NAME: SUFYAN ALI

ROLL NO: 21L-7541

SECTION: BSCS 3N EXPAND BS

PROJECT 1

SEP 30,2022

Prepared for

Sir Salmaan Rehman

Prepared by

Sufyan Ali

October 22, 2022

Table of contents

LIST OF FIGURES…………………………………………………………………………………………………………………………… iii

LIST OF TABLES..…………………………………………………………………………………………………………………………… iii

EXECUTIVE SUMMARY…..…………………………………………………………………………………………………………….. iv

PROBLEM………..……………………………………………………………………………………………………………………………..01

BACKGROUND………………………………………………………………………………………………………………………………..01

DISCUSSION OF FINDINGS………………………………………………………………………………………………………………02

THE BIGGEST CYBER ATTACKS IN HISTORY…………………………………………………………………………..02

THE RISE OF CYBER ATTACKS IN 2022……..…………………………………………………………………………..04

CYBER CRIME IN PAKISTAN.……………………..………………………………………………………………………….04

CYBER SECURITY FOR BUSINESS………………………………………………………………………………..…………05

* IMPACT OF CYBER ATTACKS ON BUSINESS………………………………………………….………..05
* ECONOMIC COST OF CYBER ATTACKS………………………………………………………..………….05

CYBER SECURITY IS A BUSINESS IMPEARTIVE……………………………………………………………………….

CYBER SECURITY BREACHES SURVEY 2022……………………………………………………………..……………06

CYBER SECURITY JOBS — A GROWTY STORY……………………………………………………………06

CYBER SECURITY IN FUTURE AFTER 2022…………………………………………………………………………….06

HOW WE AS A CYBER SECURITY COMPANY HELP PEOPLE…………………………………………………..

CYBER SECURITY INDUSTRY TRENDS……………………………………………………………………………………

* INDUSTRY SIZE AND GROWTH………………………………………………………
* TRENDS AND CHALLENGES…………………………………………………………

HOW MUCH DOES IT COST FOR START A CYBER SECURITY BUSINESS...………………………….

HOW MUCH YOU EARN FROM A CYBER SECURITY BUSINESS……………………………………………..

CONCLUSION AND RECOMMENDATIONS………………………………………………………………………………………09

WORK SITED………………………………………….………………………………………………………………………………………10

LIST OF FIGURES

FIGURE

1 Cyber Crime Damege cost………………………………………………………………………………………….6

2 Cyber Crime Damege cost………………………………………………………………………………………….8

LIST OF TABLES

1 STARTUP COSTS OF CYBER SECURITY BUSINESS

LIST OF FIGURES

1 **Rank of Pakistan in Cyber Crimes**…………….…………………………………………………………………5

EXECUTIVE SUMMARY

INTRODUCTION

**PROBLEM**

The purpose of this study was to give the idea about expand the business in IT Sector. Specifically study seeks to answer these questions:

The need of Cyber Security in this Modern Era.

How cyber security helps people in their business?

Feature of Cyber Security.

**BACKGROUND**

Cyber Security is the practice of Protecting computers, mobile devices, Servers, electronic Systems, networks, and data from malicious attacks. It is also known as Information Security (INFOSEC) or Information Assurance (IA), System Security. The first cyber malware virus developed was pure of innocent mistakes. But cybersecurity has evolved rapidly because of the impeccable increase in the cybercrime law field on the Web.

The [Cybersecurity](https://www.geeksforgeeks.org/cyber-security-types-and-importance/)checking began in the 1970s when researcher Bob Thomas created a computer program called Creeper that could move across ARPANET’s network. Ray Tomlinson, the innovator of email, wrote the program Reaper, which chased and deleted Creepers. Reaper was the very first example of checking a malware antivirus software and the first self-replicating program i.e. Viruses, as it made first-ever computer worms and trojans.

In 1971s, Programmer Bob Thomas made history by innovating a program that is widely accepted as the first incident ever computer trojan as the worm and trojan bounced between computers pc, which has groundbreaker at the time. The trojan was not at all malicious.

**Birth of commercial antivirus in the 1980s:**

The Year 1987 was the birth year of commercials malware examining antiviruses although there are competing the enabling the claims for the innovators of the first antiviruses are products and Andreas Lüning and Kai Figge has released their first antiviruses software product at for the Atari ST – that has also seen the releasing of the Ultimate Virus Killer (Malware Virus Killer) in 1987 and the Three Czechoslovakians to created the first new version of the NOD antivirus in the same year and in the US, famous John McAfee founded McAfee and released VirusScan software.

**Threats diversify and multiply in the 2000s:**

In the early 2000s criminal organizations started to heavily fund professional cyberattacks and governments began to clamp down on the criminality of hackings, giving much money serious sentences to those culpable hackers and Information security continues to advance as the internet grows as well but, unfortunately so having the viruses.

**DISCUSSION OF FINDINGS**

**The Biggest Cyber Attacks in the History**

Cyber attacks are on the rise. Whilst modern technology presents many conveniences and benefits, there are people who misuse it which can pose a threat to our privacy.

Cybercrimes often have a tremendous impact on companies and individuals. It is expected that the cost of cybercrimes may reach **$10.5 trillion** by 2025.

Let’s take a look at some of history’s biggest cyber attacks

**1. The Melissa Virus**

One of the earliest and biggest cyber threats was started by the Melissa Virus. In 1999, the Melissa Virus was unleashed by programmer David Lee Smith by sending users a file to be opened by Microsoft Word. The virus caused severe destruction to hundreds of companies, including Microsoft. It is estimated that repairing the affected systems cost around $80M.

**2. NASA Cyber Attack**

In 1999, 15 year old James Jonathan was able to hack and shutdown NASA’s computers for 21 DAYS! Around 1.7M software were downloaded during the attack, which cost the space giant around $41,000 in repairs.

**3. The 2007 Estonia Cyber Attack**

In April 2007, Estonia witnessed what is thought to be the first cyber attack on an entire county, during which about 58 Estonian websites went offline, including websites of governments, banks and media outlets.

**4. A Cyber Attack on Sony’s PlayStation Network**

A cyber attack on Sony’s PlayStation Network in April 2011 claimed the personal information of 77M users.

**5. Adobe Cyber Attack**

The cyber attack which was first thought to have breached the data of 2.9M users went on to compromise the personal data of up to 38M users! Adobe claims that only the passwords and credit card information of the first 2.9M were compromised, whereas the remaining 35.1M only suffered the loss of their passwords and IDs.

**6. The 2014 Cyber Attack on Yahoo**

In 2014, Yahoo witnessed one of the biggest cyber attacks of the year when 500M accounts were compromised. However, it is reported that basic information and passwords were stolen, whereas bank information was not.

**7. Ukraine’s Power Grid Attack**

In what was the first cyberattack on a power grid, the attack left around half of the homes in the Ivano-Frankivsk region in Ukraine without power in 2015 for a few hours.

**8. 2017 WannaCry Reandomsware Cyber Attack**

One of the biggest ransomware of all time took place in 2017, when around 200,000 computers were affected in more than 150 countries. This outbreak had a massive impact across several industries and had a global cost of about 6B pounds!

**9. A Cyber Attack on Marriott Hotels went unnoticed for years**

A cyber attack was lurking in the shadows for quite awhile when Marriott acquired the Starwood Hotels group, and it did not come into light until 2018. However, by then the attacker continued to have access to personal information of guests. An estimated 339M guests have had their data compromised. This had led the UK’s data privacy watchdog to fine the Marriott Hotels 18.4M pounds.

**10. The biggest password leak yet**

It was reported earlier this June that a compilation of about 8.4b passwords were leaked. This by far is the biggest password leak and is referred to as RockYou2021 in reference to the 2009 breach of RockYou site that compromised around 32M accounts.

**The Rise of Cyber Attacks in 2022:**

 Through the pandemic, cyber criminals took advantage of misaligned networks as businesses moved to remote work environments. In 2020, malware attacks increased 358% compared to 2019.

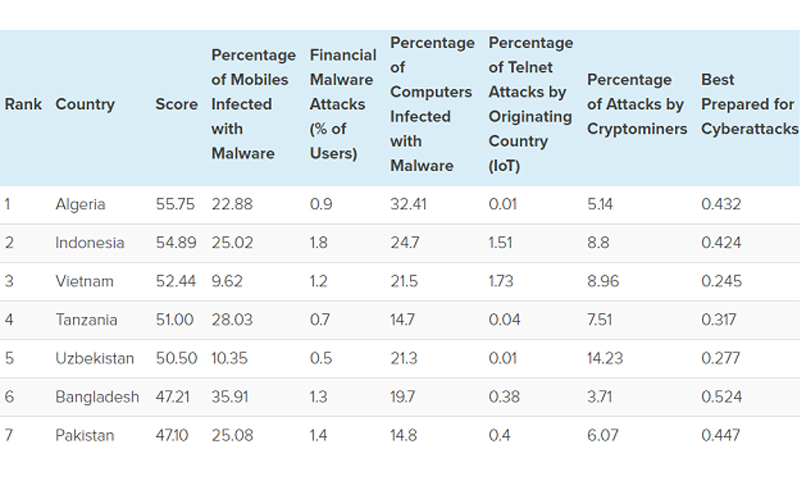
From here, cyber attacks globally increased by 125% through 2022, and this upward trend is expected to continue in 2023.

## Cyber crime in Pakistan

Cyber crime has become an increasingly severe problem in Pakistan in recent years. Financial fraud is the most common type reported; in 2020 alone, of 84,764 total complaints, 20,218 Pakistanis reported falling victim to financial fraud-related online crimes. This is ahead of hacking (7966), cyber harassment (6023) and cyber defamation (6004).

An increasing number of Pakistanis have experienced cyber crime through social media. Between 2018-2021, financial fraud through social media increased 83%. Of 102,356 total complaints received in 2021, 23% of cyber crimes used Facebook.

(Source: Pakistan Federal Investigation Agency)



**Table 1: Rank of Pakistan in Cyber Crimes**

**Cyber Security For Business:**

* Impact of cyber attack on business:

A successful cyber attack can cause major damage to business. It can affect bottom line, as well as business' standing and consumer trust. The impact of a security breach can be broadly divided into three categories: financial, reputational and legal.

* Economic cost of cyber attack:

Cyber attacks often result in a substantial financial loss arising from:

* theft of corporate information
* theft of financial information (e.g bank details or payment card details)
* theft of money
* disruption to trading (e.g inability to carry out transactions online)
* loss of business or contract

In dealing with the breach, businesses will also generally incur costs associated with repairing affected systems, networks and devices.



Figure 1: Cyber Crime Damege cost

**CYBER SECURITY IS A BUSINESS IMPEARTIVE:**

Industrial cybersecurity has a direct and significant impact on business decisions, particularly when it comes to risk assessment and management, which is without doubt for the majority of persons close to the OT cybersecurity industry.

It may not be as evident to those people who aren't working directly on finding solutions to these difficult problems and don't often see the data. Instead of being a fundamental component of an organization's DNA, like your attitude to safety or your dedication to sustainability, it can be perceived as a "plant floor problem" or an IT endeavour.

It's time to integrate cybersecurity into our culture not only in the boardrooms where policies and plans are made but also in the factories and facilities around the world. According to studies, 47% of industrial computers experienced attacks last year. According to the same polls, only 23% of businesses adhere to industry best practises, and 58% said it was extremely difficult to recruit qualified workers. From where we're standing, it appears like every industrial computer faces a considerable risk of assault. Without making cybersecurity a top priority for the company, it is very possible that a particular facility isn't adhering to best practises and norms, and it would likely struggle to make significant improvements.

Cyber Security Breaches Survey 2022:

The latest [**UK government survey**](https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022) showed that in the last 12 months, 39 per cent of UK businesses identified a cyber attack. Within this group:

* 31 per cent of businesses estimate they were attacked at least once a week
* 1 in 5 say they experienced a negative outcome as a result of an attack

In terms of material outcomes, the average estimated cost of cyber attacks in the last 12 months is £4,200. However, within medium and large businesses group, this figure rises to £19,400.

## Cybersecurity jobs — a growth story

Cybersecurity jobs are exciting. According to data collected by the Bureau of Labor Statics (BLS), the demand for cybersecurity jobs like information security analysts will grow by as much as 31 percent over the next ten years.

When you think about it, the above average growth in cybersecurity jobs makes sense. As technology becomes more and more intertwined with everyone’s day to day lives, there are much more experienced cybersecurity professionals.

The cybersecurity field includes a wide range of different jobs from entry-level up to executive management and everything in between.

**Cybersecurity in the future After 2022:**

The cybersecurity industries are continuing to grow. The most global cybersecurity market size is forecast to grow to $345.4bn by 2026 according to Statista. Ransomware is one of the most common threats to any organization of data security and is forecast to continue to increase applications.

[Cyber attacks](https://www.geeksforgeeks.org/types-of-cyber-attacks/) usually confirm to a general multistep process are as the first step of this process is surveillance, then is the collection of the information about specified targeted networks, as Examples- are ping scan and port scans to find out how hosts exist and how services are provided by each host. The second step is the remote exploitation of vulnerabilities associated with the services that were identified during the first step. When it is successful, this gives an attacker access across the system and the time between each of the phases of a multi-step attack may be in just seconds, or it may be days or even months.

Understanding the history of cybersecurity says an overview of how cybersecurity has evolved from once being simple experiments. Current statistics indicate that cybersecurity prevalence will continue growing. The Cybercriminals are experts in using new incidents strategies for executing the stealth stock attacks by leveraging emerging technologies like AI-artificial intelligence, blockchain, and machine learning(ML).

The Pakistan lawmakers hurriedly passed an amendment to the IT Act of 2000 with debate or opposition from civil society. The Amended Acts (under sections 66-69) listed a host of actions that considered computer-based cybercrimes, charge to perform various cyber security functions, such as:

* The Collection, analysis and dissemination of the information on cyber securities incidents
* Forecasts and alert for Website cyber security incidents
* emerging these measures for handling the cyber security incidents
* The Coordination of cyber incidents are response activities
* The guidelines, advisories, and vulnerability notes as whitepapers are related to information security practices and procedures, prevention, response and reporting of cyber security incidents another functions related to cyber security as may be prescribed

While intensifying threats, these solutions developed, as new detection methods developed. New solutions for examining unprecedented threat were created within this included the use of new technology and approaches as some examples including:

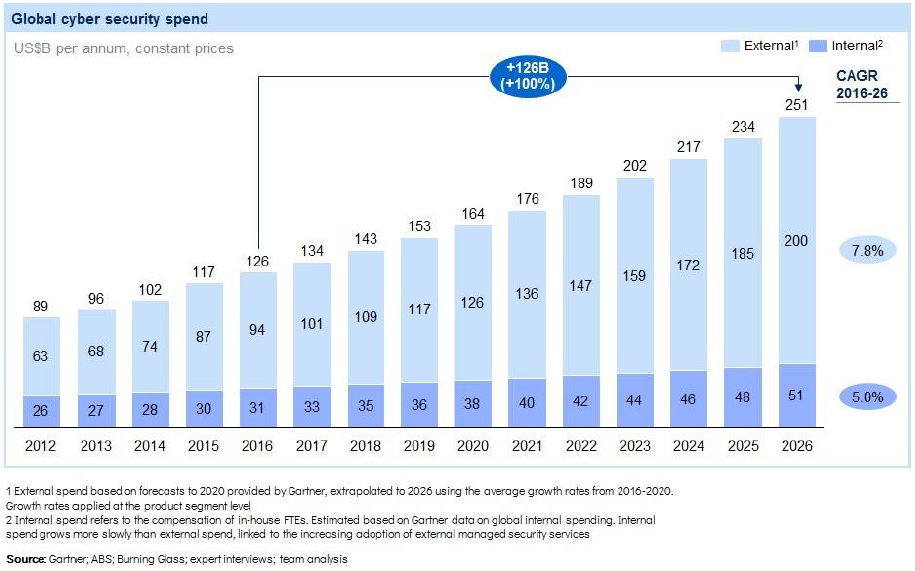
* Computer forensics
* Multi factor authentications
* The Network Behavioral Analysis-(NBA)
* The Real time protections for System
* The Systems Threat intelligence and updated automation
* Sandboxing
* Back ups and mirroring
* Multi vectors attacks
* Social engineering
* Website applications firewalls

Besides, cyberattacks have shown the data that attackers are capable of bypassing recognized security controls like two-factor authentication thus Organizations and security companies have More ever to think about their approach towards cybersecurity.

Cybersecurity in the future means that researchers and securities experts need to direct all their efforts towards leveraging the benefits of emerging technologies. They must reduce cyber-attack incidences and minimize their effects when they cure them.

Now, artificial intelligence is integrated into antivirus and firewall solutions to achieve smarter detection and response capabilities, However since all organizations are automated most of their processes, cyberattacks are more concerned with compromising system security. The intention is to prevent malware from accomplishing normal operations by locking out of system users or stealing critical data. The emergency future of a 5G network is set to automate critical infrastructure like transportation advances in technology propel and cyberattacks to evolved

By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.



**Figure 2: Rise in Cyber Security in Future**

**HOW WE AS A CYBER SECURITY COMPANY HELP PEOPLE:**

It is hardly surprising that cybercrimes are on the rise in a world that is becoming more digital. The cost to firms in terms of money is also soaring. According to a 2021 IBM analysis, the average cost of a data breach is $4.24 million.

The demand for cybersecurity services is quite strong due to these large financial stakes. Large businesses have the resources to employ cybersecurity personnel. However, most small and medium-sized organizations cannot afford to hire full-time cybersecurity personnel.

Here is where our knowledge of cybersecurity can help you launch a profitable security solutions company.

We may assist in defending these smaller businesses against cyberthreats like malware, phishing scams, cyberattacks, and data breaches.

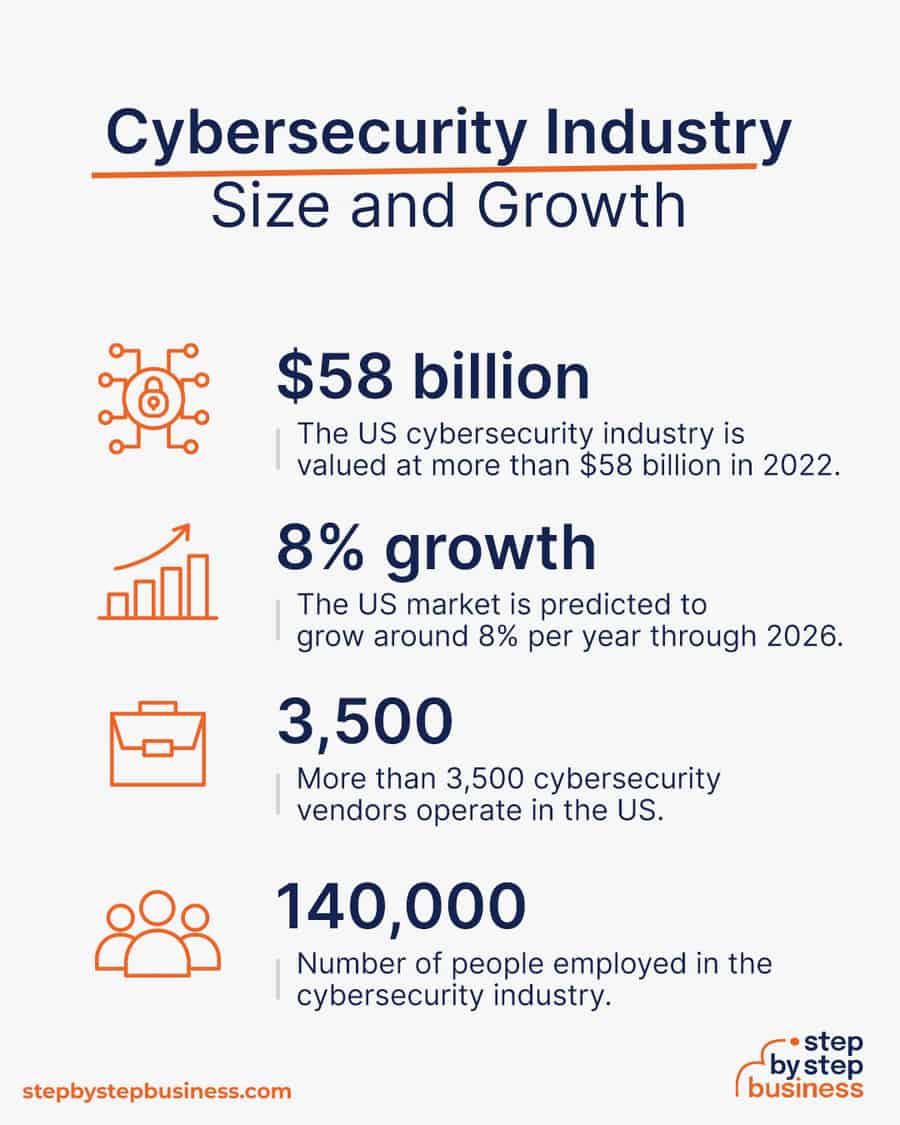
Businesses are paying experienced cybersecurity consultants $150 per hour or more to help protect systems and networks from hackers, according to PayScale statistics.

**CYBER SECURITY INDUSTRY TRENDS:**

The cybersecurity market is being driven by the increase in computer and internet usage, improved hacker skills, and various regulations.

#### **Industry size and growth:**

* **Industry size and past growth –** The US cybersecurity industry is valued at more than $58 billion in 2022.
* **Growth forecast –** The US market is predicted to grow around 8% per year through 2026. Globally, the $150 billion cybersecurity industry is expected to grow more than 13% annually through 2027.
* **Number of businesses –**Research platform Cyber DB says it has listed more than 3,500 cybersecurity vendors in the US.
* **Number of people employed –** The Bureau of Labor Statistics says there were more than 140,000 jobs for information security analysts in 2020, and the career is growing 33% per year through 2030.



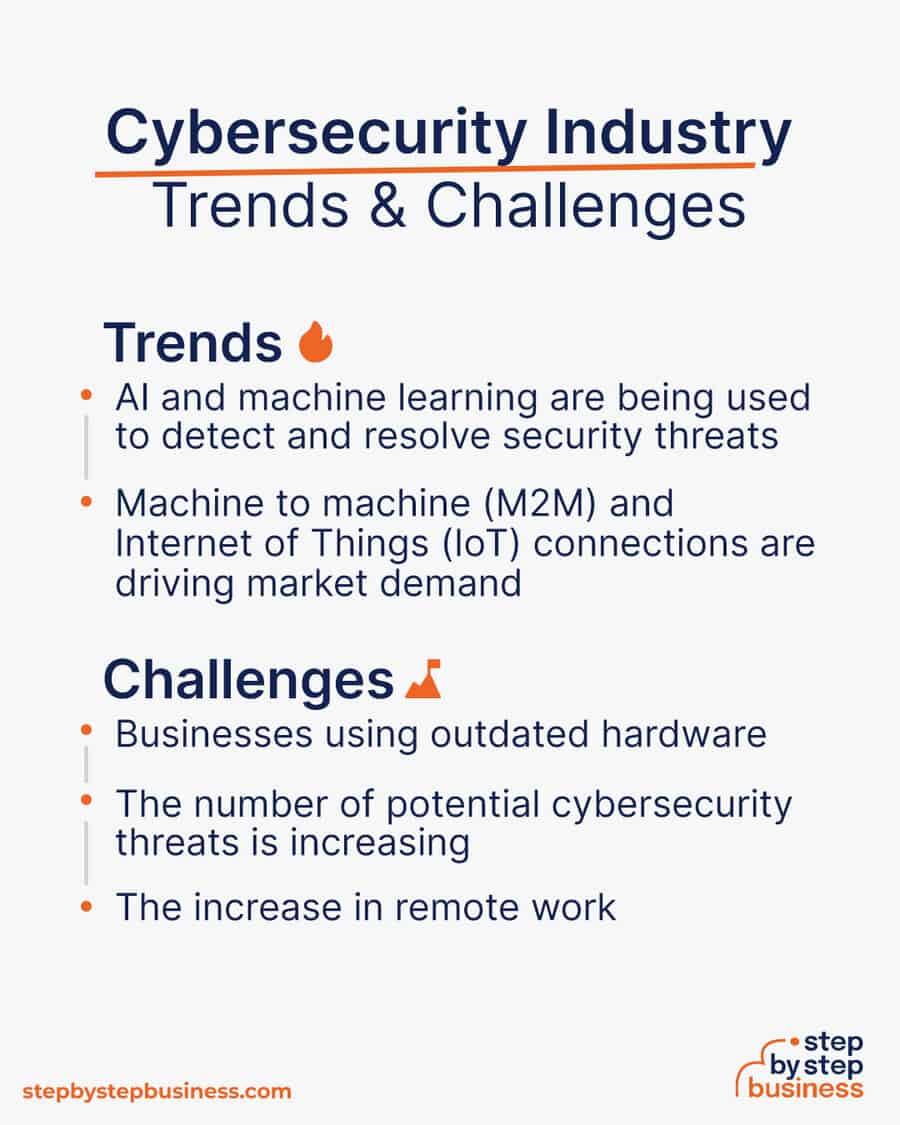
#### **TRENDS AND CHALLENGES:**

Trends in the cybersecurity industry include:

* Artificial intelligence (AI) and machine learning are being increasingly used to [detect and resolve security threats](https://www.itransition.com/machine-learning/fraud-detection). These are important tools for cybersecurity professionals to use.
* Machine to machine (M2M) and Internet of Things (IoT) connections are increasing the need for cybersecurity, driving demand in the market. The need for cloud security and information security is also boosting demand.

Challenges in cybersecurity include:

* Businesses using outdated hardware make it difficult to ensure cybersecurity.
* The number of potential cybersecurity threats is increasing, and each requires threat detection abilities and a security solution.
* The increase in remote work represents a new challenge for cybersecurity firms, as they have to find ways to protect distant connections.



### HOW MUCH DOES IT COST TO START A CYBER SECURITY BUSINESS?

A cybersecurity company's startup costs might range from $7,000(RS 1,547,000) to $20,000(RS 4,420,000). High-end hardware and necessary software are costs. If we don't already have them, high end involves education and certificates.

There are several other certificates available, including big data analysis, threat intelligence, cybersecurity expert, and information security analyst. The National Initiative for Cybersecurity Careers and Studies has comprehensive information.

We willl need a handful of items to successfully launch your cybersecurity business, including:

* A computer system
* Network security monitoring tools
* Encryption tools
* Web vulnerability scanning tools
* Penetration testing tools
* Antivirus software
* Network intrusion detection tools
* Packet sniffers

| **Start-up Costs** | **Ballpark Range** | **Average** |
| --- | --- | --- |
| Setting up a business name and corporation | $150 - $200 | $175 |
| Business licenses and permits | $100 - $300 | $200 |
| Insurance | $100-$300 | $200 |
| Business cards and brochures | $200 - $300 | $250 |
| Website setup | $1,000 - $3,000 | $2,000 |
| Computer system | $2,500 - $5,000 | $3,750 |
| Software | $3,000 - $5,000 | $4,000 |
| Education and certification | $0 - $5,000 | $2,500 |
| **Total** | **$7,050 - $19,100** | **$13,075** |

TABLE : 1 STARTUP COSTS

### HOW MUCH YOU CAN EARN FROM A CYBER SECURITY BUSINESS?

Prices for cybersecurity system analysis and installation range from $1,000 to as much as $10,000. Monthly costs for ongoing security monitoring range from $1,000 to $10,000. The calculations that follow assume that each would cost $2,500. You should be able to generate a profit margin of roughly 80% if you operate from home.

One new client each month at $2,500 upfront may be possible in the first two years of business, along with a steady stream of three regular clients. Assuming an 80% margin, this would generate $120,000 in revenue each year and a tidy profit of $96,000.

Sales may increase to 10 new clients per month and 20 clients paying for monitoring as your business becomes more well-known and you begin to receive referrals. At this point, you would rent a business location and recruit personnel, bringing your profit margin down to about 30%. You would earn a very comfortable $270,000 with remarkable annual income of $900,000.

**CONCLUSIONS AND RECOMMENDATIONS**

Analysis of Rise of Cyber Attacks, Impact on Business of Cyber Attack, Cyber Crime in Pakistan and Future of Cyber Attacks leads to following conclusions and recommendations about expand business toward Cyber Security.

1) By 2025, 60% of firms will see cybersecurity risk as their main consideration when engaging in business with third parties.

2) Cybercriminals benefited from misaligned networks during the epidemic as businesses shifted to remote working environments. Malware attacks rose 358% in 2020 compared to 2019.

3) Social media has been used by an increasing number of Pakistanis to commit cybercrimes. Financial theft on social media climbed 83% between 2018 and 2021. Facebook was utilized in 23% of the 102,356 cybercrimes reported in 2021.

4) Most business failures in the past were caused by cyberattacks.

5) Industrial cybersecurity affects business decisions directly and significantly, especially when it comes to risk assessment and management, which is undeniably true for the majority of those associated with the OT cybersecurity sector.

6) The surveys found that only 23% of organizations followed industry best practices and that 58% found it very difficult to find skilled staff.

7) By 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements.

**WORK CITED**

[**https://www.geeksforgeeks.org/history-of-cyber-security/**](https://www.geeksforgeeks.org/history-of-cyber-security/)

[**https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/**](https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/)

[**https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:~:text=Through%20the%20pandemic%2C%20cyber%20criminals,expected%20to%20continue%20in%202022**](https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:~:text=Through%20the%20pandemic%2C%20cyber%20criminals,expected%20to%20continue%20in%202022)

[**https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:~:text=Through%20the%20pandemic%2C%20cyber%20criminals,expected%20to%20continue%20in%202022**](https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:~:text=Through%20the%20pandemic%2C%20cyber%20criminals,expected%20to%20continue%20in%202022)

[**https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business**](https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business)

[**https://cybersecurityguide.org/resources/cybersecurity-jobs/**](https://cybersecurityguide.org/resources/cybersecurity-jobs/)

[**https://www.insureon.com/blog/how-to-get-into-the-cybersecurity-industry**](https://www.insureon.com/blog/how-to-get-into-the-cybersecurity-industry)

[**https://stepbystepbusiness.com/business-ideas/start-a-cybersecurity-business/**](https://stepbystepbusiness.com/business-ideas/start-a-cybersecurity-business/)