public and private entities. There are no traditional geographic boundaries in cyberspace. To further complicate issues, it is much easier to mask the source of a attack in cyberwarfare than in conventional warfare. Country practice, opinio juris (a sense on behalf of a country that it is bound to the law in question) and any treaties drafted will shape international cybersecurity law.

5.1.4 Corporate Ethical Issues

Many professional IT organizations such as the Information Systems Security Association (ISSA) have published Codes of Ethics to help guide employee actions and behaviors. Cisco also has a team devoted exclusively to ethical business conduct and a Code of Business Conduct to help employees make business decisions and resolve any issues they may encounter.

5.2.1 Become a Cybersecurity Guru

start looking at job search engines, such as Indeed, LinkedIn, Monster and CareerBuilder to get a sense of what kind of jobs are available, all over the world!

5.2.2 Professional Certifications

Cybersecurity certifications are a great way for you to verify your skills and knowledge and can also boost your career.

Cisco Certified Support Technician (CCST) Cybersecurity : entry-level certification for newcomers who are preparing to start their career in the cybersecurity field. This certificate does not expire or require periodic recertification.

CompTIA Security+ : entry-level security certification.

EC Council Certified Ethical Hacker (CEH) : This certification tests your understanding and knowledge of how to look for weaknesses and vulnerabilities in target systems using the same knowledge and tools as a malicious hacker but in a lawful and legitimate manner.

ISC2 Certified Information System Security Professional (CISSP) : This is the most recognizable and popular security certification. In order to take the exam, you need to have at least five years of relevant industry experience.

Cisco Certified CyberOps Associate : This certification validates the skills required of associate-level cybersecurity analysts within security operations centers.

5.2.3 Cybersecurity Career Pathways

CyberSeek is a tool that provides detailed data about supply and demand in the cybersecurity job market to help close the cybersecurity skills gap. The interactive career pathway which shows the range of jobs in

cybersecurity, as well as detailed information about the salaries, credentials and skill sets associated with each job.