**Team C: Riordan Security Plan**  
Bachmeier, Blanchette, McKenzie  
CMGT 430: Enterprise Security  
University of Phoenix  
Facilitator: David Fedorchak

# Riordan Security Plan

*Ryan you need to insert an executive summary in this part and fill up around 300 words or so.*

# Physical Vulnerabilities

*Jennah you need to write 750 words spanning Physical vulnerabilities may include access to servers, communications interruption, or web presence interruption.*

# Logical Vulnerabilities

*Darnell, great start you will need another 300 words during week 5.*

When you look at the top threats that affects a business, you have to look at the ones that threatens the day to day operation of the business as a whole. As we compile the list of threats, the ones that really stand out are the ones that dealt with hackers taking over control of a user profile or communication between the user and network was not connecting properly.

They are many ways that a hacker can penetrate the network; it can be internal or external. One of the threats we placed on the list that may be overlooked is not deactivating an ex-employee account. Now a day with remote access to job sites, an employee does not have to be in the building to access the network. Not deactivating an ex-employee account gives them the right to have the ability to gain access to sensitive information within the organization. Even though most companies do a thorough background check on their potential employees, it cannot measure the trust level throughout business transactions. There is still the time that transpire while the person is employed, at times a person may have a bad experience with the company or just have outside influences during time of employment. (Clarke)There should be a written out step by step process when terminating someone to assure they have no access to the company and they do not leave with any confidential information about the company.

When it comes to external problems with a company like Riordan who has clients that order from them, having a denial of service can affect their day-to-day operation as well as lose trust from their clients. This attacks the company’s main server or master computer, they are two different ways this attacked can affect the server. One of the attacks is network centric attack, which overloads services by using up bandwidth. At times the company may not even be aware of the attack and could be controlled by a zombie attack. This is even worst for the company, because it means the intruder or intruders are in control of system.

The zombie attacker is able to set up his or her own motives within the system. The fact the company has client’s information within their system and clients are at times placing orders, it places not only the company in a vulnerable predicament, but also their clients as well.

# Other Vulnerabilities

*Nate will convert this into paragraphs during week 5*

* Unpatched systems
* Public endpoints
* Relaxed permissions
* Malware infected devices on corporate network

# Remediating and Mitigating Top Threats

*Marc great start, 325 more words will be needed during week 5.*

One vulnerability that many companies, including Riordan Manufacturing, can potentially face is having no printer threshold which causes an overload to the printer’s memory. This can easily be done by too many print jobs being executed and stored within a printer’s memory at the same time. Because of this overload, a denial of service (DoS) attack can inadvertently occur. On the other hand, if someone were to maliciously attack a system and overload all of the printers’ memory with print jobs, thus causing an intentional DoS attack and purposely freezing any future print jobs. One way of mitigating this attack is to use an authentication method by associating each print job with a username/password that has been stored in the company’s database so there is no unauthorized printing.

Another vulnerability to an enterprise is having bugs in their web servers that allow for Cross-site request forgery (CSRF) or cross-site scripting (XSS) exploits. These bugs allow attackers to trick the system into thinking that a command is coming from a trusted source and location. One way of avoiding these bugs is to perform validation techniques and keeping the software current to the latest version. A different type of web server vulnerability is having traffic limits. This can cause communication degradation and slow down productivity. A solution is to incorporate traffic or packet shapers, which is a type of quality of service (QoS). Traffic/packet shaping, according to Rouse, “…is the practice of regulating network data transfer to assure a certain level of performance.” (Traffic Shaping (packet shaping)).

All of these attacks can be controlled by one security method known as virtualization compliance. Compliance is “…the use of internal controls to satisfy external requirements…It can be checklist-based…” (Wiley & Ottenheimer, 2012, p. 330). Basically, it’s a resourceful tool consisting of a list of mitigation techniques to the most common virtual attacks that can occur within an organization. This list, of course can be tailored to custom-fit any organization’s requirements.

# Conclusions

*Ryan you need to insert the conclusion in this part and fill up around 300 words or so.*