IT 201 Assignment 8
Clarence V. Kimbrell Jr.

Sadly, malware is something that everyone should be worried about when doing things online. Malware is software programs that contain computer viruses. It has been stated that over three hundred and fifty thousand malware variants are discovered daily around the globe. The most common types of malware include things such as viruses, worms, and trojan horses. Most people are aware of these existing but are unaware of their potential dangers of them. A computer virus is defined as a rogue software program that attaches itself to other software programs. These are the most common among the three main types of malware. Worms are programs that replicate themselves from computer to computer over a network. Worms can be dangerous because they can compromise multiple computers at once. Then trojan horses are cleverly named after the real event that took place a thousand years ago. They are hidden malware that is normally undetectable and when in operation that can cause devastating damage. They can remain hidden for as many years are the program is scheduled to. These are worrisome because users can have information stolen without them knowing for months or years at a time before realizing it. People should be instructed at a young age and be updated throughout their lives about these because they can ruin someone's life if they are not careful.

Hackers are a large portion of the internets' users which is astonishing because of how much information they can extract from everyone. A hacker is a user who intends to gain unauthorized access to a computer system. Many of the mainstream methods were mentioned above but there are thousands of types of malware used by hackers to gain information. We live in an age where information is one of the biggest assets to run a modern society. So, hackers would like to manipulate it for their personal or organizational gain. Hackers create security problems for companies and individuals by accessing information that is supposed to be confined so that it can be exploited. For example, if a company's bank accounts are hacked into their entire investment and intellectual property can be ruined permanently. They are known for damaging systems with the use of malware and cyber vandalism. These can include spoofing, sniffing, dos, and DDoS, and computer crime. Hackers can create chaos among individuals and companies alike, so they should not be forgotten about.

Briefly mentioned above bank accounts can be stolen and drained of all their funds which is one of the number one ways individuals are hacked. This is done by identity theft which is a crime where an imposter obtains personal information to impersonate someone else. This is damaging to the individual that was hacked because all of their online presence can be compromised nearly all at once. The use of identity theft has soared over the past decade thanks to banks offering online banking and transactions over the internet. This great convenience can come with scary consequences.

Security is one of the biggest defenses against these types of crimes. In turn, having great reliable security provides value for businesses because customers can trust their information with a business. So, from a business perspective, this will create profit because customers trust the company with their information. Without security and control, it can cause distrust among customers and investors.

IT 201 Assignment 8
Clarence V. Kimbrell Jr.

Policies are put in place in companies to regulate information that could have harmful effects in the wrong hands. There are many and three main ones that come to mind when discussing information policies in a company and those are security policy, acceptable use policy, and identity management. Security policy at the basic level ranks information risks and identifies security goals and mechanisms for achieving said goals. So, it looks at the information of a company and lists vulnerable assets. Then creates goals and mechanisms to secure the information that could be damaging to hackers. The acceptable use policy looks above information and defines the uses of resources and mechanisms to secure information. So, they have to evaluate things that would be beneficial before just jumping onto one resource and hoping everything is all right. Identity management can be described as user authentication for valid users to access private information knowing that the information will not be obscured after inspection. These policies are put in place in companies to secure information throughout their business which provides more value.

There are many ways for an individual or a company can protect itself from hackers with malicious intent. Many traditional ones include firewalls, intrusion detection systems, and anti-malware software to bulk up their security. A large business will incorporate all of these techniques and many more to protect assets. Firewalls prevent unauthorized users from accessing private networks. Internet connection between sites is sent by packets so a firewall would allow certain packets to enter and restrict ones that have to be highlighted not to pass. This can prevent you from accessing the website entirely due to firewalls blocking traffic between you and the site. This also can be used to prevent hackers from getting into systems that are using one. Intrusion detection systems are full-time monitoring tools that are in place at the most vulnerable points to detect hackers continually. This can reroute traffic into a dead end so the system is still safe from attackers. These are always operational because the second that it is down it can cause many problems to a system. Anti-malware software is similar to anti-virus software, in that it prevents the use of viruses if a computer is comprised. Most technology is equipped with some form of anti-malware programs but can be upgraded further with commercial programs like Norton and Avast.

Planning for the worse in a company can be a great way to recover after something happens. Many companies have two main types of planning which are disaster recovery planning and business continuity planning. Disaster recovery planning is planning for the restoration of broken or disrupted services. In the case of a natural disaster if planned accordingly customers should see no change, but in the company, information can be outsourced to a different location. Business continuity planning focuses on restoring business operations after a disaster. Both of these work hand in hand and they can be viewed as step one and step two. So, after an event occurs with proper planning it focuses on getting your business up and running as quickly as possible.

IT 201 Assignment 8
Clarence V. Kimbrell Jr.

In my Pc repair business, I would employ many of these techniques to protect my information and my customers. Such as firewalls and anti-malware services for all my devices in my business. Then create policies to prevent information within my business from being tampered with. In my case, it would heavily focus on identity management for accessing server information. In my business, I would try to inform my employees about malware and things to look out for so my workplace is safe and secure from hackers.