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

# Riordan Security Plan

Riordan is a plastics manufacturing company with three offices in the United States and another in China. They are currently in need of an enterprise security plan that needs to address the threats, vulnerabilities, and risks to their organization. To accomplish this, an assessment of the top 50 vulnerabilities was created. From this list the most critical ones were selected to be discussed in greater detail.

# Physical Vulnerabilities

Physical vulnerabilities are weaknesses in the company’s buildings, structures, or other properties. For instance, if the back door did not latch properly, then there is a threat that an actor might exploit this flaw and gain entry into the facility. Riordan Manufacturing will be faced with the task of dealing with physical vulnerabilities within its company. To fully understand where these risks come from, the company will need to first look at the physical access it is dealing with. A good approach to dealing with access to company data floors is to start from the street and work your way into the actual computer room. To fully protect the Riordan data, cameras should be present on the outside of the facility to oversee all entry points and exit points. Once inside the building, all employees should be mandated to wear a security badge that gives them clearance to whatever rooms or floors they need to be on. Riordan will be working with a least privilege model, so only granting access to people who need to be in the rooms or floors will be important. The actual floor that Riordan stores its infrastructure should be locked at all times with badge swipe entrance only with only one person allowed in per badge swipe. Once inside the computer room, access to the servers will be granted using a Role Base Access Control (RBAC) system where each employee will be put into groups that predetermine their level of access.

Communications interruptions can happen from time to time and Riordan needs to be prepared to deal with these occurrences. A recommended suggestion to deal with communication outages can be a fully operational DR site that allows Riordan to pickup communications if the main site were to fail. Using the DR site, Riordan could use block data replication to always keep the cold site up to date to limit any customer outages. With using a DR site, Riordan would have the ability to have a fully operational offsite up and running in a matter of minutes to make sure their company is fully operational at all times.

Another example might be a poorly lit parking lot that the employees and customers need to cross. A threat might be that an actor waits in the parking lot at night; attacking and robbing a person as they cross. To address this issue, cameras, security guards, and of course bright lights make the area less of an easy target.

Not all vulnerabilities in this class are so easily seen and an example could include the protection of the IT infrastructure servers. If the servers are left out in the open, someone could easily walk up to them and tamper with their configuration. Even worse, that person could power off and steal the entire machine.

Once the thief had the server at home, it would be straightforward for them to remove the hard drives and plug them into their own servers. After booting up the drives, security permissions could be ignored and all the data read.

This would not be the case if the drive were encrypted. A common hardware technology for implementing this protection is a Trusted Platform Module (TPM), which acts as a certificate store embedded in the motherboard. Many users of the Windows platform enable this solution through the Windows Bitlocker feature (Morimoto, 2010).

# Logical Vulnerabilities

When you look at the top threats that affect a business, you have to look at the ones that threaten 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 motives on the system. The fact the company has clients 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. Incorporating a policy that helps prevents this situation is the best solution (Conklin, White, Williams, Davis, & Cothren, 2012). Having management organize an IT team that can oversee the project of analyzing the company as a whole and what will be the best solution of preventions.

In most cases, the first thing the IT team will do is oversee the current state of the security policy (Cooper & al., 2005). They will point out what part of the already established policy is good and what needs to be added. The main concern is to be able to layer the networks vulnerable parts of the system and assure that the internal users are also following day-to-day procedures to also prevent external threats.

As stated before, internal threats can be done on purpose, but at times, they cause a threat intentional. This is from not following the company’s policy of how to protect the network. It could be something simple as checking personal e-mail or opening an e-mail from an unknown source. These are ways that an internal can aide an external source. In these cases making sure that new employees are properly trained in properly performing task assigned to them (Hernandez, 2012). This will limit the chances of internal sources creating external threats.

**Shared Context**

Shared context vulnerabilities are weaknesses in the system caused by the using an asset for multiple purposes. Consider a single server that has both the web server role and a public file server role. Access to one role grants a degree of control over the other, which can be leveraged to bypass policy. This needs to be addressed through service isolation technologies, such as deploying the two roles into separate virtual machines (Erl, Carlyle, & al., 2014).

Sharing context is not limited to services it can also become an issue with improper role isolation. If Abby can write checks, approve checks, and controls the audit record; then vulnerability exists in the oversight of Abby’s spending. This can lead to a threat of Abby embezzling funds from the organization.

Alternatively a separation of roles needs to exist so that checks and balances are in place. For small companies this is difficult due to the small number of employees that work there. In those cases the problem can be addressed through policy (Cooper & al., 2005). An example might be no one is allowed to approve a check they wrote, or two approvers are needed per expense.

## Implementation Flaws

A common method to introduce vulnerabilities into a system is to have it incorrectly deployed or implemented. Consider a web site that accepts payments from customers. The web site might be using SSL/TLS to protect the communication, however they used a self-signed certificate. In this case the conversation can only be seen between the client and the server, though there is no way to confirm which client or which server (Boneh, 2013).

Imagine that Riordan does not want to do business with anyone in Egypt or Nigeria; this could be due to any number of perceived threats. To mitigate those risks the network isolation policy is deployed and the attack surface is reduced. However this does not mitigate the threat as expected. Attackers in Egypt can easily bypass this check through traffic forwarding services such as Virtual Private Networks (VPN) or Web Proxies.

This class of issues is often hard to identify due to things working correctly and presenting a high change of regression risk, if changed (Marchewka, 2012). There are many security auditing tools which can be purchased or freely acquired to validate some of these configuration flaws.

Though some of these vulnerabilities can be very costly to discover, such as vulnerabilities in custom code. Common classes of issues are encoding bugs. An encoding bug can occur anytime data, state, and/or code are combined without a clear isolation. For instance a buffer overflow is vulnerability where more data in stuck in memory than can fit, resulting in random memory being replaced (Anley, C; Felix, J; Richarte, L, 2007). If that random memory is replaced with properly formatted code, then the computer cannot tell the difference. This can result in remote arbitrary code execution.

Advancements in Operating System protections have made this more difficult, such as Data Execution Protection (DEP) and Address Space Layer Randomization (ASLR) (Morimoto, 2010). DEP adds an extra flag to every memory page stating if it holds data or code. If a data page is attempting to run code a hardware exception will prevent the attack. ASLR controls the way objects are loaded into a process, so they are randomly placed (Silberschatz, Galvin, & Gagne, 2012). Having random process states makes it more difficult to successfully exploit vulnerability.

While these technologies are useful, they do not cover the entire breath of protections about code level implementation flaws. In addition to this low level guards need to be installed inside of each process. An example of this would be the Enhanced Mitigation Experience Toolkit (EMET), which injects additional validation into system calls (Kreb On Security, 2013).

# Remediating and Mitigating Top Threats

There have been approximately numerous different vulnerabilities, both physical and virtual, that Riordan Manufacturing can potentially face. Out of those vulnerabilities, there are 20 that have been determined to be the most threatening and have the highest impact on the company. A lot of the vulnerabilities have the same category, such as different types of escalation of privileges (EoP) exploit, denial of service (DoS) attack, flooding, etc. The same security techniques can be distributed to each category of attack in order to have them mitigated. Therefore, it isn’t necessary to explain the mitigation technique for each separate vulnerability, but rather each category of vulnerability.

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 prints 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 (Conklin, White, Williams, Davis, & Cothren, 2012).

A type of EoP vulnerability that an enterprise can face 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 not having traffic limits. When the network becomes congested, information transport is significantly reduced and any voice-over Internet protocol (VoIP) service can be compromised. If this happens, efficiency in communication can be adversely affected. A cause of this problem is having multiple senders and multiple receivers communicating through one router with infinite buffers and no retransmission (Goleniewski & Jarrett, 2007).

This set up can cause large delays during congestion with maximum achievable output. A more efficient router configuration would help mitigate this problem. Both of these attacks 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), paragraph 2).

Another type of DoS vulnerability that all companies using databases can fall victim to is a SQL injection attack due to weak or improper database security. Since Riordan Manufacturing is dealing with large accounts on a global scale and sensitive product information, their databases could be considered very desirable, which increases risk.

An attacker needs a security vulnerability in order to execute the SQL attack by inserting or “injecting” malicious code into an entry field. This injection will allow the attacker to gain access and copy, edit, or delete the data in the database (Conklin, White, Williams, Davis, & Cothren, 2012). A solution for preventing these types of attacks is proper validation. Any input from an application, whether it be from a user or another application, needs to be validated. This security practice will ensure that the input won’t have the necessary characters for a SQL injection attack. Proper validation will help prevent these types of attacks along with others, such as XSS attacks and buffer overflows (Conklin, White, Williams, Davis, & Cothren, 2012).

Something that Riordan needs to enforce to their employees is the importance of changing their passwords at least every 90 days. A lot of companies tend to take this practice for granted. Simple passwords are often created so they’re easily remembered. If someone creates a complex password, sometimes it can be found written down near the system that it is used for. Simple passwords make it extremely easy to hack a system.

There are many tools easily available to the public that be used for password cracking such as Brutus or RainbowCrack. There are also many tools online where anyone can check the strength of a password before it is used. If employees use weak passwords, an attacker can crack it and gain access to whatever tools and resources that employee uses.

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.

# Conclusion

Having a good security plan provides company with a backbone in the case of an emergency. This plan lays out what the security goals for a company are and how to follow them to best protect the assets of the company. These standards are created to protect the resources and assets Riordan Manufacturing provide to its customers. Without a security plan in place, companies leave themselves open for attacks on their physical infrastructure as well as their IT network. Riordan Manufacturing is a company that has a lot to lose if a good security plan in not in place and working for the company. Identifying the risks that Riordan will face gives the company a real look at the potential threats it may face. Making sure they know the importance of those risks and how they rank amongst the others provides the company with a good insight as to the severity of the risks provided. Knowing the fix techniques that will mitigate these risks to the best of the companies’ ability gives the Riordan the shell of their security plan and how to address the risks. This plan for Riordan will need to be a working document that grows with the company. As new risks become apparent, new techniques and identification processes will be added and delivered within this security plan.

# References

Anley, C; Felix, J; Richarte, L. (2007). *The Shellcoder's Handbook.*

Boneh, D. (2013). *Cryptography.* Stanford Publishing.

Clarke, M. W. (n.d.). *Today's Employee, Tomorrow's Defendant?* Retrieved from Smith, Gambrell, & Russell LLC: http://www.sgrlaw.com/resources/trust\_the\_leaders/leaders\_issues/ttl17/827/

Conklin, W., White, G., Williams, D., Davis, R., & Cothren, C. (2012). *Principles of Computer Security: CompTIA Security+™ and Beyond (Exam SY0-301), Third Edition.* McGraw-Hill Company.

Cooper, D., & al., e. (2005). *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements.* John Wiley & Sons, Ltd.

Erl, T., Carlyle, B., & al., e. (2014). *SOA with REST: Prinicpals, Patterns, & Constraints for Building Enterprise Solutions with REST.* Peason Education.

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications Essentials. The Complete Global Source, Second Edition.* Pearson Education.

Hernandez, S. (2012). *Official Guide to the CISSP CBK, Third Edition.*

Kreb On Security. (2013, June). *Windows Security 101 EMET 4.0*. Retrieved from Kreb On Security: http://krebsonsecurity.com/2013/06/windows-security-101-emet-4-0/

Marchewka, J. (2012). *Information Technology Project Management. Providing Measurable Organizational Value, Fourth Edition.* John Wiley & Sons Inc.

Morimoto, R. (2010). *Windows Server 2008 R2 Unleased, 1st Edition.* Pearson Education, Inc.

Silberschatz, A., Galvin, P., & Gagne, G. (2012). *Operating System Concepts, Eighth Edition.* John Wiley & Sons.

Clarke, M. W. (n.d.). *Today's Employee, Tomorrow's Defendant?* Retrieved from Smith, Gambrell, & Russell LLC: http://www.sgrlaw.com/resources/trust\_the\_leaders/leaders\_issues/ttl17/827/

Rouse, M. (2010). Searh networking. Retrieved from http://searchnetworking.techtarget.com/definition/traffic-shaping

Rouse, M. (n.d.). *distributed denial of service attack*. Retrieved from Search Security: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

 Microsoft. (n.d.). *Protecting your software*. Retrieved from http://www.microsoft.com/security/sir/strategy/default.aspx?\_escaped\_fragment\_=section\_3\_2#!section\_3\_2

Wiley, J., & Ottenheimer, D. (2012). Securing the Virtual Environment: How to Defend the Enterprise Against Attack, 1e. Retrieved from The University of Phoenix eBook Collection database.