

Trinity International College

(Under the affiliation of Tribhuvan University)

Dillibazar, Kathmandu, Nepal

A Seminar on

“**Computer Security**”

Submitted to:Abhishek Dewan

Department of Computer Science and Information Technology

Trinity International College

By: **Pradeep Thapa**

Roll No: 16

Semester:1st semister

Batch:BCA

Date:2079/12/1

**Table of Contents**

1. INTRODUCTION
2. HISTORY / BACKGROUND
3. WORKING MECHANISM
4. APPLICATION IN REAL LIFE
5. ADVANTAGES & DISADVANTAGES
6. FUTURE OF THE TECHNOLOGY
7. CONCLUSION
8. REFERENCES

**1. INTRODUCTION**

**Computer security is the protection that is set up for computer systems and keeps critical information from unauthorized access, theft, or misuse. There are various practices in place that are widely in use, mainly for the protection of computer systems and networks and preventing potential malicious activities.**

**While computer hardware is secured in the same way that sensitive equipment such as lockers and doors are protected, critical information and system access and authorization, on the other hand, are protected through complex security tactics and practices.That’s all for computer security definition. Let’s move on to the section on security threats and issues.Computer security threats are potential risks that have the capability of disrupting the normal functioning of computer systems. Cyber threats are on the rise each day, especially with the digitization of the world. Let’s take a look at all kinds of major computer security threats, issues, and vulnerabilities.**

**A**[**Computer Virus**](https://intellipaat.com/blog/computer-virus/)**is a malicious program that is installed into a computer without the knowledge of its user. This program can replicate itself and infect all the programs and files that are in the system. These viruses make the victim’s computer malfunction or, at the worst, completely unusable.**

**If a computer security system is not put in place until a problem arises, it could lead to major issues and concerns, and it will be too late to resolve them. Especially in a data-driven world, it is imperative to keep all kinds of information from malicious hackers and prevent vital information from falling into the wrong hands for misuse.**

**Computer security helps keep valuable information protected and maintain the health of a computer with no disruptive behavior in its performance caused by viruses and malware.**

**2**.**History/Background**

**Since computers got connected to the internet and began exchanging messages, cybercrime has substantially changed. Even if the amount of risk is substantially higher now than it was back then, computer users have been understandably concerned about these threats for a long time**.

### ****The 1940s:**** The Time Before Cybercrime

**Cyberattacks were challenging to execute for about 20 years after the first digital computer was built in 1943.**

### ****2. The 1950s:**** The Phone Phreaks

**Computer information gathering was not the original purpose of hacking. It may be more accurate to say that early telephone use is where computer hacking originated.**

### ****3. The 1960s:**** All Quiet On the Western Front

**Even by the middle of the 1960s, most computers were massive mainframes kept in temperature-controlled, safe environments. .**

### ****4. The 1970s****: ARPANET and the Creeper

**The 1970s saw the actual start (and need) of cybersecurity. It was an important decade in the evolution of cyber security.**

### ****5. The 1980s:****The Birth of Commercial Antivirus

**High-profile attacks increased in frequency in the 1980s, including those at National CSS, AT&T, and Los Alamos National Laboratory. In the 1983 movie War Games, a malicious computer software commands nuclear missile systems while pretending to be a game.**

### ****6. The 1990s:****The World Goes Online

**The internet saw growth and development of mammoth proportions during the whole decade. Along with it, the cybersecurity sector expanded.**

* **.**

### ****7. The 2000s:****Threats Diversify and Multiply

**The internet's growth during this time was amazing. The majority of homes and businesses now had computers. There were numerous benefits, but, unfortunately, cybercriminals also got new opportunities. A brand-new infection type that didn't require file downloads appeared at the beginning of this decade in the history of computer security.**

**Just going to a website with a virus on it was enough. This type of covert infection posed a serious threat. Additionally, instant messaging systems were compromised.**

**The number of credit card hacks also increased in the 2000s. There have been massive credit card data leaks.**

**3.Working Mechanism**

**This collection of topics describes aspects of security to consider in your IBM® WebSphere® MQ installation.**

**The commonly accepted aspects of security are as follows:**

* [**Identification and authentication**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.html)
* [**Authorization**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009750_.html)
* [**Auditing**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009760_.html)
* [**Confidentiality**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009770_.html)
* [**Data integrity**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009780_.html)

***Security mechanisms* are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows:**

* [**Cryptography**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009800_.html)
* [**Message digests and digital signatures**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009810_.html)
* [**Digital certificates**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009820_.html)
* [**Public Key Infrastructure (PKI)**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009900_.html)

**When you are planning a IBM WebSphere MQ implementation, consider which security mechanisms you require to implement those aspects of security that are important to you. For information about what to consider after you have read these topics, see**[**Planning for your security requirements**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q010270_.html)**.**

* [**Identification and authentication**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.html) ***Identification* is the ability to identify uniquely a user of a system or an application that is running in the system. *Authentication* is the ability to prove that a user or application is genuinely who that person or what that application claims to be.**
* [**Authorization**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009750_.html) ***Authorization* protects critical resources in a system by limiting access only to authorized users and their applications. It prevents the unauthorized use of a resource or the use of a resource in an unauthorized manner.**
* [**Auditing**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009760_.html) ***Auditing* is the process of recording and checking events to detect whether any unexpected or unauthorized activity has taken place, or whether any attempt has been made to perform such activity.**
* [**Confidentiality**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009770_.html) **The *confidentiality* service protects sensitive information from unauthorized disclosure.**
* [**Data integrity**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009780_.html) **The *data integrity* service detects whether there has been unauthorized modification of data.**
* [**Cryptographic concepts**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009790_.html) **This collection of topics describes the concepts of cryptography applicable to WebSphere MQ.**
* [**Cryptographic security protocols: SSL and TLS**](https://www.ibm.com/docs/en/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009910_.html) **Cryptographic protocols provide secure connections, enabling two parties to communicate with privacy and data integrity. The Transport Layer Security (TLS) protocol evolved from that of the Secure Sockets Layer (SSL). IBM WebSphere MQ supports both SSL and TLS.**
* APPLICATION IN REAL LIFE

**4.APPLICATION IN REAL LIFE**

[**Cybersecurity**](https://www.knowledgehut.com/blog/security/nist-cybersecurity-framework)**threats change over time, and it is important for organizations to counter these threats. Intruders adjust by creating new tools and tactics to undermine security when new protections are developed to counter more recent attacks.**

### 1. Network Security Surveillance

**Continuous network monitoring is the practice of looking for indications of harmful or intrusive behavior. It is often used in conjunction with other security tools like firewalls, antivirus software, and IDPs. Monitoring for network security may be done manually or automatically using the software.**

### 2. Identification And Access Control (IAM)

**The**[**management**](https://www.knowledgehut.com/blog/others/what-is-management)**has control over which individual can access which sections of the data. Usually, the management regulates who has access to data, networks, and computer systems. Here is where [cybersecurity](https://www.knowledgehut.com/blog/security/cyber-security-demand" \t "_blank) comes into the picture by identifying users and executing an access control. Various**[**cyber security applications**](https://www.knowledgehut.com/blog/security/applications-of-cyber-security)**ensure IAM across an organization. IAM may be implemented in both software and hardware, and it often makes use of role-based access control (RBAC) to limit access to certain system components.**

**.**

### 3. Software Security

**Applications that are crucial to company operations are protected by application security. It contains controls like code signing and application whitelisting and may assist unify your security rules with things like file-sharing rights and multi-factor authentication. With the application of AI in**[**cyber security**](https://www.knowledgehut.com/blog/security/importance-of-cyber-security)**, software security is bound to increase.**

### 4. Risk Management

**Risk management, data integrity, security awareness training, and risk analysis are all covered by**[**cyber security**](https://www.knowledgehut.com/blog/security/cyber-security-tips)**. The evaluation of risks and the control of the harm that may be done as a result of these risks are important components of**[**risk management**](https://www.knowledgehut.com/blog/project-management/risk-management)**. The security of sensitive information is another issue covered by data security.**

### 5. Planning for disaster recovery and business continuity

**Data recovery enables organizations to continue working in the event of data loss, assaults, or calamities. By regularly data backup and spending money on a system that will enable corporate activities to continue, this application offers models or techniques that may help firms manage with severe data loss. Thus, this application of cybersecurity ensures business continuity.**

### 6. Physical Security

**System locks, intrusion detection systems, alarms, surveillance systems, and data-destruction systems are a few examples of physical security measures. These allow organizations to secure their IT infrastructure.**

### 7. Compliance And Investigations

[**Cybersecurity**](https://www.knowledgehut.com/blog/security/computer-science-vs-cyber-security)**is helpful during the examination of suspicious situations. Additionally, it helps to upkeep and adhere to regulations.**

### 8. Security During Software Development

**The software aids in detecting software flaws when they are being developed and ensuring that regulations and standards are followed. Cybersecurity tools thoroughly test, scan, and analyze the software to identify any bugs, openings, or weaknesses that hackers or competing businesses might exploit.**

### 9. Security Against DDoS

**Cybersecurity aids in providing a mitigation solution to deal with DDoS. It redirects traffic to other cloud-based servers and resolves the issue.**

### 10. Protecting Critical Systems

**Cybersecurity aids in preventing assaults on huge servers linked to wide-area networks. It upholds industry-standard, strict safety standards for users to abide by cybersecurity precautions to secure the devices. It keeps track of all apps in real time and routinely evaluates the network security, servers, and users themselves.**

**5.ADVANTAGES & DISADVANTAGES**

**Cyber security safeguard business: The most significant benefit is that the best in IT security cyber security solutions can give your company comprehensive digital protection. This allows flexibility of accessing the internet by the staff and ensuring the safety and protection from possible threats and risks.**

****

**Protects Personal Information: In this age of a digitally-driven world, one of the most valuable commodities is personal information. If a virus is able to collect personal information about your employees or customers, it is quite likely that it will be sold or used to steal their money.**

**Protects and Enhances Productivity: Viruses infecting your systems and network will result in functioning resulting in the almost impossibility of further working. In effect, this will cause downtime in work for your staff and wastage additionally bringing the entire company to a halt.**

**Prevents crashing of websites: If you're a small business, you're probably hosting your own website. If your system is infected, there's a good risk your website will be forced to go down. This means that not only will you incur losses due to missed transactions, but you will also run the risk of losing trust from your clients, and some viruses may cause long-term damages to your systems.**

**Support Your IT Professional: Typically, a good security system equips your organization and employees with the best tools, techniques, and assistance in combating cyber attacks and criminals.**

**In a nutshell, we can list out the advantages of cyber security as follows:**

****

* **It will safeguard your company.**
* **Please keep your personal information private.**
* **Enables users to work in a relaxed environment.**
* **It also maintains efficiency.**
* **Various jobs are mechanized as a result of this.**

**6. FUTURE OF THE TECHNOLOGY**

**Let us explore the future of the cybersecurity industry:**

### ****1. Cyber crime-as-a-service (CaaS)****

**Cyber crime-as-a-service (CaaS) refers to the use of cybercrime services that are offered online. The potential for CaaS is huge because it offers criminals a way to monetize their skills without committing crimes themselves.**

### ****2. Malware Automation****

**Malware automation is automating one or more aspects of malware research. Automated tasks could include source code analysis, network traffic analysis, and endpoint detection. This method can make it easier to discover new types of malware, but it also has the potential to introduce errors.**

### ****3. Polymorphic Malware****

**Polymorphic malware is a new type of malicious software that is designed to be resistant to traditional antivirus software. Polymorphic malware takes the form of many different types of files, but it is always spread in the same way: by email.**

### ****4. Third-party Risks****

**Third-party risks are the most obvious and potentially the most damaging to cybersecurity. These include the risks posed by third-party employees, partners and vendors. Third-party risk can be broadly broken down into four categories: insider threats (employee theft, bribery, etc.), external threats (hackers, cyberattacks, etc.) and compliance risks (e.g., data breaches).**

**Insider threats typically involve staff members stealing data or sabotaging systems. External threats come from hackers or other outsiders. Compliance risks are typically related to data security policies and procedures. Not all third-party risks are part of a malicious campaign. For example, mistakes made by third-party vendors can result in customer data being exposed.**

### ****5. The Human Element****

**The human element is the biggest threat to cybersecurity. Increased access to technology, especially for younger generations, is resulting in a rise in cybercrimes and security breaches. As people become more comfortable with technology and less apprehensive about using it, they are also becoming more vulnerable to hackers.**

**Companies need to take steps to keep their employees safe from cyber threats. Increasing awareness of cyber threats can also help reduce the number of attacks that occur. By creating a safe environment where employees feel comfortable reporting any issues they see, companies can help ensure that their systems remain secure.**

**Disadvantages**

**1) Regular Update:**Businesses need to regularly update their software, hardware, and security strategy to be one step ahead of the attackers.

**2) Needs Continuous learning:** The threats are new and never-ending, and so is the learning process to keep up with the threats.

**3) Complex to Setup:**Setting up security architectures and tools like a firewall can be complicated and could take a long time.

**4) Slower Systems:**Over time, Systems tend to become sluggish as running these security applications takes up a lot of resources.

**5) Constant Monitoring:**An effective Cyber Security strategy involves continuous monitoring of new threats. An organisation needs to monitor its system and network constantly, and that's the only way it can detect threats well in advance. Also, it enables them to assess the threat level and develop a solution quickly.

**6) Talent Shortage:**Cyber Security is vast, and there's a significant talent shortage in this field. It will take a lot of work for organisations to fulfil the scarcity.

**7) Expensive:** Implementing Cyber Security can be very expensive as it is an ongoing process that requires consistent learning and spending. So, it can be challenging for many small businesses to bear the costs. Despite that, most companies with more than 1000 employees in the west plan to increase their spending on Cyber Security.

**7.CONCLUSION**

**As the world becomes increasingly digitized, the need for strong cybersecurity measures becomes more and more apparent. Businesses of all sizes need to be aware of the potential risks and take steps to protect themselves and their customers. In addition, students can also pursue [KnowledgeHut Security certifications](https://www.knowledgehut.com/cyber-security-courses" \t "_blank) to grasp the concept of cybersecurity.**

**Organizations that need cybersecurity always deploy measures to ensure solid and safe data retention. Moreover, individuals also need to be vigilant about their online activity and take steps to protect their personal information. We can help make the internet safer for everyone with the right precautions.**

**8.REFERENCES**



#### KnowledgeHut

**Website:**[**https://www.knowledgehut.com**](https://www.knowledgehut.com/)

**Google**