**Edward Jackson**

7/3/2015 12:20:03 PM

**Encryption rollout**

**Project overview**
My project deals with adding security to company workstations. Due to recent security breaches across the nation, my mock company has become increasingly concerned about protecting the contents of company computer hard drives. As of right now, they do have anti-virus software, but no form drive encryption. Without encryption, the data on computers could be stolen, hacked while offline, and viewed by unauthorized people.

 Thus, as a solution, I have recommended that the company implement Microsoft’s Bitlocker on all business computers. Bitlocker is a full disk encryption solution, which will work by using technology that already exists on the workstations. Something worth mentioning, I will be rolling out a “free” or nearly free management solution. This is to forego the costs of $150 (per workstation) 3rd party solutions, and to not have to pay the $10 per seat by using MBAM and MDOP. The project will have a budget for implementing Bitlocker, however, the TCO will be very low, while the ROI will be high, and continue to grow over time. When using this cheaper method, companies can save hundreds of thousands of dollars (potentially millions of dollars) in Bitlocker implementation and management.

**Major milestones**
Although Bitlocker is already in Microsoft operating systems, it is off by default. Also, Bitlocker is dependent on recovery keys, which are stored in a TPM chip.

**-Milestone 1**
So, the first step in the Bitlocker rollout is to develop and test all the code that will be necessary to manage Bitlocker recovery keys. The deliverable will be code to report on TPM chips, code to manage the recovery keys, and code to report on Bitlocker compliance.

**-Milestone 2**
Once all the code has been developed and tested, the next milestone will be to enable TPM chips on all workstations. This stage is critical to the overall process, because without the TPM being turned on, the recovery keys have no place to be stored. Now, there is a possible USB storage solution, however, to keep project costs (and TCO) low, the TPM chip has been selected as the best, cheapest recovery key storage option. This milestone will be complete when all TPM chips have been enabled. The deliverable will be a report stating the status of all TPM chips.

**-Milestone 3**
After the TPM chips have been enabled, the step stage of the process will be to collect Bitlocker recovery keys. Because I have chosen not to buy a Bitlocker management system, I will use code I have created to manage the retrieval and storage of Bitlocker recovery information. For this step, I will use SCCM or LANDesk (desktop management software) to deploy my TPM management scripted application. The TPM management does four things (1) Activates the TPM Chip, (2) takes ownership of the TPM, (3) adds protectors to the TPM, and (4) starts and pauses Bitlocker encryption. The deliverable for this milestone is a report verifying that TPM Management was indeed successful.

**-Milestone 4**
In fourth and final milestone, the user will resume the Bitlocker encryption process. The recommended time to begin this process is at the end of the work, just before going home. This time has been recommended because while Bitlocker is encrypting the hard drive, the computer will run extremely slow; too slow to work on. The deliverable for this milestone is a report that returns the compliancy status of Bitlocker on workstations.

**Estimated budget (scope, time, and cost)**
The scope of the project includes all company workstations, some 10,000 computers. The time is set at 6 months, which is 2000 workstations a month. If the timeline is shortened, that is quite alright. If the project needs to be extended, that will also work just fine, as long as the entire project does not go over 8 months. The ultimate goal is to have all workstations fully encrypted by the 1stquarter of 2016. Costs will be set to $25,000. This includes development costs, paying for technical support for failed Bitlocker installations, purchases for new, working computers for broken TPM chips, and training costs for support staff.

**Key stakeholders**
The stakeholders will include the CIO, CFO, the Change Management Team, the Senior Developer, and the Manager and Team Leader from the IT department.

**Potential sources of research**<http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview>

<http://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html>

<https://www.technibble.com/bitlocker-101-easy-free-full-drive-encryption-for-windows/>

<http://blogs.technet.com/b/uspartner_ts2team/archive/2010/03/17/what-is-bitlocker-what-does-it-do-what-does-it-not-do.aspx>

**Your role in the Project (IT Project Manager or IT Specialist)**

The expected role will be that of an IT Specialist. As the IT Specialist, a project plan will be created, milestones will be achieved, I will create a budget, budgets will be adhered to, and total governance of the project will fall under me. I will be doing all the coding, testing, reporting, and management of the project. While there will be other people carrying out essential tasks, I am the one that will follow up with them, and make sure the project stays on track.

\* If anyone has questions or suggestions, please post in this discusses. I am still in the tentative stages of project design.

References

BenefitOf. (n.d.). Benefits of Bitlocker. Retrieved from http://benefitof.net/benefits-of-bitlocker/
Brown, Dehayes, Hoffer, Martin, & Perkins. (2012). Managing information technology, 7th ed. Prentice Hall, Pearson.

Microsoft. Bitlocker overview. Retrieved from http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview