**Week 4: Outsourcing Risks**

Nate Bachmeier  
August 4th, 2014  
CMGT 442: Risk Management  
University of Phoenix

# Outsourcing Risks

I recall being a child and the family car broke down and needed to be taken to the mechanic for repairs. I asked my father, who was an accountant by profession, why he didn’t fix the car instead. He replied if someone wanted their taxes done he was the guy, otherwise it was not his core business or area of expertise.

The same lessons can be used by organizations deciding on investments toward labor and resource acquirements. For instance a finance company may buy many calculators, but that doesn’t mean they should be manufacturing them. Reducing scope and focusing on the core business allows the company invest more time into making profits and delighting customers.

# Common Risks with Outsourcing

While there are many benefits to outsourcing sections of the business, it is not without its risks to the organization (Cooper & al., 2005). Depending on the type of area such as data storage, hosted service, external network support, or external helpdesk support – there will be common risks along with specific areas of concern.

## Common Security Concerns

Confidentiality, Integrity, and Availability (CIA) of the resource is the first common area that needs to be reviewed (Hernandez, 2012). The third party needs to have systems for assuring all data is encrypted and not susceptible to theft. Next solutions need to exist to know that the state of the ecosystem is not tampered with and consistency checks are able to pass. Lastly if the service is not accessible when needed, then it is useless.

To reduce these issues an organization can create policy that it will only use third parties with industry approved certifications. Another option is to require background checks on the directly related employees of the third party (Conklin, White, Williams, Davis, & Cothren, 2012).

Availability can be addressed by working with larger organization that have the redundant staff or the additional hardware on hard. For instance a down server is game over if there is only one, if there are spares the load can be transitioned until a long term solution is in place.

## Common Quality of Service Concerns

The next challenge is ensuring the outsourced resource is capable of running with at an acceptable quality. Quality can be measured on the dimensions of response time, reliability, availability, and throughput (Elliot, 2014). If any of these drop the cost of the service increases due to more support calls, loss of potential sells, and disgruntled end users.

To keep quality high key metrics need to be defined and stated in the service contract. For example a network support contract may state that throughput cannot decrease below X gigabytes per second. If it does an alert is raised and the issue will be resolved within Y hours according to the agreed upon Service Level Agreement (SLA).

# Risks with External Data Storage

## Location Affinity Concerns

Once a third party data storage provider has been found it is important to understand their location affinity policy. For example documents may by cheaper to store in Nigeria, but that doesn’t mean one would want to use a destabilized region with relaxed government enforcement of the law.

To remove this point of concern the affinity of the data needs to be called out during the procurement state (Nickels & al, 2013). Agreements also need to be in place for how the affinity can be changed later, such as if the third party wants to move the data warehouse to a different state.

## Backup and Recovery Concerns

In addition to the standard security concerns the third party needs to have a solid backup and recovery model. Hard drives fail, accidental and malicious updates will occur periodically and cannot be stop the business from functioning.

To remove this potential train wreck the third party needs to have proper backup and recovery policies in place. The organization should review these policies before enrolling in the service. Solutions such as geographic redundancy between multiple datacenter; alternatively having hot/cold sites could also address the problems (Cooper & al., 2005).

# Risks with External Hosted Systems

## Future Supportability Concerns

If a third party creates a custom solution or migrates exist data onto their platform, what happens if that third party goes out of business? Another scenario could be business relations sour and a different provider is desired. At this point the system needs to be moved, which can be expensive and highly disruptive to the business (Marchewka, 2012).

To reduce these concerns any custom solutions need to leverage industry standards, and the source acquired when possible (Valacich, 2012). The selected platform needs to also follow standards such as service oriented architectures (SOA) with RESTful endpoints and XML serialized data contracts.

## Political and Branding Concerns

Political risk can come from a wide range of locations such as people discovering key differentiators are no longer performed by the original company. Another place could be the third party is discovered to contribute funding toward hate groups, establishing guilt by association. To remove this concern to the brand, a morality clause be put into the contract; allowing the relationship to be terminated in the event of such a scenario.

# Risks with External Helpdesk and Support

## Social Engineering Attacks

Helpdesk employees are the front line of the IT department and will get questions from low level grunts through executives. If they are unable to properly distinguish legitimate requests from fraud, they may disclose credentials or provide other sensitive information.

To reduce this risk security teams should actively be attempting to break into the company. When problems are detected those contingent staff taken aside and provided with proper training. Having a company culture of assuming constant attack will keep everyone more attentive to detail and increase the overall security posture.

## Customer Satisfaction

Similar to storing our files in Nigeria maybe cheaper, but unwise; so can the same be said about using people with thick foreign accents. If the customer cannot understand what is being asked the call will take longer, cause frustration, and result in a poor experience. Instead using people of the same nation or text based chat instead of phone based systems can mitigate the problems.

# Risks with External Network Support

## Regressions to Ecosystem

A challenge with networking in house or outsources is that it is very easy to change a small thing and cause a ripple of disruption across the other nodes (Goleniewski & Jarrett, 2007). Because of this risk it is important to only allow certified engineers to make changes. Those changes also need to be in compliance with an already established change management policy.

# Conclusions

Outsourcing is great, and enables organizations to gain highly specialized employees for specific projects or grunts for the tedious parts. However like many solutions it comes with a collection of risks.

Many of these risks are common such as security or quality of service. Others will be unique to the service type such as data storage affinity or social engineering attacks. Each of these failure points can be addressed through proper planning and contractually enforceable service agreements.

# References

Conklin, A., 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.

Elliot, K. (2014). Quality of Service Indicators. Microsoft Internal Training.

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

Greenstein, M., & Vasarhelyi, M. (2002). *Electronic Commerce: Security, Risk Managemetn and Control.* McGraw-Hill.

Hernandez, S. (2012). *Official (ISC)² Guide to the CISSP CBK.*

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

Nickels, W., & al, e. (2013). *Understanding Business, 10th Edition.* McGraw-Hill Company.

Valacich, J. (2012). *Essentials of Systems Analysis and Design, 5e.* Pearson Education, Inc.