**Week 2: Risk Management Consulting**  
Nate Bachmeier  
CMGT 430: Enterprise Consulting  
University of Phoenix  
August 25, 2014

# Risk Management Consulting

McBride Financial Services has hired an external consultant to review their enterprise security and assess any areas where risk management is not correctly applied. In addition to general information on risk management principal, they also want information on protection efforts over time and examples of potential vulnerabilities and their mitigations.

# Applying Risk Management Principles to Secure Systems

Risk management principles need to be applied each phase of a system, in order to successfully design a secure system (Cooper & al., 2005). This idea is expressed in many software design standards such as Security Development Lifecycle (SDL) and Project Management Book of Knowledge (PMBOK).

## Design Phase

At the beginning of the design phase the project has a significant amount of risk, few restrictions have been put on the blank canvas. If engineers start dreaming in one direction, while the business needs another this presents a huge risk for lost time and effort. To mitigate that the attack surface needs to be reduce.

For example identify the requirements of the environment where the system will run. Will it accept credit cards and need PCI compliance or work with government and need FIPS encryption? Will it be in the cloud, on premise or a hybrid deployment? These along with dozens more questions will shape the direction and final product.

Identifying the environment will also help set the tone, for how which security solutions are needed. Consider the difference between a read-only web server and a highly interact e-Commerce portal (Greenstein & Vasarhelyi, 2002). They are both the fundamentally doing the same task, but it is much easier to justify biometric logins on the later.

## Implementation Phase

As each component is authored care needs to be taken that it is correctly constructed. Correctly designed components are easy to regression test, deploy, and make smart dependency choices (Humble & Farley, 2010).

If a dependency is taken on a third party there needs to be sufficient support in case of catastrophic failure (Cooper & al., 2005). This would be analogous to running a bakery and getting all of the flour from either the kid next door or an established grocery supply store. The neighbor might be a great person, but if he disappears for two weeks would your business survive?

Another aspect of correctly implementing components is validate they use the third party components in expected and recommended patterns (Venit & Drake, 2011). This is very easy to get wrong with complex libraries such as crypto systems, and worst difficult to identify is incorrect (Bluehat, 2013).

Lastly instrumentation needs to exist throughout the entire component. Instrumentation can be as simple as “*printf statements*” or very complex such as the X-Box One stack (Microsoft, 2014). These traces of the program then need to be aggregated to central points. This provides the ability to funnel all the needles into a single hay stack, making issues more discoverable.

## Maintenance and Monitoring Phase

Assuming stake holders were involved in the design and implementation is sufficiently high quality; the maintenance and monitoring phase will be the longest phase (Marchewka, 2012).

During this phase operations teams will be reviewing the instrumentation and other logging to find signs of trouble. This could be misconfigured endpoints or intentionally malicious communication.

An analogy might be a security guard watching the cameras at a retail store. Most of the customers are there to browse or participate in legitimate commerce. Some of the clientele might be drunk and making a scene, but are harmless while the group of punk kids is stealing products.

As the volume of collected data increases so does the complexity of processing it. Similar to having ten cameras might require two staff, having terabytes of signals could require dozens of logs parser servers. Being able to laterally scale is critical if all risks are to be reactively caught.

Alternatively to being reactive to risk is to be proactive. For example having proper central authentication solutions to validate user’s identities and their authorization policy will keep many problems from happening in the first place.

## Disposal Phase

The final stage is the disposal of the system, which includes securely clearing any previous application state and recycling in an environmentally sound manner. Hard drives and similar media needs to be sent to a disposal facility where it can be demagnetized and melted (Hernandez, 2012).

Once the drives have been removed the remaining hardware can be donated to a PC recycling facility or other organization. Alternatively if cloud services were used none of these risks exist as the resources are freed and blanked for use by the next tenant.

# Protection Efforts vary Over Time

One of the challenges to information security is that it is not intended to stop attackers, only deter them to a different target. It is an ongoing arms race of building ten foot walls, which is good enough until someone creates an eleven foot latter.

Cryptography, is one such area due to its heavy reliance on high CPU time needed to solve complex mathematical equations. However due to improvements in cloud and grid computing CPU time no longer maps to wall clock time. For instance on a 750$ budget it is possible to compute 1 CPU Year within 60 minutes (Microsoft, 2014).

Crime rates are not uniformly distributed, with a larger number occurring during the holiday seasons. It can be useful to identify these peaks and ensure employees are aware of the higher risk. Awareness and training gives the employees the tools to be proactive though reactive counter measures may also be required. For instance a branch office might hire additional temporary guard to increase patrol of the area.

# Additional Example Sets

Financial service organizations need to operate in an environment that assumes constant attack. These attacks come from every direction such as customers, bank reform lobbyist, market movements, network attacks, and insider threats. To ensure the longevity of the organization a large percentage of these attacks need to be mitigated or reduced to an acceptable level.

Consider the following, the customer is responsible for the password needed to access their account. However if they choose poorly and the account is compromised, the business will have to accept the loss on behalf of the customer. To reduce the risk of loss, safeguards need to be in place. Examples might include a daily withdrawal limit, two factor authentication, or an e-mail notification of transaction.

Attacks on the corporate IT infrastructure are another high risk area, which can be mitigated through risk management. For instance, segmenting the environment into different trust zones and prevent a low integrity system (ex: public web server) from communicating with a high integrity system (ex: backend data store) (Goleniewski & Jarrett, 2007). Another solution is to follow the Golden Rule and Authentication, Authorize, then Audit all transactions.

The hardest threats to see can be the ones right under your nose, such is the case with insider threats. These could be people that have worked for the company for years and are trusted members of the community. Regular background checks of the employees can detect these risks and provide them help a head of time (Cooper & al., 2005).

# Conclusions

McBride Financial Service is a prime target for many through numerous vectors. Over time they will need to upgrade their previous protections as they will be deprecated. As these new systems are brought online they will need to apply risk management principals. Risk management is applicable to design through disposal phases. Using these steps are more likely to end up with a high quality and long lasting solution.

# References

Bluehat. (2013). Various Security Talks. Microsoft Corp.

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

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.*

Humble, J., & Farley, D. (2010). *Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation.* Addison-Wesley Signature Series.

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

Microsoft. (2014). *Azure Pricing*. Retrieved from Azure: http://azure.microsoft.com/en-us/pricing/details/virtual-machines/

Microsoft. (2014). Xpert Instrumentation System. *Microsoft Big Data Conferance.*

Venit, S., & Drake, E. (2011). *Prelude to Programming. Concepts and Design, Fifth Edition.* Pearson Education.