With the rapid development of network, network security has also attracted more and more attention. Academically, network security is also known as “cybersecurity”. The definition of cybersecurity is measure taken to protect network systems and their data against attacks or intrusions [1]. Nowadays, due to the problem of network security, the world will suffer economic losses every year. According to a recent report released by Intel Security and the Center for Strategic and International Studies, cybercrime costs the global economy up to $575 billion [£367 billion] a year - that is bigger than the economies of many countries [2]. Network security is especially important because many countries lost money and security information. This essay aims at outlining some potential problems and talks some solutions about it.

Network security can cause many problems if we do not pay attention to it. Network virus can paralyze personal computers or servers. It was May 2017 when the ransomware attack WannaCry made headlines around the world. The virus brought unprecedented attention to malicious software-based threats that do not just infect technology systems but also demand money [3]. In addition. Trojan can control equipment and let it to spread some information. TELEPHONE boxes are being used as Trojan horses to sell adverts, councils have complained as applications to install them have soared by 900 percent [4]. The most severe problem caused by network security is information leakage. The National Cyber Security Centre (NCSC), a branch of GCHQ, said it had found evidence that a cyber hacking group, Advanced Persistent Threat 29 (APT29) known colloquially in the cyber sphere as Cozy Bear, had attempted to steal vaccine secrets being developed in the UK at both the University of Oxford and Imperial College London [5]. The security information is especially important especially for a country, if these information leaks, this may cause losses to national interests.

Fortunately, there are some solutions to solve these problems. One solution is for the country to enact laws, because it can prevent hackers to create new viruses. On November 7, 2016, the Network Security Law of the People's Republic of China (the "Network Security Law") was adopted at the twenty-fourth meeting of the 12th National People's Congress after the third draft. The Network Security Law is composed of 7 chapters and 79 articles and will come into effect on June 1, 2017 [6]. Another solution is layout network firewall. The basic function of firewall is to filter out some dangerous messages. Firewalls allow only authorized traffic or content using configured controls, like access denial to IP addresses known to deliver malware. Even if a malicious payload is delivered, firewalls can prevent it from communicating with control-and-command servers [7]. The third solution is developed antivirus software, it can detect and kill virus. Microsoft has been committed to developing anti-virus software. Bill Gates, Microsoft's chairman and chief software architect, confirmed last week that the company will offer free anti-spyware software and sell an anti-virus product [8].

Each solution has its advantages and disadvantages. Solution 1(enacts laws) stipulates which acts on the Internet are illegal and sets standards. It can let people know what is illegal and avoid doing it. Otherwise, the law cannot change a person's mind, it can't prevent hacker who wants to create a virus. Moreover, internet is a virtual world, it's very hard to arrest these hackers. The law is difficult to enforce. Solution 2(layout network firewall) can discover and deal with potential security risks, data transmission and other problems. It can detect and filter dangerous information to ensure that computers can run normally. The major problem with solution 2 is firewall cannot eliminate the source of the attack and it cannot defend against internal attacks such as Trojan and virus. Solution 3(develops antivirus software) is very convenient and effective. Users only need stall a software on their computer, then the software can detect and eliminate viruses and Trojans. Having said that, antivirus software cannot detect and eliminate some new viruses. More seriously, the software itself may also be infected with viruses.

Overall, through network security is a very serious problems for telecom operators, we have several solutions to solve it. From my point of view, the network firewall is the most effective measure because it can defend more network attacks.

Reference list:

[1] Risk and the Five Hard Problems of Cybersecurity
[2] Never underestimate the hackers; In association with EE The rapid increase in connected mobile devices offers greater convenience but presents serious security challenges for IT departments, Chris Price reports

[3] Learning the lessons of WannaCry
[4] 'Trojan horse' phone boxes used to carry adverts
[5] Kremlin's Cozy Bears sought to get their claws into vaccine test secrets; Cyber hacking; Britain, US and Canada call out Moscow's attempts to steal valuable research into treatment for Covid-19
[6] China: Comments on The Network Security Law
[7] 4 network security tips for the hybrid workplace
[8] Microsoft's IT security plans spark controversy, Symantec, with almost half the anti-virus market, questions software giant's move