Final project assignment

System security has been very important ever since the beginning of the computer age. Security is setup for a number of reason whether it be to protect data from those who are not supposed to see it or hide it from those who are supposed to security at any point is important. Security can be physical, virtual or a mixture of the two, but in this day and age it is definitely needed. In the following I will give my opinion on how to increase or the steps would use to implement security to a certain situation. BESS or the Blackberry encryption server is one of the most effective tools in security with blackberry products.

All communications between BESS and BlackBerries are encrypted with Triple DES or AES encryption and only the company running the BESS instance have the encryption keys. That means that RIM cannot provide these keys to government organizations. This is a great tool for companies who want to be the only ones with the keys to their data. PKZIP is paramount at this point and the less you have to worry about the better. Most blackberries that are not connected to a BlackBerry Enterprise Server, you’re using the BlackBerry Internet Service or IBIS. IBIS provides the benefits of push-email to the masses.

You can organize a riot, or orchestrate assignation, and you don’t even have to be wearing a suit and tie. Instead of connecting to corporate BESS, you connect to a IBIS server operated by your mobile carrier. This also secures incoming data from anyone not using a blackberry to contact you. This is why most people complain about lag with blackberries. Unlike BlackBerry to BlackBerry communication on BESS, IBIS email messages are not encrypted

before they travel over a mobile carrier’s network. For IBIS users, only the mobile carrier’s standard G/G protection applies.

Your IT department has the option of encrypting the body -? not the PIN -? of your PIN-to-PIN IBM messages with a key unique to the company. By default, however, IBM messages are not encrypted because it restricts PIN-to-Plan IBM communication to only employees of the company, instead, they are scrambled. Scrambling is done with a universal cryptographic key that every BlackBerry has. Most if not all enterprises choose to support one smartened operating system, such as the BlackBerry SO, but may have certain users that use different devices like the Apple phone or Android phone.

An encryption product that is available for multiple platforms is preferable to one that is only available for one type of device. Ability to manage devices centrally such as smartened encryption, as well as monitor the status of each phone’s encryption in real time, is often a necessity for enterprises with numerous devices”. As well, there may be compliance requirements for logging and reporting. Managing encryption keys is most Often a part Of an enterprise-level product. Out of the box, Android phones do not come with encryption software.

As with other handheld, there are third party applications that will allow a user to encrypt data or the device itself. The Touchdown application can encrypt data at rest as well as attachments on an SD card. Whipcord is another Android app that offers full-disk encryption, encrypted backups, and fine-grained control over what data APS have access to. Both are enterprise driven which offers over-the-air and on-device encryption of enterprise data.

Blackberry devices as of version 4. 2 of the Blackberry SO and later, can encrypt data on the device.

Users have the option to encrypt emails, contacts, browser cache, and other data. Note that if user contacts are encrypted, incoming caller ID will not be available. Be aware of the possibility of theft. Cell phones are small and easily misplaced or lost. If an individual steals your cell phone, it may be only a matter of time before even the best secured device is compromised. Because BlackBerry’s Enterprise Service is widely used, the move to BESS 10. 1, which is required to support the Secure Work Space, is easy to integrate, since it requires few if any changes to the existing BlackBerry environment.

IT managers won’t need to change their company’s security infrastructure to work with the new capabilities. The new APS that come with BlackBerry Secure Work Space are modified versions of APS that already exist for BlackBerry 10 and are used with BlackBerry Balance. There’s the secure HTML browser that allows users to connect securely to existing Web services behind the corporate firewall, secure email for use with BESS 10. 1 and the corporate email service. The calendar and contact APS work with their corporate analogs, and all connect using the secure BlackBerry environment.

Now moving on to the next part of the assignment which covers implantation of monitoring internet access and removable media devices in the workplace. In most cases the best practices for password creation, passwords aging, minimum password length , characters to be included while choosing swords, password maintenance, tips for safeguarding

accounting data; the dangers to each of these issues. Once training has been completed ensuring that employees know how to safe guard their account this is when you should have them sign a disclaimer acknowledging what type of websites can be accessed.

Although employees may be of legal age to view any type of website they choose certain types of sites like adult and social media tend to be blotted with ad and spare. When you start explaining what a virus is, limit it to the facts, for example like how destructive it is, what damage it can cause, the possible financial losses related to a virus outbreak, etc. Don’t bother staff with the specific technical information such as ways viruses function, how they hide, and many other topics that will not be of interest to them.

Instead, provide those who are most interested, with some external internet links to the subject. Freeware, or any other type of software, obtained or downloaded from unknown or untrustworthy sources could easily affect company security, exposing critical business data and corrupting sensitive ones. A lot of users tend to install such programs from screen savers o games and funny cartoons in Flash as they put it, for various personal needs and activities; to entertain, have something nice to look at or relax themselves.

At the same time, they do not realize the potential threats they are exposing the company systems and networks to, from malicious software viruses to legal actions against the company for installing possibly pirated software on the company workstation. Thus, you need to familiarize users with the potential problems attached to each of these issues, and also explain the

company policy towards installation of any unauthorized software on any f the company workstation.

Files downloaded from the Internet, copied from a CD or a floppy coming from an unknown source, or anything else that has not been reviewed by the Information Security Office or not been scanned for potential malicious code by the corporate VA systems could actually be classified as untrustworthy, unknown and dangerous. Freeware applications, due to their nature of origin, are a significant source of threat and should be approached with caution. Using simple storage media may seem innocuous, but it has the potential to cause many problems for a user or an organizations.

These devices such as a jump drive or music player plug into the USB port of your PC and may contain mallard that you copy unknowingly or that gets launched automatically by the Outrun or Outplay feature of your PC. And attacks are growing even more sophisticated and hard to detect as attackers use small circuit boards inserted in keyboards and mouse devices to launch malicious code when a certain key is pressed or condition is met. Once mallard infects your PC to steal or corrupt your data, it might spread to other PC’s on your home or organizational network.

And these vices are an easy way for attackers to quickly propagate mallard by passing it across all PC’s that the device connects to. Because these storage devices can install mallard inside of any firewalls set up on your PC or network, you might not detect the mallard until major damage has been done. Storage devices can also give malicious insiders the opportunity to steal data easily and inconspicuously because the devices are easy to hide

and their use is hard to track. Smart devices also have the potential to surreptitiously infect your PC or network when you download applications or games containing mallard or viruses.

Their use by a large population, emphasis on usability, and immature security tools make them ripe for mallard attacks. Also, the potential for irreparable data exposure or loss arises from practices commonly used for storing sensitive data on smart devices. For example, users frequently keep personal bank account numbers or proprietary client information on their smart device that may be running entrusted applications or be connected to entrusted and vulnerable networks. Whether you are a home user or work in an organization, there are things you can do to reduce the risks associated with using portable devices.

Recommended best practices for individuals and organizations are listed below. Install anti-virus software that will scan any device that connects to your PC via a peripheral port such as USB. Never connect a found jump drive or media device to a PC. Give any unknown storage device to security or IT personnel near where you found it. Disable the Outrun and Outplay features for all removable media devices. These features automatically open removable media when its plugged into your USB port or inserted into a drive. With the steps above anyone should be able to maintain a safe and functional enterprise network.