International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 05 | May 2024 www.irjet.net p-ISSN: 2395-0072

STUDY ON DIFFERENT TYPES OF CYBERCRIMES

Nitya Modupalli

3rd year student, Dept. Of Computer science Engineering, Sir M Visvesvaraya Institute of Technology, Karnataka, India.

Abstract - *The term "cybercrime" refers to illegal activities that aim to harm or steal data from a computer or network. Additionally, it covers the use of computers for illegal purposes, including as facilitating the trade or sale of illicit goods like narcotics or weapons online. [1] Cybercrime changes as technology does, figuring out ways to get around current security measures. Early versions first surfaced as email-based viruses and scams in the 1980s. The emergence of AI-powered phishing and social engineering, ransomware as a service (RaaS), commercial spyware, and extortionware are some of the current trends in cybercrime[2].And we must be aware of the security risks and breaches that occur, as well as how to protect ourselves against such cybercrimes.*

***Key Words*: Security breach, data, theft, cybercrime, malware, hacker.**

1.INTRODUCTION

What does a security breach entail? Any event that permits unauthorized access to computer data, applications, networks, or devices is referred to as a security breach. Unauthorized access to information results from this. It usually happens when an intruder manages to get past security measures. [3] The seven primary forms of security breaches are listed below:

1.1 MAN IN THE MIDDLE ATTACK

An attacker who inserts himself into a communication between a user and an application with the intention of eavesdropping or pretending to be one of the parties and creating the impression that a regular information flow is taking place is known as a man in the middle (MITM) attack. The purpose of an attack is to obtain personal data, including credit card numbers, account information, and login credentials. Users of financial apps, SaaS companies, e-commerce websites, and other websites requiring logins are usually the targets. In general, a Man-in-the-Middle (MITM) attack can be compared to the mailman reading your bank statement, noting your account information, resealing the package, and having it delivered to your door.[4] How are MitM attacks conducted? Cybercriminals stoop down in the middle of internet communications or data exchanges during MiTM attacks. The attacker can easily access the user's web browser and the data it sends and receives during transactions by spreading malware. Due to their requirement for secure authentication using a public and private key, online banking and e-commerce websites are often the focus of Man-in-the-Middle (MitM) attacks, which allow attackers to obtain sensitive data such as login credentials. [5]

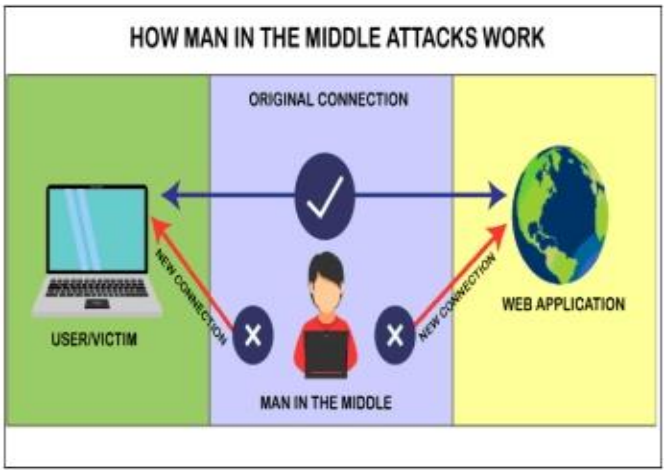

Fig 1: Representation of how man in the middle attack works.

1. 2 DENIAL-OF-SERVICE ATTACK

An attack known as a denial-of-service (DoS) aims to bring down a computer or network so that the intended users cannot use it. DoS attacks achieve this by transmitting information that causes a crash or by overloading the target with traffic. The denial of service or resource to legitimate users, such as employees, members, or account holders, is the result of a denial of service assault in both cases. DoS attack victims frequently target the web servers of well-known businesses, including banks, media, and commerce firms, as well as trade associations and governmental bodies. Even though DoS assaults seldom result in the loss or theft of important data or other assets, they can be extremely expensive and time-consuming for the victim to deal with[6] DoS attacks typically fall in 2 categories:

- Attacks using buffer overflow a kind of attack where a machine can run out of RAM, hard disk space, or CPU time due to a memory buffer overflow. This type of exploit frequently causes system crashes, sluggishness, or other harmful server behaviors, which leads to denial-of-service. [7]

- Attacks by floods A malicious actor can oversaturate server capacity and cause a denial-of-service by flooding a targeted server with an excessive number of packets. Most DoS flood attacks require the malicious actor to have more available bandwidth than the target in order to succeed.[8]

How to recognize a DDoS attack? DDoS attack symptoms can resemble computer problems, such as sluggish website file access, website inaccessibility, or even internet connection troubles. Nevertheless, there are a few primary signs that a denial of service assault may be occurring, and using website monitoring tools might assist you in identifying them. One or more of the following indicators could indicate that you are the target of a DDoS attack.

1.3 PHISHING AND SPEAR PHISHING

Phishing is a type of email attack when a hacker poses as a representative of a reliable company in order to get users' sensitive information fraudulently through electronic contact. Attackers deliberately craft emails to target a certain group, and clicking on a link in an email installs harmful code on the computer. Spear phishing is a kind of email attack when a particular individual or group is the target. In spear, a phishing attacker deceives the victim into clicking on links that download malicious programs and let the attacker to access private data on the target system or network. [10] Examples: The Puerto Rican government fell victim to a spear phishing attack that stole more than $4 million. Ubiquity Networks Inc. Lost $46.7 million as a result of spoof emails. Attackers Started a Zero-Day Exploit by Sending Skillfully Crafted Emails to Junior Staff at EMC Corp. [11]

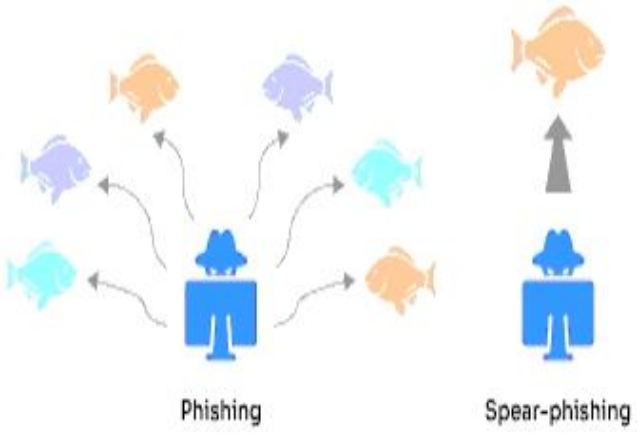

Fig 2: General representation of Phishing and Spear-phishing attack.

1.4 PASSWORD ATTACK

Cybersecurity password attacks call for specialized methods and tools. If you are in close proximity to a hacker, they might attempt to guess your password by combining names, interests, significant years, or numbers. In the event that it fails, they employ sophisticated software that goes through a list of frequently used terms as passwords. Remarkably, more than 75% of people who use the internet create passwords that are limited to the first 500 characters. [12] Password attacks leverage automated password attack tools that expedite the process of guessing and cracking passwords, along with a compromised authorization vulnerability in the system.The attacker uses a range of strategies to obtain credentials from an authorized user, expose them, and assume their identity and privileges. One of the earliest methods of account authentication that is known to exist is the username-password combination. Adversaries have had time to come up with a number of strategies for getting easily guessed passwords. Additionally, programs that depend only on password authentication are susceptible to password attacks since their flaws are widely known. [13]

1.5 EAVESDROP ATTACK.

Password When a hacker intercepts, removes, or alters information being exchanged between two devices, it is known as an eavesdropping assault. Sniffing, snooping, and eavesdropping all rely on unprotected network connections to obtain data that is being transferred between devices.

If someone joins to a network where traffic is not encrypted or secured, they are usually "attacked with eavesdropping" when they communicate confidential business information to a colleague. Since the data is being transferred via an open network, there is a chance that an attacker will be able to take advantage of a weakness and intercept it in several ways. Eavesdropping assaults are frequently hard to identify. In contrast to other types of cyberattacks, the performance might not be negatively impacted by the existence of a bug or listening device.Password.[14]

Let's look at the general steps in order to launch an eavesdropping attack

Finding an individual or group to attack is the first step in the process. The attacker begins to gather information about the target as soon as it has been identified. The communication systems and exploitable flaws are among the valuable data the attacker hopes to obtain.

Selecting a suitable approach to ensure the attack is carried out successfully is the next stage. An attacker has a variety of techniques at their disposal. A few instances include employing hardware devices, employing malware

to access a device, and intercepting communications via unprotected networks.

The selected method must now be implemented in the target system in order to intercept target communications. Ultimately, the assailant examines the intercepted correspondence and retrieves important data. Additionally, they could discard or exfiltrate data for additional study.[15]

1.6 CROSS-SITE SCRIPTING ATTACK

Injection attacks known as Cross-Site Scripting (XSS) occur when malicious scripts are inserted into websites that are otherwise trustworthy and safe. XSS attacks happen when a hacker sends malicious code—typically as a kind of a browser side script— to a different end user via an internet application. The vulnerabilities that facilitate the success of these attacks are fairly pervasive and arise each time user input is incorporated into a web application without verifying or encoding it in its output. An unknowing user may receive a malicious script from an attacker using XSS. The script will run because the end user's browser is unable to determine that it is not reliable. Because the malicious script thinks it is from a trustworthy source, it can access any cookies, session tokens, or other sensitive data that the browser stores and uses with that website. These scripts have the ability to modify the HTML page's content.

How to Determine If You Are Vulnerable

It might be challenging to find and fix XSS vulnerabilities in a web application. The best method to identify vulnerabilities is to do a security assessment of the code and look for any possible points of entry for input from an HTTP request into the HTML output. Be aware that a malicious JavaScript can be transmitted through a range of different HTML tags. While they can only look for surface-level issues, Nessus, Nikto, and other tools can assist in scanning a website for these vulnerabilities. It's highly likely that a website has further issues if even one component is weak.[16]

1.7 MALWARE ATTACK

A typical cyberattack, malware is a catch-all word for a variety of malicious programs that are installed and distributed on servers and end-user computers. Cybercriminals utilize these attacks, which are intended to damage a computer, server, or computer network, in order to collect data for financial benefit.[17]

Types of Malware Attacks

Most malware types can be classified, enter one of the subsequent categories:

1. Virus: A computer virus can spread by altering other programs and adding its malicious code when it is executed. It is one of the hardest malware kinds to get rid of and the only one that has the ability to "infect" other files.

2. Worm: By traveling from one system to another, worms can swiftly infect large networks and have the ability to replicate themselves without the assistance of end users

3. Trojan: One of the hardest kinds of malware to identify is Trojan software, which poses as a trustworthy application. When the victim executes the harmful code and instructions contained in this sort of malware, it can continue to function covertly. It is frequently used to allow malware of various kinds to infect the system.

4. Hybrid malware: These days, most malware is "hybrid," or a mix of different kinds of harmful software. For instance, "bots" initially manifest as Trojans and subsequently become worms when they are executed. They are commonly employed in larger-scale network-wide cyberattacks to target specific users..

5. Adware: Adware is software that shows users intrusive and unsolicited advertisements, such as pop-up windows.

6. Malvertising: This technique spreads malware to end-user computers by using genuine advertisements.

7. Spyware: Spyware eavesdrops on unwary users, gathering passwords, browser history, and other personal information.

8. Ransomware: Machines are infected with ransomware, which encrypts files and withholds the necessary decryption key until the victim pays. Rising ransomware assaults that target businesses and government agencies cost victims millions of dollars, with some having to pay the attackers to get their critical systems back up and running. Loky, Petya, and Cyptolocker are a few of the most well-known and prevalent ransomware families.[18]

2. THE BIGGEST DATA BREACHES OF ALL TIMES

No matter how big or small a business is, everyone is susceptible to a data leak or cyberattack. Cybercriminals and hackers devise new methods every day to obtain private or private information that they might sell or demand a ransom for. In 2023 and beyond, a lot of cyber security specialists think this number will keep going up.[19]

2.1 CAM4 DATA BREACH

Date: March 2020

Impact: 10.88 billion records.

Over 10 billion data were exposed due to a compromise in Elasticsearch on the adult video streaming website CAM4.

Sensitive data from the compromised records included the following:

- Full names
- Email addresses
- Sexual orientation
- Chat transcripts
- Email correspondence transcripts
- Password hashes
- IP addresses
- Payment logs

Email addresses that have been made public frequently refer to cloud storage providers. Hackers may have more intimate access to private images and company data if they were to carry out successful phishing attempts on these users.[20]

2.2 ALIBABA[TIE WITH AADHAAR]

Date: November 2019

Impact: 1.1 billion pieces of user data.

A developer employed by an affiliate marketer used his own crawler software to extract user information, such as usernames and cell numbers, from Taobao, the Chinese Alibaba shopping website, over the course of eight months. Although both the developer and his company received three-year prison sentences, it appears they were gathering the information for their personal use rather than selling it on the black market.[21]

2.3 YAHOO! DATA BREACH

Date: 2013-2016

Data breached: 3 billion user accounts

Based on data breach statistics, Yahoo!'s multi-year data breach is the biggest data breach in history. In addition to being the largest breach in terms of the total number of impacted users, the volume of headlines makes it seem much more significant. The outlook for the security breach became even more dire when it was found that Russian operatives had compromised the organization. Due to a class action lawsuit and settlement payments made to impacted consumers, the largest data breach in history has made a comeback to the news. [22]

2.4 FIRST AMERICAN FINANCIAL

Disclosure date: May 2019

Records compromised : 885 million.

885 million files belonging to First American Financials were reportedly exposed on the insurance company's website in May 2019, according to security expert Brian Krebs. The documents, which went back to 2003, contained photocopies of driver's licenses details on bank accounts, Social Security numbers, mortgage paperwork, and tax records. There was no password needed to access the files on the website.[23]

2.5 LINKEDLN

Date: June 2021

Impact: 700 million users.

In June 2021, professional networking company LinkedIn discovered that 700 million of its users' data had been exposed on a dark web forum, affecting almost 90% of its user base. under abusing the site's (and others') API, a hacker going under the handle "God User" employed data scraping techniques to release a first information data set that included over 500 million consumers. They boasted that they were selling the entire 700 million client database after that. While LinkedIn contended that the incident was a breach of its terms of service rather than a data breach because no sensitive, private personal data was exposed, the UK's NCSC warned that a scraped data sample posted by God User contained information such as email addresses, phone numbers, geolocation records, genders, and other social media details that would provide malicious actors with plenty of material to craft convincing, follow-on social engineering attacks following the disclosure.[24]

2.6 ADULT FRIEND FINDER

Date: October 2016

Impact: 412.2 million accounts

Cybercriminals stole 20 years' worth of user data from six databases of the adult-oriented social networking site The Friend Finder Network in October 2016. The company provides adult content and casual hookup websites such as Adult Friend Finder, Penthouse.com, and Stripshow.com. Because these are sensitive services, the breach of data from over 414 million accounts, which included names, email addresses, and passwords, could be especially damaging to the victims. Furthermore, by the time LeakedSource.com published its study of the data set on November 14, 2016, 99% of the leaked passwords had been cracked. This was due to the fact that the vast majority of the passwords had been hashed using the infamously weak SHA-1 method.[25]

3. NOTEWORTHY HACKING STATISTICS

- In 2023, the typical price of a security breach reached a record high of $4.45 million. (IBM)
- Human error accounts for 74% of cyber security breaches. (Verizon)
- A breach takes 207 days on average to find. (IBM)
- A breach typically takes 277 days to identify, contain, and resolve. (IBM)
- It is anticipated that there is a 0.05 percent chance that a cybercrime entity will be found and prosecuted in the United States. (Foreign Economic Forum)
- A human factor was implicated in 74% of breaches in 2023. (Verizon)
- The Federal Trade Commission received over 1.1 million identity theft reports in 2022 (US News).Security breaches increased in 2021 by 68 percent. (CNET)
- Apathy towards taking proactive measures to guard against cyberattacks, often known as cyberfatigue, impacts up to 42% of businesses. (Cisco)
- Of all Americans, 64% have never looked up if they were impacted by a data leak. (Vacronis)
- In 2020, the United States was the subject of 46% of cyberattacks, more than twice as many as any other nation. (Microsoft).
- 56% of Americans are unsure about the steps to take in the event of a data breach. (Vacronis)
- Since the beginning of the Russia-Ukraine war in 2022, 97% of enterprises have noticed an increase in cyber (Accenture). [26]

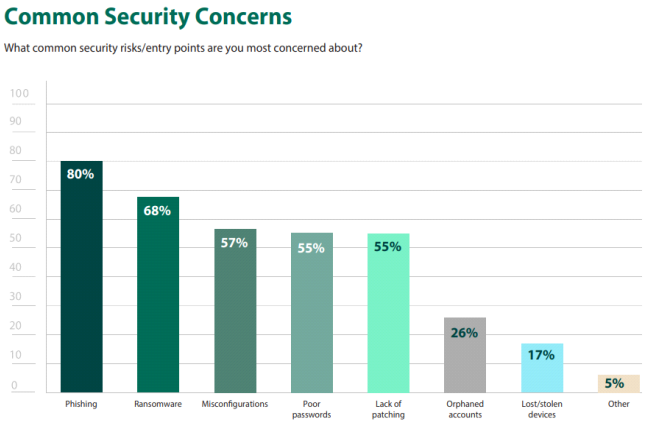

Fig 3: Graphical representation of different types of security breaches.

The graph depicted above compares several security breach types, with the Prishing kind of breach occurring at a rate of 80 percent on average.

4. PREVENTION OF BREACHES

After examining the various attack types, let's investigate ways to stop these security lapses from happening.

- Use strong passwords:

  Weak passwords are still the most frequent source of data breaches because they allow hackers to obtain user credentials and gain access to company networks. Additionally, since passwords are frequently recycled or reused across several accounts, attackers can use brute-force assaults to break into additional accounts. Use strong passwords to stop hackers from stealing login credentials. Don't forget to use a password manager.27]

- Update software regularly:

  Experts advise updating operating systems and all application software on a regular basis. When a patch is available, install it. When programs are not routinely patched and updated, your network becomes insecure. Baseline Security Analyzer, a software from Microsoft, may now be used to periodically verify that all programs are patched and up to date. This is a reasonably simple and

affordable method to fortify your network and thwart attacks before they occur.[28]

- Avoid data hoarding:

  When you find it difficult to get rid of data, you may engage in data hoarding. This is physically represented in episodes of Hoarders, if you've ever watched them. Although there is a legitimate concern of data loss, not everything needs to be kept. In actuality, there is a higher risk of exposure if personal data is never deleted. For instance, the outdated records may contain password suggestions that you currently use. Such kind of theft of obsolete data is one of the numerous reasons that data breaches occur as regularly as they do. [29]

- Restrict access to your systems:

  It may surprise you to learn that legitimate physical access to computers can result in significant data breaches. Imagine that anybody could enter your workplace, insert a malicious USB key into your computer, and have full access to the whole network.[30]

- Wifi Security:

  Even with universal wifi in 2021, there is always a risk of cyberattacks. Any connected device has the potential to get infected. In exchange, the entire enterprise's data will be seriously jeopardized if this gadget is connected to a business network.It is essential to safeguard your wifi network in order to prevent data breaches because multiple devices will connect to it. To learn more about protecting your wifi network, get in touch with a reputable Melbourne corporate IT support provider.[31]

- Create a response plan:

  Businesses need a reaction strategy in case the worst happens, as cybercriminals are growing more skilled and cyberattacks are becoming more frequent. They must have a clear plan in place for the actions that must be taken, as well as know who is in charge of informing the proper authorities about the attack. Finding out what information was taken and of what kind, updating and fortifying passwords, and keeping an eye out for hostile behavior on networks and systems are all necessary steps in this process. [32]

- Elevate Your Security Using Advanced Security Monitoring Tools:

  Using cutting-edge security solutions to keep an eye on your infrastructure is a crucial additional security measure for your data. Because networks and information technology are more sophisticated than ever, even highly skilled security experts may fall victim to hackers if they don't have the appropriate software. These days, IT specialists use artificial intelligence (AI) and systems that track network traffic variations to find anomalies and alert security experts to any observed deviations.[33]

5. CONCLUSIONS

As technology advances, more complex cyberthreats have emerged. By addressing potential cyberattacks and the various methods that hackers can obtain access to privileged or private data, we can avoid and raise awareness of these frauds. Cyberattacks can be avoided by installing many antivirus programs and adhering to a few security precautions. Taking everything into account, this study highlights the importance of cyber security and the need for additional research in this field.

ACKNOWLEDGEMENT

My heartfelt appreciation goes out to everyone who helped me finish my research paper successfully. First and foremost I would like to convey my appreciation to Dr. Savita Choudhary, my supervisor, for her steadfast support and important counsel over the whole study process. I am incredibly grateful to Sir MVisvesvaraya Institute of Technology for giving me the tools and direction I needed to finish the project successfully.Finally, but just as importantly, I want to sincerely thank my family for their unwavering affection and assistance. Their support and empathy have been invaluable to me during this research's difficult stages.This study article is the result of a team effort, and I am appreciative of everyone who helped to make it happen.

REFERENCES

[1]https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be#:~:text=Cybercrime%20generally%20includes%20criminal%20activities,like%20illegal%20drugs%20or%20weapons.

[2]https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html

[3]https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

[4]https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/#:~:text=App%20SecurityThreats-

,What%20is%20MITM%20attack,exchange%20of%20information%20is%20underway.

[5]https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM

[6]https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash.

[7]and [8]https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/#:~:text=of%2Dservice%20attack%3F-,A%20denial%2Dof%2Dservice%20(DoS)%20attack%20is%20a,interrupting%20the%20device's%20normal%20functioning.

[9]https://blog.sucuri.net/2023/03/how-to-know-if-your-site-is-under-ddos-attack.html#how-to-tell-if-you-are-being-DDoSed

[10]https://www.geeksforgeeks.org/difference-between-phishing-and-spear-phishing/

[11]https://easydmarc.com/blog/seven-examples-of-spear-phishing-attacks/

[12]https://securityboulevard.com/2022/05/what-is-a-password-attack-in-cyber-security/

[13]https://www.educative.io/answers/what-is-a-password-attack

[14]https://www.fortinet.com/resources/cyberglossary/eavesdropping

[15]Eavesdropping Attack https://www.baeldung.com/cs/eavesdropping-attack#:~:text=Some%20common%20eavesdropping%20attacks%20are,intercepts%20communication%20between%20two%20parties

[16]Overview and How to Determine If You Are Vulnerable https://owasp.org/www-community/attacks/xss/#:~:text=Overview,to%20a%20different%20end%20user.

[17]Malware Definition https://www.proofpoint.com/us/threat-reference/malware

[18]Types of Malware Attacks https://www.cyberark.com/what-is/malware/

[19]https://www.upguard.com/blog/biggest-data-breaches-us

[20]https://www.upguard.com/blog/biggest-data-breaches

[21] and [22]https://dataprot.net/articles/biggest-data-breaches/

[23]https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them

[24]https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

[25]https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

[26]https://www.varonis.com/blog/cybersecurity statistics#:~:text=The%20global%20average%20cost%20of,(IBM).

[27]https://www.fortinet.com/resources/cyberglossary/data-breach

[28]https://techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches

[29]https://surfshark.com/blog/how-to-prevent-data-breaches

[30]https://www.telcoict.com.au/8-ways-to-prevent-cyber-attacks-and-data-breaches/

[31]https://www.telcoict.com.au/8-ways-to-prevent-cyber-attacks-and-data-breaches/

[32]https://www.fortinet.com/resources/cyberglossary/data-breach

[33]https://www.globalsign.com/en/blog/preventing-data-breaches

[Fig 1]https://www.javatpoint.com/cyber-security-mitm-attacks

[Fig 2]https://www.valimail.com/guide-to-phishing/spear-phishing-vs-phishing/

[Fig 3] https://terranovasecurity.com/blog/cyber-security-statistics/