International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 12 | December - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies

Radhika Dwivedi, 2ND YEAR
NMIMS, INDORE

ABSTRACT

Information technology is central to various other areas, especially healthcare, transportation, government, finance, and entertainment, but it is equally critical to creativity as well. In today's world, securing data has become a huge problem. When it comes to the world of cyber security, the number of criminal incidents continue to rise day by day. There are several initiatives being implemented to combat these types of online crimes. Also, cyber security has become a significant issue for many businesses and governments. There is no detail on cyber security threats in this paper, but this paper mostly deals with the difficulties posed by the most recent technological advances. Cyber security emphasis is primarily on current happenings, it also examines current developments and fashion trends in the field, and contains insights on a range of the ethical issues relate to cyber security.

RESEARCH OBJECTIVES

- Critical national information infrastructure should be protected (CII)
- Protect computer system from day vulnerabilities through cooperation, as well as incident and attack resolution, and recovery through fast dissemination of knowledge.
- Set up a legal and regulatory system to make sure that a secure and versatile cyberspace can exist.
- A secure and productive working environment for all concerned individuals in which to us and create system of information.
- To aid in the creation and nurturing of the national cyber security of our citizens.

INTRODUCTION

Today, man is capable of sending and receiving any type of data, whether it is e – mail, audio, or video, with the click of a button, but has he ever considered how securely his data is being transmitted or sent to the other person without information being leaked? Cyber security is the solution. Today, the Internet is the most rapidly growing infrastructure in daily life (Gade, 2014). In today's technological world, several cutting – edge innovations are reshaping the human race. However, as a result of these new technologies, we are unable to protect our private information effectively, as a result, cyber – crimes are on the rise. Today, more than 60% of all commercial transactions occur online, implying that this area requires a high level of protection to ensure transparent and efficient transactions. As a result, cyber security has become a hot topic (Gade, 2014). Cyber security is a broad term that encompasses not only information security in the information technology industry, but also numerous other field such as cyber space.

Just as with the new technology, including cloud computing, electronic banking, and Internet commerce, privacy is essential. The most critical in this day and age is the protection of personal details. Cyber security is important to every national's security and economic well – being (Reddy, 2014). Security of the internet has become a critical to both private and public initiatives. I think we need a through and safer solutions cannot stop any crimes, it is important that government entities be permitted to use their own technological methods in their investigations and prosecutions. As the number of countries and states are adopting strict legislation on cyber securities in an effort to avoid critical information loss, it is everybody must learn these cyber – attacks and stay safe from them.

On top of these new and old technologies, some of the emerging one like cloud competing, mobile computing, E – Commerce, and internet banking, customer are top – notch security. Since these technologies store some important information about their physical and personal security, they are of significant importance. Enhancing computer and data technology protection and protective infrastructure are an important part of each nation's economy. A general social service requirement in recent years, government policy has included the development of the safety and protection of the networked user's privacy in the construction of the framework (Reddy, 2014).

Our approach to fighting cybercrime must be both systematic and proactive, with regard to be effective. Existing technological solutions can not deter crimes. It is equally critical that police officers have the ability to do so thoroughly investigate and prosecute cyber – crime be permitted to use all available measures. Professionally and commercially valuable data as a result of poor data management practises. Cybersecurity

training should be offered to all individual staff members of a company and even beyond, so they can fight these emerging new kinds of cyber – crime.

LATEST ON CYBER SECURITY ISSUES

Data privacy and protection will be the greatest threats facing businesses in the future. It is now an accepted assumption that all knowledge exists in digital form. In addition to offering a venue for users to connect with their peers, social networking sites allow them to build meaning relationships with family and loved ones (Ali, 2019). In the event of individuals who use the internet at home, cyber criminals will continue to exploit social media websites to steal their personal data. Unfortunately, there will be no longer be mass attacks on Android operating system – based computers, but rather on individuals and small groups of determined and highly organised hackers, possibly military, to further expand the impact and damage Android. This observation is consistent with what is known that reality tablet being vulnerable to malware: They use the smart phones. However, malware levels for the Mac will probably continue to rise, but much less rapidly than on account of its platform diversity (Thakur, 2019). Nowadays, Window type operating systems are most commonly being used by the users, adversaries with malicious intentions try to take advantage of this by continuously working on to create malicious code to successfully exploit any known or zero – day vulnerabilities rom the Windows system and create large sized impacts as they are able to target numerous system at the same time.

RECENT SURVEY ISSUES ON CYBER SECURITY TRENDS

The following list was developed by utilizing cyber security research and survey (Gade, 2014).

MOBILE DEVICE AND APPS

With the explosive growth of mobile storage and use of personal data, data security concerns become even more prevalent (Reddy, 2014). This can be said of every new mobile device as well as every new pathway for hackers to find the system they wish to target. Participants computers are not only protected as long as mobile users fall short on adequate security awareness and prepared to be the next victim for malicious software and attack. In a similar vein, the concern over missing and stolen devices would further involve these latest as well as older innovations will remain for quite some time.

SOCIAL MEDIA NETWORKING

The increased use of social media would increase the possibilities of cyber based threats to everyones security. Since many people have started using social media in their lives, a lot of their personal information can now be found on their social media web pages. As their personal information can be found online because of its

open source ability, adversaries can now take advantage of that personal data like date of birth, recent places that users visited, etc. to gain reconnaissance and utilize that the data to make cyber threats. Adversaries or hackers also try to gain advantage of the most common technique to infiltrate users' accounts and passwords by performing social engineering (Thakur, 2019). One of the sub techniques that adversaries can use in phishing by sending original looking like emails to targeted user and gain any vulnerable information that can be used for further exploitation.

CLOUD COMPUTING

A great number of companies have already begun to implement cloud computing. Most businesses have adopted and migrated towards cloud computing from on – premises physical infrastructure due to the huge cost and performance savings that it can deliver. Although, migrating to cloud computing brings a lot of security issues when it comes to protecting the data of the users (Atobatele, 2019). One of the biggest challenges that cloud computing faces in terms of security is actually identifying and maintain the access controls and shared responsibility between the company and the cloud service provider.

APT's AND TARGETED ATTACKS

The APTs (Advanced Persistent Threat) are the newest and most advanced type of threats that can affect companies and groups at a large level rather than just individuals drive based attacks, and has also been an important tool in discovering these precise, highly targeted attacks, even though the advanced security controls such as Web filtering and IPS (Intrusion Prevention System) have been used for several years now (mostly after the initial compromise). In the current environment, attacking approaches are becoming more ambiguous, so increasingly security demands that system integration with other resources, including monitoring and administration. Since threats are constantly emerging in order to avoid the possibility of future invasions, one must improve on security measures.

WEB SERVERS

Likelihood of attack on web applications to spread malicious code and data is gone, and is growing (Gade, 2014). A malicious script maybe distributed through an Internet connection that has been compromised using a well – known legitimate web server. But media knowledge of data theft, which also interest the public, is major threat. In this context, "We need to increase our focus on web servers and web applications". The web servers are a perfect target for these Internet offenders. You must always use a safe browser when you are making important transactions.

PROTECT SYSTEM RATHER INFORMATION

Protecting our privacy will be our primary concern, not information systems. As people transfer more and more of their information to the web, the need of encryption will become just for maintain and safeguarding the system that house data, as granular control will be demanded by both businesses and consumers.

NEW PLATFORMS AND DEVICES

New platform and applications can bring new threats and new risks for cyber criminals. Threats to personal computer security have long been associated with Windows, such as viruses, Hacking, Malware, and spyware, but it is also possible that with the introduction of new platforms and smartphones like the iPhones and Android would lead to new dangers (Reddy, 2014). Reports of trojans in the Android have kept coming over the summer, and have since been joined by malicious apps and malware for which trojans on some other operating system.

PRACTISES AND CONCERN BY GOVERNMENTS FOR CYBER SECURITY

Ensure that all residents have complete, equal and timely access to a robust cyber security is also includes balancing the responsibilities of managing local governments and federal requirements. Propose the signing of other future international treaties that encourage widespread ratification of the Cybercrime Convention. Supporting end – users education to prevent cyber – crime by protecting everyone but most importantly protecting the system – administered machines that aren't already under the control of those who might use them to hijack as well (Thakur, 2019).

Influence computer manufactures to provide reliable equipment and software by using the various types of procurement tools and metrics, as well as licencing to ensure adequate testing. To employ more personnel and expand the use of computers to support police investigations via funding, so that the International Computer Emergency will support work such as investigation into the vulnerability of Internet protocols, contingency planning, risk analysis, and disasters recovery.

CYBER CRIME

Cyber criminals are those who use a machine as their primary means of committing a crime. That activity that's conducted in or involves the use of a computer system to store evidence or carry out criminal schemes can be defined as a form of crime by the U.S. Department of Justice. The increasing number of crimes that have been facilitated by computers involves crimes like identity theft, as well as terrorism – related ones like

network intrusions (Ali, 2019). Cybercrime is mostly described as criminal activities that are conducted using computers and the internet for harmful purposes including using steel and illicit programmes to sell or to go after people, or otherwise interfere with contraband, or programmes which are out to hunt down. People's use of technology is now a large part of daily life, and this will only grow with time.

CYBER SECURITY

Privacy and information safety is among the most important and time – sensitive security procedures an organisation values. Measurements in a highly structured in a digital or cyber – specific environment are more convenient to us. Although these sites foster the community aspect of being with friends and family – like, cyber criminals tend to gather personal information as well.

LITERATURE REVIEW

According to Julian Jang – Jaccard improvement cyber protection is essential for the security and prosperity of each nation. The application of emerging technologies and procedures to increase the security of the Internet has been a major contribution factor to the development of new services and public policy (Reddy, 2014).

According to MdLiakat Ali – this study provides a concise discussion of recent developments in the field of technology and in regard to the current security techniques as well as various ethical considerations related to the field (Thakur, 2019).

According to Kutub Thankur – Cyber security was previously used interchangeably with knowledge security; however, it now recognises the human element in the safety phase, despite previously considering it an additional dimension. However, such a discussion on cyber security has significant ramification, as it touches on the ethical fabric of the entire community (Atobatele, 2019). Numerous system and models have been developed to address the cyber security problem.

CYBER SECURITY TECHNIQUES

Cyber – attack on cyberspace can expand as new techniques are developed. Cybercriminals often modify existing malware signatures in order to exploit newly discovered technological flaws. In order cases, they actively seek out unique characteristics of new technologies in order to identify vulnerabilities in malware injection. (Reddy, 2014) Cyber criminals are using emerging Internet infrastructure and millions and billions of active users to gain easy and effective access to a large number of people.

Access Control and Password Security

Protection given by the use of a username and password is a straightforward method of safeguarding private information and preserving privacy. This method of providing protection is one of the most important aspects of cyber security.

Authentication of Data

Until the information can be authenticated as having been obtained from a reliable sources, untainted sources, it is unverified. These records are always authenticated via a gift from the adversary's virus security kit installed on computers. Anti – virus software that is truly opposed to viruses is more important for protecting computers from viruses.

Malware Scanners

A platform which routinely looks inside all the files and documents on the platform for malicious code or malware. All of the system in this area are categorised as harmful by viruses, such as worms and trojans (Thakur, 2019) (Gade, 2014).

Anti – virus software

The Antivirus software is a computer programme that detects, avoids, and disables, such as harmful software. Most antiviruses software programmes include an auto – update feature that allow the software to retrieve virus definition in real time to stay protected from the Internet when a new one is detected (Reddy, 2014). It is absolutely essential to keep your device free of malware and unwanted application.

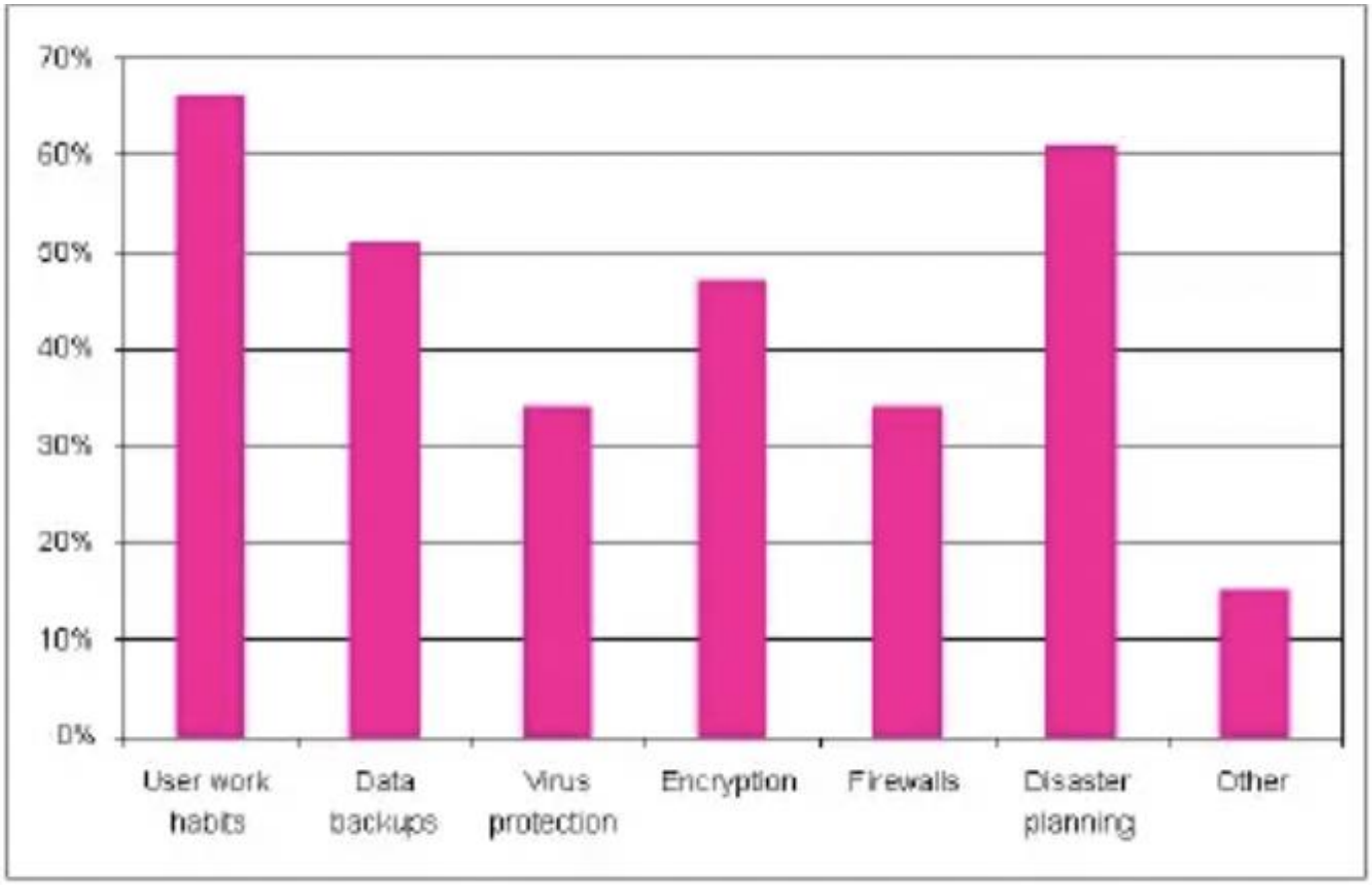
Firewall

It protects your PC from viruses and malware that they try to access it via the internet by protecting your PC from hackers. The firewall enforces rules for conformance with all messages coming and reject all the messages that are incompatible with those specifications. While Firewalls are commonly used to prevent malware from spreading, they are also important in malware detection (Atobatele, 2019).

Role of Social Media in Cyber Security

In modern times, companies of the 21st – century kind, there is a growing need for organisations to protect people's personal information in an interconnected setting. Some believe that social media can help fight the issue of cyber – attacks, although others contend that it is more likely to be attacked because of its importance

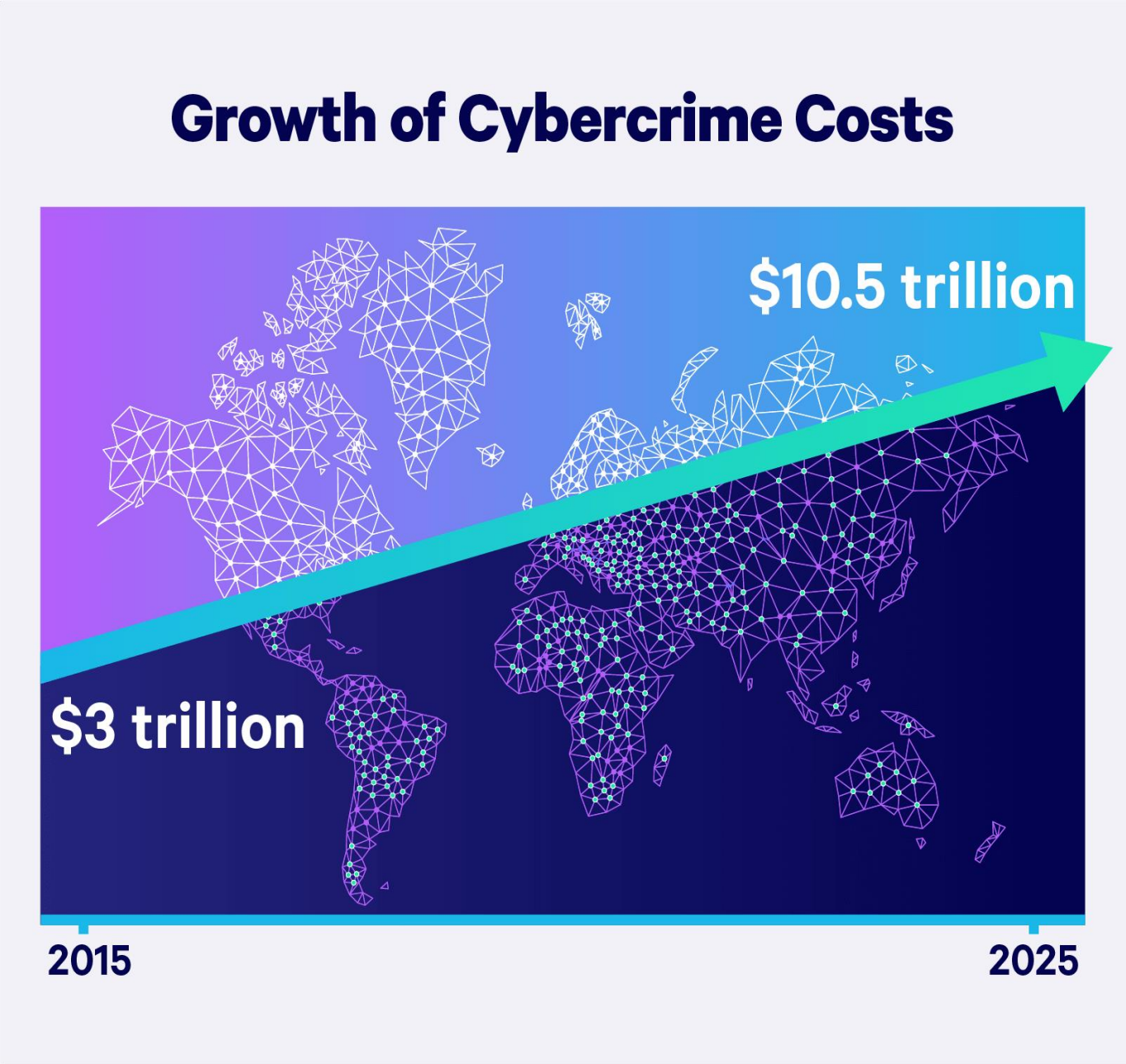
(Reddy, 2014). Adoption of social media in workplace is increasing, and therefore attacks on its security is on the rise. In modern times, it's incredibly simple to disseminate personal information, and companies must be both proactive and reactive when protecting it. The power of social media, such as Facebook and Twitter, has enabled individuals to post private information and is used by hackers to obtain it. Therefore, social media users ought to employ fair measures to safeguard their information from being misused and compromised.



CYBER ATTACK STATISTICS AND TRENDS

Cyberattacks have been ranked as the fifth most significant risk for 2020 and have established themselves as the new norm in both the public and private sectors. This high – risk industry is predicted to continue growing in 2021, with loT cyberattacks alone anticipated to double in size by 2025. Additionally, the World Economic Forum's 2020 Global Risk report claims that the detection (or prosecution) rate in the United States is as low as 0.05 percent.

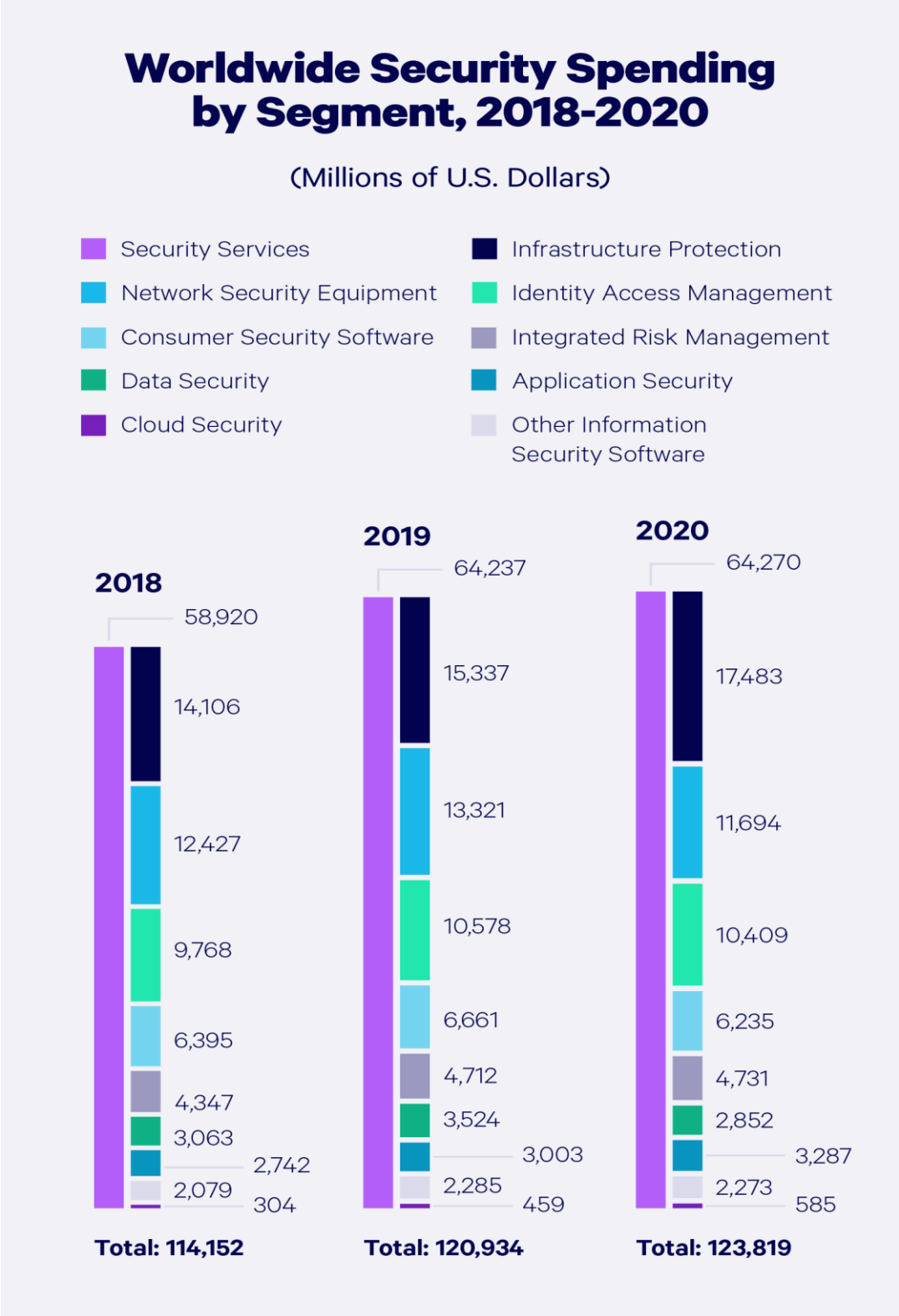
GROWTH OF CYBERCRIME



Cybercrime is expected to cost businesses globally $10.5 trillion annually by 2025, up from $3 trillion in 2015. Cybercrime, which is growing at a 15% annual rate, also constitutes the greatest transfer of economic value in history, according to Cybersecurity Ventures (Embroker , n.d.).

GLOBAL SECURITY SPENDING

Let's take a look at how cybersecurity spending has grown around the globe – broken down by the product or service (Embroker , n.d.).



HOW TO REDUCE THE RISK OF CYBER ATTACKS

CONCLUSION

Computer security is a large subject that is growing increasingly vital as the world becomes more linked and networks are utilised to conduct crucial transactions. Cybercrime continues to evolve and the security of information deteriorates with each passing year (Ali, 2019). Thee latest and most innovative technologies, together with the new cyber tools and threats that emerge daily, are presenting companies with a new set of challenges regarding not just how they defend their infrastructure, but also how they secure it with new platforms and intelligence. While there is no ideal answer to cybercrime, we should do all possible to minimise it in order to ensure a safe and secure future in cyberspace (Reddy, 2014) (Gade, 2014)

Bibliography

Gade, N. R. (2014, February). *A study of Cyber Security Challenges and its And Its Emerging Trends On Latest Technologies* . Retrieved from Research Gate : https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

Reddy, U. G. (2014 , February). *A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies*. Retrieved from Research Gate : https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

Ali, M. L. (2019, July). *Challenges of Cyber Security and the Emerging Trends July 2019*. Retrieved from Research Gate : https://www.researchgate.net/publication/334343860_Challenges_of_Cyber_Security_and_the_Emerging_Trends

Thakur, K. (2019, July). *Challenges of Cyber Security and the Emerging Trends*. Retrieved from Research Gate : https://www.researchgate.net/publication/334343860_Challenges_of_Cyber_Security_and_the_Emerging_Trends

Atobatele, B. (2019 , July). *Challenges of Cyber Security and the Emerging Trends.* Retrieved from Research Gate : https://www.researchgate.net/publication/334343860_Challenges_of_Cyber_Security_and_the_Emerging_Trends

(n.d.). Retrieved from Embroker : https://www.embroker.com/blog/cyber-attack-statistics/