# Threats to information security & communication security and various countermeasures

## A White Paper

***25/March/2022***

***SHUBHAM AGARWAL***

***19BIT0010***

# Contents

1. Introduction ..... 2
2. Abstract ..... 2
3. Problem Statement ..... 2
4. Proposed Solution(s) ..... 4
   **1.** Introduction of Solution ..... 4
   **2.** Application of Solution ..... 5
5. Future Direction ..... 7
6. Conclusion ..... 7

# 1. Introduction

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various actors, including corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers and disgruntled employees.

In recent years, numerous high-profile cyber-attacks have resulted in sensitive data being exposed. For example, the 2017 Equifax breach compromised the personal data of roughly 143 million consumers, including birth dates, addresses and Social Security numbers. In 2018, Marriott International disclosed that hackers accessed its servers and stole the data of roughly 500 million customers. In both instances, the cyber security threat was enabled by the organization's failure to implement, test and retest technical safeguards, such as encryption, authentication and firewalls.

Cyber attackers can use an individual's or a company's sensitive data to steal information or gain access to their financial accounts, among other potentially damaging actions, which is why cyber security professionals are essential for keeping private data protected.

# 2. Abstract

A cybersecurity threat is a **malicious** and **deliberate attack** by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

# 3. Problem Statement

Top 10 cyber security threats are as follow:

### 1) Malware

Malware attacks are the most common cyber security threats. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.According to Accenture, the average cost of a malware attack is USD 2.6 million.

### 2) Phishing

Cybercriminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware

installation or disclosure of sensitive information like credit card details and login credentials. Phishing attack accounts for over 80% of reported cyber incidents.

**3) Spear Phishing**

Spear phishing is a more sophisticated form of a phishing attack in which cybercriminals target only privileged users such as system administrators and C-suite executives. More than 71% of targeted attacks involve the use of spear phishing.

**4) Man in the Middle Attack**

Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication. Once the attacker interprets the communication, they may filter and steal sensitive data and return different responses to the user. According to Netcraft, 95% of HTTPS servers are vulnerable to MitM.

**5) Denial of Service Attack**

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack. The year 2019 saw a staggering 8.4 million DDoS attacks.

**6) SQL Injection**

A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database. SQL injection accounts for nearly 65.1% of all web application attacks.

**7) Zero-day Exploit**

A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploit the vulnerability before a patch or solution is implemented.It is predicted that zero-day attacks will rise to one per day by 2021.

**8) Advanced Persistent Threats (APT)**

An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.45% of organizations feel that they are likely to be the target of an APT.

**9) Ransomware**

Ransomware is a type of malware attack in which the attacker locks or encrypts the victim’s data and threatens to publish or blocks access to data unless a ransom is paid. Learning more about ransomware threats can help companies prevent and cope with them better. Ransomware attacks are estimated to cost global organizations USD 20 billion by 2021.

### 10) DNS Attack

A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems (DNS Tunneling).

# 4. Proposed Solution(s)

## *1. Introduction of Solution*

### 1) Create an Insider Threat Program

Creating an insider threat program is imperative for organizations to prevent employees from misusing their access privileges to steal or destroy corporate data. The IT security team should not delay and gain the approval of top management to deploy policies across departments.

### 2) Train employees

Employees are the first line of defense against cyberthreats for every organization. Thus, organizations must conduct comprehensive cybersecurity awareness programs to train employees on recognizing and responding to cyber threats. This dramatically improves an organization's security posture and cyber resilience.

### 3) Maintain Compliance

Irrespective of the level of cybersecurity an organization implements, it must always maintain compliance with data regulations that apply to their industry and geographical location. The organization must stay informed with the evolving compliance regulations to leverage its benefits.

### 4) Build a Cyber Incident Response Plan

In the present digital era, no organization is exempt from cyberattacks. Thus, organizations of all sizes must build an effective Cyber Security Incident Response Plan (CSIRP) to navigate cyber adversaries. It enables businesses to prepare for the inevitable, respond to emerging threats, and recover quickly from an attack.

**5) Regularly Update Systems and Software**

As cyber threats are evolving rapidly, your optimized security network can become outdated within no time, putting your organization at the risk of cyberattack. Therefore, regularly update the security network and the associated systems and software.

**6) Backup Data**

Backing up data regularly helps reduce the risk of data breaches. Backup your website, applications, databases, emails, attachments, files, calendars, and more on an ongoing and consistent basis.

**7) Initiate Phishing Simulations**

Organizations must conduct phishing simulations to educate employees on how to avoid clicking malicious links or downloading attachments. It helps employees understand the far-reaching effects of a phishing attack on an organization.

**8) Secure Site with HTTPS**

Organizations must encrypt and secure their website with an SSL (Secure Sockets Layer) certificate. HTTPS protects the integrity and confidentiality of data between the user and the website.

## *2. Application of Solution*

**Preventing viruses and worms**

To reduce the risk of these types of information security threats caused by viruses or worms, companies should install antivirus and antimalware software on all their systems and networked devices and keep that software up to date. In addition, organizations must train users not to download attachments or click on links in emails from unknown senders and to avoid downloading free software from untrusted websites. Users should also be very cautious when they use P2P file sharing services and they shouldn't click on ads, particularly ads from unfamiliar brands and websites.

**Preventing drive-by download attacks**

One of the best ways a company can prevent drive-by download attacks is to regularly update and patch systems with the latest versions of software, applications, browsers, and operating systems. Users should also be warned

to stay away from insecure websites. Installing security software that actively scans websites can help protect endpoints from drive-by downloads.

## Preventing phishing attacks

Enterprises should train users not to download attachments or click on links in emails from unknown senders and avoid downloading free software from untrusted websites.

## Preventing DDoS attacks

To help prevent DDoS attacks, companies should take these steps:

- Implement technology to monitor networks visually and know how much bandwidth a site uses on average. DDoS attacks offer visual clues so administrators who understand the normal behaviors of their networks will be better able to catch these attacks.
- Ensure servers have the capacity to handle heavy traffic spikes and the necessary mitigation tools necessary to address security problems.
- Update and patch firewalls and network security programs.
- Set up protocols outlining the steps to take in the event of a DDoS attack occurring.

## Preventing ransomware

To protect against ransomware attacks, users should regularly back up their computing devices and update all software, including antivirus software. Users should avoid clicking on links in emails or opening email attachments from unknown sources. Victims should do everything possible to avoid paying ransom. Organizations should also couple a traditional firewall that blocks unauthorized access to computers or networks with a program that filters web content and focuses on sites that may introduce malware. In addition, limit the data a cybercriminal can access by segregating the network into distinct zones, each of which requires different credentials.

# 5. Future Direction

Cyber security practices continue to evolve as the internet and digitally dependent operations develop and change. According to Secureworks, people who study cyber security are turning more of their attention to the two areas in the following sections.

### The Internet of Things

Individual devices that connect to the internet or other networks offer an access point for hackers. Cytelligence reports that in 2019, hackers increasingly targeted smart home and internet of things (IoT) devices, such as smart TVs, voice assistants, connected baby monitors and cellphones. Hackers who successfully compromise a connected home not only gain access to users' Wi-Fi credentials, but may also gain access to their data, such as medical records, bank statements and website login information.

### The Explosion of Data

Data storage on devices such as laptops and cellphones makes it easier for cyber attackers to find an entry point into a network through a personal device. For example, in the May 2019 book Exploding Data: Reclaiming Our Cyber Security in the Digital Age, former U.S. Secretary of Homeland Security Michael Chertoff warns of a pervasive exposure of individuals' personal information, which has become increasingly vulnerable to cyber attacks.

Consequently, companies and government agencies need maximum cyber security to protect their data and operations. Understanding how to address the latest evolving cyber threats is essential for cyber security professional

# 6. Conclusion

As reliance on digital technologies continues to increase, cyber attacks have become too sophisticated. Thus, organizations that rely on outmoded cybersecurity strategies leave themselves vulnerable to a potential cyberattack.

To prevent these threats, organizations must refine their cybersecurity program. An effective cybersecurity program can help organizations disrupt attacks as they occur, reduce recovery time, and contain future threat.