1,5 MILLION JOBS OPENINGS UNTIL 2020

THE CYBER SKILL GAP

SHORTAGE OF SKILLED PROFESSIONALS TO WORK IN THE INFORMATION SECURITY FIELD

In this book you will find everything you need to know to thrive in the information security arena

VAGNER NUNES

The Cyber Skill Gap

Shortage of Skilled Professionals to Work in the Information Security Field

Vagner Nunes

Copyright © 2017 by Vagner Nunes

Disclaimer

All the material contained in this book is provided for educational and informational purposes only. No responsibility can be taken for any results or outcomes resulting from the use of this material.

While every attempt has been made to provide information that is both accurate and effective, the author does not assume any responsibility for the accuracy or use/misuse of this information.

FOREWORD

Are you ready for the coming cyber challenges? Here’s how to prepare yourself for this brave new world AND make a living at the same time...

As the world becomes more digital the threat of cybercrime and cyber terrorism increases exponentially.

Not only that, cyber-crime now costs billions and citizens are mostly helpless.

We live in a world where government sponsored hackers wage war against multinational corporations while cyber dons run teams of social engineers who extract millions from their gullible marks.

And will there be a Cyber 9/11?

Who knows but…

The next big trend in IT is cyber security

A recent white paper by Frost and Sullivan surveyed more than 13,930 qualified information security professionals and concluded ***"There is no shortage of vulnerabilities to address."***

The paper goes on to state that, 20% of managers and 12% of c-level executives agree that ***"Security concerns will continue to escalate."*** And this goes across all sectors from manufacturing to banking, insurance and finance (Even healthcare workers are now being affected)

What are they concerned about?

Application vulnerabilities, malware, hackers and cloud-based services mostly.

That's not to mention untrained staff who are vulnerable to the most basic phishing techniques which can cost companies ***billions***.

In fact, 85% of these executives reported that removing and remediating malware attacks now took up a significant amount of resources. More terrifying is the fact that…

No one is ready for this

What this paper also found that NO ONE is ready for this.

Over half of respondents believe their organization is losing the war against security threats and in 2011 one-third of survey respondents indicated that remediation would occur within one day. (By 2015 this percentage dropped to one-fifth of survey respondents.)

The reality is that keeping up with security threats will require a continuous and coordinated investment in security technologies, personal and external resources.

Which is why there is a growing need for information security specialists

Increasingly large amounts of information are being stored online and this information needs to be protected.

This is true from the highest level of government down to your local lawyer and doctor.

And this trend will continue to be fueled by the emerge of new technologies like IOT and BYOD.

(Plus, the continued evolution of sophisticated phishing and cybercrime techniques.)

And believe it or not there is a major skills shortage in this area

It’s estimated that until 2020 there will be a shortage of 1,5 million jobs in cyber security all around the world.

This is why cyber security presents a ***major opportunity*** for people in the IT field.

(62.2% of survey respondents said they had too few security workers and were desperate to hire more.)

What the survey also found is that companies found it increasingly difficult to retain Info sec specialists. This is mostly because of the unique challenges and speed at which this industry moves.

But it’s also why there has been a dramatic rise in salaries, all around the world.

More impressive than net salaries reported, security professional salaries showed an average increase by 2.1% since 2013. Surprisingly, this was found to be the same across developed and non-developed countries.

But this isn’t something you can study at college or university.

They have yet to catch up. And in truth ***they can’t*** because technology changes at lighting pace.

Instead, to enter into this field, you’ll need the help of a ***professional organization*** which can provide the tools knowledge and contacts needed to succeed.

To help you with this I've put together a field guide to the info sec industry

In this book, you learn what IT professionals need to understand about this brave new world, and about the organizations and credentials available to you.

Not only that it also explores:

- The threat posed by today's advanced malware, DDoS attacks, phishing, tailgating and the most lethal of all Social Engineering.
- Cyber security: What it is and what you need to know about this field.
- Why this industry is going to become so important over the coming years.
- How to identify theft and the dozens of internet frauds out there.
- Why Networking and Information Security Organizations are so important.
- How to get the training, tools, networking opportunities and experience needed to become a successful.

- Plus, you'll also learn about (ISC)², the main Global Information Security organization, what they can offer you and how to join.

This guide covers everything needed to become a successful InfoSec specialist

Remember, as the world become more digital the threat of cyber terrorism and crime increase exponentially. And according to current trends there will be a desperate need for people who can combat these threats.

This could be a highly lucrative and exciting career

If these trends continue (and they will) then you're almost guaranteed to find highly paid employment in the cyber security industry.

And if you're interested then take a look at my field guide to the info sec industry.

SUMMARY

The issue of cyber-security has been paid less attention over the years, but in the light of the massive technological advancement, which also comes with a lot of cybercrime advancement, companies, government of nations and other institutions are now paying a lot of attention to the subject of cyber security and the safety of information within their organization.

There is a bigger issue being faced by these institutions at the realization for their need to secure their cyberspace, which is that of skill gap in cyber security. The realization that there are very few skilled hands in the cyber-security business has made it a very lucrative one to be in for skilled people, but with the world still lacking skilled hands; this book intends to show you through the path of becoming a cyber-security professional; the right steps to take, the right courses to undertake and of course, the right institution where you can get the best on your path to being a cyber-security professional.

Chapter One

- Cyber crime
- Cyber war
- Types of Cyber Security

This chapter introduces us to the concept of cyber security. Also, it puts a spotlight on the elements of cyber security and all the types of possible attack that a cybercriminal could deploy on a cyberspace.

Chapter Two

This chapter talks about the void in the cyber security profession which is not being filled and may pose a threat to both the profession and cyber space if the situation is not salvaged in time. The chapter is an outreach to tech inclined people to get into the cyber security field and fill the void in the skill gap.

Chapter Three

- Why is the Cyber Security Shortage Occurring?
- Social Engineering
- Why the Shortage of Cyber Security Experts is hitting businesses hard

This chapter explains the reason for shortage in cyber security professionals with facts and figures. It also talks about social engineering and the types of social engineering methods deployed to attack cyber space.

Chapter Four

- What is needed to Thrive in the Cyber Security Field?
- Ethics in Cyber Security

This chapter highlights the DOs and DON'Ts in the cyber security profession, what is needed to become a professional and the code of conduct in the profession.

Chapter Five

- Why you should trust (ISC)^2
- Training delivery methods
- What the (ISC)^2 certification is for
- The certification process at (ISC)^2

- The Career path to (ISC)^2
- Certification courses you will go through at (ISC)^2

This chapter talks about the organization (ISC)^2 where you can become a professional cyber security expert. The chapter points out the ethics of the organization and how it is run to deliver top notch service to their students. It also contains an outline of the courses and procedures (ISC)^2 offers to their prospective students.

Table of Contents

INTRODUCTION

The Facts

For a sector so important and vast, there is a glaring shortage of skilled professionals to work in the Information Security field. Research shows that by 2020, there will be a skill shortage of 1.5 million jobs in cyber security around the world. If this figure is not disconcerting for something so vital, I do not know what is. The trend grows exponentially as the new technologies emerge, like IOT, BYOT, Phishing, Cybercrime and Cyber terrorism.

Notwithstanding the seriousness of the topic at hand, it is interesting to note that there are a lot of opportunities in this particular area with high-paying salaries. However, without adequate training, one simply cannot have access to this land of untapped resources. It is highly agreed that those who work in this field must be professionals with specialized skills that most colleges cannot provide. In addition, there is the need to update one’s knowledge in this field as the threats in the cyber world progresses. The need for constant updates is crucial as one cannot claim to be an information security professional without the help of a professional organization capable of providing knowledge, the networking community and the tools needed to succeed.

This book strives to expose the gap in cyber security, how Information Technology and related professionals can prepare themselves to thrive in this new arena. Also, buried in this book is the necessary information needed to understand the changes in this cyber arena, as well as a deep understanding of the organizations and credentials available to be part of this new community.

CHAPTER ONE

❖

The Basis

Cyber Security: A Definition

Cyber security is the assemblage of technology, procedures and practices intended to shield and protect data, projects, codes and valuable information from unapproved access. In other words, it means unauthorized eyes are supposed to be kept out -for good. In the computing setting, this kind of security incorporates both cyber security and physical security.

Cyber security has never been as easy as it sounds. In a fast paced technology driven world, cyber-attacks turn out to be more innovative as time progresses. It is therefore expedient to appropriately characterize cyber security and recognize what constitutes great cyber security.

Cyber security is essential because year in and year out, the expenditure on cyber security keeps growing. In reference to Forbes, the global cyber security market reached $75 billion for

2015 and is expected to hit $170 billion in 2020. Organizations are beginning to comprehend that malware is a publicly accessible product that makes it simple for anybody to end up distinctly as a cyber-attacker. Sadly, more organizations offer security arrangements that do little to guard against cyber-attacks. Cyber security requests deep focus and a whole lot of commitment.

Cyber security protects the information and integrity of computing resources having a place with or interfacing with an organization’s system. Its purpose is to protect those assets against dangerous threats all through the life cycle of a cyber-assault.

Worthy of note amongst the trickiest components of cyber security is the rapidly and continually advancing nature of security dangers. The conventional approach has been to concentrate most resources on the most critical system segments and secure against the greatest known dangers. This requires abandoning some less vital system parts undefended and some less perilous dangers unprotected.

Cyber criminals, risk performing artists, hackers—they all know what you know- cybercrime pays. Your IT, put away in systems and the cloud, can do little. What's more, despite the fact that the strategies, targets and technology of assaults are exceedingly critical, your most intense protection against cyber-crime is to understand how attackers work in their own domain.

Cyber-attacks have changed and may go undetected for a while. Talk about a thief in the night! Expansive, scattershot assaults intended for fiendishness have been supplanted with cutting edge relentless determination. Dangers are concentrated on securing profitable information from a particular source. Modern cyber assaults are frequently led over various vectors and stages. They have an arrangement to get in, flag again from the bargained system, and collect significant information in spite of system security measures. To viably anticipate and react to cyber-crime, you have to understand what the inspirations and philosophy of cyber attackers are, in addition to all the levels and forms which cyber-attacks could come as.

Cyber Risks can be isolated into three unmistakable territories:

Cyber Crime

Cyber-crime is usually conducted by people working alone, or in groups, with their major aim being on extricating cash, information or bringing about disturbance. Cyber-crime can take many structures, including the procurement of credit/debit card information, intellectual property, and hindering the operations of a site or service.

Cyber War

Cyber war comes about when a nation intends to bring harm on another nation by trying to gain access to classified information not meant for public consumption. In most cases, wars have been started for less. Cyber wars lead to harm and it involves undercover work against another country keeping in mind the end goal is to bring about disturbance or to extract information. This could include the utilization of Advanced Persistent Threats (APTs).

Cyber Terror

An organization, working freely of a nation state can decide to instigate terrorist activities through the medium of cyberspace. This is known as cyber terror. Organizations need to consider measures against all these including governments of nations, those inside the basic national framework, and prominent establishments. It is possible that most organizations will suffer from cyber war or cyber terror.

Types of Cyber Security

They include virus, spyware and malware. Be that as it may, those are just the tip of ice berg. To help you comprehend the types of computer security, I have separated the whole hypothesis into the accompanying three sections:

- Internet and Network Security
- Standalone Computer Security
- Information Loss by Accidents

Web Security gives sleepless nights to a lot of organizations. Majority of people and organizations are worried about malware and hackers. **Network Security**, manages the security issues on systems of any size. This incorporates outer issues and additional issues of computers inside the system**.** **Standalone computers** allude to computers that are not associated with any system (but rather might be associated with Internet). This part covers the conceivable security vulnerabilities on such systems. Lastly, **data loss** is pertinent to systems and computers in addition standalone computers.

There are many types of computer security dangers today. Some are really unsafe while some are absolutely innocuous albeit irritating. In addition, there are some viruses which do not harm your computer rather, they have the ability to empty the numbers in your bank account.

Here are some threats you really should avoid. They are as dangerous as they come:

- **Trojan**

Trojan standouts as the most dangerous of them all. Trojan is a menace to most banking apps. Also originating from the Trojan family include Zeus and Spy Eye. How Trojan works is this: It can conceal itself from antivirus detection and steal banking information to compromise financial balance. In the event that the Trojan is truly intense, it can assume control over the whole security system. Thus, a Trojan can bring about many sorts of harm beginning from your own computer to your online record.

- **Virus**

In times past and as of ten years ago, Virus was something truly mainstream. Virus is a malevolent program that duplicates itself with the aim of pulverizing a computer. A definitive objective of a virus is to guarantee that the casualty's computer will never have the capacity to work properly or even work at all by any means. It is not all that mainstream today on the grounds that malware is intended to acquire cash over obliteration. Thus, virus is accessible for individuals who need to utilize it for some kind of requital reason.

- **Worms**

One major characteristic of worms is that they are developed just to spread and destroy all they see in their path. It doesn't modify your system to make you have a bad day with your computer, however it can spread starting with one computer then onto the next computer inside a system or even the web. The computer security hazard here is, it will occupy your computer hard disc space because of the replication and take up the greater part of your bandwidth capacity because of the spread.

- **Spyware**

Spyware is a malware which is intended to keep an eye on the victim's computer. If by chance that you are tainted with it, there is a likelihood that your daily action or certain movement will be spied by the spyware and it will get itself an approach to contact the host of this malware. Mostly, the utilization of this spyware is to realize what your everyday action is, so that the assailant can make utilization of your data. For example, let’s say that you view a lot of sex sites consistently, the attacker will attempt to lure you with a sex toy trick to take away your cash.

- **Scareware**

Scareware is a kind of virus that is planted into your system and on arrival, promptly puts up a notification that you have hundreds of infections which do not exist. The thought here is to deceive you into obtaining an unreasonable anti malware which claims to expel those dangers. It is about tricking you off your cash yet the approach is somewhat unique here in light of the fact that it alarms you with the goal that you will purchase.

- **Key logger**

Key logger is something that keeps a record of each keystroke you make on your keyboard. Key logger is a very potent danger that takes individuals' login details, such as username and password. In addition, it is a powerful Trojan.

- **Adware**

This is a type of risk where your computer will begin tossing out a considerable measure of commercial pop ups. It can be from non-adult materials to grown-up materials in light of the fact that any advertisements will profit the hosts. It is not by any stretch of the imagination a destructive danger, however the pop ups can be entirely irritating.

- **Backdoor**

Backdoor is not so much of a malware but it is a type of technique where once a system is helpless against this strategy, attackers will have the capacity to sidestep all the consistent validation parameters. It is typically introduced before any infection or Trojan contamination in light of the fact that having a backdoor passage will facilitate the exchange exertion of those dangers.

- **Wabbits**

This is another self-recreating threat. However, it doesn't work like a virus or worms. It doesn't hurt your system like a virus and it doesn't replicate through your LAN like worms do. A case of Wabbit's assault is the ‘fork bomb,’ a type of DDoS attack.

- **Exploit**

Exploit is a type of programming which is customized particularly to assault certain vulnerabilities. For example, if your web program is powerless against some outdated defenseless glimmer module, exploit will work just on your web browser and plugin. The best approach to abstain from hitting into exploit is to dependably fix your system since programming patches are there to settle vulnerabilities.

- **Botnet**

Botnet is something which is introduced by a BotMaster to take control of all the computer bots through the Botnet contamination. It for the most part, infects through drive-by downloads or even Trojan infections. The after-effect of this danger is the casualty's computer, which the bot will utilize for a substantial scale assault like DDoS.

- **Dialer**

This risk is no longer mainstream today yet taking a look at the technology 10 years ago, one would finger dialer as a major culprit of destruction. Dialer signified prominent danger. How it operates is that it makes use of your web modem to dial international numbers which are entirely costly. Today, this sort of danger is more on Android and iOS since it can make utilization of the telephone call to send SMS to premium numbers.

- **Dropper**

As the name implies, a Dropper is intended to drop into a computer and introduce something helpful to the attacker, i.e., malware or backdoor. There are two types of Dropper. One is to promptly drop and install so as to dodge Antivirus recognition. Another kind of Dropper will drop a little document where this little record will auto trigger a download procedure to download the Malware.

- **Fake Antivirus**

Fake Antivirus threat is an extremely popular threat among Mac users. How it works is this: Mac clients occasionally get a terrifying message which lets them know that their computer is compromised with infection. This tactic is really valuable because it pushes users into acquiring a false antivirus which does nothing.

- **Phishing**

A fake site which is intended to look practically like the real site is a type of phishing assault. The notion of this attack is to trap the client into entering their username and password into the fake login frame which effectively steals the character of the casualty. Each frame conveyed from the phishing site won't go to the genuine server but to the attacker’s controlled server.

- **Cookies**

Cookies is not by any means a malware. It is just a tool utilized by most sites to store something into your computer. It is here on the grounds that it can store things into your computer and track your exercises inside the site. On the chance that you truly don't care for the presence of cookies, you can dismiss these cookies for a portion of the sites which you don't know.

- **Bluesnarfing**

Bluesnarfing is about having an unapproved access to a particular cell phones, portable PC, or PDA by means of bluetooth association. By having such unapproved access, private information like photographs, calendar, contacts and SMS will all be uncovered and stolen.

- **Blue jacking**

Blue jacking additionally utilizes the bluetooth technology. However, it is not as genuine as Bluesnarfing. What it does is that it will interfere with your bluetooth gadget and send a message to another bluetooth gadget.

- **DDoS**

A very popular threat done by Anonymous sends a great activity to a solitary server to bring about the system breakdown. This is a façade and a deliberate security breach so that the threat can hack into the system and go away with any information. This sort of trap sends a considerable measure of activity to a machine known as Distributed Denial of Service, otherwise called DDoS.

- **Boot Sector Virus**

It is a virus that places its codes into computer DOS boot sector or otherwise called the Master Boot Record. It will begin if it is infused amid the boot up period where the harm is high but hard to contaminate. All the casualty needs to do in the event of a boot segment infection is to evacuate all the bootable drives so that this specific infection won't have the capacity to boot.

- **Browser Hijackers**

A browser hijacker utilizes the Trojan malware to take control of the casualty's web browsing session. It is to a great degree hazardous particularly when the casualty is attempting to send some cash by means of online banking. That is usually the best time for the attacker to adjust the destination of the financial balance and sum.

- **Chain letters**

Chain letters are usually very common on our mobile phones and social media accounts. It used to be popular as kids where we make each other do things by adding a mandatory clause which are usually lies. Individuals get a kick out of sending junk letters. For example, the Facebook account delete letter. It typically says if you do not forward that specific message or email to 20 individuals or more, your record will be erased and individuals truly believe that.

- **Virus Document**

Today, viruses can be spread through document files particularly through pdf files. Most of the time, individuals will counsel you not to execute an exe record. It is ideal in the event that you utilize an online virus scanner to verify first before opening any single document which you feel is suspicious.

- **Mousetrapping**

The mousetrapping virus is quite rare and uncommon even among techies. What mousetrapping does is that it traps your web program to a specific site. In the event that you attempt to go to another website, it will naturally divert you back to the initial site. If you take a stab at clicking forward/in reverse of the route catch, it will likewise divert you back. If you attempt to close your program and re-open it, it will set the landing page to that site and you can never escape this danger unless you expel it.

- **Obfuscated scam**

Simply put, obfuscated Spam is spam mail. It is obfuscated in the way that it doesn't resemble any spamming message with the goal that it can trap the potential casualty into clicking it. Spam mail today looks extremely bonafide and in the event that you are not cautious, you may very well fall for what they are putting forth.

- **Pharming**

Pharming works pretty much like phishing yet it is somewhat trickier. There are two sorts of pharming where one of it is DNS poisoning. Here, your DNS is compromised and all your activity will be diverted to the attacker's DNS. The other sort of pharming is to alter your HOST document and divert you to another website. One thing they have in common is that both are similarly hazardous.

- **Crime ware**

Crime ware is a type of malware that takes control of your computer to carry out a computer crime. Rather than the programmer himself perpetrating the crime, it plants a Trojan or whatever the malware is called to request you to carry out a crime. This will make the hacker himself clean from the crime that he had done.

- **SQL Injection**

SQL injection does not affect the clients specifically. It works towards affecting a website which is helpless against this assault. What it does is it that it will increase unapproved access to the database and the attacker can recover all the significant data stored in the database.

Who are Cyber Criminals?

Most cybercrimes are perpetuated by individuals or small groups. In any case, a person who offers an item on the web and does not send it, or somebody who professes to be another person keeping in mind that the end goal is to acquire private information for blackmail purposes is a cybercriminal. However, while they are without a doubt obnoxious people, they don't pose much hazard to large organizations. The hazard to businesses usually comes from attackers with higher desires or personal vendetta.

"Prankster" is a name given to individuals who hack into systems for no particular reason. A case is the notorious cyber bunch called LulzSec who were students of computer science at school. Their name was inspired by their yearning to “laugh in the face of the casualty's security measures”. However, cybercrime is no laughing matter. In 2011, LulzSec partook in an extensive assault on Sony, completing DDoS assaults and purportedly taking source codes from their Developer Network.

A second group can be alluded to as 'attackers with a cause'. They, more often than not, have a political or social cause and normally work as a little or closely associated gathering of criminals. Like these are the ‘nation/ state attackers’ who likewise serve a cause and are frequently the most in fact advanced of their type. One late case of country state assaults happened directly under the nose of a noteworthy cyber security firm, Kaspersky Labs. Kaspersky reported that Stuxnet and Duqu malware dug in themselves with an end goal to leech data about national-state attacks that were under scrutiny, and in addition, information in regards to the recognition programming that can alleviate attacks. These attackers additionally pose a threat to organizations on the grounds that their political targets are very much served by producing salary from cybercrime in nations other than their own.

According to a survey by 'Flipping the Economics of Attacks' by Palo Alto Networks and the Ponemon Institute, 67% of UK hackers conceded that cash is their principle motivating force for their criminal activities, despite the fact that the same research uncovered that the normal UK cyber-criminal makes simply over £20,000 every year (a normal of £8600 per attack). These are not over the top measures of cash and are lower than one would have expected, particularly when you consider a cyber-security expert can make up to four-times that much in wages. This suggests that cyber-hackers will probably center their endeavors on brisk, simple focuses with reasonable budgetary payouts.

What do Hackers really want?

With the data breach ticking higher than at any other time in the world today, it shows plainly that cyber security is one of the greatest difficulties confronting organizations today. Also, with every breach affecting at least 20,000 individual records, consumers can no longer choose not to see.

Cybercrime does not discriminate. It affects organizations of all sizes. However, we can distinguish the trends and high-risk sectors that will probably pull in their attention and endeavors.

Here are four focuses that are at the highest point of hackers' list:

- **Identity**

Identity extortion is not specifically new. However, reports of late recommend that while it is hard for newer technology create fake identities, cybercriminals are resorting to take genuine identities with more steadiness.

The Veda 2015 Cybercrime and Fraud Report found that almost 60 percent increment in fake credit applications including identity takeovers in Australia in the previous two years and a 17 for every penny increment took place in the previous year. Furthermore, with every data breach of consumer information, identity theft turns into a very easy thing.

- **Company Information**

Smaller companies/ businesses are almost always defenseless against cyber-attacks. Cyber storms that numerous large companies can go through easily can without much of a stretch sink littler ones. Tragically, private ventures hoping to upgrade their financial plans frequently see vigorous security arrangements as resentment buy.

Be that as it may, the most perilous thing for small business proprietors to believe is, "We're not big enough for cyber attackers." Research has found that Ransom ware assaults are presently focusing on SMBs because of their more careless security measures and ability to pay.

- **Convenient Cloud based platforms**

Some platforms like MyGov offer consumers a helpful approach to get to government organizations and data. Utilizing only one login and password, the platform empowers you to do everything from recording pay charges or applying for kid support to dealing with your ABN. Be that as it may, this basic or combined arrangement makes a nectar pot for hackers.

Organizations entrusted with shielding these sorts of platforms need to guarantee the strictest levels of security, particularly in the wake of the late breach of finance systems and assessment document numbers.

- **Medical**

It might appear to be surprising for cybercriminals to be bothered with what occurred amid your last visit to the hospital, yet healthcare and medical associations offer a fortune of data rich information. That information, if utilized as a part of the correct route by the wrong individuals, can pulverize for purchasers and organizations.

Gossipy titbits around the strength of the late Steve Jobs created a sharp fall in Apple stocks and it was later uncovered that Charlie Sheen's HIV diagnosis was initially revealed in the Sony hack. In any case, you don't need to be a big name or prominent focus to be a casualty of hackers utilizing your very individual data for their own gain.

Consumers take a huge risk each time they trust their own information to poorly prepared and underprepared organization and they're beginning to take note. A late review found that, while considering new innovations, privacy is presently the greatest concern toward more than 66% of customers in the world.

It is high time organizations and businesses made full moves to secure their IP and all their client data. Encrypting what you deem important to your business is a decent place to begin. However, far superior are arrangements that use multilayer encryption with private keys that are claimed and overseen by the client. It's about discovering arrangements that strike the correct adjust of security and efficiency.

It is quite safe to state that this is a fight that won't be won at any point in the near future yet in the event that cyber-criminals can misuse human vulnerabilities for 'snappy wins', IT needs to venture in and proffer security that permit to human shortcoming.

CHAPTER TWO

❖

The GAP

What is Cyber Security Gap?

Cyber security is a basic worry that touches each industry and each person, and the dangers just keeping on expanding.

In a recent review by some top cyber security companies, 52% of worldwide cyber security and IT chiefs and professionals concluded that a fourth of candidates for cyber security positions have the fundamental abilities for the vacant position. 53% said it can take three to six months just to locate a qualified candidate after taking three months to get them on board. This problem of delay begs to be addressed. How did this lack or "talent gap" occur? Are people aware of this deficiency?

At the point when the data security industry initially started to be a concentration territory, about three decades back, companies did not foresee the inconceivable progressions in technology, the quick increment in cutting edge cyber assaults and the steady need to protect sensitive information. The real headways of technology alone - from portable applications to cloud to World Wide web- has sparkled a focus on both the security vulnerabilities these advancements show, and the absence of cyber security experts who know how to fix them.

In any case, rather than trying to pull in and hold on to cyber talents, numerous associations took an option course of outsourcing their security groups. As breaks kept on increasing in both sophistication and frequency, this prompted organizations to do a change in procuring an internal group of devoted data security experts, which are difficult to find and even more difficult to keep. This move-in approach towards inner venture security made a prompt need to search out and prepare qualified security experts. Throughout the years, this requirement for qualified and talented security experts has become quicker than the workforce accessible to fill the employments, prompting to this major skill gap.

In spite of the developing expansiveness/profundity of security dangers in the ordinary organizations, it is run of the mill to locate an unstructured security group that is not giving proficient development or proceeding with instruction openings. Moreover, the couple of experts who are qualified are spread too thin and tend to wear out rapidly. This has profoundly affected the security business, which is currently observing 1 million unfilled cyber security employments in 2016 alone, and that number is projected to increase to 6 million worldwide following employment opportunities by 2019 with a projected shortfall of 1.5 million.

According to a Forbes article, if you are already in the tech field, then crossing over to security can mean a rise in pay for you. Cyber security workers can command an average salary premium of nearly $6,500 per year, or 9% more than other IT workers, according to the Job Market Intelligence.

A Forbes article noted that “For newbies in the tech field who are contemplating a career in cyber security, they will often start out as information security analysts. U.S. News and World Report ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. They state the profession is growing at a rate of 36.5% straight through 2022. Many information security analysts earn a bachelor’s degree in computer science, programming or engineering”.

Another review discharged by Intel Security with the Center for Strategic and International Studies (CSIS) investigates the cyber security workforce deficiency crosswise over eight nations including Australia, France, Germany, Israel, Japan, Mexico, the U.K., and the U.S.

Generally speaking, it affirmed that the talent shortage was genuine and boundless. The CSIS study uncovered that 82% of correspondents report a deficiency of cyber security abilities in their organizations. One in four affirmed that their organizations were casualties of cyber theft of exclusive information because of the absence of qualified workers. The analysts inspected open-source information, focused on meetings with specialists, and a review of 775 IT leaders in both public and private sector organizations in eight nations. The investigators likewise took a look at four measurements of every respondent's cyber security workforce advancement endeavors: add up to cyber security spending, training programs, business progression, and open approaches.

You might have seen the headline in the wake of the alleged hack of the 2016 electoral process by Russians were it said "Donald Trump Advised to Train 100,000 Hackers to Protect the US".

Even though the headline might have not been properly constructed, yet one should be in concurrence with the hidden point: the US President's Commission on Enhancing National Cyber security has emphatically prescribed that the nation "ought to increase … endeavors on preparing security specialists that would work for the nation and not leave for the private division, which has turned into an emotional issue in the most recent couple of years". Also, you may have seen different features, similar to this one from Forbes toward the beginning of this current year: "One Million Cyber Security Job Openings In 2016". This is an issue that is contrarily affecting governments, organizations, non-benefits, and even shoppers (lacking IT security staffing can prompt to information ruptures that uncover your data).

Taking a look at all that has been said above about the market development and occupation figures, what is there to take away? Basically, the cyber security work deficiency will deteriorate before it shows signs of improvement. Businesses need to get ready for this coming storm.

Women and minorities speak to an undiscovered asset, however they should be proactively enlisted and grasped by the cyber group before this skill gap gets out of hand again.

IT specialists can be broadly educated, however that is in the case that they are excited to do the switch - and willing to possibly venture down to passage level security positions before working themselves up to more lucrative pay. Security suppliers and IT security outsourcing firms are tested around selecting as their organizations scale, and many directed partnerships cannot hand off their security administration so effortlessly.

Even in college, students graduate from top computer science programs without taking a class in cyber security. If this is fixed, it could go a long way to help out in filling the cyber security skill gap that is getting wider by the second now. There is a large influx of tech grads who are not necessarily cyber security grads.

CHAPTER THREE

The Reasons

Why is the Cyber Security Shortage Occurring?

For a fact, there is without a doubt a deficiency of security experts.

Why is there no rush for new graduates to end up as security experts despite the fact that it is a highly monetarily remunerating vocation? Is it so hard to understand tech? Is the job exhausting, as every day includes similar issues? Do they not get regard or respect from their associates and peers? We need to ask ourselves the reason for this. Is the long haul anticipation for profession advancement not positive or promising? The generally few security experts today are moving from organization to organization for higher pay rates. It is practically as though they are as mobile as a professional soccer player.

At the entry level, there is no doubt that the technology is hard to understand. It is not as though there are essential standards to ace, as you would discover in a standard engineering discipline. Cyber security requires "on the job" adaptation, particularly since there are a wide range of obscure ways security breaches happen. We require formal techniques to assemble mastery. There are some great cases at both the school and industry level. Without more available open doors, for example, these, genuine security capability will be elusive at the entry level.

For some security analysts, the occupation is plain exhausting and redundant. You handle similar issues without stopping for even a minute, similar sorts of false positives, comparable missteps by workers, and so forth. The best way to show signs of improvement is to assemble devices and procedures, and, let's be honest, who appreciates composing process documents? There must be approaches to make the part all the more intriguing, gainful and successful so as to draw in and hold best ability. Analysts need not manage false positives and the systems ought to naturally have the capacity to manage them. Furthermore, arriving with up-to-date arrangements offering coordination and computerized reactions will help with decreasing cautions.

Security groups believe clients are the weakest connection and workers think security groups are there to keep them from doing their job. Neither one of the sides is correct, yet that is the perception. On the off chance that security groups have the devices to help clients make sense of where they are committing errors that could trade off security, it will go far in building trust inside the organizations. Clients will turn out to be more mindful. Clients will feel they have a part in security. That will likewise make the security group's occupation less demanding and additionally satisfying.

None of these issues are anything but difficult to fathom. In any case, they should be tended to in the event that we need to make security a priority not a shortcoming. Grasping new innovations that help insightfully computerize parts of security to give overpowered security groups a hand is a beginning. Be that as it may, in the long run, greater changes to security techniques should occur.

There are a few more reasons behind these shortage issues. One is the changing way of cyber-attacks. It used to be emails that were most normally focused on. For example, counterfeit messages from banks advising individuals they are expected to email their banking details to reboot their online access because of maintenance work. Others scams where individuals were advised they were to get a vast entirety of cash, yet expected to send some money first. The modernity of the technology and strategies utilized by online criminals – and their constant endeavours to rupture systems and take information – have outpaced the capacity of IT and security experts to address these dangers.

Secondly, is the Internet of Things. A bigger number of things are connecting with the Internet than individuals – a year ago there were more than 5 billion cell phones, 2 billion broadband connections and 1 billion individuals who are on Facebook and Twitter. With those gadgets come a lack of resources to bolster them. Therefore, the surface of the assault has turned out to be progressively noteworthy. The test of a security group has become fundamentally more noteworthy and will continue to increase. By 2020, there will be 50 billion gadgets that will be connected with some system and security wise, that is a little bit scary with the shortage of security personnel.

The security ability deficiency exacerbates this issue. Notwithstanding when spending plans are liberal, CISOs are attempting to contract individuals with cutting-edge security aptitudes. This year, says John Stewart, boss security officer and SVP at Cisco, the industry is short more than one million security experts over the globe. Additionally, hard to come by are security experts with information science aptitudes – as understanding and breaking down security information can enhance arrangement with business destinations.

Like it has been highlighted in the first chapter, there are different ways a system can be attacked. More of the previously mentioned viruses or attack methods are most likely to be curbed before it gets out of hand even by basic computer enthusiasts, sometimes it might be through the help of more knowledgeable professionals in the IT field. Malwares, DDOs Attacks et al are all common attacks on systems which are even usually the most encountered form of attack. However, there is a more lethal attack that has been giving even cyber security experts headache of recent. For every other attack, there is either a tool or process to curbing like has been highlighted above, but for social engineering, there has not been a verified thought pattern or process to curb it and most of the people affected by the attack even have no inkling of the problem they are facing or neither do they understand that they are under cyber-attack.

Social Engineering

We have become acquainted with the kind of attackers who leverage their specialized expertise to invade secured computer systems and trade off delicate information. We find this type of programmers in the news constantly, and we are inspired to counter their endeavours by putting resources into new innovations that will support our system defenses.

In any case, there is another sort of attacker who can utilize their strategies to skirt our devices and arrangements. They are the social engineers, hackers who exploit the one shortcoming that is found in every possible organization: human psychology. Utilizing an assortment of media, including telephone calls and web-based social networking, these assailants trap individuals into offering them access to sensitive data.

Simply put, social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering is a term that envelops a wide range of malicious movement. For the motivations behind this book, in any case, we will concentrate on the five most regular assault sorts that social designers use to focus on their casualties: phishing, pretexting, baiting, quid pro quo and tailgating.

Social engineering is just the same old thing, nothing new. In 1849, Samuel Williams, the first "confidence man," as the daily papers named him, worked guileless outsiders out of their assets basically by asking "Have you trust in me to trust me with your watch until tomorrow?" Through the late nineteenth and mid twentieth century Joseph "Yellow Kid" Weil ran an assortment of tricks, including conning Benito Mussolini out of $2 million by offering him fake rights to mining lands in Colorado. Furthermore, obviously in the 1960s, Frank Abagnale, subject of the film Catch Me If You Can, brought home the bacon faking personalities and passing terrible checks. A social engineer now runs using the same style in what used to be known as a "con game." Techniques, for example, advance to vanity, bid to power and advance to voracity are frequently utilized as a part of social engineering attacks. Numerous social engineering adventures essentially depend on individuals' ability to be useful. For instance, the attacker may profess to be a collaborator who has some sort of critical issue that obliges access to extra system assets.

There are a few methods of social engineering techniques, you might want to ask “What does social engineering look like in action? It could look like an email that has been designed to seem like it is from a credible organization, like your message administration or Fed Ex or even your bank. In any case, in the event that you open it and tap on that connection, you could introduce malware or ransomware. Then again, it could be camouflaged to seem as though it originates from somebody inside your organization (like an unusual title such as it@yourorganization – someone whom you trust). In any case, on the off chance that you react to that email with your user name and password, your computer is effectively traded off.

The idea is for you to think Before You Click.

Let’s talk more about social engineering attacks in its wholesome state. These bad folks are for the most part not attempting to exploit technical vulnerabilities in Windows. They are coming after you. "You don't require the same number of specialized aptitudes to discover one individual who may be willing, in a snapshot of shortcoming, to open up a connection that contains malevolent substance." Only around 3% of the malware they keep running into tries to abuse a technical flaw. The other 97% is attempting to trap an individual through some sort of social engineering plan, so at last, it doesn't make a difference if your workstation is a PC or a Mac.

So what are methods of social engineering attacks deployed by these attackers? Social engineering attacks come in a wide range of structures and can be performed anyplace where human collaboration is included. Below are the most basic types of advanced social engineering attacks.

- **Phishing**

The most well-known social engineering attacks originate from phishing or spear phishing and can differ with ebb and flow occasions, debacles, or expense season. Since around 91% of information breaks originate from phishing, this has turned out to be a standout amongst the most abused types of social engineering. As a standout amongst the most well-known social engineering attack types, phishing tricks are email and instant message crusades which goes to give a feeling of earnestness, interest or dread in casualties. It then nudges them into uncovering delicate data, tapping on connections to pernicious sites, or opening connections that contain malware.

A case is an email sent to clients of an online administration that alarms them of an arrangement infringement requiring prompt activity on their part, for example, a required secret word change. It incorporates a connection to an ill-conceived site—almost indistinguishable in appearance to its authentic rendition—inciting the clueless client to enter their present qualifications and new secret word. Upon shape submittal the data is sent to the assailant.

Given that indistinguishable, or close indistinguishable, messages are sent to all clients in phishing effort, identifying and blocking them are much simpler for mail servers having entry to danger sharing stages.

Most phishing tricks show the accompanying attributes:

- Look to get individual data, for example, names, locations and social security numbers.
- Utilize link shorteners or embed links that divert

clients to suspicious sites in URLs that seem genuine.

- Fuses dangers, fear and a feeling of direness trying to control the client into acting quickly under duress.

Some phishing messages are more ineffectively created than others to the degree that their messages as a rule display spelling and linguistic mistakes. However, these messages are more or less centered around guiding casualties to a fake site or shape where they can take client login qualifications and other individual data.

Here are a couple of social engineering tricks executed by means of phishing:

Banking Link Scam: Hackers send you an email with a fake connection to your bank, deceiving you into entering in your bank ID and password.

A billion-dollar heist covering 30 nations and almost a billion dollars in lost assets, nicknamed Carbanak by security firm Kaspersky, occurred in February 2015. In the Carbanak scam, spear phishing messages were sent to workers which contaminated work stations, and from that point, the hackers burrowed further into the banks' frameworks until they controlled worker stations that would permit them to make money exchanges, work ATMs remotely, change account data, and roll out authoritative improvements.

It was quite a standard plan: an email with a connection that appeared as though it was originating from an associate contained the malevolent code, which spread from that point like a computerized rhinovirus. The hackers recorded everything that occurred on the influenced PCs to figure out how the organization got things done. When they had aced the framework, they commandeered it for a progression of exchanges that incorporated the ATM hits, additionally a routine of falsely expanding bank adjusts and afterward redirecting that sum, so a client's record adjust may go from $1,000 to $10,000 and after that $9,000 would go to the programmer.

Dropbox Link Scam: Two or three varieties of this were running 2014. One was a fake Dropbox secret key reset phishing email that when clicked, drove clients to a page saying their program is obsolete and they have to redesign it (with a "button" to the update). This would dispatch a Trojan in the Zeus group of malware.

Another was an email with Dropbox joins that facilitated pernicious programming like "CryptoWall" ransomware.

We also have the spear phishing, which is a more refined or concentrated type of Phishing. This is a more focused adaptation of the phishing trick whereby an attacker picks particular people or enterprises. They then tailor their messages in light of attributes, employment positions, and contacts having a place with their casualties to make their assault less prominent. Spear phishing requires substantially more exertion for the benefit of the culprit and may take weeks and months to pull off. They're much harder to identify and have better achievement rates if done skillfully.

A spear phishing situation may include an assailant who, in imitating an organization's IT personnel, sends an email to at least one of the workers. It's worded and marked precisely as the personnel typically does, along these lines misleading employees into intuition if it's a legitimate message. The message prompts employees to change their secret word and gives them a link that sidetracks them to a malicious page where the attacker now catches their credentials.

Quid Pro Quo- Essentially, compensation attacks guarantee an advantage in return for data. This advantage more often than not expect the type of an administration, while goading much of the time appears as a decent.

A standout amongst the most widely recognized types of quid pro quo attacks include fraudsters who imitate IT service individuals and they go ahead to spam call a great number of direct numbers that have a place with an organization as they can discover. These attackers offer IT help to every single one of their casualties. The fraudsters will guarantee a quick fix in return for the worker incapacitating their AV program and use the opportunity in introducing malware on their PCs that comes in the appearance of programming upgrades.

It is essential to note that assailants can utilize a great deal less refined quid pro quo offers than IT fixes. As certifiable cases have appeared, office laborers are more than willing to give away their passwords for a shoddy pen or even a bar of chocolate.

Pretexting- Pretexting is another type of social engineering where attackers concentrate on making a decent appearance, or a manufactured situation, that they can use to attempt and take their casualties' personal data. These sorts of attacks usually appear as a con artist who pretend that they require certain bits of data from their objective keeping in mind the end goal to affirm their personality.

More advanced attacks will likewise attempt to control their targets into playing out an activity that empowers them to exploit the structural shortcomings of a company or organization. A decent case of this would be an attacker who imitates an outer IT administrations inspector and controls an organization's physical security staff into giving them access to the building.

Dissimilar to phishing messages which utilize dread and direness further bolstering their good fortune, pretexting attacks depend on building a misguided feeling of trust with the casualty. This requires the aggressor to construct a solid story that generally rules out uncertainty with respect to their objective. Pretexting attacks are usually used to increase both delicate and non-touchy data. Back in October 2016, for example, a gathering of tricksters acted like agents from displaying offices and escort administrations, concocted fake foundation stories and inquiries keeping in mind the end goal to have ladies, including high school young ladies, send them bare pictures of themselves. All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Tailgating- Another social engineering assault type is known as Tailgating or "piggybacking." These types of attacks include somebody who does not have the best possible verification going after a representative or employee into a confined region. In a typical sort of tailgating assault, a man imitates a delivery driver and holds up outside a building. At the point when a worker picks up security's approval and opens their entryway, the attacker might ask that the staff hold the door, in this manner obtaining entrance of somebody who is approved to enter into the organization or company.

Tailgating does not work in every corporate setting. For example, in bigger organizations where all people entering a building are required to swipe a card, this may not be realistic. In any case, in fair size endeavours, attackers can hit up discussions with workers and utilize this show of commonality to effectively move beyond the front work area.

Actually, Colin Greenless, a security expert at Siemens Enterprise Communications, utilized these same strategies to access a few unique floors in addition to the information room at a FTSE-recorded money related firm. He was even ready to base himself in a third floor meeting room, out of which he labored for a few days.

Baiting -Baiting can be described from numerous points of view like phishing attacks. Notwithstanding, what differentiates them from different sorts of social engineering is the guarantee of a thing that programmers use to allure casualties. Baiters may offer clients free music or motion picture downloads, on the off chance that they surrender their login qualifications to a specific website. Baiting attacks are not limited to online plans, either. Attackers can likewise concentrate on abusing human interest by means of the utilization of physical media.

One of such assaults was reported by Steve Stasiukonis, VP and originator of Secure Network Technologies, Inc., in 2006. To survey the security of a monetary customer, Steve and his group contaminated many USBs with a Trojan infection and scattered them around the association's parking garage. Inquisitive, a large portion of the customer's workers grabbed the USBs and connected them to their PCs, which actuated a keylogger and gave Steve access to some of representatives' login qualifications.

Scareware- Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem. In reality, the victim is simply tricked into downloading and installing the attacker's malware.

Why the shortage of Cyber Security Experts is hitting businesses hard

With our expanding dependence on new innovations and the steadily developing danger of cybercrime, the deficiency of gifted cyber security experts is a noteworthy concern. A late report by seek.com demonstrated the year-on-year development sought after for these specialists at 57%, and it's apparent that while organizations require experts to keep their systems and organizations secure, there is an inadequate number of talented workers accessible to fill these parts.

In Australia for example, it is nearly at a basic point. As a digital security organization, to discover products aptitudes in the market is hard. On the off chance that you can't draw in skills locally, organizations need to go overseas and discover individuals to bring into the nation.

So, what is the business danger of this deficiency? Frequently, the 'out of the picture, therefore irrelevant' mind-set becomes an integral factor and the significance of procuring a cyber-security expert is just acknowledged when it's past the point of no return. Organizations are seeing less and less confirmed staff prepared to handle these parts and enlisting full time IT security experts gets put in the "too hard" basket.

In any case, the importance of having technically savvy cyber security specialists on board to alleviate dangers is basic to the fruitful execution of any cyber usefulness inside the work environment. Cyber security ruptures are a tragic unavoidable truth and the expenses connected with them are developing widely. Here are some of the impacts:

▪ People Cost

By a wide margin, the biggest and most impactful cost of this abilities deficiency is the "General population cost". Apprehensive corporates, security merchants and governments are offering up cyber security pay rates to new highs with an end goal to pick up and hold talent of the most noteworthy calibre. Employees with demonstrated cyber security abilities are forcefully scouted and displayed offers they essentially can't refuse, including lucrative remuneration bundles, workplace advantages, adaptable hours and intensive preparing for aptitudes improvement.

Organizations that have fabricated great security groups are under a considerable pressure on the grounds that there's dependably a rival who is attempting to pull in the talent they have over to their own side. Staff maintenance is hard no matter how you look at it. Organizations need to put in counter measures.

The stream -on impact is expanded dread in organizations that lose security experts who have inside and out knowledge of their casual incident detection and reaction forms. Significant data that is frequently kept "in their heads". This alone is a key motivation to execute an Information Security Management System with archived strategies, procedures and controls, another expensive practice in itself.

- **Operational Costs**

From an operational cost point of view, organizations are perpetually swinging to technological arrangements as they explore new roads to get to clients and make progress and have upper hands over their business. In doing such, not only do organizations need to wear the expenses of enhancing their offerings to stream-line and automate processes, and to make direct (web and mobile) channels to serve and support clients, however those organizations should likewise consider the related security costs as well.

Similarly exposed to cyber security hazards inside and remotely, organizations dependent on innovative framework as their center, regularly can't bear the cost of the time and budgetary costs required on account of a cyber-intrusion.

- **Reputational cost**

Chief amongst the most hindering costs credited to this deficiency is the reputational harm connected with cyber issues. Without investing properly in cyber security experts to execute powerful danger security protection measures, organizations risks disintegration in business trust and it lessens the confidence which customers have in them, which are conceivably far more prominent expenses than absolutely money related ones.

There is no chance to get around this problem. Industries and governments must advance cyber security as an aspirational career pathway, and put resources into the improvement of gifted cyber security experts to take care of this expanding demand.

The cost of working together will keep on rising unless we stand up to the skill gap that as of now exists and put resources into building the skills of the up and coming era of IT experts. That is the reason the most brilliant organizations are proactively future-sealing against this deficiency. Internally, organizations can broadly educate existing IT workers to convert them into security experts, alongside consistently instructing the cyber security experts of tomorrow.

Pioneers in the cyber security business additionally need to effectively work with colleges to outline entry level position programs that open understudies to the security scene. Giving colleges' access to cyber security specialists who can impart their true involvement to college understudies is the path forward in lessening this aptitudes deficiency and protecting the condition of the country against digital assault. In addition, by ensuring your basic resources, client points of interest and your working frameworks form an integral part of the work. Viable digital security can likewise help associations win new business by giving confirmations of their dedication to digital security to their inventory network accomplices, partners and clients.

To accomplish genuine digital security, today's associations need to perceive that costly programming alone is insufficient to shield them from digital dangers. The three essential areas of powerful digital security are: individuals, process and innovation.

CHAPTER FOUR

The Profile

What is Needed to Thrive in the Cyber Security Field?

Apparently, all organizations are almost in the same situation, yet technology only goes so far. To thrive in this new arena, the professional will need a good training – here an InfoSec certification is paramount – but not only this. As the threats expand globally, the professional will need a strong and reliable network of professionals to share experience – mostly in privacy – to look for solutions. The professional needs to be part of a global organization dedicated to cyber and Information Security. Only an organization can provide the right training, the code of ethics, the networking for professionals to share experiences and opinions, and the tools to help them to execute their job. Skilled individuals have resorted to certain measures in a bid to ensure sensitive data in their care. Ensuring the safety of sensitive information is critical now than any other time in recent memory. Public and private sectors have started preparing and employing cyber security experts.

IT has developed from a back-office capacity to the fundamental vein that keeps an association running easily. Accordingly, bosses are not searching essentially for enlisted people who can keep up firewalls and relieve chance. They need balanced experts who can apply their security aptitude over the business keeping in mind the end goal to yield main concern comes about.

If you are thinking about a profession in cyber security, here is the skill set that different industry experts would most likely need from you and which you also need to excel in the field:

- **Strong Research and Writing Instincts:**

One of the most critical errands that endeavour cyber security groups to go up against its policy creation and enforcement is this. Recent survey showed that, 45 percent of hiring executives. They conceded to having a key security skill gap around "policy development and implementation" in their organizations. Organizations of any size and industry requires some kind of security plan that incorporates end user rules, incidence reaction protocol and administration structures. To set up sound strategies, cyber security staff must be prepared to direct thorough research into industry best practices and work with end clients to see how they utilize innovation regularly –

then blend those experiences into an astute strategy.

- **An Instructor's aura:**

Along with making strategies, cyber security experts must have the capacity to teach their colleagues about safe technology habits, and impart mindfulness about the dangers of poor IT habit. A 2015 review of full-time employees found that half don't get any kind of cyber security training at work – showing organizations' tireless requirement for interior cyber security coaches. To show significantly more value to potential employers, cyber security work seekers ought to highlight their capacity to impart thick, specialized data to others within the organization.

- **Collaboration:**

In the U.S., 49 percent of business and IT administrators rank cooperation as the top delicate expertise any IT expert ought to have. Knowing how to explore ventures and troublesome discussions with anybody from the CIO to end clients, and even merchants, is a basic quality for cyber security specialists. More lines of organizations are getting included in their associations' IT basic leadership process, and cyber security groups must have the capacity to band together with each of them successfully. A comprehensive, patient, and liberal disposition can go far when overseeing significant IT security activities crosswise over groups or office areas.

- **Consultative Thinking:**

In numerous ways, cyber security experts (even the individuals who work in-house) need to take on a similar mind-set as a consultant, whether they're advising the IT division on another investment, or helping the bookkeeping group assess the security of a cloud-application they plan to receive. Cyber security specialists ought to have the capacity to take a look at the comprehensive view and solicit the correct inquiries from their associates and senior administration keeping in mind the end goal to take care of genuine business issues. Instead of work at an absolutely strategic level, security staff ought to know how to format and layout plans that their efforts can be executed and measured against (and see how their work impacts the association's main concern.)

- **A Passion for Learning:**

To work in cyber security, you should be a lifelong student as much as an educator. The IT threat scene is always showing signs of change: today's issues run the extent from cutting edge industrious dangers to phishing and inside vulnerabilities, yet the scene could look incomprehensibly changed months or years from now. As the playing field moves from customary equipment and programming to Internet-empowered gadgets and the cloud, the nature of cyber-attacks against customers and organizations will advance. Businesses need proactive cyber security specialists who are continually investigating, and discovering approaches to stretch out beyond, tomorrow's greatest difficulties.

Ethics in Cyber Security

Ethics oversees a man's conduct. It is a basic part of any solid cyber security barrier methodology. Without clear ethical measures and standards, cyber security experts are practically undistinguishable from the dark cap hoodlums against whom they try to secure systems and information. The study of cyber security ethics, which incorporates a wide array of methodologies and schools of thought, does not offer a basic answer for the numerous complex moral issues IT experts, Chief information security officers (CISOs) and organizations confront on a daily basis.

The cyber security scene moves each year. As a growing industry, organizations are eager to fill the developing gorge of security jobs in the midst of a genuine setback of lack of skilled graduates. In this frenetic atmosphere, we tend to concentrate on building up people's cyber security know how and ability and putting them on the front line as fast as could be expected under the circumstances. In the distraught surge, we frequently neglect to consider how newcomers could conceivably manhandle these capacities at work or in nature. Lacking proper context on cyber security ethics, people must concede to their own ethical compass. This prompts to great choices as regularly as it prompts to bad choices equally.

In what capacity can administration imbibe the highest of cyber security ethical models and intrinsic qualities? Per chance that your organization has not done such as of now, you ought to unequivocally think about actualizing an ethical practice policy, rules as well as codes of conduct for your IT and security staff to take after. Audit this policy frequently with regards to accessible industry rules and best practices. Subsequent to detailing a reasonable arrangement, make certain to draw in your workers in the ethics discussion by offering training and guidance.

Indeed, even the most ethical and very technical of cyber security teams cannot prevent a very determined attacker. It is wise, along these lines, to completely get ready for cyber security occurrences. This requires a very much prepared incidence reaction plan that includes the technical points of interest, handy guidelines for official and legal team, and any key ethical considerations.

Harrowing Headlines

Aside their employees, organizations themselves must satisfy certain moral and lawful commitments in case of a security incident, especially an information breach. Time is without a doubt a key factor in reacting to cyber-attacks. However, telling clients and customers about any genuine, immediate ramifications, for example, stolen information and credentials, is likewise a vital part of the incident response process. At the point when an organization leaves the general population oblivious after a disastrous breach, customers stay helpless.

At the point when an organization's information is traded off, it might confront lawsuits, reputational harm and questions regarding its ethical benchmarks. Delaying an open declaration can aggravate these consequences. Those in charge of administering data security practices inside organizations, for example, CISOs and supporting executive management, must be engaged fully and show others how it’s done to cause a culture of high ethical standards.

Where do White Hats Draw the Line?

Outside of college courses and industry certifications, there is minimal institutionalized training or formal accreditation required to fill in as a cyber-security professional, yet they confront day by day ethical predicaments exceptional to their profession. Cyber security experts are the technological watchmen in their respective organizations, endowed with incredible duty and the abnormal amounts of access expected to complete their parts adequately.

White hats work with delicate information, come across organization secrets and wield extraordinary control over PC networks, applications and frameworks. How an individual deals with this power comes down to his or her own moral measuring stick, which is the reason organizations should precisely choose security specialists who display adequate standards and specialized competency. Be that as it may, is this enough? Can we put our trust in our regarded experts?

Without classified cyber security ethical rules set up at the industry and employer levels, it is to a great extent up to the person in charge to decide the most morally solid reaction to a given episode.

Ethics can be subjective, impacted by an individual's experience, culture, education, personality and other different components. Some white-hat hackers, for instance, have no issue coolly testing their telephone company's billing platform for vulnerabilities. By poking openings in the telephone providers' security framework, they believe they are honestly adding to the benefit of the common good of cyber security.

Others may view these exercises as criminal, or if nothing else unethical, well-meaning or not.

Hats of All Colours

Indeed, even the lines between the distinctive shades of the hacker spectrum — white hat, grey cap, black cap, and so on can be a bit hazy. Truth be told, black and white hat hackers frequently utilize similar tools and techniques to accomplish vastly different finishes. This muddies the ethical waters of cyber security much additionally, making it hard to decide precisely where the ethical line falls with regards to delivering productive, genuine and morally solid security research.

While legitimate, medical, accounting and other established professions have lawfully restricting implicit rules supervised by longstanding administrative bodies, IT security experts have yet to set up formal direction or general governing rules. The industry does not have an independent register to figure out who can practice ethical hacking or security investigation.

Cyber security pioneers must depend on reputation and individual verifications alone to decide the dependability of potential employees. In the event that IT experts deceive this trust by acting unscrupulously, there is no outsider panel or board to assess the results of these activities and administer with regards to the calling all in all. Rebel security experts can't be struck off the list or expelled from a database, on the grounds that such a database does not exist.

A few affiliations, for example, (ISC)² have volunteered to handle representing ethical issues in IT and cyber security. Notwithstanding, industry experts are once in a while required to subscribe to these bodies or hold fast to their sets of accepted rules.

Movie Plot Hacking and Real Life Challenges

In the principal scene of "Mr. Robot," the Emmy-selected, cybercrime-themed anecdotal TV arrangement, the show's hero, Elliot, a disappointed cyber security guy working in New York, confronts a basic moral choice at work. The character, played by Rami Malek, goes over a suspicious record on a customer's bargained server when diagnosing a circulated foreswearing of-administration (DDoS) assault. This irregular record has a baffling message for Elliot: "leave me here."

In this essential snapshot of the show, Elliot can decide to either erase the record (the moral choice) or abandon it on the customer's server. Charmed, Elliot acts dishonestly and leaves the record on the server without telling his episode reaction group, administration or the server proprietor. This choice is the impetus whereupon the entire story bend pivots, prompting to the hero's contribution with the baffling illicit cybercrime pack society and a huge information break for the critical customer.

While the delineation of cyber security morals in "Mr. Robot" is a to some degree overdramatic Hollywood version, it is not absolutely unlike this present reality moral difficulties security experts regularly experience in the field. Through both consider and inadvertent activities, a cyber-security expert can mismatch the regularly mind boggling and fragile moral line. Like Malek's character in "Mr. Robot," even the littlest preoccupation in the subtleties of moral basic leadership could open a container of worms with extensive results, conceivably putting the business, client base and individual at hazard.

Security scientist and One World Labs originator Chris Roberts stood out as truly newsworthy in 2015 in the wake of tweeting that he was thinking about doing a live infiltration trial of his household United Airlines flight to Syracuse, New York. Roberts, who was the subject of a FBI sworn statement, purportedly held a Boeing air ship by messing with the push administration PC through its in-flight entertainment framework, making "one of the plane engines to climb, bringing about a horizontal or sideways movement" of the aircraft.

It is arguable that Roberts proposed to debilitate or hurt himself, carrier staff or alternate travellers on-board. Regardless of evident white-hat intentions, be that as it may, the results of

Roberts' charged activities against such basic frameworks could have been grave.

After the story broke, a few prominent cyber security experts talked freely about the questionable morals and legalities at play. As indicated by Business Insider, Alex Stamos, then CISO at Yahoo, tweeted, “You cannot promote the (true) idea that security research benefits humanity while defending research that endangered hundreds of innocents.."

Education, Awareness and Outreach

While a profoundly incorporated code of cyber security ethics and lead is fundamental, it is likewise critical to develop ethical lessons among students and young understudies — the security experts of tomorrow. By advancing their attention to cyber security ethics at the early phases of learning and professional development, we can guarantee that future white caps remain on the correct side of the ethical gap.

Bug bounties and hacking competition give moral sandboxes where maturing youthful hackers and senior professionals can mess around and challenge themselves. Many major organizations, including Facebook, Google and a few prominent airlines, offer crowd sourced bug bounty programs in which programmers are remunerated for finding vulnerabilities in chosen targets. This model enhances the security of the organization's benefits while offering a characterized structure and rules under which eager global security experts can lawfully hack, learn and receive nice looking benefits.

Cyber security devotees can likewise utilize an assortment of purposely powerless recreation stages to learn entrance testing abilities inside a protected domain. It is imperative that such training instruments furnish clients with the essential moral setting to guarantee that their lessons are not lost.

Who do we fault?

Youthful maverick programmers regularly fall under the control of law implementation when directing exercises against genuine, clueless targets. Many argue numbness, affirming that they didn't understand the exercises were unlawful.

Who is at fault in these circumstances? Sometimes, hacking devices, including those that add to DDoS botnet attacks, are a piece of the issue. Regularly, at a centre level, this product has turned out to be so natural to utilize that it empowers unwitting beginners to conjure conceivably unlawful harm over the web with only a solitary mouse click.

Then again, numerous programmers have purposely crossed moral limits with numbness missing the mark as a safeguard. In the event that a youthful cyber security aficionado carried on deceptively in his or her adolescent hacking past yet demonstrates a promising future, would he be able to or she be trusted by a potential manager? Regardless of the prominent interest for cyber security experts, associations are typically reluctant to procure skilled ex-dark caps.

CHAPTER FIVE

A Global Body

Why should you trust (ISC)^2

(ISC)^2 is an international non-profit membership association focused on inspiring a safe and secure cyber world. The company is best known for its acclaimed Certified Information Systems Security Professional (CISSP) certification, (ISC)^2 offers a portfolio of credentials that are part of a holistic, programmatic approach to security. They have a membership of over 123,000 individuals in more than 160 countries. (ISC)^2 is the largest not-for-profit membership body of certified information and software security professionals worldwide. It is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. The company's vision is supported by their commitment to educate and reach the general public through a charitable foundation they run- The Center for Cyber Safety and Education.

(ISC)² certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK, a compendium of information security topics. The (ISC)² Foundation is a non-profit charitable trust that aims to empower students, teachers and the general public to secure their online life by supporting cyber security education and awareness in the community, including industry research like the (ISC)² Global Information Security Workforce Study, through its programs and the efforts of its members. (ISC)² was the first information security certifying body to meet the requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for personnel certification. To date, the CAP, CSSLP, SSCP, CISSP and the CISSP concentrations have been accredited against this standard, making (ISC)² credentials a must-have among professionals and employers.

There are very few cyber security institutions out there, but with over 25 years of service, students are in great hands with (ISC)². The company which reflects on the achievements of its founders and members and how they have help shaped the information security profession. The company's vision is to inspire a safe and secure cyber world, and their mission is to support and provide members and constituents with credentials, resources, and leadership to address cyber, information, and software and infrastructure security to deliver value to society.

As organizations are increasingly recognizing information security as imperative, (ISC)² members are in greater demand than ever before. With the majority of security breaches attributed to human error, (ISC)² believes in focusing beyond hardware and software as sole solutions to these problems. The company understands the need to rely on another approach: professionalizing the information security workforce.

(ISC)² is dedicated to professionalizing the cyber security workforce by providing organizations with the assurance that their staff has been tested on industry best practices and possess broad knowledge of their fields along with sound professional judgment. This is why our certifications are required or preferred for many cyber, information, software, and infrastructure security jobs around the world.

Training Delivery Methods

(ISC)² understands the importance of dynamism in the method in which they deploy in educating their members. The Official (ISC)² CBK Training Seminars are available in a classroom-based, live online, private on-site, or on demand setting:

Official (ISC)^2 Education, Classroom-based Training

Attend a Multi-Day Classroom-based Training Seminar

Delivered in a classroom setting over the course of 3-5 days for 8 hours a day, the Official (ISC)^2 CBK Training Seminars are available at (ISC)^2 facilities and (ISC)^2 Official Training Providers worldwide. Led by authorized instructors, these training seminars are perfect for hands-on learners and are the most comprehensive review of the certification’s CBK, industry concepts, and best practices.

Each training program features:

- Up-to-date courseware
- Taught by an authorized (ISC)^2 instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios
- Interactive and engaging learning techniques

Training Seminars

CERTIFICATION	# OF DAYS
CISSP	5 days
SSCP	5 days
CAP	5 days
CSSLP	5 days
CCFP	5 days
HCISPP	3 days
CCSP	5 days
CISSP-ISSAP	4 days
CISSP-ISSEP	4 days
CISSP-ISSMP	5 days

Official (ISC)^2 Education, Private On-site Training

(ISC)^2's private on-site training provides a cost-effective and convenient training solution for organizations with 10 or more employees planning to sit for an (ISC)^2 certification examination. Private on-site CBK training seminars are led by (ISC)^2-authorized instructors and are conveniently taught in your office space or a local venue.

An (ISC)^2 dedicated account executive will serve as a training advisor and will ensure that your private training seminar fits your schedule, budget, and certification requirements.

Private, on-site training features:

- Up-to-date, official (ISC)^2 courseware
- Taught by an (ISC)^2-authorized instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios
- Interactive and engaging learning techniques

Exam scheduling assistance through Pearson Vue or mobile testing at your location

Official (ISC)² Education, Live Online Training

Participate in (ISC)² CBK training from the convenience of your computer! (ISC)²'s Live online training saves you travel time and expense. Led by (ISC)² authorized instructors, these trainings are the most comprehensive review of the CBK. Live online Seminars are delivered with a variety of schedules to suit your needs:

- Weekday courses delivered in 8-hour sessions over 3-5 days
- Weekend courses delivered in 8-hour sessions over 3-5 weekend days
- Evening courses delivered in two 2.5-hour sessions per week over 5-8 weeks

(ISC)² Live Online CBK Training Seminars feature:

- An (ISC)² authorized instructor
- Official (ISC)² courseware
- An (ISC)² student handbook in PDF format
- Real-world case studies and examples
- Access to recordings of all course sessions for 60 days

Live Online courses utilize VOIP, when you become a member, you should ensure you have access to a computer with speakers and a microphone to maximize your participation!

Official (ISC)² On Demand Training

Learn at Your Own Pace

Training Seminars On Demand

(ISC)² On Demand Training is a self-paced learning solution delivering modular training combined with interactive study materials, giving you a powerful alternative to traditional classroom training. With On Demand, you can spend extra time on material and reinforce concepts with flash cards, quizzes, and games.

Compelling: Virtual lessons taught by (ISC)² authorized instructors through HD video.

Comprehensive: Rich content equivalent to classroom training that meets certification course requirements, including interactive flashcards and games, reference materials, and sample exam questions throughout the courseware.

Convenient: 120 days to access the content from any web-enabled device at any time and as often as you want.

This learning solution is currently available for CISSP and CCSP.

What the (ISC)^2 Certification is for?

Why You Need (ISC)^2

So, you might as well be asking the question ‘What are the benefits of learning at (ISC)^2? To become certified, it is more than just passing an exam. Candidates must meet an experience requirement and be endorsed by an (ISC)^2 member, confirming their professional experience.

One major reason you need (ISC)^2 is because of their drive. The (ISC)^2 programs are designed to cover current global topics and also certifications which are industry focused and industry driven. They always ensure their certifications remain very relevant, as they update the certification and the process as a whole every two to three years by conducting a job task analysis (JTA). Required or Preferred by the Most Security Conscious Organizations (ISC)^2 certifications are listed on the most job boards for security positions. Seven of our certifications are listed on the U.S. DoD Directive 8570.1.

Other than the above mentioned point, when you become certified through (ISC)^2, you gain:

- Tested and verifiable proof of proficiency in your field.
- Higher salary and promotion potential.

Entry into one of the largest communities of recognized information security professionals in the world.

Access to unparalleled global resources, peer networking, mentoring, and a wealth of ongoing information security opportunities.

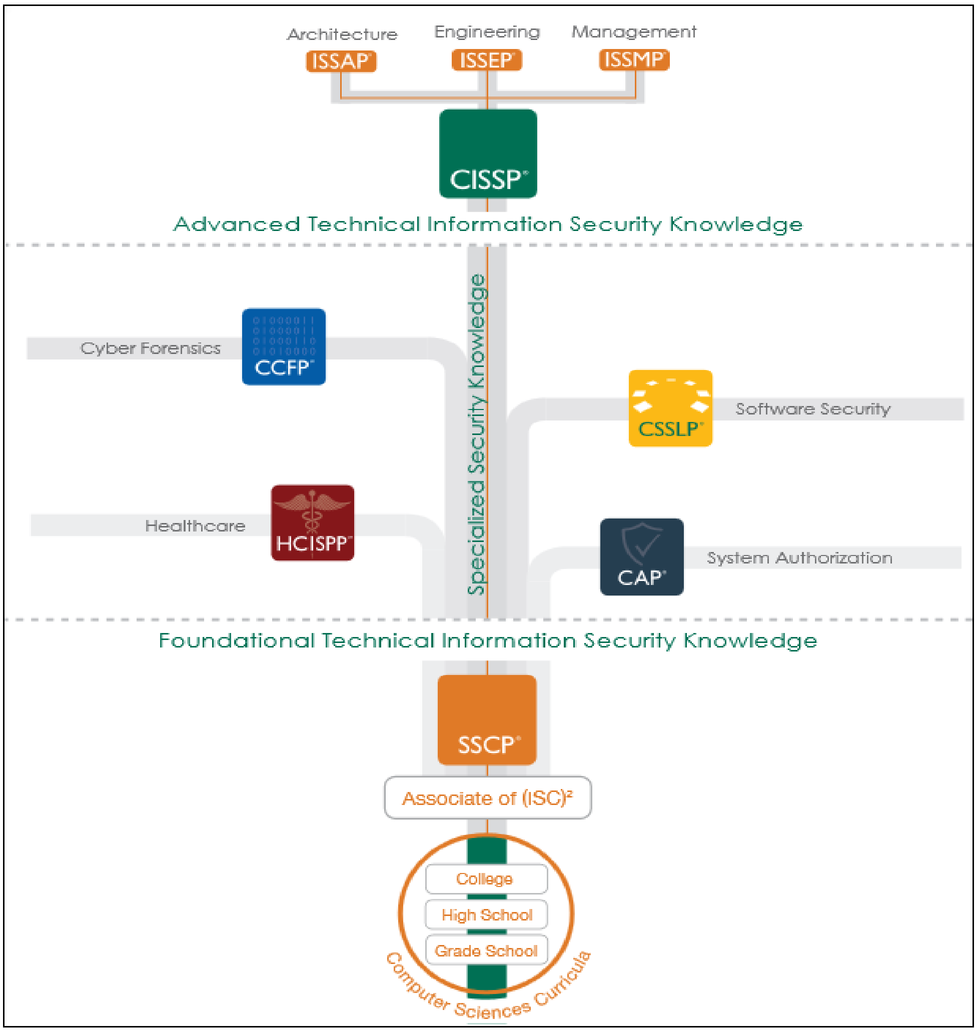
The Certification Process at (ISC)²

Why Certification Matters

In a world fraught with security threats, the need for skilled and knowledgeable information security professionals has never been greater. Your experience in the field is an important component of your value to an employer, but experience isn’t enough. Employers need something quantifiable and verifiable to show them you have the expertise they need.

(ISC)² is acknowledged as the global, not-for-profit leader in educating and certifying information security professionals throughout their careers. Our reputation has earned our information security certifications and information security training programs recognition as the Gold Standard of the industry.

The Career Path to (ISC)²



The (ISC)² Career Path is designed to cover a wide range of job functions within the information security organization. If you are the hands-on practical type the credentials we suggest to enhance your career will be very different from those we offer a candidate who intends to pursue a managerial or governance position. Hiring first-rate information security personnel is now critical to mitigating risks that can destroy a company's reputation, violate a consumer’s privacy, result in the theft or destruction of intellectual property, and, in some cases, endanger lives.

Driven by increasing regulations and the desire to maximize global commerce opportunities, protecting information assets has become one of the most important functions within any organization, public or private. For this reason, organizations increasingly rely on information security professionals to implement a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions. These controls need to be established, implemented, monitored, reviewed and continually improved to ensure that the specific security and business objectives of the organization are met.

Certification Courses you will go through at (ISC)²

The courses currently ran at the (ISC)² are universally recognized as the Gold Standard in information security certifications, our credentials are essential to both individuals and employers for the seamless safety and protection of information assets and infrastructures. All the courses are expatiated below with all requirements that needs to be met by individuals;

CISSP

CISSP® - Certified Information Systems Security Professional

This particular program is for the next generation of information security leaders all around the world.

The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.

Backed by (ISC)², the globally recognized, non-profit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.

So, who should obtain the CISSP certification?

The CISSP is ideal for those working in positions such as, but not limited to:

- Security Consultant
- Security Manager
- IT Director/Manager
- Security Auditor
- Security Architect
- Security Analyst
- Security Systems Engineer
- Chief Information Security Officer
- Director of Security
- Network Architect

The CISSP draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices. The CISSP exam tests one's competence in the 8 domains of the CISSP ***CBK, which cover:***

- Security and Risk Management

- Asset Security
- Security Engineering
- Communications and Network Security
- Identity and Access Management
- Security Assessment and Testing
- Security Operations
- Software Development Security

CISSP Exam Information

The CISSP Exam Information	Requirements
Length of exam	6 hours
Number of questions	250
Question format	Multiple choice and advanced innovative questions
Passing grade	700 out of 1000 points
Exam availability	English, French, German, Brazilian Portuguese, Spanish, Japanese, Simplified Chinese, Korean, Visually impaired
Testing Center	Pearson Vue Testing Center

Study tools

- Official (ISC)² Guide to the CISSP CBK Textbook
- Official (ISC)² CISSP Study Guide
- CISSP for Dummies
- CISSP Practice Tests
- Official Study App
- Exam Outline
- Official (ISC)² Training
- Interactive Flashcards

How to Get Your CISSP® Certification

Here are the steps to become a CISSP:

- Obtain the Required Experience

Candidates must have a minimum of 5 years cumulative paid full-time work experience in two or more of the 8 domains of the (ISC)² CISSP CBK®. Candidates may receive a one-year experience waiver with a 4-year college degree, or regional equivalent or additional credential from the (ISC)² approved list, thus requiring four years of direct full-time professional security work experience in 2 or more of the 8 domains of the CISSP CBK.

Don't have the experience?

Become an Associate of (ISC)^2 by successfully passing the CISSP exam. You'll have 6 years to earn your experience to become a CISSP.

CISSP-ISSAP

CISSP®-ISSAP®: Information Systems Security Architecture Professional

CISSP-ISSAP requires a candidate to demonstrate 2 years of professional experience in the area of architecture and is an appropriate credential for Chief Security Architects and Analysts who may typically work as independent consultants or in similar capacities. The architect plays a key role within the information security department with responsibilities that functionally fit between the C-suite and upper managerial level and the implementation of the security program. The candidate would generally develop, design, or analyze the overall security plan. Although this role may typically be tied closely to technology, it may be fundamentally closer to the consultative and analytical process of information security.

Who should obtain the ISSAP certification?

The ISSAP is ideal for CISSPs working in positions such as, but not limited to:

- System architect

- Chief technology officer
- System and network designer
- Business analyst
- Chief security officer

To qualify for the CISSP-ISSAP, you must have at least 2 years of cumulative paid, full-time professional work experience in the area of architecture, maintain your CISSP credential in good standing, and pass the ISSAP examination.

What domains are in the ISSAP CBK?

The ISSAP examination domains and weights are:

Domains	Weights
Access Control Systems & Methodology	21%
Communications & Network Security	22%
Cryptography	11%
Security Architecture Analysis	25%
Technology Related Business Continuity Planning (BCP) & Disaster Recovery Planning(DRP)	11%
Physical Security Considerations	10%

ISSAP Exam Information

ISSAP Exam Information	Requirements
Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out English of 1000 points
Exam Language	English
Testing Center	Pearson Vue Testing Center

CISSP-ISSMP

CISSP®-ISSMP®: Information Systems Security Management Professional

This concentration requires that a candidate demonstrate two years of professional experience in the area of management on a large enterprise-wide security model. This concentration contains deep managerial elements, such as project management, risk management, setting up and delivering a security awareness program, and managing a business continuity planning program. A CISSP-ISSMP establishes, presents, and governs information security programs demonstrating management and leadership skills. Typically, the ISSMP certification holder or candidate will construct the framework of the information security department and define the means of supporting the group internally. ISSMPs have a far better-rounded and complete comprehension of information security than other popular management credentials.

Who should obtain the ISSMP certification?

The ISSMP is ideal for CISSPs working in positions such as, but not limited to:

- Chief information officer
- Chief information security officer
- Chief technology officer
- Senior security executive

To qualify for the ISSMP, you must have at least 2 years of cumulative paid, full-time professional work experience in the area of management, maintain your CISSP credential in good standing, and pass the ISSMP examination.

What domains are in the ISSMP CBK?

The ISSMP examination domains and weights are:

Domains	Weights
Security Leadership and Management	38%
Security Lifecycle Management	21%
Security Compliance Management	14%
Contingency Management	12%
Law, Ethics and Incident Management	15%

ISSMP Exam Information

ISSMP Exam Information	Requirements
Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English
Testing Center	Pearson Vue Testing Center

CISSP-ISSEP

❖

CISSP®-ISSEP®: Information Systems Security Engineering Professional

The CISSP-ISSEP certification is for CISSPs who specialize in the practical application of systems engineering principles and processes to develop secure system.

ISSEP Course Overview

Led by an (ISC)² authorized instructor, the Official (ISC)² CBK Training Seminar for the ISSEP provides a comprehensive review of information security concepts and industry best practices, covering the 4 domains of the ISSEP CBK:

- Systems Security Engineering
- Certification and Accreditation (C&A) / Risk Management Framework (RMF)
- Technical Management
- U.S. Government Information Assurance Related Policies and Issuances

Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

This training course will help candidates review and refresh their information security knowledge and help identify areas they need to study for the ISSEP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Who should attend?

This course is intended for CISSPs who have at least 2 years of recent full-time professional work experience in engineering and are pursuing ISSEP training and certification to demonstrate mastery in security engineering to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to:

- Senior systems engineer
- Information assurance systems engineer
- Information assurance officer
- Information assurance analyst
- Senior security analyst

Learning Objectives

With a primary focus on the U.S. government policy and regulations, this course examines the process that is applied throughout the life cycle of the systems that comprise the ISSE model and ensures that security is included in these systems. After completing this course, participants will be able to:

- Describe concepts related to how certification and accreditation and risk management framework processes are applied and integrated/implemented with systems security engineering
- Explain the details of technical management, including how to design, implement, and execute technical aspects related to systems security engineering
- Describe how U.S. Government Information Assurance laws, regulations, policies, and standards apply to information systems security

- Apply knowledge of systems security engineering to protect organizational information through a process, which includes identifying needs, designing the architecture, developing systems security requirements, and implementing those requirements.

The ISSEP examination domains and weights are:

Domains	Weights
System Security Engineering	50%
Certification and Accreditation (C&A)/Risk Management Framework (RMF)	15%
Technical Management	15%
U.S. Government Information Assurance Related Policies and Issuances	20%

ISSEP Exam Information

ISSEP Exam Information	Requirements
Length of exam	3 hours
Number of questions	150
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English
Testing center	Pearson Vue Testing Center

Study tools

- Official (ISC)^2 Training Seminar
- Exam outline

SSCP

❖

SSCP® - Systems Security Certified Practitioner

The SSCP certification is the ideal credential for those with proven technical skills and practical security knowledge in hands-on operational IT roles. It provides industry-leading confirmation of a practitioner's ability to implement, monitor and administer IT infrastructure in accordance with information security policies and procedures that ensure data confidentiality, integrity and availability.

The SSCP indicates a practitioner's technical ability to tackle the operational demands and responsibilities of security practitioners, including authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, malicious code countermeasures, and more.

The SSCP is ideal for those working in or towards positions such as, but not limited to:

- Network Security Engineer
- Systems/Network Administrator

- Security Analyst
- Systems Engineer
- Security Consultant/Specialist
- Security Administrator
- Systems/Network Analyst
- Database Administrator

The course is globally recognized proficiency in information security and it is offered by (ISC)^2, the world leader in educating and certifying security professionals worldwide, SSCPs benefit from a global network of certified members and valuable resources and support to help them to continually develop and advance in their careers.

The SSCP credential draws from a comprehensive, up-to-date global body of knowledge that ensures candidates have the right information security knowledge and skills to be successful in IT operational roles. It demonstrates competency in the following ***CBK Domains:***

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring, and Analysis

- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security

SSCP Exam Information

The SSCP Exam Information	Requirements
Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam languages	English, Japanese, and Brazilian Portuguese
Testing Center	Pearson Vue Testing Center

Study tools

- Official (ISC)² Guide to the SSCP CBK Textbook
- Official (ISC)² SSCP Study Guide
- Official Study App

- Official (ISC)² Training
- Exam Outline
- Interactive Flashcard

CAP

CAP® - Certified Authorization Professional

The Certified Authorization Professional (CAP) certification is an objective measure of the knowledge, skills and abilities required for personnel involved in the process of authorizing and maintaining information systems. Specifically, this credential applies to those responsible for formalizing processes used to assess risk and establish security requirements and documentation. Their decisions will ensure that information systems possess security commensurate with the level of exposure to potential risk, as well as damage to assets or individuals.

The CAP credential is appropriate for commercial markets, civilian and local governments, and the U.S. Federal government including the State Department and the Department of Defense (DoD). See CAP and DoD 8570. Job functions such as authorization officials, system owners, information owners, information system security officers, and certifiers as well as all senior system managers apply.

The ideal candidate should have experience, skills or knowledge in:

- IT security
- Information assurance
- Information risk management
- Certification
- Systems administration
- 1-2 years of general technical experience
- 2 years of general systems experience
- 1-2 years of database/systems development/network experience
- Information security policy
- Technical or auditing experience within government, the U.S. Department of Defense, the financial or health care industries, and/or auditing firms
- Strong familiarity with NIST documentation

The CAP examination tests the breadth and depth of a candidate's knowledge by focusing on the 7 domains of the ***CAP CBK:***

- Risk Management Framework (RMF)

- Categorization of Information Systems
- Selection of Security Controls
- Security Control Implementation
- Security Control Assessment
- Information System Authorization
- Monitoring of Security Controls

CAP Exam Information

The CAP Exam Information	Requirements
Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English
Testing Center	Pearson Vue Testing Center

Study tools

- Official (ISC)^2 Guide to the CAP CBK Textbook

- Official (ISC)^2 training seminar,
- Interactive Flashcards,
- Exam outline

CSSLP

❖

CSSLP® - Certified Secure Software Lifecycle Professional

Attackers and researchers continue to expose new application vulnerabilities, and it's no wonder that application vulnerabilities are ranked the #1 threat to cyber security professionals (according to the 2015 (ISC)² Global Information Security Workforce Study). Web application security must be a priority for organizations to protect their business and reputation. For this reason, it is crucial that anyone involved in the software development lifecycle (SDLC) be knowledgeable and experienced in understanding how to build secure software.

The CSSLP certification validates software professionals have the expertise to incorporate security practices – authentication, authorization and auditing – into each phase of the SDLC, from software design and implementation to testing and deployment.

CSSLPs have proven proficiency in:

- Developing an application security program in their organization
- Reducing production costs, application vulnerabilities and

delivery delays

- Enhancing the credibility of their organization and its development team
- Reducing loss of revenue and reputation due to a breach resulting from insecure software

Who should obtain the CSSLP certification?

The Certified Secure Software Lifecycle Professional (CSSLP) is for everyone involved in the SDLC with at least 4 years of cumulative paid full-time work experience in 1 or more of the 8 domains of the CSSLP CBK. CSSLPs often hold positions such as the following:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst

- Project Manager
- Security Manager
- IT Director/Manager

Don't have the application security experience to earn your certification? Earn your experience to become a CSSLP as an Associate of (ISC)^2 by successfully passing the CSSLP exam. You'll have up to 5 years to earn your experience.

The CSSLP draws from a comprehensive, up-to-date, global common body of knowledge that ensures software professionals have deep knowledge and understanding of how to build secure software. CSSLP tests one competence in the following 8 domains:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Coding
- Secure Software Testing
- Software Acceptance
- Software Deployment, Operations, Maintenance and Disposal

- Supply Chain and Software Acquisition

CSSLP Exam Information

CSSLP Exam Information	Requirements
Length of exam	4 hours
Number of questions	175
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English
Testing Center	Pearson Vue Testing Center

Study tools

- Official (ISC)^2 Guide to the CSSLP CBK,
- Official (ISC)^2 training seminar,
- CSSLP eLearning,
- Interactive Flashcards,
- Exam outline

CCFP

❖

CCFP® - Certified Cyber Forensics Professional

The evolving field of cyber forensics requires professionals who understand far more than just hard drive or intrusion analysis. The field requires CCFP professionals who demonstrate competence across a globally recognized common body of knowledge that includes established forensics disciplines as well as newer challenges, such as mobile forensics, cloud forensics, anti-forensics, and more.

The CCFP credential indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible in a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response. In other words, the CCFP is an objective measure of excellence valued by courts and employers alike.

Who should obtain the CCFP credential?

CCFP addresses more experienced cyber forensics professionals who already have the proficiency and perspective to effectively apply their cyber forensics expertise to a variety of challenges. In fact, many new CCFP professionals likely hold one or more other digital forensics certifications.

Given the varied applications of cyber forensics, CCFP professionals can come from an array of corporate, legal, law enforcement, and government occupations, including:

- Digital forensic examiners in law enforcement to support criminal investigations
- Cybercrime and cybersecurity professionals working in the public or private sectors
- Computer forensic engineers & managers working in corporate information security
- Digital forensic and e-discovery consultants focused on litigation support
- Cyber intelligence analysts working for defense/intelligence agencies
- Computer forensic consultants working for management or specialty consulting firms.

For those who qualify, the CCFP exam will test their competence in the 6 CCFP domains of the (ISC)² CBK, which cover:

- Legal and Ethical Principles
- Investigations
- Forensic Science
- Digital Forensics
- Application Forensics
- Hybrid and Emerging Technologies

Candidates must have a 4-year college degree leading to a Baccalaureate, or regional equivalent, plus 3 years of cumulative paid full-time digital forensics or IT security experience in 3 out of the 6 domains of the credential.

Those candidates who do not hold a 4-year college degree leading to a Baccalaureate, or regional equivalent, must have 6 years of cumulative paid full-time digital forensics or IT security experience in 3 out of the 6 domains of the credential. Candidates without the required degree may receive a 1-year professional experience waiver for holding an alternate forensics certification on the (ISC)² approved list.

Don't yet have the necessary experience? If you're working on building your experience right now, you may earn the Associate of (ISC)² designation by passing the required CCFP examination.

Exam Availability

The CCFP exam is available worldwide with regional adaptation for the following countries/regions:

- European Union (CCFP-EU): offered in English and German languages
- India (CCFP-IN): offered in English language
- South Korea (CCFP-KR): offered in Korean language
- United States (CCFP-US): offered in English language

CCFP Exam Information

CCFP Exam Information	Requirements
Length of exam	4 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Availability	The CCFP exam is available worldwide with regional adaptation for the following countries/regions: • European Union (CCFP-EU): offered in English and German languages • India (CCFP-IN): offered in English language • South Korea (CCFP-KR): offered in Korean language • United States (CCFP-US): offered in English language
Testing Center	Pearson Vue Testing Center

HCISSP

HCISPP® - HealthCare Information Security and Privacy Practitioner

As the rapidly evolving healthcare industry faces increasing challenges to keeping personal health information protected, there is a growing need to ensure knowledgeable and credentialed security and privacy practitioners are in place to protect this sensitive information.

HCISPPs provide the front-line defense in protecting health information. Backed by (ISC)², a global not-for-profit organization that delivers the gold standard for information security certifications, the HCISPP credential confirms a practitioner’s core knowledge and experience in security and privacy controls for personal health information.

What domains are in the HCISPP CBK?

The HCISPP exam will test the candidate's knowledge in the 6 domains of the (ISC)² HCISPP CBK, which cover:

- Healthcare Industry
- Regulatory Environment

- Privacy and Security in Healthcare
- Information Governance and Risk Management
- Information Risk Assessment
- Third Party Risk Management

HCISPP candidates must have a minimum of two years of cumulative paid full-time work experience in one domain of the credential with the exception that one year of the cumulative experience must be in any combination of the first three domains in Healthcare (Healthcare Industry, Regulatory Environment, and Privacy and Security in Healthcare). The remaining one year of experience can be optionally in any of the remaining three HCISPP domains (Information Governance and Risk Management, Information Risk Assessment, and Third-Party Risk Management), and does not have to be related to the healthcare industry. Learn more.

Who should obtain the HCISPP certification?

HCISPPs are at the forefront of protecting patient health information. These are the practitioners whose foundational knowledge and experience unite healthcare information security and privacy best practices and techniques under one credential to protect organizations and sensitive patient data against emerging threats and breaches. HCISPPs are instrumental to a variety of job functions, including:

- Compliance officer
- Information security manager
- Privacy officer
- Compliance auditor
- Risk analyst
- Medical records supervisor
- Information technology manager
- Privacy and security consultant
- Health information manager
- Practice manager

Who should employ HCISPPs?

Solidify a frontline defense with qualified, experienced, and credentialed healthcare information security and privacy practitioners. HCISPPs are instrumental to a variety of employers, including:

- Hospitals
- Health centers and clinics

- Group practices
- Privacy and security consulting firms
- Regulatory agencies
- Claims processors
- Health clearing houses

HCISPP Exam Information

HCISPP Exam Information	Requirements
Length of exam	3 hours
Number of questions	125
Question format	Multiple choice questions
Passing grade	700 out of 1000 points
Exam Language	English

Study tools

- Official (ISC)² Guide to the HCISPP CBK Textbook,
- Official (ISC)² training seminar,
- Exam outline,
- Interactive Flashcards

CCSP

CCSP® - Certified Cloud Security Professional

As powerful as cloud computing is for the organization, understanding its information security risks and mitigation strategies is critical. Legacy approaches are inadequate, and organizations need competent, experienced professionals equipped with the right cloud security knowledge and skills to be successful. They need CCSPs.

Backed by the two leading non-profits focused on cloud and information security, the Cloud Security Alliance (CSA) and (ISC)², the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

Who should obtain the CCSP credential?

The CCSP credential is designed for experienced information security professionals with at least five years of full-time IT experience, including three years of information security and at least one year of cloud security experience. The CCSP credential is suitable for mid-level to advanced professionals involved with IT architecture, web and cloud security engineering, information security, governance, risk and compliance, and even IT auditing.

CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. In other words, CCSPs are heavily involved with the cloud. Many CCSPs will be responsible for cloud security architecture, design, operations, and/or service orchestration.

Example job functions include, but are not limited to:

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager

- Systems Architect

CCSP is a global credential born from the expertise of the two industry-leading stewards of information systems and cloud computing security, (ISC)² and CSA. The CCSP credential is appropriate and applicable to cloud security in a global environment. This is especially important given the legal, regulatory and compliance concerns that come with multi-jurisdictional housing of personally identifiable information (PII).

For those who qualify, the CCSP exam will test their competence in the six CCSP domains of the (ISC)² Common ***Body of Knowledge (CBK), which cover:***

- Architectural Concepts & Design Requirements
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Operations
- Legal & Compliance

CCSP Exam Information

CCSP Exam Information	Requirements
Length of exam	4 hours
Number of questions	125
Question format	Multiple choice
Passing grade	700 out of 1000 points
Exam Language	English
Testing Center	Pearson Vue Testing Center

Study Tools

- In-Class or Live OnLine Training
- OnDemand Training
- Interactive Flashcards
- Exam Outline

CONCLUSION

Final Words

In conclusion, in becoming a cyber-security professional, there are a few courses you could take to direct you on your path to keep the cyber world safe and in turn also make revenue for yourself. Qualify and be part of a global organization that is able to provide the networking, tools and the best practices in the InfoSec field. This knowledge can be passed down from person to person or organization to organization depending on where you find yourself. The job of a cyber-security professional is sometimes underestimated but the value is inestimable.

ABOUT

The Author

Vagner Nunes is the lead Business Development and Corporate Relations Manager for (ISC)² in Latin America. He is an (ISC)² executive with a comprehensive background in information Technology, product management and strategic planning.

Vagner is Responsible for the Business Development and Corporate Relations in Latin America and has more than 20 years of experience on management in international corporations like EDS, HP, TIVIT and Tata on the infrastructure and Datacenter field.

He joined (ISC)² in 2015 with vast wealth of knowledge in Technology Infrastructure and Datacenter, Tools and Automation, Capacity Planning and Project Management.

Vagner has presented at numerous industry events, including (ISC)² Secure Chile, (ISC)² Security Congress Latam, 8.8 in Chile and IT Universities in Brazil.

You can connect with Vagner on LinkedIn (Profile on LinkedIn: https://br.linkedin.com/in/vnunes)