# CYBERSECURITY TRENDS

L.Petkova. PhD
University of Library and Information studies (ULIS)

lilyanapetkova92@gmail.com

***Abstract:*** *With the evolution of the digital world and the constant interaction in the real time world, even the casual user must be constantly aware of all possible threats and all possible protection actions or at least follow the trends. The vulnerabilities' definitions depend on their attacking area but with the huge space of data we never know what exactly is happening and to what is the harmed area. This article is going to provide a basic definition on the term cybersecurity and some of the most common threats along with giving some real vulnerabilities with their impact for the past decade. And as each action needs the actor, at the end there are some of the most popular academies which provide qualitative education to those who want.*

**Keywords**: CYBERSECURITY, VULNERABILITY, THREATS, SAFETY TIPS, TRAININGS

## *1. Introduction*

Globally the term **cybersecurity** refers to the infrastructure of the ICT, unlike information security which is usually related to different organizations and refers to personal information. According to NIST, cyber security is about everything in the cyber environment, and information security's scope refers to the security of the information and information systems independent of a specific area.

According to some experts, information security can be reviewed as a sup majority of cyber security. [1] But as per the definition from CyBOK, cyber security refers to the protection of information systems (*hardware, software, and associated infrastructure*), the data on them, and the services they provide, from unauthorized access, harm, or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, caused by failing to follow security procedures. [2]

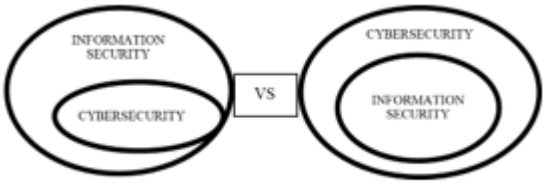



*Figure 1. Information security vs cybersecurity*

This brings the question of whether cyber security is a sup majority of the information security (*Figure 1. Information security vs cybersecurity*)! And even though in the practice, everybody is using both terms for the same thing, the context is clear. The information and cyber security must go all along!

The present article provides information on several most common attacks by giving some basic user-friendly definitions on each of them. The impact of those attacks can be proven by describing some of the most popular attacks in the last 10 years. Finally, as the digital world needs someone to try and protect it, there is some information on some popular world-wide academies which provide some quality education on cybersecurity.

## *2. Types of attacks*

Although a lot of professionals are working hard against different types of attacks and vulnerabilities, threats emerge constantly (see *Chart 1. Number of New Vulnerabilities Per Year 1988-2020*).

Below are some of those evolving threats:

**Malware**. Malicious software variants that provide unauthorized access or cause damage to a computer. Malware attacks are increasingly "fileless" and designed to get around familiar detection methods, such as antivirus tools, that scan for malicious file attachments. [5] Some of those malwares include: [6]

**(1) Virus:** A self-replicating program that attaches itself to clean files and spreads throughout a computer system, infecting files with malicious code.

**(2) Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computers causing damages or collecting data.

**(3) Spyware**: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

**(4) Ransomware**: Malware that locks down a user's files and data or systems, with the threat of erasing, destroying, or making it public, unless a ransom is paid.

**(5) Adware/Spamming**: Advertising software that can be used to spread malware.

**(6) Botnets**: Networks of malware-infected computers which cybercriminals use to perform tasks online without the user's permission.

**Phishing / social engineering**. Social engineering or Phishing is a tactic that adversaries use to trick users into providing sensitive information. In phishing scams, emails or text messages appear to be from a legitimate company asking for sensitive information, such as credit card data or login information. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source. The FBI has noted a surge in pandemic-related phishing, tied to the growth of remote work. [5][6][7]

**SQL injection**. A type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained in the database. [6]

**Insider threats**. An insider threat are current or former employees, business partners, contractors, or anyone with access to systems or networks in the past with desire to abuse their access permissions. Insider threats can be invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats. [7]

**Distributed denial-of-service (DDoS) attacks**. A DDoS attack attempts to crash a server, website, or network by overloading it with traffic, usually from multiple coordinated systems. DDoS attacks overwhelm enterprise networks via the simple network management protocol (SNMP), used for switches, modems, routers, printers, and servers. [7]

**Advanced persistent threats (APTs)**. Attack by intruder/s that infiltrates a system and remains undetected for an extended period. The intruder leaves networks and systems intact so that the intruder can spy on business activity and steal sensitive data while avoiding the activation of defensive countermeasures. An example of an APT is the recent Solar Winds breach of United States government systems. 7]

**Man-in-the-middle attacks**. A dynamic eavesdropping attack, where a third-party intercepts and takes over communications between two parties to steal data (*Figure 2. Man-in-the-middle*

*scheme*). Examples: simple eavesdropping; on an unencrypted Wi-Fi network, an attacker can intercept data being passed between a guest's device and the network. [8]

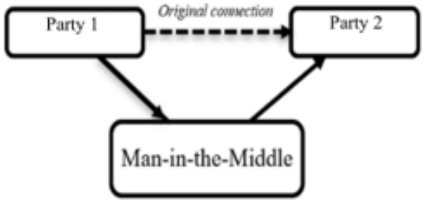



*Figure 2. Man-in-the-middle scheme*

## *3. Cyber safety tips*

There is no 100% effective protection but there are a lot of useful tricks for applying another level of security against cyber threats. Here are some of the top cyber safety tips:

**Up-to-date operating system/software**: The best option is setting up the automatic updates for never missing the latest upgrades. Otherwise keep checking manually for updates.

**Anti-virus software**: There are several free anti-virus tools which can apply a level of security to the device but limited options. More featured are the paid applications which contain a set of tools for protecting against some of the most common threats in cyberworld. Security solutions like Kaspersky Total Security will detect and remove threats. [6]

**Strong passwords**: As part of my work experience, always suggesting clients to use passwords with more than 10 (*more the better*) characters which contain at least one capital, one lower, one special character and one number.

**Frequently updated passwords**: Updating more often the passwords used on most used applications can bring another level of security. Azure Cloud sets a period after which the user is obligatorily asked for updating the password.

**Two-factor authentication**: If possible, apply 2FA to the account as it provides an additional layer of protection. Each attempt for login will be prompt with notification for suspicious action against personal data.

**Avoid sharing confidential data offline:** Data such as Social Security Number should not go online. In the hands of attackers can lead to banking account access, fake profiles and more. In need, be sure to send it encrypted.

**Avoid Suspicious Downloads**: Downloading suspicious applications or files is the most common source of attack. Some browsers have extensions limit and whenever the user is trying to download such a file, a notification message displays untrusty content.

**Avoid Suspicious email attachments**: As downloading a suspicious file, those attachments might be malwares with far more damages to apply.

**Avoid Suspicious links:** One of the most common malwares. Such spamming can lead to accessing or spreading personal data, to accessing devices, accounts and far more.

**Turn privacy settings on:** Taking care of the shared information will lead to protection against marketers and hackers' data breach. A lot of bigger applications like Facebook, LinkedIn, Twitter have privacy enhancing settings.

**Avoid Suspicious "friends' requests"**: The so-called Romance scam can lead to a fake close relationship with a goal of accessing the victim's personal data or even blackmailing. That kind of threat can be not only virtually but also by phone, flyers, and more daily stuff.

**Avoid public Wi-Fi networks**: Unsecure networks leave you vulnerable to man-in-the-middle attacks. If urgent transactions are needed, then the use of VPN can bring a level of protection against unwanted and unsafe access.

## *4. Cyber Threats examples*

Sony, Target, JPMorgan, Dropbox, Evernote, Home Depot, eBay are just a small part of the examples of companies for data leaks only since 2014. And here are some of the latest cybersecurity threats presented by Kaspersky reported by the U.K., the U.S., and Australian governments:

**Dridex malware**. A financial trojan targeting banking information. Affecting victims since 2014, it infects computers through phishing emails or existing malware. Capable of modification of directory files, firewall rules for facilitating peer-to-peer communication for extraction of data, remote execution of code, stealing passwords, accessing banking applications and websites, and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions. [9] In December 2019, the U.S. Department of Justice (DoJ) charged the leader of an organized cyber-criminal group for their part in a global Dridex malware attack. This malicious campaign affected the public, government, infrastructure, and businesses worldwide. In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, antivirus is turned on and up to date and files are backed up". [6]

**Emotet malware**. A sophisticated Trojan identified in 2014 spread through spamming that can steal data and load other malware worm-like. Originally designed as a banking malware for stealing sensitive information. One of the simplest ways of protection is creating a secure password as Emotet can be spread using a list of commonly used passwords in a brute-force attack. [10] In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware. [6]

**Romance scams**. The use of fake online identity for gaining victim's trust by creating an illusion of a romantic relationship for stealing sensitive information. For 2019 Internet Crime Complaint Center (IC3) reported this scam as the seventh most used attack and second costliest in terms of victim loss. [11] In February 2020, the FBI warned U.S. citizens to be aware of the confidence fraud that cybercriminals commit using dating sites, chat rooms, and apps. Perpetrators take advantage of people seeking new partners, duping victims into giving away personal data. The FBI reports that romance cyber threats affected 114 victims in New Mexico in 2019, with financial losses amounting to $1.6 million. [6]

**DearCry & Hafnium ransomware**. Zero-Day attacks on Microsoft Exchange. In March 2021, Microsoft released patches for critical vulnerabilities within Microsoft Exchange servers. The DearCry malware performs drive enumeration to identify all accessible storage media from an infected machine. For each of these drives, the DearCry ransomware will encrypt certain types of files (based on file extensions) using AES and RSA-2048. After encryption is complete, DearCry will display a ransom note instructing users to email the ransomware operators to learn how to decrypt their machines. [12]

## *5. Cybersecurity education*

There are a lot of cybersecurity education and training programs in preparing cyber security practitioners. Each provides a necessary basis for everybody ready for the battle:

**SANS CYBER ACADEMIES** created by CyberTalent Immersion Academy provides accelerated training program and GIAC certifications in cybersecurity in four types: (1) **VetSuccess** – for veterans in cybersecurity; (2) **Women's Academy** – for career-changers and college seniors with a background in IT; (3) **Cyber Workforce** – sponsored in looking to hire cybersecurity talents; (4) **Diversity Cyber Academy** – in partnership of SANS and International Consortium of Minority Cybersecurity Professionals

(ICMCP) for increasing the career opportunities for minorities and women in cybersecurity. [13]

**UK CYBER RETRAINING ACADEMY** provides an opportunity for those with high natural aptitude, but no formal cyber background, to undergo an intensive 10-week program for cybersecurity careers. This initiative is funded by the government's National Cyber Security Program and developed in partnership with the SANS Institute. [14]

**THE NATIONAL CENTERS OF ACADEMIC EXCELLENCE** (CAE) program is a U.S. government program that focuses on improving cybersecurity education in the United States by encouraging colleges with cybersecurity degrees to meet a set of academic standards developed by experts at the NSA and DHS. Over 230 schools have been designed as Centers of Academic Excellence in **Cyber Defense (CAE-CD)**, focusing on reducing vulnerabilities in our national information infrastructure. More than 20 are recognized as Centers of Academic Excellence in **Cyber Operations (CAE-CO)**, concentrating on specialized offensive cyber operations to enhance U.S. national security. [14]

**THE U.S. CYBER CHALLENGE (USCC)** is a national program supported by DHS that consists of two complementary initiatives: the **Cyber Quests** online challenge series and the **Cyber Camp** program for aspiring cyber professionals. The **Cyber Quests** are a series of online challenges demonstrating knowledge and aptitude in information security and cover tasks ranging from secure coding to network monitoring. Some quests are focused on potentially vulnerable web servers, others – around forensic analysis, packet capture analysis, and more. Based on the performance in the Cyber Quests, participants are invited to one of USCC's Cyber Camps. The **Cyber Camps** are a week-long cybersecurity training focused on a variety of topics like intrusion detection, penetration testing and forensics. [14][15]

**CYBERCAMP** is a live-online course led by Israeli experts. Contains over 300 academic hours workshops incorporating over 150 hours of hands-on security labs, hacking competitions, and instruction by leading university and industry professionals in topics like penetration testing, packet crafting, and TCP/IP warfare and tools like Wireshark, nmap, Metasploit, Hydra, sqlmap, Autopsy, Nesus, Burp Suite and more. This program provides hands-on training and preparation for the following industry certifications: CompTIA Security+ and CEH: Certified Ethical Hacker. [16]

## *6. Results*

The constant evolution comes with constant vulnerability issues. Only for 2020, the number of vulnerabilities is 17991 which is more than 500 more than the previous year (not to mention years before that). And according to most recent reports only for the first half of 2021, this number is already over 12000. [3][4]

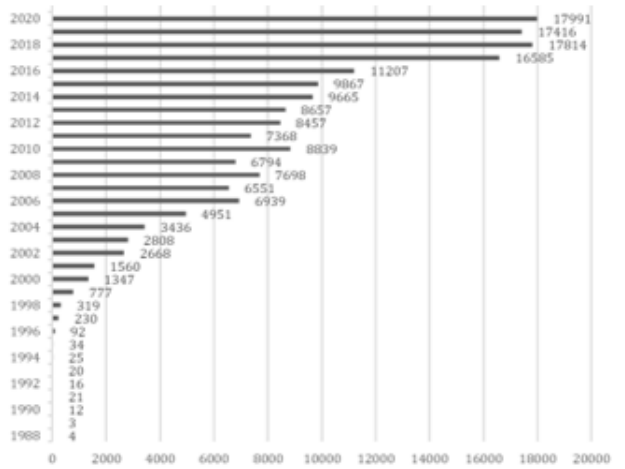



*Chart 1. Number of New Vulnerabilities Per Year 1988-2020*

According to research from 2019, each attack's results can be based on three factors according to its damages: **Materiality**, **Insignificance**, **Uncertainty.** (*See Chart 2. Cyber Threats for 2019*)

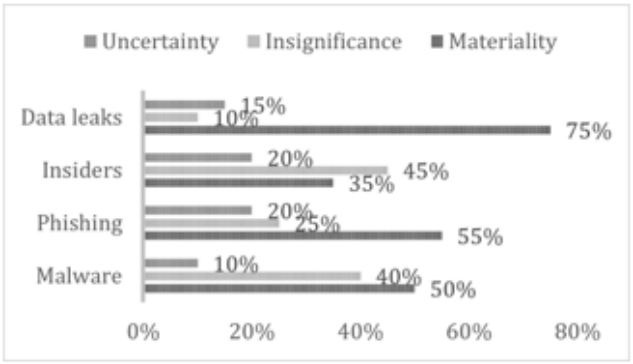



*Chart 2. Cyber Threats for 2019*

Based on that analysis, the following results are presented: (1) The material damages from 3 out of 4 presented attacks are critical (*over 50%*). (2) The significance level has almost the same risk level as the material damage. Two out of 4 are around 40% insignificant. (3) The level of uncertainty of each of the attacks is less than 20% per each predicting future lack of sureness.

In conclusion for 2019 we can say that more than 50% of the attacks are with high risk of damages and around 11% are insignificant.

Compared with another research from 2020, critical attacks jump off to over 80% and 6% with low risk.

And if we consider *Chart 1. Number of New Vulnerabilities Per Year 1988-2020* and the number present in this article for 2021 (*almost 12000 just for the first half of the current year*), we can even say that that number is already higher compared to the entire previous year.

## *7. Conclusion*

As already mentioned, the definitions of information security and cybersecurity can be equally used. Or at least are always going together. This digital evolution is good in some perspectives, but worst in another. The constant battle between users and attackers becomes more and more dangerous. And the numbers prove it (*Chart 1. Number of New Vulnerabilities Per Year 1988-2020*)! The level of protection depends on the experience of people who need to work even harder in order for them to be in this profession. And that is just because of that evolution…of that constant innovative digital world.

Hence, the question is always about the future. What will happen tomorrow when a new threat comes up? What will happen if those who have worked hard to try to protect us as users from that highly increasing vulnerable world are not good enough for that job?

And unfortunately, the answer is as "simple" as the questions: while there are obstacles on the road, there will be someone to try and remove them! There is no universal and complete way of protection against it. This is just a constant battlefield for security. And each year those security trends will leave the same or enhance according to the need.

**References**


[1] Dimitrov, W. (2017). *ICT Security Trends.* Sofia: Avangard, ISBN 978-619-160-766-2

[2] CyBOK (October 2019). Retrieved from https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

[3] StatCounter. (n.d.). Retrieved from https://gs.statcounter.com/

[4] CVE details (n.d.). Retrieved from https://www.cvedetails.com/

[5] Petkova, L. (2019). SEO SPAM AND MALWARE. *Proceedings Knowledge Society and 21st Century Humanism* (pp. 407-415). Sofia, Bulgaria: UNIBIT., ISSN 2683-0094

[6] Kasperski (2021). What is Cyber Security? Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[7] IBM (2021). What is cybersecurity? Retrieved from https://www.ibm.com/topics/cybersecurity

[8] Mallik, Avijit. (2019). Man-in-the-middle-attack: Understanding in simple words

[9] Cybersecurity&Infrastructure Security Agency (June 2020). Retrieved from https://us-cert.cisa.gov/ncas/alerts/aa19-339a

[10] Malwarebytes (2021). Retrieved from https://www.malwarebytes.com/

[11] FBI (2021). Retrieved from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams

[12] Cyberint Research (March 2021). Dearcry Ransomware Microsoft Exchange Exploited. Retrieved from https://blog.cyberint.com/dearcry-ransomware-microsoft-exchange-exploited

[13] SANS (2021). SANS Cyber Academies. Retrieved from https://www.sans.org/about/academies/

[14] Lewis, J. A. (2019, January). The cybersecurity workforce gap. Retrieved from https://www.csis.org/analysis/cybersecurity-workforce-gap

[15] US Cyber Challenge (2021). Retrieved from https://www.uscyberchallenge.org/

[16] CyberCamp (2021). Retrieved from https://www.cybercamp.co/academy