**Edward Jackson**

7/24/2015 5:02:48 PM

**Learned a few things**

As the IT Specialist in my project, I basically was responsible for the entire project. I did have a few local site technicians assisting with “hands-on” problems, but mostly, I was the one leading the project, doing all the software development, deploying scripts, and running reports. In lessons learned, the initial problems were determining scope, figuring out the budget for the proposed “cheap” solution, and performing a risk analysis.  
  
For scope, I needed to determine how many computers would be receiving the Bitlocker encryption solution. This was no easy feat, as the workstations in the enterprise span three corporate sites, and not all computers were actively being used. The best solution I came up with was to use our desktop management software, and run a report on computers that had checked in within the last month. This returned around 10,000 computers, which were added to the project’s scope and become the targeted list. This was specifically added to lessons learned because there were several ideas that came up on how to retrieve the targeted list. For example, it was suggested we use our inventory software, except the inventory software did not return *online* machines. Another suggestion was to just have the local technicians compile a list, and then that list could be imported into our desktop management software. This would work, except it would require a lot of time and effort. The best solution was definitely to use our desktop management software.  
  
Next in lessons learned, I spent a long time trying to figure out exactly what the budget was for this project. There meetings held, emails sent, and phone calls made. In the end, it came down to figuring out software development time, and how many computers would need to be purchased as replacement computers, if the need arose. I think, especially because I was the one doing most of the work, it was hard to build a solid budget around the many tasks I would be doing. The lessons learned part of this is that I should have just estimated a flat cost for my own time based upon (hours worked) *x* (how much I was being paid per hour). I actually came in under budget, due to the fact that there were very few problems, and I only had to use 10 of the 20 computers that were allocated for in the risk analysis.   
  
The final lessons learned item I would like to discuss is the risk analysis itself. What a risk analysis is supposed to do is to find potential problems, and then allow us to come up with mitigation solutions (Brown, Dehayes, Hoffer, Martin, & Perkins, 2012). I actually did quite well in this area, but only because I have experience deploying Bitlocker, and have seen numerous problems during the roll out of the Bitlocker solution. For example, a common problem when enabling Bitlocker is that the TPM chip is disabled, or broken. Because I created a script to “enable” the chip, I knew that would not be a problem. However, broken chips was a whole different story. For some reason, some motherboards just are not compatible with Bitlocker, or in some cases, the TPM chip is broken. In the risk analysis, I did anticipate non-working TPM chips, so I had 20 computers allocated for in the budget. We ended up using 10 of those computers, which I thought was not a bad estimate. I think a better solution would have been just to order 10 computers, and then on a case by case basis, order extra computers. This would have saved us roughly $10,000. But, I’d say overall the project went as intended, and the company and the customers were pleased to now have secured hard drives.  
  
Reference

Brown, Dehayes, Hoffer, Martin, & Perkins. (2012). *Managing information technology, 7th ed. Prentice Hall, Pearson*.