Week 2: Risk Analysis of Benefit Election System  
Nate Bachmeier  
CMGT 442: Risk Management  
University of Phoenix  
July 21st, 2014

**Contents**

[Risk Analysis of Benefit Election System 2](#_Toc393631864)

[Security Risk Assessment 3](#_Toc393631865)

[Spoofing 3](#_Toc393631866)

[Tampering 4](#_Toc393631867)

[Information Disclosure 4](#_Toc393631868)

[Denial of Service 4](#_Toc393631869)

[Elevation of Privilege 5](#_Toc393631870)

[Risk associated the System Being Requested 5](#_Toc393631871)

[User Acceptance / Application Compatibility 5](#_Toc393631872)

[Political Acceptance 6](#_Toc393631873)

[Legal Risk 6](#_Toc393631874)

[Budgeting and Resource Planning 7](#_Toc393631875)

[Environmental Issues 7](#_Toc393631876)

[Project Abandonment Strategy 7](#_Toc393631877)

[Conclusions 8](#_Toc393631878)

[References 9](#_Toc393631879)

[Architecture Diagram 10](#_Toc393631880)

# Risk Analysis of Benefit Election System

Huffman Trucking is in the process of developing then deploying a benefits election system to support the tracking and reporting of employee benefits. There is risk associated with each phase of the software lifecycle (Cooper & al., 2005). To increase the likelihood of success, an analysis is required for each aspect of the system.

# Security Risk Assessment

A benefit election system is a great target for attack. If an actor is able to gain unauthorized access, they can: change pay, view other employee’s usages, and remove the company’s ability to process legitimate requests. To assess the vulnerable points the first step is to create a high level architecture of the system, as is provided in Figure 1. Then each class of issues in the STRIDE model need to be visited (Hernan, Lambert, Ostwald, & Shostack, 2006).

## Spoofing

The system will need to be resistant to spoofed objects such as fictional claims or one employee masquerading as another. To reduce the risk the new system will need to connect into the already deployed centralized authentication system. Then by forcing the user to login through user name and password the identity can be confirmed (Morimoto, 2010).

Once the identity has been discovered each service will need to impersonate the security context to make sure the caller is authorized to perform the action (Stallings & Brown, 2008).

## Tampering

Traffic between each component, need to communicate in a secure manner where the information is signed and encrypted. If an attacker is able to modify the communication they might be able to bypass certain protections (Stallings & Brown, 2008).

To mitigate this attack vector all systems need to be protected by IPSec, SSL/TLS, and WPA technologies (Morimoto, 2010). Having such a system also enables traffic authorization between nodes.

For instance the Auditing Service should be allowed to communicate with the Auditing Data Store, while the Web UI should not. With reduced attack surface the system will be more fault tolerant and perform in more expected ways (Stallings & Brown, 2008).

## Information Disclosure

The system needs to have mitigations for information being shown too unauthorized individuals. An example might include accidently showing another employee’s benefit details. To verify this does not work all callers need to be impersonated, which causes them to be denied read access (Stallings & Brown, 2008).

## Denial of Service

An actor could reduce the availability of the system by overloading any components with expensive, malicious, or high volume data (Stallings & Brown, 2008). To partially reduce this IPSec needs to be deployed to limit the number of path ways (Goleniewski & Jarrett, 2007). Each component also needs to be scalable to meet the normal load of the customers. Malicious traffic can be removed by using a network intrusion system that is capable of updating network access control lists (NACL) (Goleniewski & Jarrett, 2007) (Stallings & Brown, 2008).

## Elevation of Privilege

The final area of security risk is elevation of privilege attacks. These occur when security policy is bypassed, such as a person breaking into the server room. To reduce the risk of these attacks auditing and alerting needs to exist (Stallings & Brown, 2008). Then when there is unexpected entry into the server room at 3am the security office can be alerted to investigate.

# Risk associated the System Being Requested

Once deployed the system needs to maintain security and reliability through Confidentiality, Integrity, and Availability (CIA). However risk does not being only when running in the production environment. There is also areas of concern from the inception of the project.

## User Acceptance / Application Compatibility

A system which is unusable by the end users is a waste of time and money. For instance if the benefit system is too slow or only works on a limited platform then the users might not experience the joy of using the system (Marchewka, 2012). Their frustration will turn into support calls which cost the company.

To reduce this risk new systems need to conform to industry standards increasing the portability of the solution (Marchewka, 2012). Extra time needs to be spent researching how the users intend to work with the service. Perhaps they prefer a mobile application instead of a web portal without understanding the customers it is hard to meet their demands.

## Political Acceptance

Along with user acceptance is political acceptance, such as if the leadership team will approve and support the project. For instance the benefit solution will need to integrate into the existing accounting ecosystem. If the leadership of that division have different opinions on direction they might be able to kill the project before it gets started.

To reduce this risk partnerships need to be established between the various stakeholders and discussions made upfront (Marchewka, 2012). By getting their feedback early it also makes them feel included which can make gaining their political allegiance later an easier task (Boyatzis, 2012).

## Legal Risk

Let’s just pause for a moment and think in the event of a “nuclear meltdown,” what the legal ramifications could include. This might include employees suing after a data leak or incorrect benefit payments (Nickels, McHugh, & McHugh, 2013). A lawyer are very expensive and if the case goes to court the costs become enormous quickly.

To reduce this risk legal and compliance teams need to be brought into the conversations early on and sign off on the risks. These peers will have knowledge of specific risks and can provide guidance to further reduce the concerns (Nickels, McHugh, & McHugh, 2013).

## Budgeting and Resource Planning

If the system is better than sliced bread, but costs one billion dollars to operate it is unlikely to come into existence. Just as money is a concern time also is a factor, such as if it would take five hundred people four years to implement.

To reduce this risk realistic assessments need to be made up front to predict the size of the project (Marchewka, 2012). Parts of the project that are too large need to be broken down into smaller parts. For example using open source software or purchasing an already existing component can be more efficient (Das, 2013).

## Environmental Issues

The additional servers required to handle the compute and storage may increase environmental issues, such as through inefficient cooling. A general study needs to be performed on a regular cadence to make sure the benefit solution is compliant.

## Project Abandonment Strategy

The final type of risk discussed is project abandonment, such as the solution is 70% implemented and suddenly lost funding. This would result in a loss of time, resources and potentially the purchase of unused hardware (Marchewka, 2012).

To reduce this risk, resources should be rented or leased so that the contract is simply not renewed (Russinovich & Minasi, 2014). Once the project has been completed and long term load is known then dedicated resources can be purchased. An example of this is cloud based solutions like Azure, Amazon, and Google. They allow the company to instantly run at any scale and free the resources when not needed.

# Conclusions

Designing and deploying a benefit election system can incur risk at every step along the way. During the inception plan political opponents may try to kill the project which needs to be meet with strategic partnerships. While the system is being built the funding might be removed and plans for partial recovery need to exist. Once it has made its way into the production environment the security needs to be resilient enough to block each STRIDE class of attack.

Through understanding where these issues exist and how to properly mitigate them, it is possible to more effectively and efficiently build enterprise software.

# References

Boyatzis, R. (2012). *Inspiring Leadership through Emotional Intelligence.* Coursera.

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

Das, S. (2013). *Your UNIX/Linux. The Ultimate Guide, Third Edition.* McGraw-Hill Company.

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

Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. (2006). *Uncover Security Design Flaws Using the STRIDE Approach*. Retrieved from MSDN Magazine: http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

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, 1e.* Pearson Education, Inc.

Nickels, W., McHugh, J., & McHugh, S. (2013). *Understanding Business, Tenth Edition.* McGraw-Hill Company.

Russinovich, M., & Minasi, M. (2014, April). *Cloud Computing TechEd 2014*. Retrieved from Channel 9: http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/DCIM-B386

Stallings, W., & Brown, L. (2008). *Computer Security: Principals and Practices.* Pearson Education, Inc.

# Architecture Diagram

