20 June 2020

|  |  |  |  |
| --- | --- | --- | --- |
| Date: | 20 June 2020 | Name: | Srinidhi J C |
| Course: | **Introduction to Cyber Security** | USN: | 4al16ec078 |
| Topic: | |  | | --- | | Compliance | | Governance and industry standards | | Career and industry landscape | | Program relevance | | Semester & Section: | 8th & b |
| Github Repository: | SrinidhiJC078 |  |  |
| FORENOON SESSION DETAILS | | | | | |
| Image of session  A screenshot of a computer  Description automatically generatedA screenshot of a computer  Description automatically generated  A screenshot of a computer screen  Description automatically generated | | | | | |

Report:

Many organizations must comply with a mixture of state-mandated, industry-specific, and international cybersecurity regulations. The challenge for an organization trading nationally, or even globally, is considerable.

According to [Tenable’s Trends in Security Framework Adoption Survey](http://www.tenable.com/whitepapers/trends-in-security-framework-adoption), 84% of organizations in the US tackle this issue with the help of a security framework, and 44% use more than one.

## **The most cyber secure sector** Of all the companies considered in the survey, those in the banking and finance sector most frequently adopted security frameworks (16%), followed closely by information technology (15%).

The health care and medical sector was the worst, with 27% not having any framework in place at all. The most frequently adopted frameworks should come as no surprise to security practitioners. In this next section, we’ll run through them and explain why they are so popular.

1. **NIST Framework for Improving Critical Infrastructure Security**

Used by 29% of organizations, the [NIST (National Institute of Standards Technology) Cybersecurity Framework](https://www.itgovernanceusa.com/nist) is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines, and practices. However, the Cybersecurity Framework has proven to be flexible enough to also be implemented by non-US and non-critical infrastructure organizations. Indeed, the document is regularly being amended to adapt to changing industry needs.

1. **CIS Critical Security Controls**

Used by 32% of organizations, the CIS Critical Security Controls are a set of 20 actions designed to mitigate the threat of the majority of common cyber-attacks. The controls were designed by a group of volunteer experts from a range of fields, including cyber analysts, consultants, academics, and auditors.

1. **ISO 27001**

Used by 35% of organizations, [ISO 27001](https://www.itgovernanceusa.com/iso27001) is the international standard that describes best practice for implementing an ISMS (information security management system).

Achieving accredited certification to ISO 27001 demonstrates that your company is following information security best practice, and delivers an independent, expert assessment of whether your data is adequately protected.

1. **1. PCI DSS**

Used by 47% of organizations, the [PCI DSS (Payment Card Industry Data Security Standard)](https://www.itgovernanceusa.com/pci_dss) governs the way credit and debit card information is handled.

The Standard applies to any organization (regardless of size or number of transactions) that accepts, stores, transmits or processes cardholder data.

Organizations that comply with its requirements are in a better position to spot vulnerabilities that could be exposed by criminal hackers or lead to internal data breaches – thus protecting customers from stressful situations and organizations from embarrassing or costly security incidents.

Although not federally mandated in the United States, PCI DSS is mandated by the Payment Card Industry Security Standard council. The council is comprised of major credit card bands and is an industry standard. Some states have even incorporated the standard into their laws.

The cybersecurity landscape has a good news/bad news outlook. The good news, according to new research from [CyberArk](http://www.cyberark.com/resource/2016-global-advanced-threat-landscape-survey/), is that the vast majority of IT professionals believe we’re making real progress in the cybersecurity battle. That feeling of confidence may come in part from the fact that three out of four IT pros say they are doing a good job at keeping hackers from breaking into the network.

However, businesses still struggling to put best practices in place when it comes to security. Areas such as privileged access, third-party vendors, and even the cloud have weak security oversight.

All of this makes companies vulnerable to hackers, who take advantage of every means possible to infiltrate networks and collect data. Take the Yahoo breach, for example. Although details about the hack that compromised more than 500 million records are still being investigated, it appeared that [Yahoo’s executives made customer convenience a higher priority than security.](http://searchsecurity.techtarget.com/news/450400084/Yahoo-breach-calls-into-question-detection-and-remediation-practices) Now, [personal information](http://www.computerweekly.com/news/450304953/Yahoo-security-still-poor-despite-massive-breach-claims-Venafi) including birth dates, addresses, passwords and even security questions and answers are among the compromised data that have been shared or sold.

In the current cybersecurity landscape, hackers use smartphones, tablets, and the many devices included in the [Internet of Things](http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#36ecfda16828) as a way to spread malware. These devices don’t have security included in the hardware or software. All too often, security for these devices is ignored, either by not adding security tools or not creating security policies to cover the devices.

There may be no bigger threat to cybersecurity today than [ransomware](https://threatsketch.com/ransomware-small-businesses/). Ransomware as an attack choice is skyrocketing, increasing more than 500 percent between 2015 and 2016. The attacks are evolving at the same time. The days of paying a couple hundred in bitcoins to release the encrypted data may soon be past. More frequently, hackers are only releasing part of the data upon payment and asking for more payments to release the rest. The [attacks are becoming more targeted](http://krebsonsecurity.com/2016/09/ransomware-getting-more-targeted-expensive/) as well. The health care industry is currently the favorite target for the hackers, with reports of 20 data-loss incidents per day.

Ransomware has become such a problem that the [FBI](https://www.fbi.gov/investigate/cyber) has released two separate public service announcements within the past three months. One is to warn against paying ransom, while recommending companies have good data backup and disaster recovery mechanisms in place so they don’t lose any down time or files. The second asks businesses to report any ransomware attacks to law enforcement immediately.

In addition to ransomware, there are a number of other cybersecurity threat vectors and problems for IT departments to be aware of and that we’ll be discussing in more depth in a series of articles. These threats include:

* [Distributed denial of service (DDoS)](https://threatsketch.com/distributed-denial-of-service/) attacks that overwhelm and take down websites
* [Mobile malware](https://threatsketch.com/need-know-mobile-malware-threats/), especially for Android
* [Inside jobs](https://threatsketch.com/insider-threats-and-byod-risks/) that include both employee mistakes and malicious intent
* [Social engineering](https://threatsketch.com/social-engineering-growing-threat-business/), particularly with an uptick in spearphishing attacks and using social networking sites as an attack vector

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date: | 20 June 2020 | Name: | Srinidhi J C | |
| Course: | Ethical Hacking | USN: | 4al16ec078 | |
| Topic: | |  | | --- | | Career and growth ladder in ethical hacking | | Program relevance | | Semester & Section: | 8th & b | |
| AFTERNOON SESSION DETAILS | | | |
| Image of session  A screenshot of a computer  Description automatically generated | | | |

Report:

Ethical Hacking has been a lucrative career option for many, and not without good reason! It’s a challenging job that never gets boring, pays well and also brings a greater sense of achievement. In this “Ethical Hacking Career” article, we are going to go over the various factors to guideline your path to become an ethical hacker: -

* + [Who is an Ethical Hacker?](https://www.edureka.co/blog/ethical-hacking-career/#who-is-an-ethical-hacker)
  + [Requirements to Become an Ethical Hacker](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-requirements)
  + [Roles & Responsibilities of an Ethical Hacker](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-responsibilities)
  + [Ethical Hacker Skill Set](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-skill)
  + [Ethical Hacker Job Trends](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-job-trends)
  + [How much money does an ethical hacker make?](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-salary)
  + [Ethical Hacker Job Profiles](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-profiles)
  + [Companies Hiring Ethical Hackers](https://www.edureka.co/blog/ethical-hacking-career/#ethical-hacker-companies)

## **Who is an Ethical Hacker?**

“To beat a hacker, you have to think like one” – Ethical Hacking Council

Hacking is the process of finding vulnerabilities in a system and using these found vulnerabilities to gain unauthorized access into the system to perform malicious activities ranging from deleting system files to stealing sensitive information. Hacking is illegal and can lead to extreme consequences if you are caught in the act. People have been sentenced to years of imprisonment because of hacking.

Nonetheless, hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as ethical hackers and the process is known as an [ethical hacking](https://www.edureka.co/blog/what-is-ethical-hacking).

## **Requirement to Become an Ethical Hacker**



How your ethical hacking career begins depends on your current field of work. If you’re not in an IT field you should definitely try shifting into one. Even though most jobs require you to have a Bachelor’s degree in computer science or cybersecurity-related field, exceptions are made for people with sound knowledge of operating systems, databases and networking! Also, it is nigh impossible to directly become an ethical hacker. Most ethical hackers begin their career as tech support engineers who climb their way up, by earning [certifications](https://www.youtube.com/watch?v=eO8l70pdVhY) like CCNA and CISSP before working towards the ultimate CEH certification. After earning your CEH certifications, is the time to market yourself as an ethical hacker!

## **Roles & Responsibilities of an Ethical Hacker**



There seems to be a general misconception that a person with an ethical hacking career is only responsible for penetration testing of systems and applications. This is not true, and an ethical hacker is responsible for much more.

* Scanning open and closed ports using Reconnaissance tools like Nessus and NMAP
* Engaging in social engineering methodologies
* Examining patch releases by performing vigorous vulnerability analysis on them
* An ethical hacker will see if he/she can evade IDS (Intrusion Detection systems), IPS (Intrusion Prevention systems), honeypots and firewalls
* Ethical hackers can employ other strategies like sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications

An ethical hacker strives to replicate the working of a black hat hacker by analyzing the defense protocols and social-engineering aspects of an organization. His job is to make sure the organization reacts to these situations well enough if they are already not doing so.

## **Ethical Hacker Skill Set**



A person with an ethical hacking career is expected to be proficient in database handling, networking, and operating systems and also have excellent soft skills as they need to communicate problems regarding security to the rest of the organization. Other than these generalized skillsets, an ethical hacker also have a good grasp on the following skills:

* Network traffic sniffing
* Orchestrate various network attacks
* Exploit buffer overflow vulnerabilities
* SQL injection
* Password guessing and cracking
* Session hijacking and spoofing
* DNS spoofing

Apart from this, an ethical hacker must be a creative thinker because black hat hackers are constantly coming up with ingenious ways to exploit a system and it is an ethical hacker’s job to predict and prevent such breaches.

**Ethical Hacking Job Trends**

[](https://www.edureka.co/blog/wp-content/uploads/2018/12/Trends-Certified-Ethical-Hacker-Career-Edureka.png)

Source: Google Trends

Growing at a rate that is outpacing all other areas of IT, [cybersecurity](https://www.edureka.co/blog/what-is-cybersecurity/) has emerged as a high-growth-field of 2017, and possibly of the entire decade. During the 5 years between 2012 and 2017, listings for cybersecurity jobs increased by a whopping 75% according to the analysis made by the Bureau of Labor Statistics. This has led to a lot of unfilled positions so jobs are plenty and they pay well too.

If you don’t understand how black hat hackers could get into your systems, you’re going to have a hard time securing them. Learning how to hack can help you implement the strongest possible security practices. It’s as much about finding and fixing security vulnerabilities as it is about anticipating them. Learning about the methods hackers use to infiltrate systems will help you resolve issues before they become dangerous.

Think of it this way: a computer network is like a yard with a fence to keep people out. If you’ve put something valuable inside the yard, someone may want to hop the fence and steal it. Ethical hacking is like regularly checking for vulnerabilities in and around the fence, so you can reinforce weak areas before anyone tries to get in.

Interested in practicing your ethical hacking skills? Check out Capella’s [*Ethical Hacking Skills Challenge*](http://media.capella.edu/CourseMedia/ITSkillsChallenges/password/wrapper.asp).

Above everything else, successful ethical hacking requires being a master at problem solving. Understanding how computer systems and programming languages work is also essential because it’s easier to anticipate ways to exploit the system.

For example, a website may use a complicated, sturdy JavaScript-based authentication system to prevent spammers from submitting thousands of bogus support emails. An ethical hacking approach to testing may be attempting to disable the JavaScript language in the web browser (a widely available feature) and submitting a support email while ignoring the authentication process. Unless the programmers have designed the site to ignore non-JavaScript enabled systems, the spam email will bypass security. After identifying the security hole, the programmers can make the necessary adjustments.

Depending on your previous experience and desired outcomes, there are different levels of ethical hacking training available. Hack training sites such as [hackthissite.org](http://www.hackthissite.org/pages/index/index.php) can help you sharpen your hacking skills, regardless of your experience level. For a deeper dive into ethical hacking and other network defense methods, an advanced degree is another option to consider.