9.8

University of Victoria

SENG 460 Practice of Information Security and Privacy

Assignment # 1 Winter 2014

Question 1:

When we discuss this business or enterprise in a contextual manner there are a number of aspects that can be considered as vital when planning the formulation of the Enterprise Security Architecture. The first phase of developing or forming such a system requires the study of the current system in place. After the current system is studied, the drawbacks, inefficiencies and risks of the current system are drawn out. Possible solutions to these risks and drawbacks of the current systems are then discussed with the current users of the system. Planning and deciding the implementation of the new system however depends on the financial resources and time constraints that the business has to follow. After the new components and equipment that can be afforded by the enterprise are bought, various ways of implementing the new system are discussed for example phased implementation, direct implementation or parallel running.

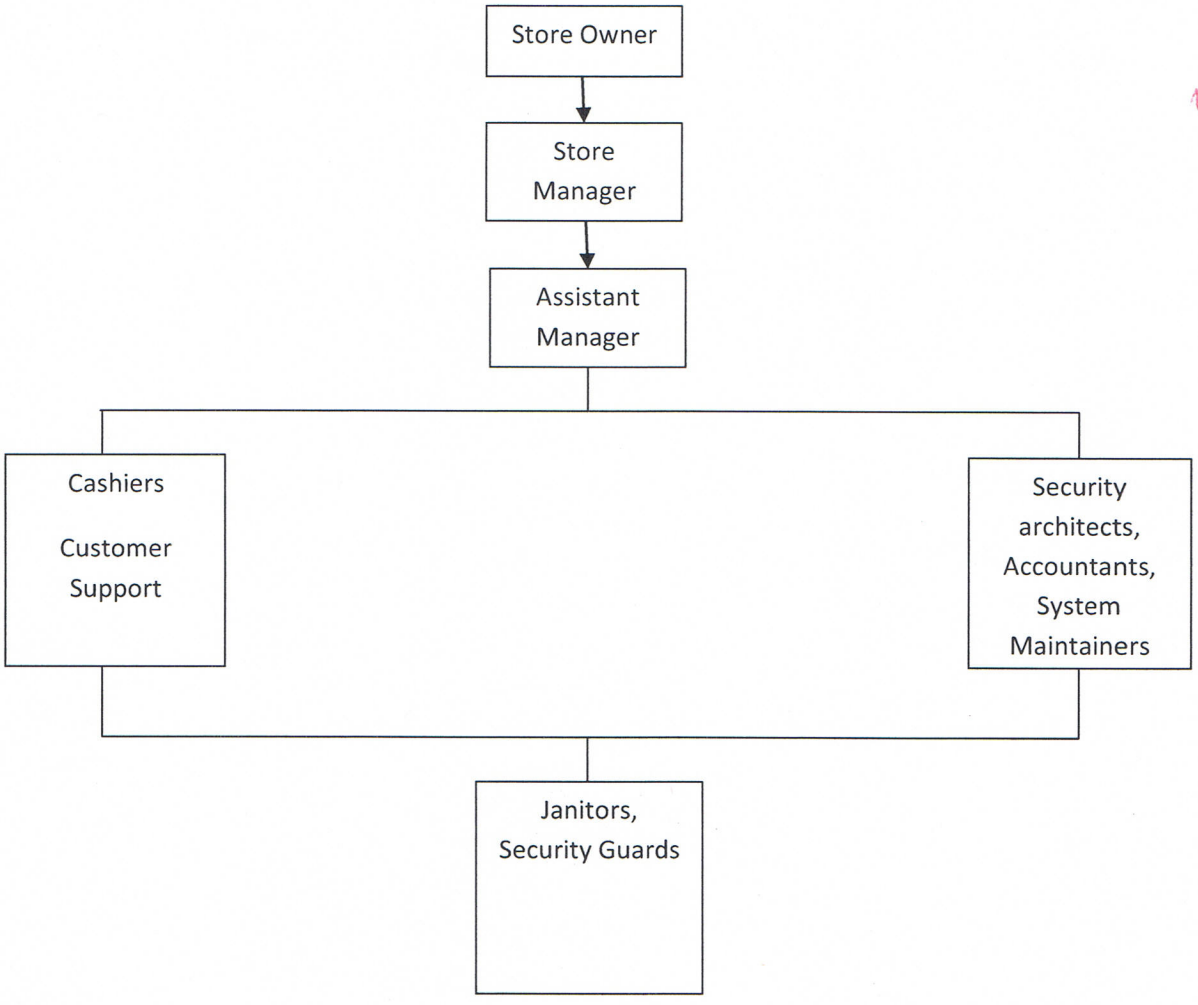
In a contextual sense, the main motive of the business is really important because as the motive and aim of the enterprise is analyzed, the ESA can be designed to focus on the achievement of those specific motives and after that is done, the rest of the aims are focused on. Risks of the current business are also kept in regard when designing the ESA since the new system cannot exhaust an extreme amount of resources or introduce a gap in the system or timing cycle that can hamper the activity of the business itself. Also, factors like time sensitivity affect the planning of the ESA because if the new system is taking up too much time to actually be implemented, it might just cause a loss of customers which cannot really be afforded by a business like friendly grocers. Since one of the motives of this business is customer satisfaction, the ESA shouldn't prove as inconvenient for the customers but should enhance their experience by providing ease and security for their information. Also, since the employees and vendors are in direct relationship to the business as well, the ESA should include components and be implemented in a way that provides them with a comfortable and secure environment to work in since loss of practiced and reliable workers or vendors might hamper everyday business and eventually slow down the progress of the business eventually hindering profit margin and client base growth.

Question 2:

The organizational structure to be followed for the ESA should be very thorough in all manners. First of all, a specific hierarchy should be followed. The store manager should have over all control of the store and all the employees working under him. The assistant store manager should also be responsible for keeping a managerial check over all the employees and should report to the store manager if he notices something odd. The security architects should be working directly with the store manager to make sure the ideas are shared directly without any loss in communication through other people. All the employees at the store should undergo a certain background check and should only be employed if their background check is successful. At the time of appointment, every employee should sign in a letter of confidentiality in which he or she undertakes the oath of working truthfully and not sharing or accessing any information that exceeds his or her clearance level. The responsibilities of each employee should be

made clear to them at the time of employment and the access to files should only be given according to the requirements of the positions they are supposed to work in.

The owners of the friendly grocers after consultation with professionals should divide the staff into four main groups. The highest level of hierarchy remains with the store owners who have ultimate authority. The two subsequent levels of the organizational structure should go to the administrative/managerial team consisting of the store manager and the assistant store manager. This is the first group. The second group should consist of employees that work in the back end of the store. This group should include the security architects, accountants and system maintainers. The third group should consist of the employees working at the front end of the store, specifically the ones who work at the cash counters or inside the store to assist the customers. These employees will have direct contact with the customers and some of them will have direct access to the customer personal information which is prone to be misused. The second and third group should be answerable to the administrative/managerial group and should generally not be sharing their work data or resources with each other in order to avoid the risk of losing personal information to unauthorized people. The fourth group should consist of the support staff which consists of the cleaning and security staff. Employees in the fourth group are answerable to all the employees since they are supposed to follow any tasks that they are given through them.



Question 3:

0.9

The key components to ESA would include hardware and software components both. The subject of interest here will be the personal and financial information of the customers and employees involved in the business. First of all, the Identification needs to be unique for each customer and employee. There will be a valid way of verifying the identification of each customer and employee. The personal information from each ID card or loyalty card issued by the business or enterprise will have a unique number or magnetic strip that holds all the information. This information will be saved in the computers of the enterprise and obviously this information should only have limited access restricted to authorized people only. It should be made sure that proper encryption of such data is done and that the data is available at all times for an authorized access only.

The key components of the ESA will consist of hardware and software. The hardware involved will include computers for each check out till, the self serve check out, for offices of the accountants, system maintainers, security architects, assistant manager and the store manager himself. Touch screen terminals will be required for the self serve check out terminal with a receipt printer along with a card reader that can support debit and credit card information. CCTV cameras will be required to keep a track of what is going in with the store along with wide screens in the security guards office to make sure he can view the tapes and surveillance carefully. Barcode readers will be required to gain information about the products at the store as well. Also, at the doors, a card reader will be required to assess the identification of the person who tries to enter specially for the inventory and the documentation room. Routers and modems are required to provide safe internet. In software, there has to be a firewall that is protecting the enterprise's system along with proper encryption tools so the information cannot be deciphered immediately by the hackers. Antivirus software should be an integral part of the system to make sure the information saved does not get corrupt.

At the point of sale terminal it needs to made sure that the information of the customer is accurately updated and validated every time. The financial information should not be leaked to any unauthorized access. The credit card numbers or PIN numbers of any sorts of cards involved shall only be entered or accepted from the card holder himself. This information should not be backed up personally without permission or against the customer rights. Other customers should be dissuaded from peaking or hearing any bits of personal information of another customer or employee. Hence a suitable physical distance also needs to be maintained to make sure no information is lost visually or verbally and is safely stored.

Question 4:

0.9

The organization should be hiring security architects to design a new ESA. As mentioned in the previous part, the enterprise will also hire system maintainers which will specifically have significant knowledge in the area of programming, computer architecture and will also be able to provide services like protection in the case of system breach or hacking. So the system maintainers that will be located in the backend of the store should be responsible for taking steps to make sure information security is maintained. Of course this is something that cannot be achieved completely only by the system maintainers. The

employees will also be responsible for following the code of conduct when it comes to dealing with personal information. For example, the employees at the checkout tills shouldn't be unlawfully recording personal information or providing unauthorized access to it. The customers on the other hand should also take care that they are not spelling out or talking about their personal information loudly so other people can hear them, also they should make sure that when they are entering personal information like PIN numbers, the cover it so not everyone can view it.

how about owner?

Ultimately, the store manager should have a complete control over the situation. Since he is the one that everyone else is answerable to, he will be made responsible for any breach in security or loss in data. Since the store manager will oversee the performance of all the employees including the system maintainers', he will have complete responsibility towards any failures. Also, since he holds the top most position in the organization hierarchy, it is only natural that customers and junior employees will turn to him in case of problems. The system maintainers or programmers are responsible for making sure the system is secure for information security and the store manager should make sure all the steps are taken to ensure information security so he or she will be the one responsible in times of security breach.

Question 5:

Everyone who is involved with the FG enterprise directly is an important factor to the successful realization of the new ESA. First of all, the employees and the enterprise owners need to be sure and aware of the fact that the business has a security risk and it is important to implement an ESA. The enterprise needs to set aside a suitable amount of budget for the realization of the ESA. The enterprise needs to be fully cooperative and open to suggestions of the security architects. The enterprise needs to hire security architects that are credible and trustworthy and the security architects need to be able to do their job successfully. The enterprise should be able to allow full access to all sorts of details about the business to the security architects so that they fully understand the business and come up with a plausible solution. The customers are also an important part of the realization of the ESA. The customers' activity in the store should not be hampered by the ESA. They need to be kept in the loop so they are fully supportive of the new idea otherwise this might cause a loss in the customer database.

negatively

The ESA should be designed in a way that it does not affect the stores quality or the profit margin. Moreover it should result in an expansion of the client base since the new security measures only enhance the experience of the customers. The ESA should have equipment that does not require maintenance very often and even if it does, the procedure should be easy so it does not take up a lot of resources or time to fix. The employees and customers should be provided with some sort of training to familiarize themselves with the new system to make the process smooth. Ultimately, the way in which the new system is implemented should be taken into account as well. It should be made sure that the system is being implemented in a manner that suits the store. There are three main ways usually to do this; phased implementation, parallel running and direct implementation. Phases implementation is when the new system is only implemented in some parts of the business for example only a few checkout tills in this case. Parallel running is when the new system and the old system are both run simultaneously. Direct implementation is when the new system is completely implemented. Direct implementation will obviously shut the business down for a while so might result in the loss of

customers. Phased implementation is usually the most plausible solution because the system can be slowly transformed while the business is running. Parallel running also does not hamper the activity of the business a lot but requires a lot of space and resources usually.

Question 6:

Before the ESA is planned there are a few steps that should be followed first. First of all the security architects need to test the current system. They need to study the current system and see what the drawbacks and inefficiencies are. Then the security architects need to view all the documentation of the current system to gain technical knowledge about the systems performance. Then interviews need to be scheduled with all the employees to gain first hand information about different components of the system and how they work. If it is possible the security architects should also establish contacts with the customers to get information about both sides of the business. After all the information about the current system is gained, the security architects need to sit down with the enterprise owners and discuss the motivations, aims and resources available. A plan can then be formed keeping in view all these aspects.

The development of ESA should start with installing safety cameras in the store. This will ensure proper surveillance in the store and will make sure that dangerous people don't enter the store or commit acts that are harmful for the business. The store should also have theft detectors and metal detectors at the door to make sure no one leaves with things that they are not supposed to have. This will also prevent the entrance of arms inside the store. Computers need to be installed with hard disks that store personal information securely. The hard disks need to be protected from unlawful or unauthorized access, viruses and physical damage. This can be achieved by having encryption and passwords for the files. A priority order then needs to be set up so that there are clearance levels for the sort of information that each employee is authorized too. This can be achieved by a sign in or log in for any terminal either through a keyboard, magnetic strip or finger print. This will also ensure that the identification is done more efficiently and accurately. After these initial settings are in place, there need to be everyday checks that make sure that none of the computers or tills have unauthorized software running or installed that get hold of personal information. The whole enterprise system needs to be protected by a firewall to prevent hacking. Antivirus software should be put in place to make sure that the new system is not invaded or corrupted by threats. After the system at the store itself is set up, the customer cards shall now be taken care of. The ESA will probably work with loyalty cards for each customer. These cards need to have a unique ID number and unique chips so that each customer is accurately identified and then the information is automatically retrieved and updated. This also reduces the risk of frauds committed by people.

SABSA Matrix:

	Assets (What)	Motivation (why)	Process (how)	People (who)	Location (where)	Time (when)
Contextual	Friendly Grocer. Taxonomy of store building, inventory and bank accounts	To serve/satisfy families. Grow a customer base, maximize profit margins, improve quality and variety of products offered	Store orders goods to suppliers, suppliers deliver, customers pay and buy the goods	120 employees of FG. Employees of IGBG. Customers of the store.	Inventory of the friendly grocer building. IGBG's warehouse.	Very time sensitive from 7am-11pm. Peak time is 4-5pm Friday.
Conceptual	Grocery, meat, produce, deli, bulk, bakery, dairy and frozen products.	Keeping customer satisfaction high. Offering secure checkouts, fresh and up to the mark goods with easy access and assistance.	Entrance of reliable people, protection from fraud, hacking. Offering secure self serve check-outs, email offers and points/miles.	Owner and employees of FG, IGBG, security companies, customers and their roles and responsibilities.	Safe parking, environment, goods, check-outs, saving of personal and financial information.	Panic and fire alarm time, lockdown time, re-shelving time, customer support time, efficient check-out time and immediate action in cases of fraud.
Logical	Advertisements, FAQs, sales information, self serve check out help, maps of physical location of the store and layout of products within the store.	Provide a safe shopping environment, check-outs and making sure personal information is not misused.	Safe ATMs, cash payments, hard disks, proper encryption, Unique IDs.	Customer and employee loyalty, IGBG (Vendor loyalty) and security analyst loyalty.	Maps of department, layout of goods, labeling of isles, location of the store.	Making sure inventory has enough goods for the next 3 weeks, sensitive opening times, peak hours and dates and expiry dates of goods.

Physical	Computers, registers, inventory list, contacts, customers directory, online database, website.	Authorized access to desks, storage files and accounts. No shop lifting, arms allowed. Employees doing only their designated jobs and ID verifications for customers.	Checkout tills, cash machines, barcode readers, computers, self serve check out terminals, cameras, theft detectors, locked doors, 911 alarms, panic buttons, automated lock system.	Human Computer Interface, touch screens, software, verification for employees, keyboards, card and ID verification systems.	Active terminal only at back end, dumb terminals outside, authorized access to repositories, star or bus line network, internet access, linked system, information sharing.	Minimum time for processing, card entered, ID verified, information updated, notification and updates given and checkout is complete.
Component	Computers, keyboards, barcode readers, card readers, touch screens, hard disks, printers, telephones, routers and modems.	Sensors or predictive modeling software, alerts if lower shelf value is reached, alarms, automatics orders to vendors.	Regular orders made, trucks deliver and shelf is stacked up with 3 weeks of groceries.	Identities of all employees and customers, their jobs and responsibilities and maintaining access to data.	GPS coordinates, address and location of the FG store.	Daily schedule and tasks to be done, time sheets of all the employees, schedule of deliveries and stock reordering.
Operational	Improved variety and quality of goods and helpful attitude towards customers.	Focus on growing client base, good attitude, quick assistance and monitoring everything.	Regular checkups of systems, assessment of employees, overseeing the whole procedure and regular comments/suggestions forms.	Personal account processing, treatment and support given to customers.	Building should be maintained, sites should be checked and networks should be repaired.	Management of deliveries calendar, computer and user timings.