Business, Society, and Private Life

Name

Institution Affiliation

Date

Project A

1. Discuss information systems use in public schools.

Student information systems offer many functions, including inquiry handling from students, admission process, and new students enrolling. Moreover, course selection, creating schedules for classes and teachers, grade management, and processing exam documents is done through information systems (Gunn, 2006). Besides, the system maintains absence and attendance records, communication records with students, course records, provision of statistical reports, information on support boards and communication of information about students to parents via the parent portal, special education services, individual curriculum development, bookkeeping and budgeting services, and even student medical records.

2. Discuss the issue of free speech versus protection of children online.

Freedom of speech is an excellent concept in the US and across the world (Dziewięck, 2016). This is the foundation of America and other freedom nations. However, to protect children, society sometimes denies their right to access materials and expressions. Many schools in the US and other countries use filters that restrict access to certain websites or applications. This type of filter has been in existence and was initially used to block pornography. It has evolved to block websites that promote drug use, depict violence, or promote self-harm activities such as anorexia. The purest interpretation of the *First Amendment* or the *Convention on the Rights of the Child* can be used to oppose the use of this filter for any purpose (Gunn, 2006). Parents are obliged to protect their children from disruptive or potentially harmful contents. Moreover, government-run public schools, have the right and responsibility to prevent children from viewing specific content in their facilities.

3. Discuss the basic functions of computer forensics.

Computer forensics is the collection, investigation, and information reporting on computers and other networks in connection with criminal or civil investigations. However, the same procedures and methods apply to corporate and other "personal" investigations. Nearly a mark is left on anything one does in the computer; from deleted files, internet history caches, registry entry, and word back-up files. Email headers and instant message logs provide clues to the intermediate server used to transmit the information. Server logs contain information about each computer system that accesses the website.

4. Discuss five information management issues and their relationship to privacy.

Some of the problems in information management are the availability and accessibility of information, quality of information, information exchange, and how information is collected. The availability and accessibility of information are related to data protection because the information received can only be seen by a certified person who has access. However, confidentiality becomes a problem when people who are not required to display it cause harm that violates the privacy of others. The quality of information is related to data protection because we expect the information received from individuals to be correct. However, if the information is inaccurate, it can cause problems which further violate users' privacy. Information exchange is directly related to data protection because only certain people are allowed to view other people's information (Broadhurst, 2017). So, it is essential to know who conveyed the information. However, the way information is collected also has a direct bearing on data protection. Typically, to get useful information about someone, one needs to intrude at least a little on their privacy, especially when spying on employee computers to see their daily activities, hopefully only work-related.

5. Discuss the impact of viruses and other malware on organizations with which you may have been involved.

Malicious software can cause computer crashes, financial and identity theft, and slow performance (Broadhurst, 2017). Computers infected with malware are almost always damaged. These unwanted programs usually occur in the form of reduced computing speed, malfunctions, program crashes, and repeated error messages. Although most malware is used for purposes such as theft or junk email, some programs are only meant to add as much malware as possible to the users' computer. The main objective of developing a malware is technology theft. Studies estimate that billions of dollars are stolen each year because of malware that allows access to business and personal financial information. Some types of malware automatically transfer funds to other bank accounts. Others provide a back door to the system and give hackers unrestricted access to users' finances for long periods. Malware built for theft is designed to be challenging to detect, so malware stays on the computer as long as possible (Broadhurst, 2017). There may not be clear warning signs for those that should be plaguing the computer.

Project B:

Research viruses, worms, and spyware are mainly developed to access personal and financial information. The target information is social security numbers, driver's license numbers, bank accounts, and other sensitive information that can be used for identity theft. This theft is mainly motivated by financial gains to the developers. Malicious software can easily access sensitive business information by compromising servers. This is one of the central business impacts malware has. This will affect the company's business in the market. It's also possible that malware can cause hardware failure in some cases. Encrypted ransomware is a financial repercussion of malware where hackers take user files and encrypt all files (Broadhurst,

2017). The hacker requires cash payment to decrypt and transmit user files. This type of ransomware is so dangerous that once a hacker has encrypted a user's documents, no security platform will work to extract the files. The user has to pay according to the hacker's requirements. All installed malware should be removed and reinstalled if the business is to recover financially. If these measures are then the entire business may collapse due to the loss of millions of dollars from the company.

Malware has a strong influence on businesses, particularly banking applications (Bowerman, 2017). For example, mobile banking malware is growing rapidly every day in this digital era. Since most people use mobile banking or network banking through their cell phones, hackers are focused on stealing sensitive user information. This malicious program interferes with user communications to steal confidential information and commit financial fraud. In other words, mobile banking malware is also described as an advanced version of phishing attacks and psychological manipulation. Hackers are mainly focused on financial institutions. However, providing cybersecurity services is the best option for avoiding such malware attacks.

Small businesses are particularly vulnerable to threats because they often lack the resources for large security products or teams such as large companies. It may be more important for small businesses to protect themselves because, unfortunately, if they do catch malware, these companies could cripple or shut down their business. However, securing these endpoints with appropriate protection policies, protocols and tools is essential. Many small businesses think they are too small to be attractive to criminals, but the opposite is true. Cybercriminals often target these organizations because small and medium-sized companies (SMEs) often lack complex layered security practices that make it easier to access the sensitive data they contain.

References

Bowerman, S. K. (2017). Cybersecurity Threats and Technology Applications in Homeland Security. *Homeland Security Technologies for the 21st Century*, 135-148.

Broadhurst, R. (2017). Cybercrime: thieves, swindlers, bandits and privateers in cyberspace. *Swindlers, Bandits and Privateers in Cyberspace (July 27, 2017)*.

Dziewięcka, N. (2016). Larry Flynt as a Controversial Advocate for Freedom of Speech in The People vs. Larry Flynt. *New Horizons in English Studies*, *1*(1), 68-78.

Gunn, T. J. (2006). The Religious Right and the Opposition to US Ratification of the Convention on the Rights of the Child. *Emory Int'l L. Rev.*, *20*, 111.