iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IX **Month of publication:** September 2021

DOI: https://doi.org/10.22214/ijraset.2021.38173

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IX Sep 2021- Available at www.ijraset.com

World of Cyber Security

Yashvi Shah
KT Resort & SPA PVT LTD, India

I. INTRODUCTION

Welcome to the world of cyber security! It's a constantly evolving area with new threats popping up all around us. The best way to combat this is by staying informed and becoming educated about what's going on in the field.
Cyber security is a constantly evolving field. One of the most fundamental ways to keep secure is to stay informed and involved with the industry. Keeping an eye on network activity is one of the most effective ways to maintain your safety.

A. Cyber crime

Cybercrime is a term used to describe any illegal activity that relies on a computer as a primary means of commencement and committing theft. Any illegal activity that uses a computer to store evidence is now considered a cybercrime by the U.S. Department of Justice (DOJ). Internet-based crimes, such as network intrusions and the spread of computer viruses are included in this growing list of cybercrimes, along with computer-based variations of traditional criminal acts such as identity theft and terrorism.

B. Cyber Security

In any organisation, privacy and data security will always be a top priority. The world we live in today is one in which all information is stored digitally or in cyberspace. Users can interact with friends and family in a safe environment on social networking sites. Cybercriminals will continue to target social media sites to steal personal information from home users. Persons are required to take all necessary security precautions not only when using social networking sites, but also when making bank transactions. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity. Cyber security is maintained or increased by 98%, and half of those companies plan to increase their efforts to combat online attacks this year.
Most companies are preparing for cyber-attacks, not if they happen. Uncertainty about the security measures of their business partners is even lower than that of the security measures of their own information. The year 2020 brought both challenges and triumphs. Businesses have been forced to create remote workforces and operate on cloud-based platforms in order to comply with COVID-19's mandates for compliance. With the advent of 5G, connected devices are now more interconnected than ever. Just to summarise: The cybersecurity industry has never been more critical!! As a result of recent events, here are some industry trends to keep an eye on in 2021 and beyond, along with the following cybersecurity statistics and figures

1) Remote workers will continue to be a target for cybercriminals.
2) As a side effect of remote workforces, cloud breaches will increase.
3) The cybersecurity skills gap will remain an issue.
4) As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber-attacks.

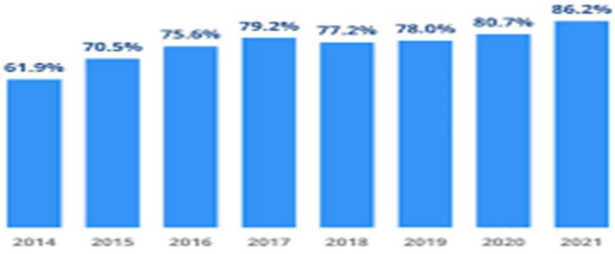


Figure 2: Percentage of organisations compromised by at least one successful attack.

Defending computers, servers, mobile devices and electronic systems, as well as networks and data from malicious attacks is the practise of cybersecurity. Computer and network security are other terms used to describe it. When used in various contexts, such as in business or mobile computing, the term falls into a few general categories.

II. NETWORK SECURITY

As the name implies, network security is the process of protecting a computer network from intruders, whether they are targeted attackers or opportunistic malware

III. APPLICATION SECURITY

It's all about keeping software and devices safe from threats. Information protected by a compromised app could be accessed. Designing a secure programme or device begins long before it is deployed.

IV. INFORMATION SECURITY

Protection and integrity of data, both in storage and in transit - that's what information security is.

V. OPERATIONAL SECURITY

Processes and decisions relating to data assets are included in operational security processes. Users' access rights to a network and the procedures that determine how and where data can be stored or shared fall under this category.

VI. DISASTER RECOVERY AND BUSINESS CONTINUITY

Cyber-security incidents or any other event that results in the loss of operations or data are examples of disaster recovery and business continuity. To restore operations and information to pre-event levels, disaster recovery policies must be followed. In the event that certain resources are lost, the organisation will fall back on its business continuity plan to continue operations.

VII. END-USER EDUCATION

End-user education focuses on the most unpredictable cyber-security factor: users themselves. An otherwise secure system can be compromised by anyone who fails to adhere to good security practises. Any organization's security depends on educating users on the need to delete suspicious email attachments and not plug in unidentified USB drives, among other important lessons.
An important aspect of cyber security is end-user protection. A user's computer, laptop, or mobile device is often infected by malware or another form of cyber threat when they unintentionally upload it.

VIII. END USER PROTECTION

An important aspect of cyber security is end-user protection. A user's computer, laptop, or mobile device is often infected by malware or another form of cyber threat when they unintentionally upload it.
Do cyber-security measures protect users and systems? Encrypting emails, files, and other critical data requires cryptographic protocols. Protecting your data in transit, as well as protecting it from loss or theft. The software also scans computers for malicious code and quarantines it before it is removed. In addition to detecting malicious code hidden in the primary boot record, security programmes can encrypt or wipe data from the hard drive.
Detection of malware in real-time is also a focus of electronic security protocols. In order to protect themselves from viruses or Trojans that change their shape with each execution, many use heuristic and behavioural analysis to monitor the behaviour of a programme and its code (polymorphic and metamorphic malware). In order to learn how to better detect new infections, security programmes can isolate potentially malicious programmes in a virtual bubble separate from the user's network.
There are always new threats and ways to combat them in cyber-security programmes. Employees must be trained on how to use end-user security software in order to get the most out of it. As a result, users are protected against the latest cyber threats by keeping it running and updating it frequently.

What are the benefits of cybersecurity?
The benefits of implementing and maintaining cybersecurity practices include:

1) Cyberattacks and data breaches protection for businesses.
2) Protecting the privacy of users and their data.
3) Unauthorized access prevention
4) Recovering faster from a breach
5) End user and endpoint device protection
6) Adherence to the law.
7) Continuity of business.
8) The company's reputation and trust among developers, partners, customers and stakeholders have improved.

IX. TYPES OF CYBER SECURITY THREATS

The process of keeping up with new technologies, security trends and threat intelligence is a challenging task. It is necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyberthreats include:

1) It is a form of malware in which any file or programme is capable of harming a computer user. Worms, viruses, Trojans, and spyware are all included in this category of threats.
2) Malware that encrypts data is called ransomware. It involves an attacker encrypting and locking the victim's computer system files, then demanding payment to decrypt and unlock them.
3) In order to gain access to sensitive information that is normally protected, social engineering relies on human interaction to trick users into violating security procedures.
4) As part of social engineering, fraudulent emails and text messages that look like they came from well-known or reputable sources are sent out. These messages, which are often random attacks, are designed to steal sensitive data, such as credit card or login information, from the victim's computer.
5) Spear phishing is an attack that targets a specific user, company, or organisation.
6) Employees, contractors, and customers are all examples of insider threats, which include security breaches and losses caused by humans. Malicious or negligent insider threats are two examples of this.
7) In a distributed denial-of-service attack (DDoS), multiple systems interfere with a targeted system's traffic, such as a server, website or other network resource. Assailants can slow or crash the target system by flooding it with messages, connection requests, or packets. This prevents legitimate traffic from using it.
8) They are long-term targeted attacks in which a hacker infiltrates a network and remains undetectable for long periods of time in order to steal confidential information
9) Neutralizing attacks, such as man-in-the-middle (MitM), involve an adversary intercepting and relaying messages between two parties who believe they are communicating with each other.

Other common attacks include botnets, drive-by-download attacks, exploit kits, advertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.

X. CYBER SECURITY CHALLENGES

Hackers, data loss, privacy, risk management, and changing cyber security strategies are all constant threats to cyber security. This trend is not expected to change anytime soon. The need to secure networks and devices is also exacerbated by the emergence of new attack vectors, such as the Internet of Things (IoT).

The ever-changing nature of security risks is one of the most problematic aspects of cyber security. As new technologies emerge and are used in new or different ways, new attack avenues are created. It can be difficult to keep up with these frequent changes and advances in attacks, as well as updating practises to protect against them. This includes updating all cyber security components on a regular basis to guard against possible vulnerabilities. Especially for smaller organisations, this can be a challenge.

People who use one or more of an organization's services can also be tracked. Additionally, as more data is collected, there is a greater chance that a cybercriminal will attempt to steal personally identifiable information (PII). PII stored in the cloud may be the target of a ransomware attack, for example. A cloud breach should be avoided at all costs by organisations.

Because employees may accidentally bring viruses into the workplace on their laptops or mobile devices, cyber security programmes should also address end-user education. When employees receive regular training in security awareness, they will be better prepared to protect the company from cyber threats.

Security personnel shortages are also a problem in the field of cyber security. Security personnel are needed to analyse, manage incidents, and respond to them as the amount of data being collected and used by businesses increases. It was estimated by (ISC)2 that there was a 3.1 million-person gap between needed cyber security jobs and cyber security professionals.

XI. CYBER SAFETY TIPS - PROTECT YOURSELF AGAINST CYBER ATTACKS

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

A. Update your software and operating system: This means you benefit from the latest security patches.
B. Use anti-virus software: Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
C. Use strong passwords: Ensure your passwords are not easily guessable.

D. Do not open email attachments from unknown senders: These could be infected with malware.
E. Do not click on links in emails from unknown senders or unfamiliar websites: This is a common way that malware is spread.
F. Avoid using unsecure Wi-Fi networks in public places: Unsecure networks leave you vulnerable to man-in-the-middle attacks.

XII. CYBER SECURITY SPENDING

The worldwide cyber security market was valued $3.5 billion in 2004 and more than $120 billion in 2017. Prior to Cyber security Ventures' most recent market estimate, the cyber security market increased by about 35X over that 13-year period.

Over the five-year period from 2017 to 2021, global spending on cyber security products and services for guarding against cybercrime is expected to exceed $1 trillion.

“Most cyber security budgets in the United States are expanding linearly or flatly, but cyber attacks are increasing exponentially,” Montgomery of CSC adds. For C-suite executives, this basic observation should serve as a wake-up call.

Healthcare has lagged behind other businesses, and the enticing target on its back is due to obsolete IT systems, a lack of cyber security measures and IT professionals, incredibly valuable data, and the urgent necessity for medical practises and hospitals to pay ransoms swiftly in order to reclaim data. From 2020 to 2025, the healthcare industry will spend a total of $125 billion to strengthen its cyber security. According to The White House, the FY 2020 U.S. President's Budget provides $17.4 billion in budget authorization for cyber security-related operations, a $790 million (5 percent) increase above the FY 2019 projection. This sum does not represent the whole cyber budget due to the sensitive nature of some activities.

Through 2025, Cyber security Ventures forecasts a 12-15 percent year-over-year increase in the cyber security market. While this is a commendable rise, it pales in contrast to the costs of cybercrime.

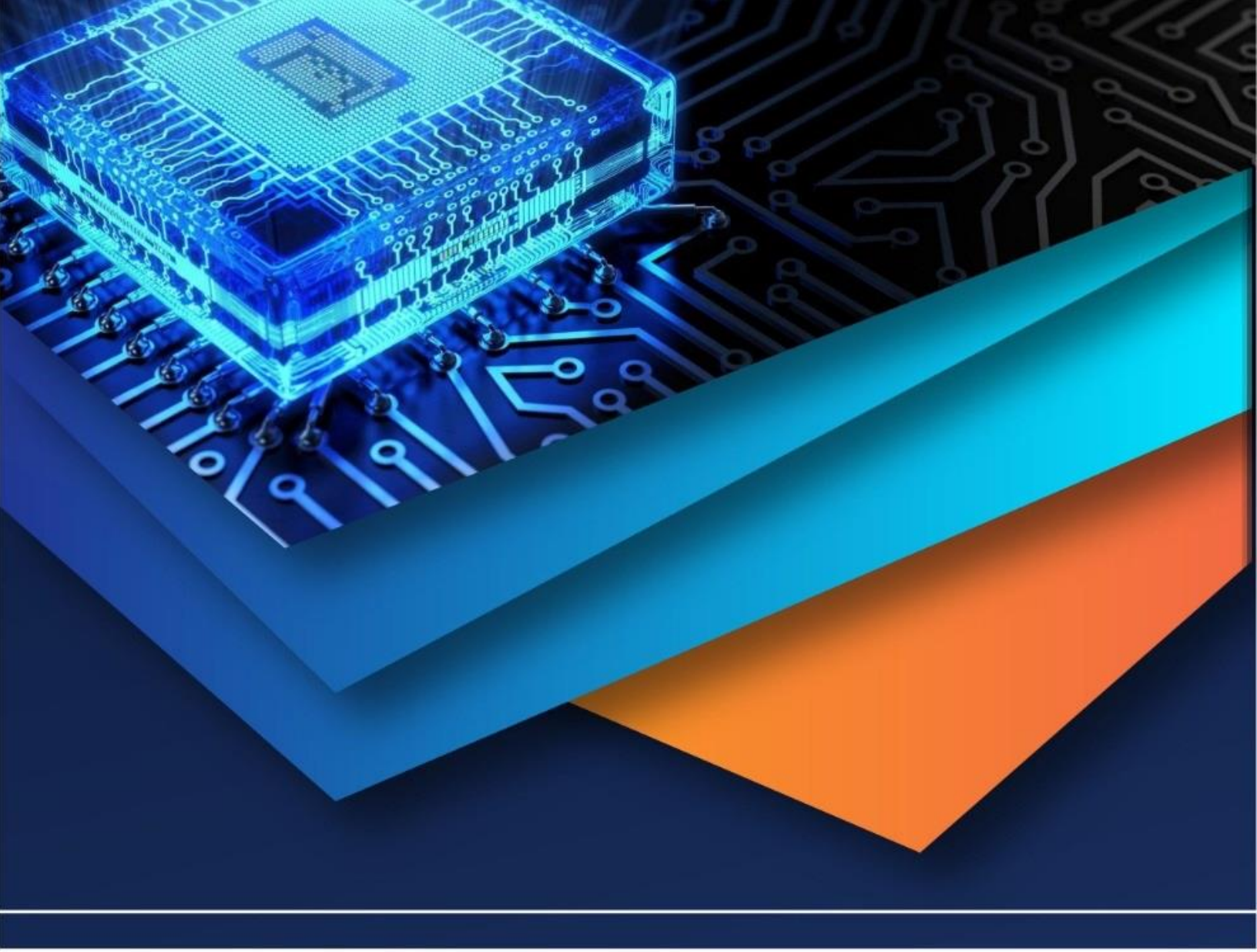
XIII. CONCLUSION

In an increasingly interconnected world, where networks are used to carry out critical transactions, computer security is a vast topic that is becoming increasingly important to society.

Cybercrime and information security continue to diverge with each passing year. In addition to the new cyber tools and threats that emerge every day, the latest and disruptive technologies are challenging organisations not only in terms of how they secure their infrastructure, but also in terms of what new platforms and intelligence they need for that. For a safe and secure future in cyberspace there is no perfect solution to cyber-crimes, but we should do our best to minimise them.

SOURCES

[1] https://danielmiessler.com/blog/
[2] https://www.csoonline.com/in/news/
[3] https://www.tripwire.com/state-of-security/
[4] https://thehackernews.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY