International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 02 | February - 2023 Impact Factor: 7.185 ISSN: 2582-3930

CYBER SECURITY

Krishna Panchal and Manas Sharma

What is Cyber Security?

- **Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

- **Information security** protects the integrity and privacy of data, both in storage and in transit.

- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Why Is Cyber Security Important?

Today, as the scope, sophistication, and strategy of cyberthreats continually evolve, legacy security tools like firewalls and antivirus are insufficient to prevent hackers from gaining unauthorized access.
At the height of the COVID-19 pandemic, many organizations adopted bring your own device (BYOD) policies for employees, partners, and other stakeholders. However, a large number of these organizations lacked malware protection or relied on legacy endpoint and network security solutions to protect BYOD. In failing to account for remote work in their cybersecurity risk management programs, many gambled with their sensitive information, and likely saw costs rise as a result.
Even now, as many organizations settle into hybrid work models, numerous factors—enabling secure remote access and connectivity, adopting technologies to maintain productivity and ensure security, enforcing remote security policies, and handling security issues such as shadow IT on home networks, to name a few—have become everyday headaches for security admins alongside the ongoing shortage of cybersecurity talent.
To this end, organizations can look to the National Institute of Standards and Technology (NIST), which develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of US industry, federal agencies, and the broader public.
Without an effective cybersecurity program, organizations can fall prey to cyberattacks that overtax budgets and harm the bottom line due to:

- Loss of intellectual property and sensitive information
- Downtime stemming from system failure or ransomware attacks
- Data compromise resulting in legal trouble and/or lost business

Types of Cyber threats

- The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
2. **Cyber-attack** often involves politically motivated information gathering.
3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

Malware

What is malware?
Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:
Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
Trojans : A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
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.
Ransomware : Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
Adware : Advertising software which can be used to spread malware.
Botnets :Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

Latest cyber threats

What are the latest cyber threats that individuals and organizations need to guard against? Here are some of the most recent cyber threats that the U.K., U.S., and Australian governments have reported on.

- Dridex malware -

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 Dried malware attack. This malicious campaign affected the public, government, infrastructure and business worldwide.
Dridex is a financial trojan with a range of capabilities. Affecting victims since 2014, it infects computers though phishing emails or existing malware. Capable of stealing passwords, banking details and personal data which can be used in fraudulent transactions, it has caused massive financial losses amounting to hundreds of millions.
In response to the Dridex attacks, the U.K.'s National Cyber Security Centre advises the public to "ensure devices are patched, anti-virus is turned on and up to date and files are backed up".

- Romance scams -

In February 2020, the FBI warned U.S. citizens to be aware of 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.

- Emotet malware -

In late 2019, The Australian Cyber Security Centre warned national organizations about a widespread global cyber threat from Emotet malware.
Emotet is a sophisticated trojan that can steal data and also load other malware. Emotet thrives on unsophisticated password: a reminder of the importance of creating a secure password to guard against cyber threats.

Cyber safety tips - protect yourself against cyberattacks
How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1.**Update your software and operating system** : This means you benefit from the latest security patches.

2.**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.

3.**Use strong passwords** : Ensure your passwords are not easily guessable.

4.**Do not open email attachments from unknown senders** : These could be infected with malware.

5.**Do not click on links in emails from unknown senders or unfamiliar websites** : This is a common way that malware is spread.

6.**Avoid using unsecure WiFi networks in public places** : Unsecure networks leave you vulnerable to man-in-the-middle attacks.

What Is the Future of Cyber Security?

Cybersecurity professionals use technologies such as artificial intelligence (AI), machine learning, and automation to create new strategies to protect information systems.
Some of the most important battlegrounds in the future of cybersecurity will be:

- **Mobile device security :** As more people connect using multiple mobile devices, organizations need to change the way they defend their systems, especially as these systems connect via home Wi-Fi networks. Agile, new cybersecurity technologies can help protect data while ensuring a smooth user experience.

- **Cloud security :** As organizations adopt a multicloud approach, the number of third-party partners working with them grows. Each of these partners have different cybersecurity mechanisms and will make it more difficult to ensure security.

- **Security as a service (SECaaS) :** The rise of SECaaS providers gives organizations access to the latest technology and practiced security professionals.

- **AI and automation :** While cybercriminals are turning to AI to exploit weaknesses in defenses, cybersecurity professionals are using the same technology to monitor and protect networks, endpoints, data, and IoT.

- **Zero trust :** The advent of BYOD and hybrid work has made organizations more flexible, but also more vulnerable, than ever. Zero trust security only grants authentication to applications based on context such as location, role, device, and user.

Who Is Responsible for Managing Cyber Security?

An effective cybersecurity strategy requires an organization-wide approach from top executives down to temporary office staff. Everyone needs to be aware of their responsibilities, the latest policies, best practices for information security, and their role in the overall strategy.
With the rise of the cloud, cybersecurity is changing. Organizations are seeing the value of moving security away from the data center and into the cloud. In doing so, they are getting the following benefits:

- Employees get the same protection whether they're in the HQ, branch offices, on the road, or at home.

- Integrated security controls and cloud services correlate information to give organizations a complete picture of everything happening on the entire network.

- Traffic is no longer backhauled to the corporate data center, eliminating much of the performance lag when accessing cloud-based applications and data.

- Stacks of single-purpose security appliances are integrated into a single platform.

- Threat intelligence can be updated much more quickly than with appliances. Any time a threat is detected in a cloud platform, that information is shared with the entire network instantaneously, and protection is deployed in real time.

- Costs can be controlled as there are no more appliances to buy, maintain, or upgrade.

Dangerous cyber Security myths

The volume of cybersecurity incidents is on the rise across the globe, but misconceptions continue to persist, including the notion that:

- **Cybercriminals are outsiders :** In reality, cybersecurity breaches are often the result of malicious insiders, working for themselves or in concert with outside hackers. These insiders can be a part of well-organized groups, backed by nation-states.

- **Risks are well-known :** In fact, the risk surface is still expanding, with thousands of new vulnerabilities being reported in old and new applications and devices. And opportunities for human error - specifically by negligent employees or contractors who unintentionally cause a data breach - keep increasing.

- **Attack vectors are contained :** Cybercriminals are finding new attack vectors all the time - including Linux systems, operational technology (OT), Internet of Things (IoT) devices, and cloud environments.

- **My industry is safe :** Every industry has its share of cybersecurity risks, with cyber adversaries exploiting the necessities of communication networks within almost every government and private-sector organization. For example, ransomware attacks (see below) are targeting more sectors than ever, including local governments and non-profits, and threats on supply chains, ".gov" websites, and critical infrastructure have also increased.