IT599: MASTER'S PROJECT IN APPLIED TECHNOLOGY

BITLOCKER PORTFOLIO

Submitted by

Eddie S. Jackson

In partial fulfillment of the requirements for the degree of

"Master of Science in Information Technology"

in the Graduate College of Kaplan University

Summer 2015

Academic Committee:

Professor: Rhonda Chicone, Ph.D.
Educational Advisor: Monica Nino
Peer Review: Wendy Woodward

TABLE OF CONTENTS

COMPANY X

July 4, 2015

Deliverables

IT Project Plan
Project Management Timeline
PowerPoint Presentation
Two Milestone Videos
Article on SDLC and the Project Management Life Cycle
Real World Example Article
Ethical, Legal, and Social Implications Article
Lessons Learned Discussion

IT Project Plan

1.0 Project Overview

Due to recent security breaches across the nation (Hardekopf, 2015), Company X has become increasingly concerned with securing data on company computer hard drives. Currently, Company X does have anti-virus software, a data loss prevention solution, and malware protection installed on all workstations, but does not have any form of drive encryption. Without encryption, the data on computers could be stolen, hacked while offline, or viewed by unauthorized persons.

For an encryption solution, Microsoft's Bitlocker has been recommended. Bitlocker is a full disk encryption solution, which can be implemented using technology that already exists on the company's workstations. Something worth mentioning, this particular solution will contain a "free" or nearly free management solution. This is to forego the costs of $150 (per workstation) 3rd party solution, and to skip the licensing costs associated with using MBAM and MDOP (Microsoft Bitlocker Reporting solutions) at an estimated $10 per seat (Dalecheck Technology Group, 2014)). The project will have a budget for implementing Bitlocker, however, the TCO is meant to be very low, while the ROI should be high and continue to grow over time. When using this inexpensive management method, companies can save hundreds of thousands of dollars (potentially millions) in Bitlocker implementation and management costs.

2.0 Project Scope

The scope of the project includes implementing Bitlocker on all company workstations (some ten thousand computers). The time is set at seven months, which includes development and testing

of management scripts, providing technical support for failed Bitlocker installations, replacing non-working machines with new, working computers, and training support staff. The end goal is to have Bitlocker deployed to all company workstations by the first quarter of 2016.

3.0 Project Budget

Budget Item	Description	Cost
Code development	Reporting and TPM Management solutions must be developed in-house	$3,500
Training	Documentation must be created and staff trained	$2,000
20 x Computers	Twenty computers have been allocated to replace non-working TPM chips: Each computer costs $1,000.	$20,000
Technical Support	$25 per hour, with a breakdown of 25 hours * $25 * 3 sites	$1,875
Miscellaneous Costs	Costs include support for Active Directory, Network computers, and the Bitlocker solution.	$2,625
	Total cost	$30,000

4.0 Project 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.

Title	Description
CFO	Chief Financial Officer, in charge of company finances
CIO	Chief Information Officer, in charge of company technology
Change Management Team	Authorizes changes to enterprise systems
Senior Developer	Responsible for software development
IT Manager	Communicates directly to IT staff
IT Team Leader	Performs training to IT staff

5.0 Project Benefits

Benefit	Description
Secure Data	The data contents of the hard drive will be secured.
Offline Attacks	Offline attacks, such as removing the hard drive and placing it into another computer, will be prevented.
Unauthorized users	If the user is not a company user, recovery keys will not be available to them, thus, any authorized user cannot access the data on the drive.
Disposal	When disposing hard drive, there is peace of mind that company data will not be leaked
Savings	A third party utility will not need to be purchased, thus saving the company the costs of maintaining a per machine license.

6.0 Project ROI

The ROI has a few variables. One, standalone encryption software applications cost anywhere from $100-$200, so I will say $150 per workstation (that is $150 * 10,000 workstations = $1,500,000) (Suneja, 2006). Next, the Microsoft reporting software costs $10 per seat, that is, 10 * 10,000 workstations = $100,000. The sum of these two figures totals $1,600,000. The proposed solution costs a maximum of $30,000 to implement.

7.0 Project Roles and Responsibilities

Role	Responsibility
IT Specialist	Develops all code, deploys code, and runs reports
Stakeholders	Authorizes the stages of the project
IT Team Leader	Creates documentation and trains staff accordingly

Ohio Technician	Site tech is responsible for local support
Arizona Technician	Site tech is responsible for local support
Florida Technician	Site tech is responsible for local support

8.0 Project Work Breakdown Structure

Project Dates: 07/1/2015-02/29/2016, 1st Quarter of 2016

** The critical path is in red*

Task Name	Duration	Start	Finish	Predecessors
BITLOCKER ROLLOUT PROJECT	174 days?	Wed 7/1/15	Mon 2/29/16	
1.0 Project Start	**8 days**	**Wed 7/1/15**	**Fri 7/10/15**	
1.1 Create Project Overview	3 days?	Wed 7/1/15	Fri 7/3/15	
1.2 Define Scope	3 days?	Mon 7/6/15	Wed 7/8/15	3
1.3 Define Business Plan	3 days?	Mon 7/6/15	Wed 7/8/15	
1.4 Perform a Risk Assessment	2 days?	Thu 7/9/15	Fri 7/10/15	5
2.0 Project Planning	**5 days**	**Mon 7/13/15**	**Fri 7/17/15**	**2**
2.1 Create Project Proposal	1 day	Mon 7/13/15	Mon 7/13/15	
2.2 Obtain Initial Approval from Stakeholders	1 day	Tue 7/14/15	Tue 7/14/15	
2.3 Create Budget	1 day	Tue 7/14/15	Tue 7/14/15	
2.4 Kickoff Meeting	1 day	Tue 7/14/15	Tue 7/14/15	
2.5 Identify Risks	1 day	Wed 7/15/15	Wed 7/15/15	11
2.6 Create Contingency Plan for Risks	1 day	Wed 7/15/15	Wed 7/15/15	
2.7 Complete Business Analysis	1 day	Wed 7/15/15	Wed 7/15/15	
2.8 Draft Project Plan	1 day	Thu 7/16/15	Thu 7/16/15	14
2.9 Draft Project Schedule	1 day	Thu 7/16/15	Thu 7/16/15	
2.10 Stakeholder Meeting for Design Approval	1 day	Fri 7/17/15	Fri 7/17/15	16
3.0 Construction	**32 days**	**Mon 7/20/15**	**Tue 9/1/15**	**7**
3.1 Design	**3 days**	**Mon 7/20/15**	**Wed 7/22/15**	
3.1.1 Coded Report for TPM status	1 day	Mon 7/20/15	Mon 7/20/15	
3.1.2 TPM Management for importing recovery keys	**2 days?**	**Mon 7/20/15**	**Tue 7/21/15**	
3.1.2.1 Active Directory Import	1 day	Mon 7/20/15	Mon 7/20/15	17
3.1.2.2 LANDesk Import	1 day	Tue 7/21/15	Tue 7/21/15	22
3.1.2.3 Email Keys	1 day	Tue 7/21/15	Tue 7/21/15	
3.1.2.4 SFTP Keys	1 day	Tue 7/21/15	Tue 7/21/15	
3.1.3 Coded Reports for Bitlocker Status	1 day	Tue 7/21/15	Tue 7/21/15	
3.1.4 Weekly Status email sent to Stakeholders	1 day	Tue 7/21/15	Tue 7/21/15	
3.1.5 Stakeholder Meeting for Development Approval	1 day	Wed 7/22/15	Wed 7/22/15	27
3.2 Development	**22 days**	**Mon 7/20/15**	**Tue 8/18/15**	**21**
3.2.1 A coded report will be required for TPM status verification	1 day	Fri 7/24/15	Fri 7/24/15	
3.2.2 Programming code to activate the TPM chip	1 day	Mon 7/27/15	Mon 7/27/15	
3.2.3 Programming code to take ownership of the TPM chip	1 day	Tue 7/28/15	Tue 7/28/15	
3.2.4 Programming code to add protectors to TPM chip	1 day	Wed 7/29/15	Wed 7/29/15	
3.2.5 Programming code to upload recovery keys to FTP server	1 day	Mon 8/3/15	Mon 8/3/15	
3.2.6 Programming code to email recovery keys to service account	1 day	Wed 8/5/15	Wed 8/5/15	
3.2.7 Programming code to import rec. keys into Active Directory	1 day	Mon 8/10/15	Mon 8/10/15	
3.2.8 Programming code to import rec. keys into LANDesk/SCCM	1 day	Fri 8/14/15	Fri 8/14/15	

3.2.9 A coded report will be required for Bitlocker status	1 day	Mon 8/17/15	Mon 8/17/15	
3.2.10 Weekly Status email sent to Stakeholders	1 day	Mon 8/17/15	Mon 8/17/15	
3.2.11 All code successfully tested in lab environment	1 day	Tue 8/18/15	Tue 8/18/15	
3.3 Software Unit Testing	**6 days**	**Wed 8/19/15**	**Wed 8/26/15**	
3.3.1 Start Alpha Testing	**3 days?**	**Wed 8/19/15**	**Fri 8/21/15**	
3.3.1.1 Identify software issues	1 day	Wed 8/19/15	Wed 8/19/15	
3.3.1.2 Fix software issues	1 day	Thu 8/20/15	Thu 8/20/15	
3.3.1.3 Test Again	1 day	Thu 8/20/15	Thu 8/20/15	
3.3.1.4 Status email sent to Stakeholders	1 day	Fri 8/21/15	Fri 8/21/15	
3.3.2 Start Beta Testing	**3 days?**	**Mon 8/24/15**	**Wed 8/26/15**	**42**
3.3.2.1 Identify software issues	1 day	Mon 8/24/15	Mon 8/24/15	
3.3.2.2 Fix software issues	1 day	Mon 8/24/15	Mon 8/24/15	
3.3.3.3 Test Again	1 day	Tue 8/25/15	Tue 8/25/15	
3.3.3.4 Status email sent to Stakeholders	1 day	Tue 8/25/15	Tue 8/25/15	
3.3.3 Prepare Report for Stakeholders	1 day	Tue 8/25/15	Tue 8/25/15	
3.3.4 Stakeholder Meeting for UaT Approval	1 day	Wed 8/26/15	Wed 8/26/15	
3.3.5 Complete Unit Testing	1 day	Wed 8/26/15	Wed 8/26/15	
3.4 User Acceptance Testing	**4 days**	**Thu 8/27/15**	**Tue 9/1/15**	
3.4.1 Start Pilot testing Group 1 Ohio Site	**1 day**	**Thu 8/27/15**	**Thu 8/27/15**	
3.4.1.1 Send emails to 5 users	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.1.2 Enable TPM chips in Pilot Group	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.1.3 Deploy TPM Management to Pilot Group	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.1.4 Assess Users 1-5 in Pilot Group	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.1.5 Address issues in hardware and/or software	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.1.6 Status email sent to Stakeholders	1 day	Thu 8/27/15	Thu 8/27/15	
3.4.2 Start Pilot testing Group 1 Arizona Site	**1 day**	**Fri 8/28/15**	**Fri 8/28/15**	**56**
3.4.2.1 Send emails to 5 users	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.2.2 Enable TPM chips in Pilot Group	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.2.3 Deploy TPM Management to Pilot Group	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.2.4 Assess Users 1-5 in Pilot Group	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.2.5 Address issues in hardware and/or software	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.2.6 Status email sent to Stakeholders	1 day	Fri 8/28/15	Fri 8/28/15	
3.4.3 Start Pilot testing Group 1 Florida Site	**1 day**	**Mon 8/31/15**	**Mon 8/31/15**	**69**
3.4.3.1 Send emails to 5 users	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.3.2 Enable TPM chips in Pilot Group	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.3.3 Deploy TPM Management to Pilot Group	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.3.4 Assess Users 1-5 in Pilot Group	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.3.5 Address issues in hardware and/or software	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.3.6 Status email sent to Stakeholders	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.4 Prepare report for Stakeholder meeting	1 day	Mon 8/31/15	Mon 8/31/15	
3.4.5 Stakeholder Meeting for Approval - Go-live approval	1 day	Tue 9/1/15	Tue 9/1/15	77
3.4.6 Transfer technical documentation to IT Team Leader	1 day	Tue 9/1/15	Tue 9/1/15	77
3.5 User Acceptance Test Complete	1 day	Tue 9/1/15	Tue 9/1/15	77
4.0 Implementation	**152 days**	**Wed 9/2/15**	**Thu 3/31/16**	
4.1 Enable TPM Chips	**61 days**	**Wed 9/2/15**	**Wed 11/25/15**	
4.1.1 Enable TPM Chips at Ohio site 3,300 computers	**20 days**	**Wed 9/2/15**	**Tue 9/29/15**	
4.1.1.1 Weekly Status Report (825 computers)	5 days?	Wed 9/2/15	Tue 9/8/15	80
4.1.1.2 Weekly Status Report (825 computers)	5 days?	Wed 9/9/15	Tue 9/15/15	84
4.1.1.3 Weekly Status Report (825 computers)	5 days?	Wed 9/16/15	Tue 9/22/15	85
4.1.1.4 Weekly Status Report (825 computers)	5 days?	Wed 9/23/15	Tue 9/29/15	86
4.1.2 Enable TPM Chips at Arizona site 3,300 computers	**20 days**	**Wed 9/30/15**	**Tue 10/27/15**	
4.1.2.1 Weekly Status Report (825 computers)	5 days?	Wed 9/30/15	Tue 10/6/15	
4.1.2.2 Weekly Status Report (825 computers)	5 days?	Wed 10/7/15	Tue 10/13/15	89
4.1.2.3 Weekly Status Report (825 computers)	5 days?	Wed 10/14/15	Tue 10/20/15	90
4.1.2.4 Weekly Status Report (825 computers)	5 days?	Wed 10/21/15	Tue 10/27/15	91
4.1.3 Enable TPM Chips at Florida site 3,400 computers	**21 days**	**Wed 10/28/15**	**Wed 11/25/15**	
4.1.3.1 Weekly Status Report (850 computers)	5 days?	**Wed 10/28/15**	Tue 11/3/15	

4.1.3.2 Weekly Status Report (850 computers)	5 days?	Wed 11/4/15	Fri 11/13/15	
4.1.3.3 Weekly Status Report (850 computers)	5 days?	Wed 11/11/15	Tue 11/17/15	95
4.1.3.4 Weekly Status Report (850 computers)	5 days?	Wed 11/18/15	Tue 11/24/15	96
4.2 Create TPM Chip Master Status Report	1 day	Wed 11/25/15	Wed 11/25/15	97
4.2 Deploy TPM Management	**68 days**	**Wed 11/25/15**	**Fri 2/26/16**	
4.2.1 Deploy TPM Management at Ohio site 3,300 computers	**21 days**	**Wed 11/25/15**	**Wed 12/23/15**	
4.2.1.1 Weekly Status Report (825 computers)	5 days?	Thu 11/26/15	Wed 12/2/15	98
4.2.1.2 Weekly Status Report (825 computers)	5 days?	Thu 12/3/15	Wed 12/9/15	101
4.2.1.3 Weekly Status Report (825 computers)	5 days?	Thu 12/10/15	Wed 12/16/15	102
4.2.1.4 Weekly Status Report (825 computers)	5 days?	Thu 12/17/15	Wed 12/23/15	103
4.2.2 Deploy TPM Management at Arizona site 3,300 computers	**20 days**	**Mon 1/4/16**	**Fri 1/29/16**	
4.2.2.1 Weekly Status Report (825 computers)	5 days?	Mon 1/4/16	Fri 1/8/16	104
4.2.2.2 Weekly Status Report (825 computers)	5 days?	Mon 1/11/16	Fri 1/15/16	106
4.2.2.3 Weekly Status Report (825 computers)	5 days?	Mon 1/18/16	Fri 1/22/16	107
4.2.2.4 Weekly Status Report (825 computers)	5 days?	Mon 1/25/16	Fri 1/29/16	108
4.2.3 Deploy TPM Management at Florida site 3,400 computers	**20 days**	**Mon 2/1/16**	**Fri 2/26/16**	
4.2.3.1 Weekly Status Report (850 computers)	5 days?	Mon 2/1/16	Fri 2/5/16	109
4.2.3.2 Weekly Status Report (850 computers)	5 days?	Mon 2/8/16	Fri 2/12/16	111
4.2.3.3 Weekly Status Report (850 computers)	5 days?	Mon 2/15/16	Fri 2/19/16	112
4.2.3.4 Weekly Status Report (850 computers)	5 days?	Mon 2/22/16	Fri 2/26/16	113
4.3 Run TPM Management Status Report	1 day	Mon 2/29/16	**Mon 2/29/16**	114
5.0 Project Closure	**1 day**	**Mon 2/29/16**	**Mon 2/29/16**	
5.1 Discuss Lessons Learned/Create PowerPoint	1 day	**Mon 2/29/16**	Mon 2/29/16	115
5.2 Project Closure Report	1 day	**Mon 2/29/16**	Mon 2/29/16	117
5.3 Close out project with Stakeholders	1 day	**Mon 2/29/16**	Mon 2/29/16	118
5.4 Project Closure is Complete	1 day	**Mon 2/29/16**	Mon 2/29/16	119

9.0 Project Milestones

Milestone	Description
Development	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 deliverables will be code (1) to report the status on TPM chips, (2) code to manage the recovery keys, (3) code to report on Bitlocker compliance, and (4) code for support staff and (5) general administration (backup).
TPM Enable	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.
TPM Management	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 deliverables for this milestone is a report verifying that TPM Management was indeed successful and a user manual explaining the segments of code used in Bitlocker reporting and management.

10.0 Project Risk Assessment

While Bitlocker is already built-in to most of Microsoft's active operating systems, some problems may arise due to hardware or software failure. It is important to note, overall risks are very low because if the Bitlocker process does not work, in nearly 100% of the cases the user's computer is fine to use; they just will not have Bitlocker. For the machines that Bitlocker was not installed, refer to the following chart.

Risk	Description	Mitigation	Role
Failed TPM due to outdated BIOS	In rare cases, less than 1%, the computer's BIOS may need to be updated to enable TPM.	BIOS will be manually updated.	Local Technician
Failed TPM due to motherboard	In rare cases, less than 1%, the computer's motherboard will not have a TPM Chip.	Computer will be replaced with either a loaner machine or new computer.	Local Technician

Failed key import into Active Directory	The recovery key does not get imported into Active Directory	Try automated process again. Import key manually.	IT Specialist
Failed key import into Active Directory	The recovery key does not get imported into Active Directory	Verify computer is in a domain, and is in the proper OU. Or, enable, 'Turn on TPM backup to Active Directory Domain Services' in Local Group Policy	IT Specialist
Failed transport of key via email	The recovery key does not transport email service account	Try automated process again. Copy key from Active Directory, or FTP. Transfer manually.	IT Specialist
Failed transport of key to FTP server	The recovery key does not transport to FTP server	Try automated process again. Copy key from Active Directory or email. Transfer manually.	IT Specialist
Failed key import into LANDesk	The recovery key does not get imported into LANDesk Desktop Management Software	Reinstall LANDesk Agent. Try automated TPM Management.	Local Technician
User is receiving prompt to enter Bitlocker Recovery Password	When the user restarts their machine, they may receive a prompt to enter the Bitlocker Recovery Key	Enter the key from AD, FTP, Email, or LANDesk. Check TPM Chip status. Try automated TPM Management	IT Specialist
TPM cannot continue due to ownership error	The TPM ownership must be set before adding protectors to the TPM Chip	Take ownership of the TPM Chip, manually. Try	IT Specialist

		automated TPM Management	

11.0 Communication Plan

Due to the magnitude of the Bitlocker project, and the impact it will have on client users, the business must communicate to end-users what Bitlocker is and why encryption is important. The users must also be notified that encryption will become mandatory and enforced via company policy. The communication plan can be seen in the following table.

Title	Communication
CIO	Will communicate to the enterprise via email and in quarterly meetings. A summary of the project will be sent out to employees to prepare them for Bitlocker deployment.
IT Team Leader	Will create documentation and train IT staff on Bitlocker maintenance and administration.
IT Specialist	Will train the IT Team Leader and demonstrate Bitlocker in Stakeholder meetings. Will also be responsible for weekly status updates via email to Stakeholders.
IT Manager	Will go over the current status of the Bitlocker in bi-weekly IT meetings.

Approval and Authority to Proceed

We approve the project as described above, and authorize the team to proceed.

Print Name	Title	Sign
Daryl Smith	CFO	Daryl Smith
John Brown	CIO	John Brown
Tina Pippins	Change Management	Tina Pippins
Larry Johnson	Senior Software Developer	Larry Johnson
Dalia Stoffer	IT Manager	Dalia Stoffer
Leslie Lee	IT Team Lead	Leslie Lee

Milestone Reports

Milestone 1 Report

In Milestone 1, the primary focus of the project is on software development. The development stage includes programming the scripts necessary for Bitlocker deployment and administration, performing all unit testing, and completing user acceptance testing, or UaT. The development portion is broken down as follows:

- A script to report the current status of TPM chips
- A script to manage Bitlocker recovery key imports
- A script to report on Bitlocker compliance in the enterprise
- A script for support staff (to return a single Bitlocker recovery password)
- A script to perform the backup of Bitlocker recovery passwords

Rather than providing the code for the scripts—which can be viewed in the Bitlocker Coding section of this project—the general ideas and concepts in the development process are discussed. To reduce problems associated with the software development stage, i.e. software quality, bugs, and scope creep, it is common that a standardized, proven methodology be applied to the coding process. One of these methodologies is SDLC. SDLC, or software development life cycle, was used as a development guideline in Milestone 1. Because the design, development, and testing of the scripts were essential to reaching Milestone 1, the SDLC methodology became critical to the overall software development and testing process. Specifically, the script development included analyzing what was needed, a script design was created around those needs, the code was developed and tested, and eventually, the scripts would reach the final stage, which meant they were ready for production. The SDLC flow chart is shown in Figure 1.

■ **Figure 1 SDLC Flow Chart**

SOURCE: http://www.sdlc.ws

Once all the coded components passed the user acceptance testing stage, the key stakeholders agreed that we were ready to move to the next stage and the go-live was approved.

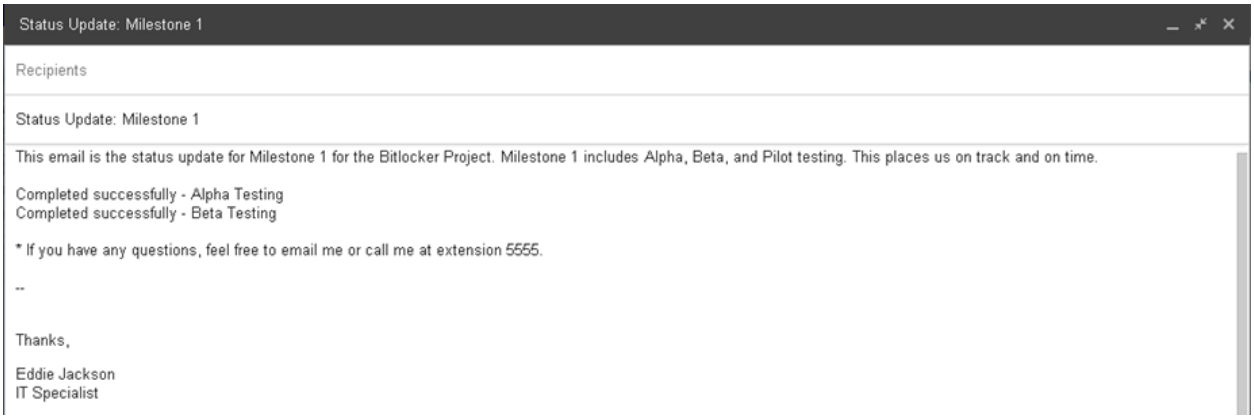
Considering each script, there were five scripts coded for the business, these were based upon business need and technical support requests. The scripts include (1) check the current status of the TPM chip, (2) TPM management, (3) Bitlocker compliance, (4) helpdesk support, and (5) backup of the Bitlocker Passwords. The basic flow and thought process behind these scripts can be seen in the following chart.

Script	Reasoning/Business Requirement
Check TPM Status	Before enabling Bitlocker, a script is required to query the current status of the chip. If off, enable chip.
TPM Management	After the TPM chip has been enabled, ownership of the TPM must be taken, protectors must be added to the TPM, and the recovery information needs to be imported into Active Directory and LANDesk.
Bitlocker Compliance	There needs to be a way to verify which workstations do and do not meet Bitlocker compliance.

Helpdesk Support	Support staff will need an easy way to retrieve a single Bitlocker password, independently of accessing Active Directory or LANDesk.
Backup	There is a business need to maintain a backup of Bitlocker passwords for disaster recovery. This should be in form of a simple text file.

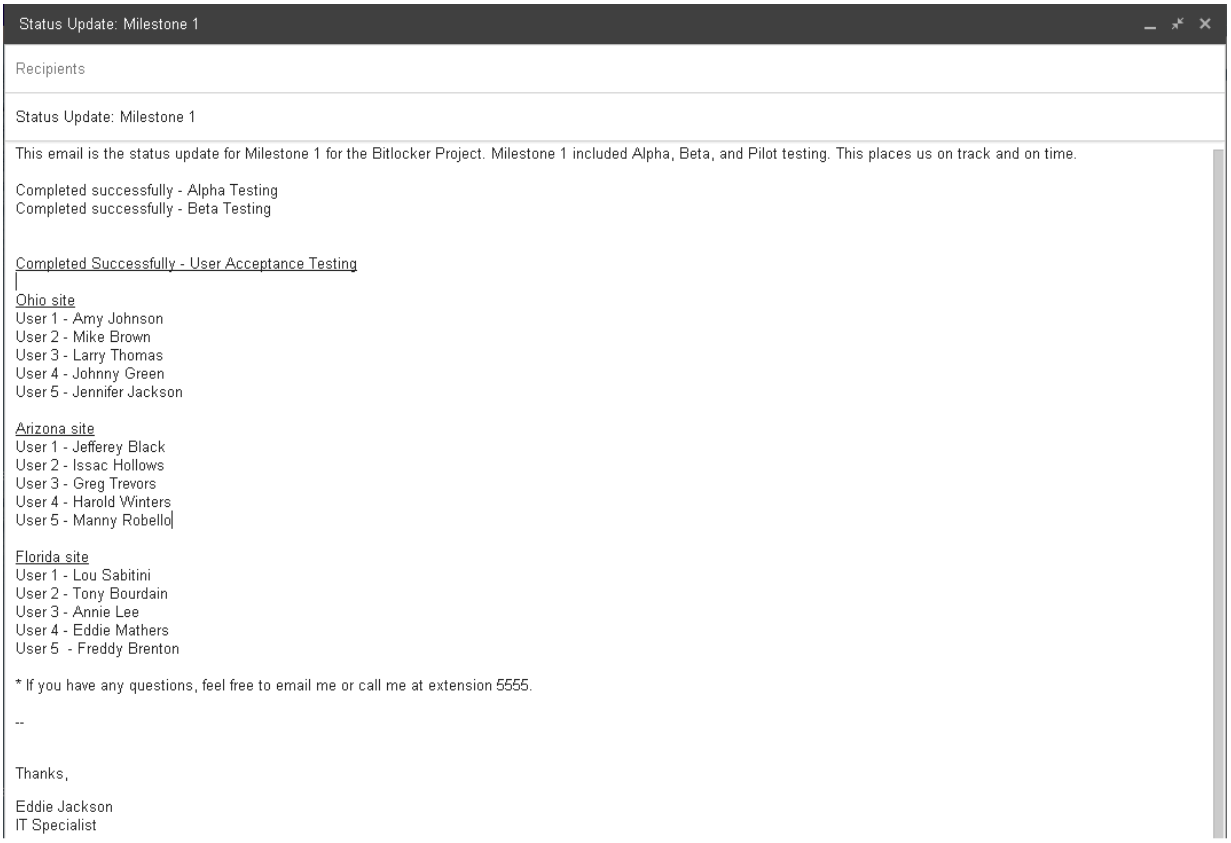
Each of the scripts were completed on time and within budget. As stated, the SDLC methodology was used to guide the development and testing process. The stages of programming went through alpha, beta, and pilot phases. In the alpha and beta phases, software issues were identified, they were fixed, and each script was tested again. At the end of alpha and beta development phases, a status email was sent to the stakeholders. The email is shown in Figure 2.

■ Figure 2 Status Update Email Sent to Stakeholders



In the pilot phase, which was officially marked the UaT stage, five test users were selected from each site—Ohio, Arizona, and Florida. These users received the TPM Status and TPM Management scripts (via LANDesk) without any issues. Once all the users had been successfully tested, a status email was sent to the stakeholders. This email can be seen in Figure 3.

■ Figure 3 Status Update Email Sent to Stakeholders



Additionally, the compliance, helpdesk support, and backup scripts were evaluated for proper operation. All scripts worked as intended, consequently leading to the go-live approval from the stakeholders. Lastly, the technical documentation was transferred to the IT Team Leader to be reviewed, updated, and disseminated accordingly. Milestone 1 is now considered complete.

** See Technical Documentation for code and screenshots on page 34.*

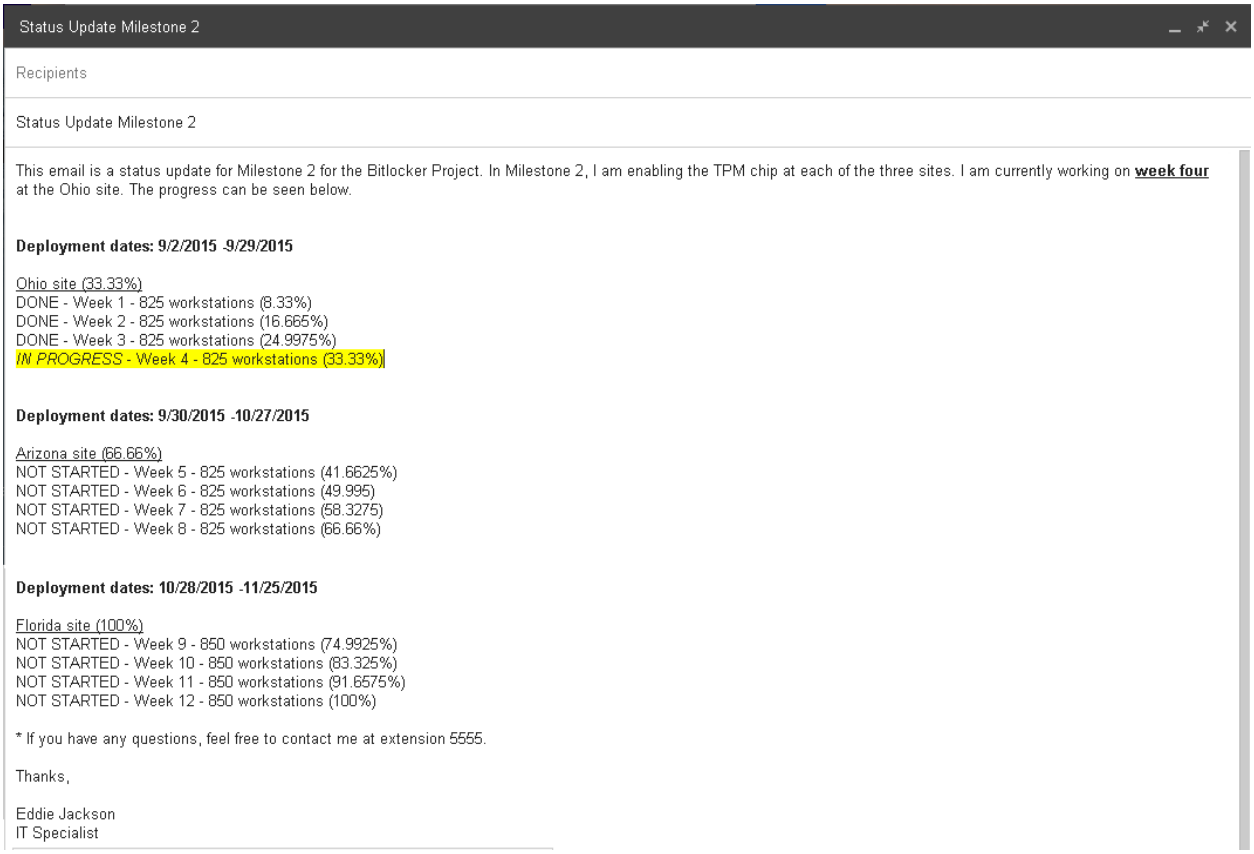
Milestone 2 Report

In Milestone 2, the main objective was to enable TPM chips on all workstations at all three sites—Ohio, Arizona, and Florida. This milestone was considered more difficult than Milestone 1, in that it required coordinated efforts with local site technicians, and had the greatest potential for hardware and software problems. Because the enabling of the TPM chips required attention to detail, one site was addressed at a time. Site 1, the Ohio site, had 3,300 computers that needed the TPM chips enabled. As the IT Specialist, and the leader of the project, I was responsible for enabling the TPM chips using the TPM script I created in Milestone 1. Rather than just deploying to all 3,300 computers at once, I setup a deployment schedule of 825 workstations a week, for four weeks. This way, it would be easier to coordinate hardware and software support issues with the local technicians (if problems came up). The Ohio schedule for the TPM status script can be seen in the following chart (note, each site schedule was similar to this schedule):

Workstation Count	Start Date	End Date
825	Wed 9/2/15	Tue 9/8/15
825	Wed 9/9/15	Tue 9/15/15
825	Wed 9/16/15	Tue 9/22/15
825	Wed 9/23/15	Tue 9/29/15

At the end of each deployment cycle, a status email was sent to the stakeholders, updating them on the progress of the project thus far (a total of four emails was sent for the Ohio site). A sample email with each site name can be seen in Figure 4. This email tracks the progress of the overall project using percentages, the percentage each deployment cycle accounts for within at each site, and the exact point in the deployment process is highlighted.

■ **Figure 4 Status Update Email Sent to Stakeholders (1 of 12)**



Status Update Milestone 2

Recipients

Status Update Milestone 2

This email is a status update for Milestone 2 for the Bitlocker Project. In Milestone 2, I am enabling the TPM chip at each of the three sites. I am currently working on **week four** at the Ohio site. The progress can be seen below.

Deployment dates: 9/2/2015 -9/29/2015

Ohio site (33.33%)
DONE - Week 1 - 825 workstations (8.33%)
DONE - Week 2 - 825 workstations (16.665%)
DONE - Week 3 - 825 workstations (24.9975%)
IN PROGRESS - Week 4 - 825 workstations (33.33%)

Deployment dates: 9/30/2015 -10/27/2015

Arizona site (66.66%)
NOT STARTED - Week 5 - 825 workstations (41.6625%)
NOT STARTED - Week 6 - 825 workstations (49.995)
NOT STARTED - Week 7 - 825 workstations (58.3275)
NOT STARTED - Week 8 - 825 workstations (66.66%)

Deployment dates: 10/28/2015 -11/25/2015

Florida site (100%)
NOT STARTED - Week 9 - 850 workstations (74.9925%)
NOT STARTED - Week 10 - 850 workstations (83.325%)
NOT STARTED - Week 11 - 850 workstations (91.6575%)
NOT STARTED - Week 12 - 850 workstations (100%)

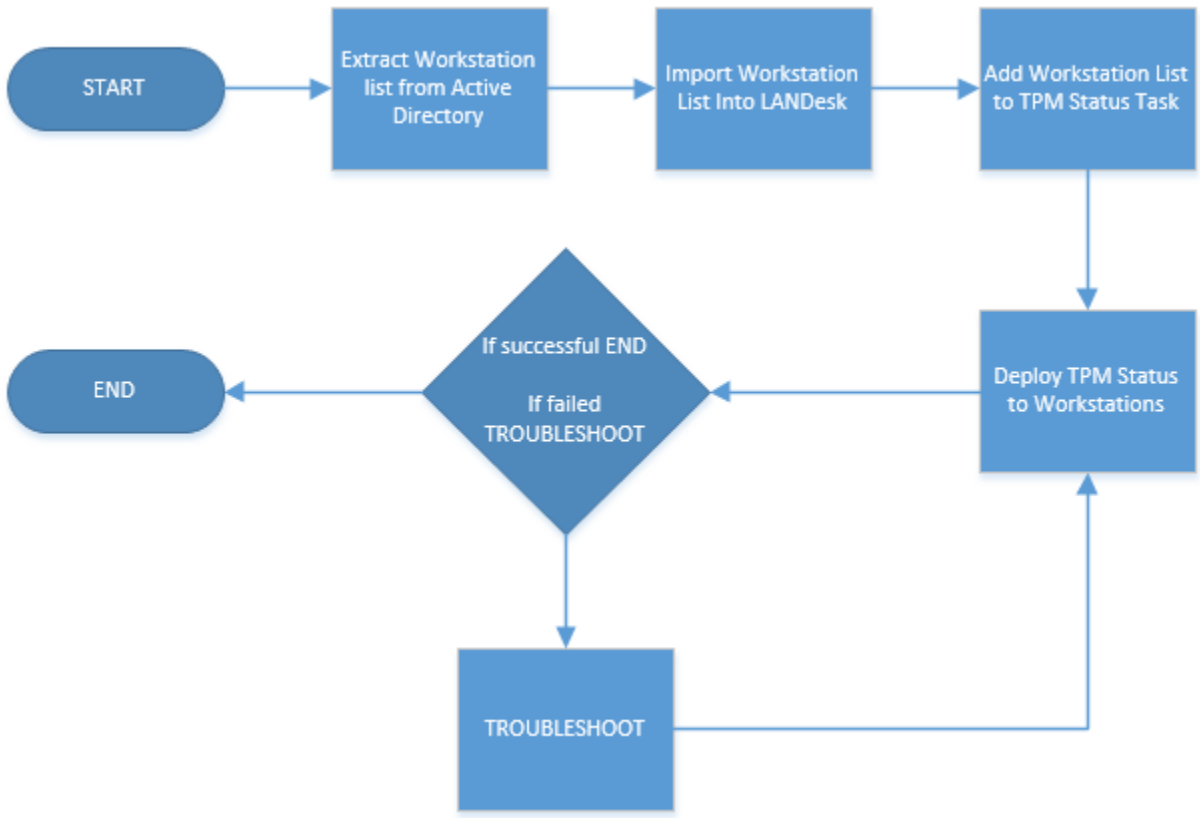
* If you have any questions, feel free to contact me at extension 5555.

Thanks,

Eddie Jackson
IT Specialist

After the Ohio site had all the TPM chips enabled, the Arizona and Florida sites followed (a total of twelve status update emails were sent). There were only minor issues associated with Milestone 2, all of which were anticipated for in the project's risk assessment stage. The two most common problems were broken TPM chips or non-working TPM chips, and misconfigured BIOS settings. In the case of a broken TPM chip, the computer was swapped out by the local site technician. There were only five computers that had to be replaced, and five computers that required hands-on support due to BIOS configuration problems. The exact process for reporting on and enabling the TPM chip is depicted in the flow chart in Figure 5.

■ **Figure 5 Flow Chart for Deploying TPM Status**



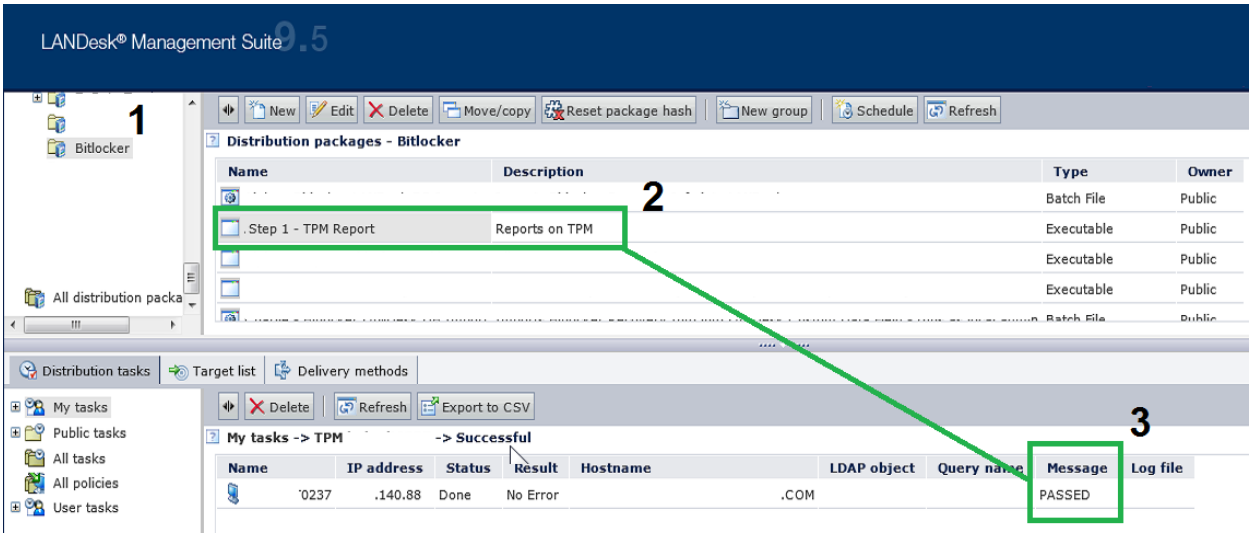
I also compiled the list of computers that had problems during Milestone 2.

Site Name	Problem	Old Computer Serial#	New Computer Serial #
Ohio	BIOS config	TQ9164	N/A
Ohio	Broken TPM	AJH2381	MQ5239
Arizona	BIOS config	JU9823	N/A
Arizona	Broken TPM	ZB3321	IU3103
Arizona	Broken TPM	WE0016	UU1636
Arizona	BIOS config	BY7153	N/A
Florida	BIOS config	MQ0138	N/A
Florida	Broken TPM	PY7714	RQ1874
Florida	Broken TPM	ZY2273	QR0125

To keep track of the status of TPM chips—which were either *enabled* or *disabled*—a script was

deployed from LANDesk. This script determined whether the TPM chip was enabled or disabled, and returned a PASSED or FAILED message back to LANDesk. If the TPM was disabled, the script attempted to enable the chip and returned FAILED back to LANDesk. If the chip was enabled, a PASSED message was returned to LANDesk. A successful message can be seen in Figure 6.

■ **Figure 6 TPM Status Check in LANDesk**



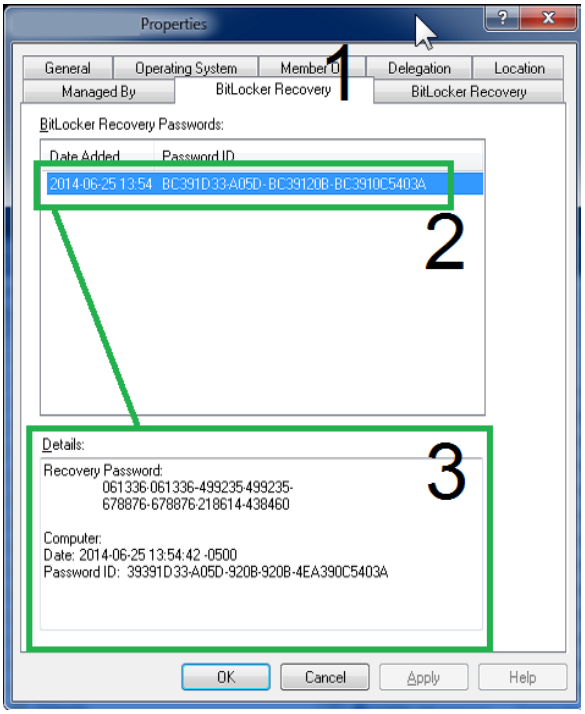
Now that all TPM chips are reporting a status of PASSED, Milestone 2 is considered complete.

** To see the scripting used to report on TPM status, see Technical Documentation on page 35.*

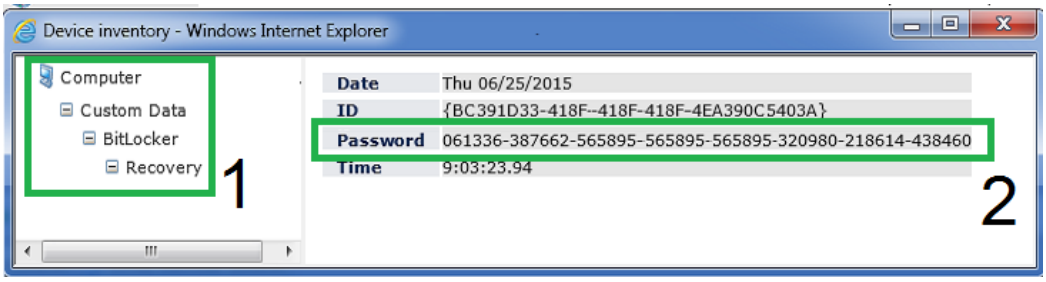
Milestone 3 Report

In Milestone 3, the objective was to acquire the Bitlocker recovery information. Obtaining and storing the Bitlocker passwords are critical to maintaining a Bitlocker solution. If the recovery information is not stored, there is the risk that data can become inaccessible. There is the scenario where the 48-digit recovery password may be required to access data. For example, if the hard drive needs to removed, the password will be required. Likewise, if the BIOS settings change on a workstation, the recovery password will need to be entered. Thus, to address the storage and access of Bitlocker recovery passwords, the passwords were stored in current server systems that Company X owns and operates. An important part of Milestone 3 was importing Bitlocker recovery passwords into Active Directory and LANDesk, which is to be used for recovery purposes. These imports—with the Bitlocker recovery information—can be observed in Figure 7 and Figure 8.

■ **Figure 7 Successful Active Directory Import**



■ Figure 8 Successful LANDesk Import



To maintain open lines of communication with the project stakeholders throughout the deployment of the TPM management script, a status update email was sent at the end of each week. The email contains the overall percentage each site accounts for in Milestone 3, the percentage each deployment cycle accounts for at each site, and the exact point in the deployment process is highlighted. The status email can be seen in Figure 9.

■ Figure 9 Status Update Email Sent to Stakeholders (1 of 12)

Status Update Milestone 3

Recipients

Status Update Milestone 3

This email is a status update for Milestone 3 for the Bitlocker Project. In Milestone 3, I am deploying the TPM Management script to all workstations at each of the three sites. This script will import the Bitlocker recovery information into Active Directory and LANDesk. I am currently working on **week one** at the Ohio site. The progress can be seen below.

Deployment dates: 11/25/15 - 12/23/15

Ohio site (33.33%)
IN PROGRESS - Week 1 - 825 workstations (8.33%)
NOT STARTED - 825 workstations (16.665%)
NOT STARTED - 825 workstations (24.9975%)
NOT STARTED - Week 4 - 825 workstations (33.33%)

Deployment dates: 1/4/16 - 1/29/16

Arizona site (66.66%)
NOT STARTED - Week 5 - 825 workstations (41.6625%)
NOT STARTED - Week 6 - 825 workstations (49.995)
NOT STARTED - Week 7 - 825 workstations (58.3275)
NOT STARTED - Week 8 - 825 workstations (66.66%)

Deployment dates: 2/1/16 - Fri 2/26/16

Florida site (100%)
NOT STARTED - Week 9 - 850 workstations (74.9925%)
NOT STARTED - Week 10 - 850 workstations (83.325%)
NOT STARTED - Week 11 - 850 workstations (91.6575%)
NOT STARTED - Week 12 - 850 workstations (100%)

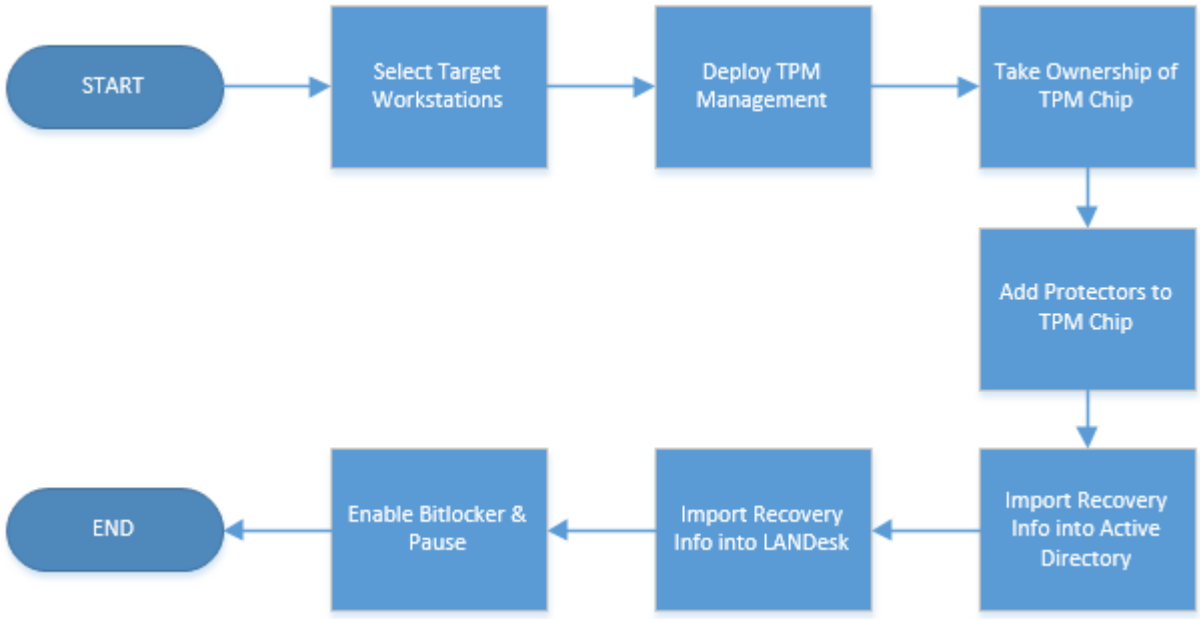
* If you have any questions, feel free to contact me at extension 5555.

Thanks,

Eddie Jackson
IT Specialist

To understand more about the TPM Management script, a flow chart has been prepared which outlines how the script is processed. The flow of the script is illustrated in Figure 10.

■ **Figure 10 Flow Chart of TPM Management**



The operational breakdown of the entire process is as follows:

- I select target machines in LANDesk. Example: 825 workstations for the Ohio site
- I deploy the TPM Management script from LANDesk to target machines
- From LANDesk, I monitor the progress
- On the workstation, the TPM ownership is taken using manage-bde
- On the workstation, protectors are added to the TPM using manage-bde
- On the workstation, the recovery password is imported into Active Directory
- On the workstation, the recovery password is imported into LANDesk
- On the workstation, Bitlocker encryption is enabled
- On the workstation, Bitlocker encryption is immediately paused

After reviewing the breakdown, it can be observed that the last step—*Bitlocker encryption is immediately paused*—stops Bitlocker from encrypting the hard drive. This is done by design. Once the drive encryption process has been started, it is not practical to use the workstation, as Bitlocker is resource intensive and the speed of the computer is negatively impacted; encrypting the hard drive may take anywhere from two to four hours, depending on the size of the hard drive. It is recommended that encryption be paused, and then started at the end of day, so that the hard drive may be encrypted overnight. Using this approach, productivity will be least affected, and the user experience will remain a positive one throughout the deployment of Bitlocker.

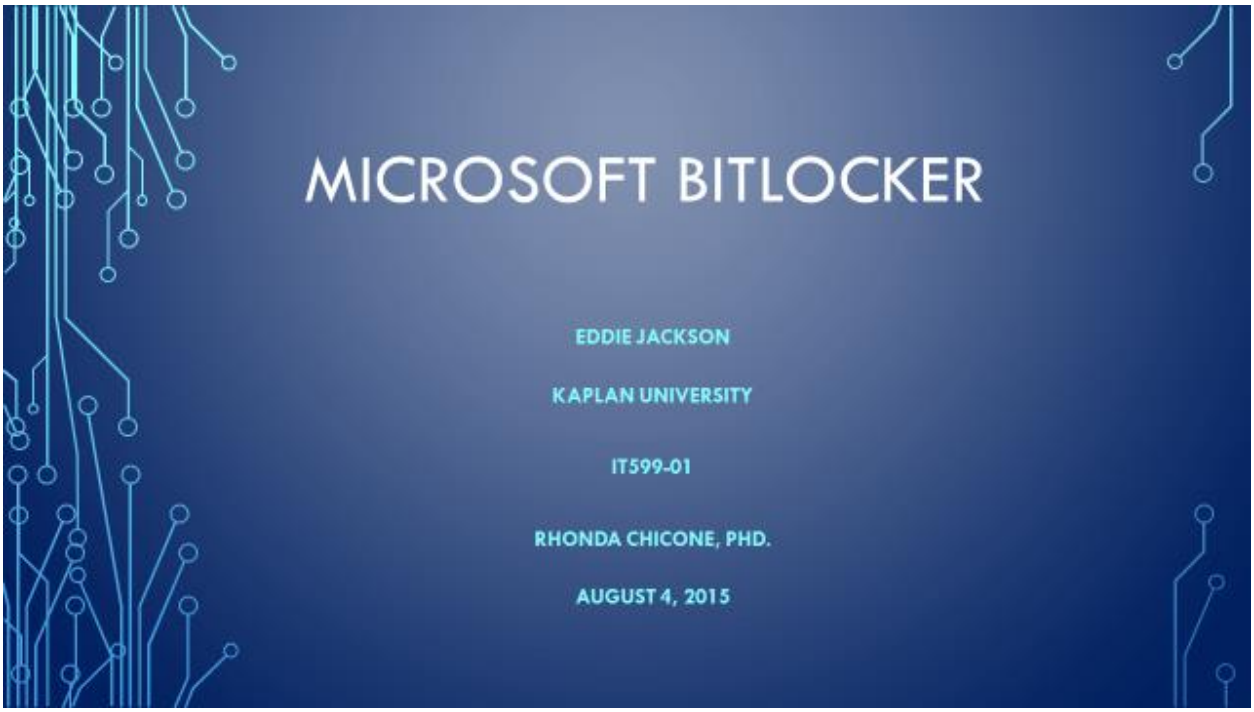
* I have also added two videos for review.

The Milestones	Milestone 3 explained
	

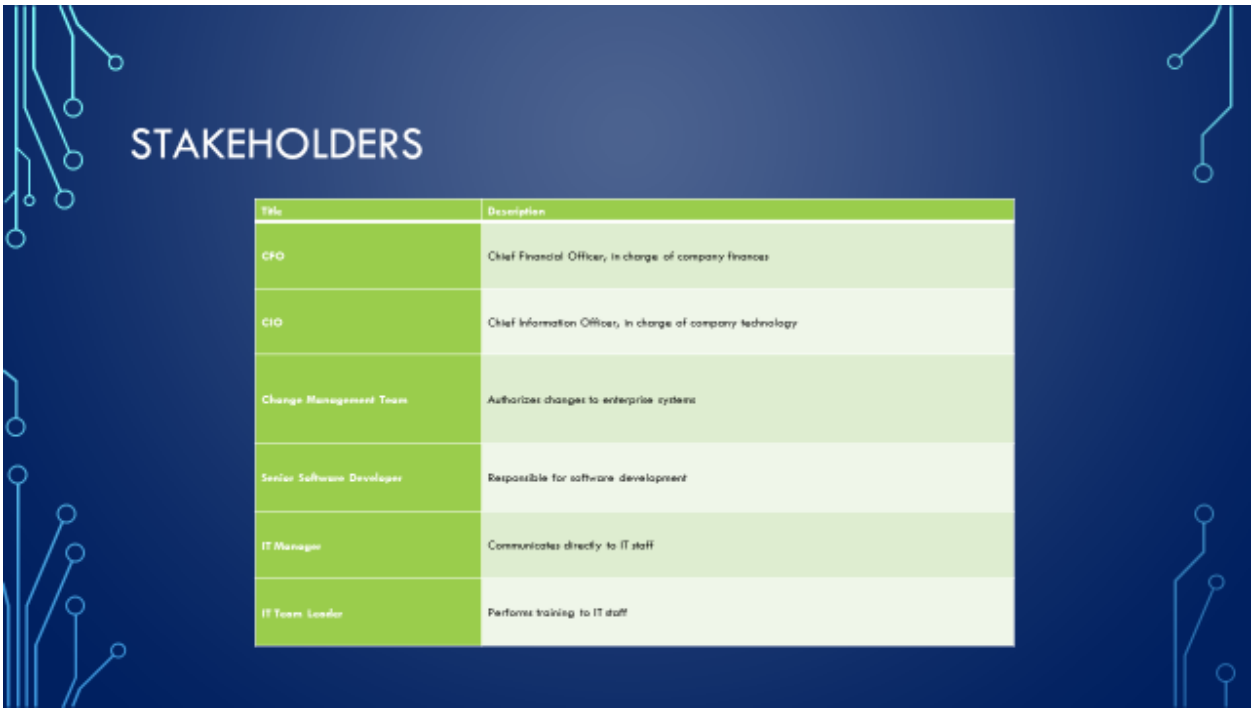
Videos were sent to the professor and discussed in class.

Bitlocker Presentation

This is the presentation given at the end of Bitlocker project. Please note, the actual PowerPoint was narrated and contains audio on each slide.




WHY DIDN'T WE PURCHASE A SOLUTION?
• MBAM/MDOP
- $10 per seat for Microsoft Management Solution
- $50-$150 per seat for a 3rd party solution
- Requires new server systems
VS.
• In-house Solution
- Less than a $1 per seat, mostly due to administrative costs
- Use existing servers
- Lower TCO
- Higher ROI


STAKEHOLDERS
Title
Description
CFO
Chief Financial Officer, in charge of company finances
CIO
Chief Information Officer, in charge of company technology
Change Management Team
Authorizes changes to enterprise systems
Senior Software Developer
Responsible for software development
IT Manager
Communicates directly to IT staff
IT Team Leader
Performs training to IT staff

BUDGET

Budget Item	Description	Cost
Code development	Reporting and TPM Management solutions must be developed in-house	$3,500
Training	Documentation must be created and staff trained	$2,000
20 x Computers	Twenty computers have been allocated to replace non-working TPM chips: Each computer costs $1,000.	$20,000
Technical Support	$25 per hour, with a breakdown of 25 hours * $25 * 3 sites	$1,875
Miscellaneous Costs	Costs include support for Active Directory, Network computers, and the Bitlocker solution.	$2,625
	Total cost	$30,000

THE IN-HOUSE SOLUTION

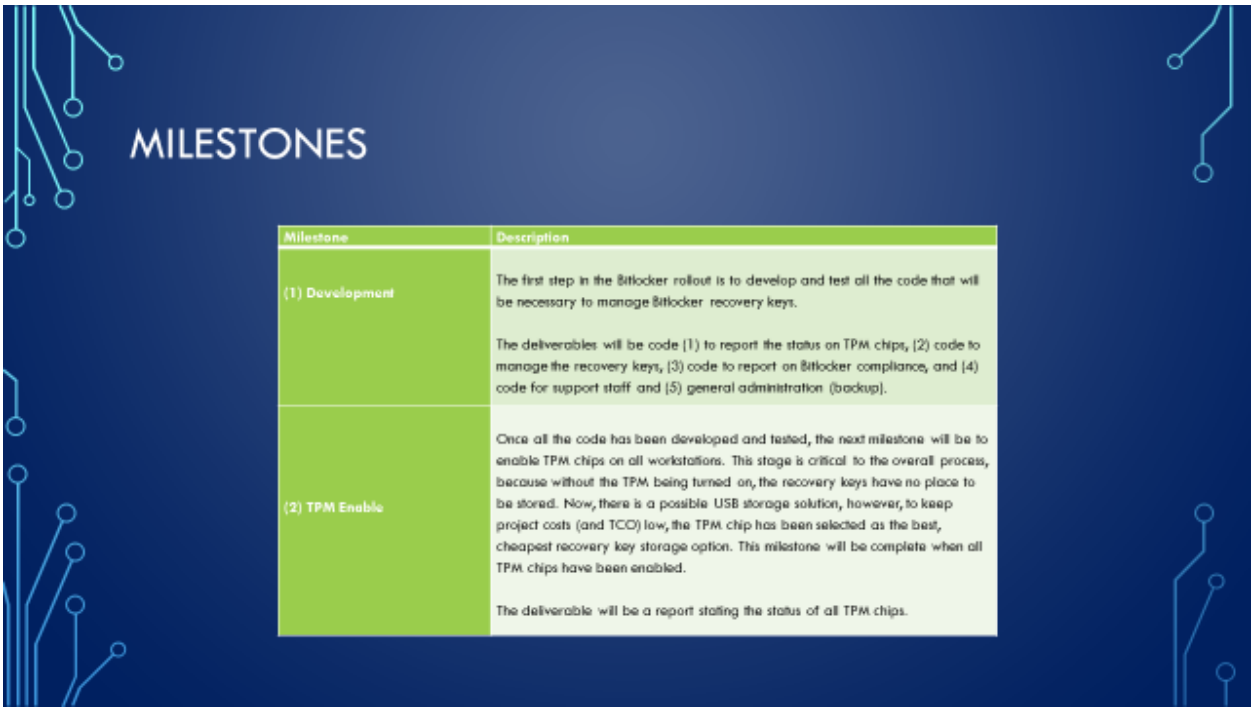
- Developing low cost, easy-to-use tools
- These tools include monitoring, management, and compliance solutions
- Specifically, the tools are to be used by
  - admins
  - technicians
  - helpdesk
  - compliance

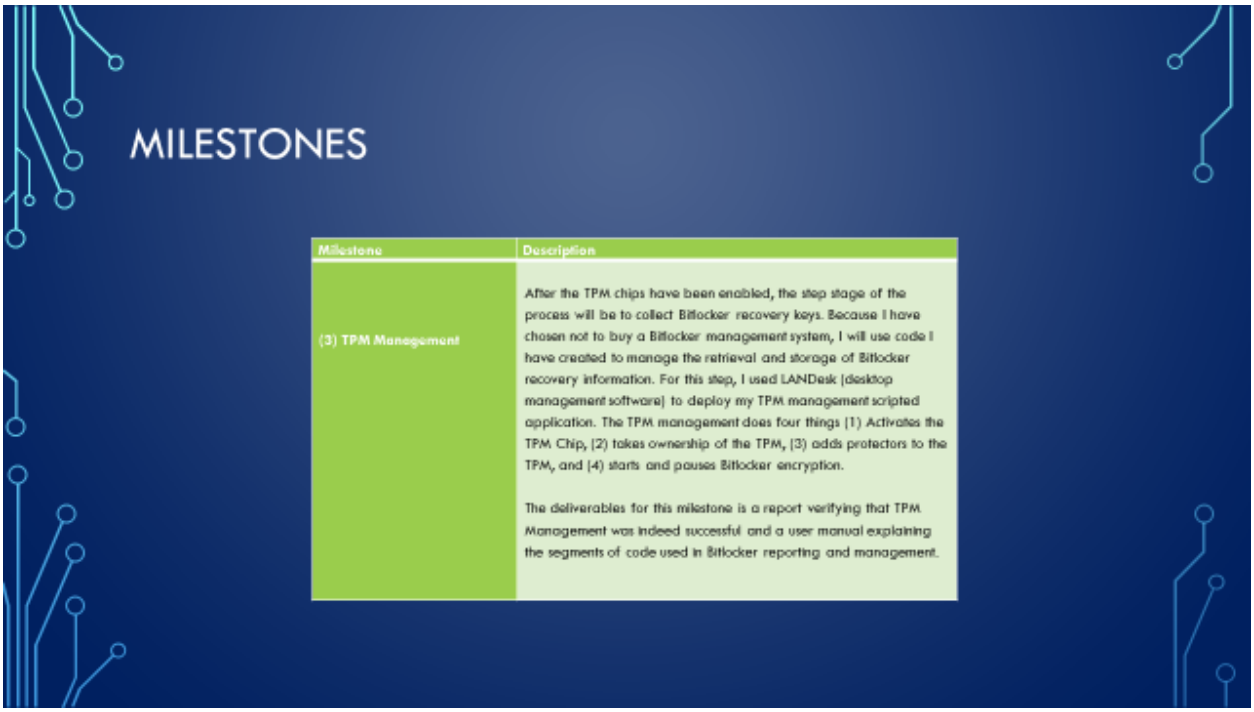
RISK ANALYSIS

Risk	Description	Mitigation	Role
Failed transport of key via email	The recovery key does not transport email service account	Try automated process again. Copy key from Active Directory, or FTP. Transfer manually.	IT Specialist
Failed transport of key to FTP server	The recovery key does not transport to FTP server	Try automated process again. Copy key from Active Directory or email. Transfer manually.	IT Specialist
Failed key import into LANDesk	The recovery key does not get imported into LANDesk Desktop Management Software	Reinstall LANDesk Agent. Try automated TPM Management.	Local Technician
User is receiving prompt to enter Bitlocker Recovery Password	When the user restarts their machine, they may receive a prompt to enter the Bitlocker Recovery Key	Enter the key from AD, FTP, Email, or LANDesk. Check TPM Chip status. Try automated TPM Management	IT Specialist

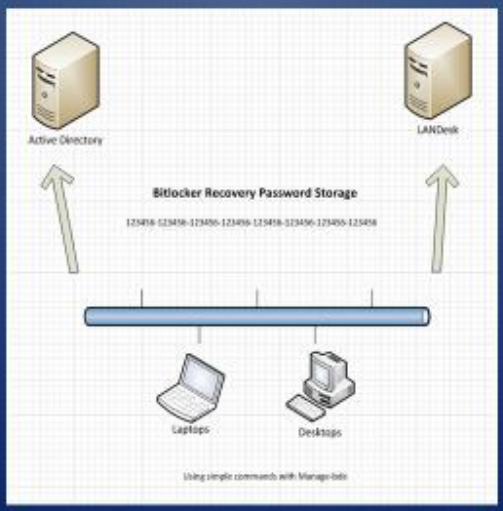
RISK ANALYSIS

Risk	Description	Mitigation	Role
Failed TPM due to outdated BIOS	In rare cases, less than 1%, the computer's BIOS may need to be updated to enable TPM.	BIOS will be manually updated.	Local Technician
Failed TPM due to motherboard	In rare cases, less than 1%, the computer's motherboard will not have a TPM Chip.	Computer will be replaced with either a loaner machine or new computer.	Local Technician
Failed key import into Active Directory	The recovery key does not get imported into Active Directory	Try automated process again. Import key manually.	IT Specialist
Failed key import into Active Directory	The recovery key does not get imported into Active Directory	Verify computer is in a domain, and is in the proper OU. Or, enable, 'Turn on TPM backup to Active Directory Domain Services' in Local Group Policy	IT Specialist

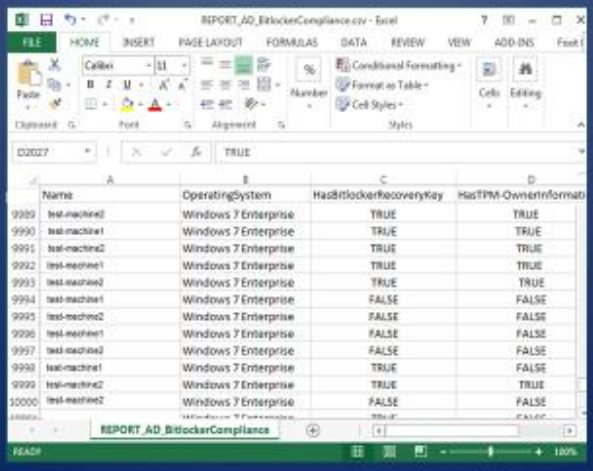

MILESTONES
Milestone
Description
(1) Development
The first step in the Bitlocker rollout is to develop and test all the code that will be necessary to manage Bitlocker recovery keys.
The deliverables will be code (1) to report the status on TPM chips, (2) code to manage the recovery keys, (3) code to report on Bitlocker compliance, and (4) code for support staff and (5) general administration (backup).
(2) TPM Enable
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.

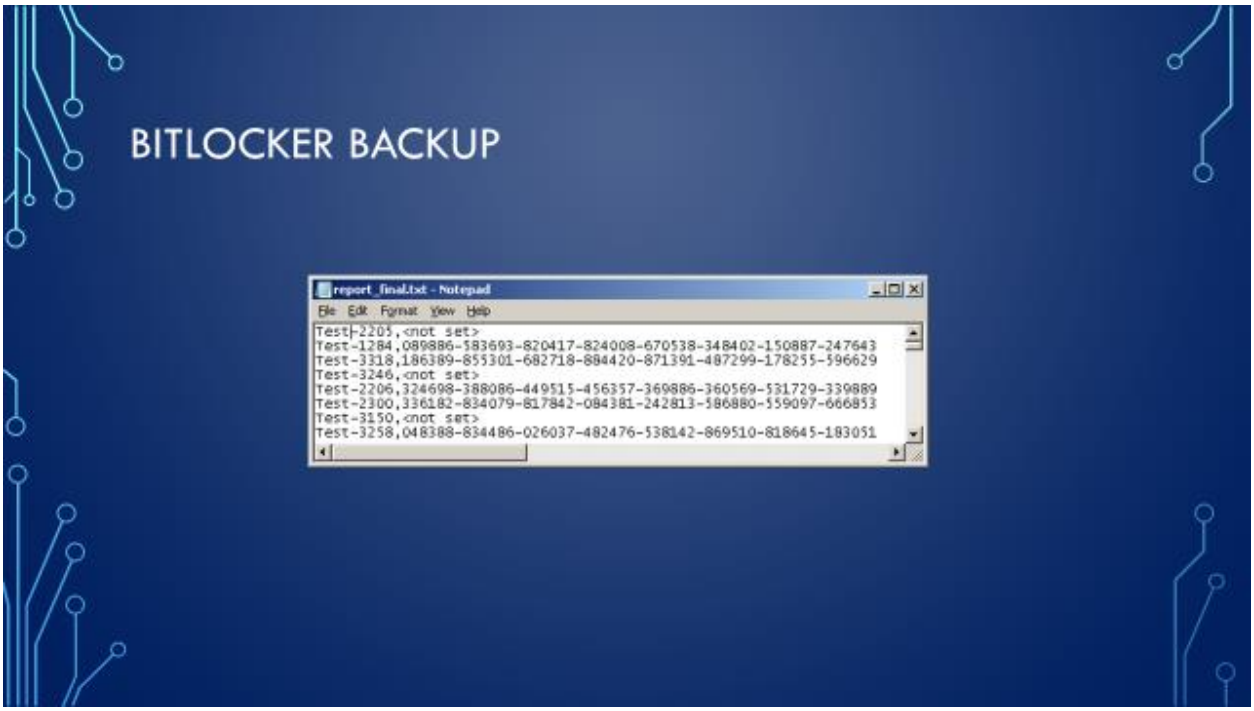

MILESTONES
Milestone
Description
(3) TPM Management
After the TPM chips have been enabled, the step stage of the process will be to collect Bitlocker recovery keys. Because I have chosen not to buy a Bitlocker management system, I will use code I have created to manage the retrieval and storage of Bitlocker recovery information. For this step, I used 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 deliverables for this milestone is a report verifying that TPM Management was indeed successful and a user manual explaining the segments of code used in Bitlocker reporting and management.

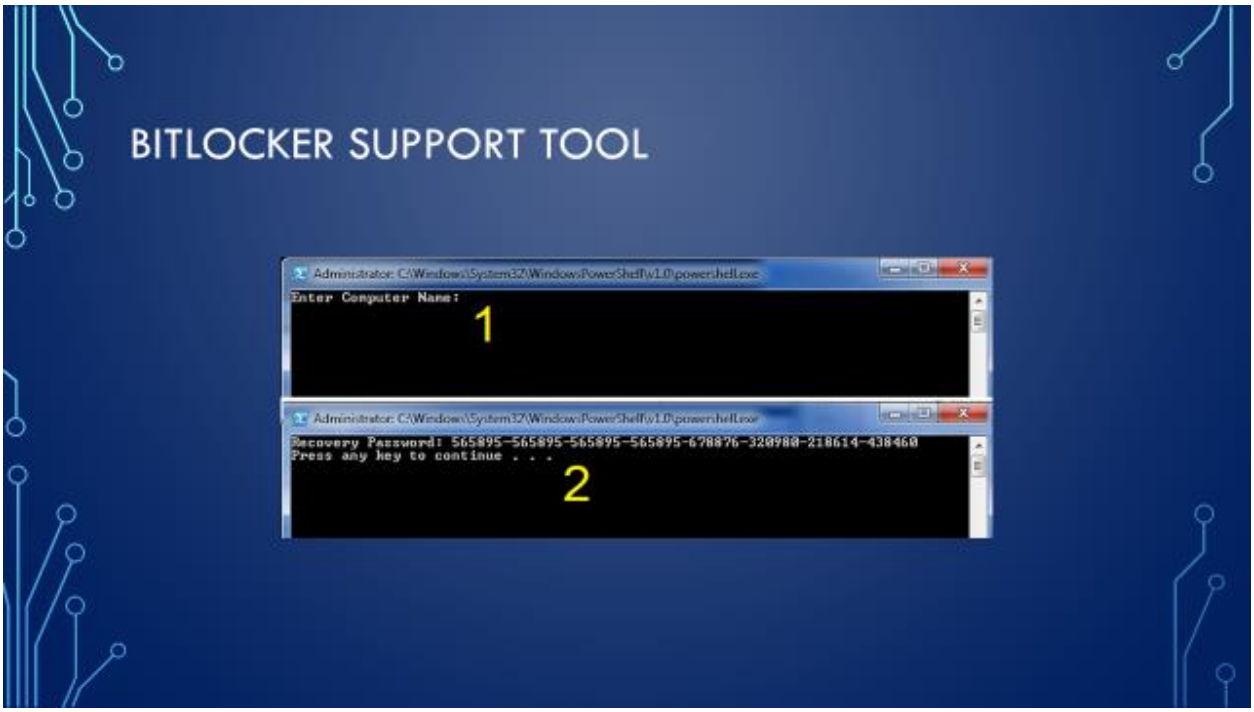
BITLOCKER PASSWORD STORAGE



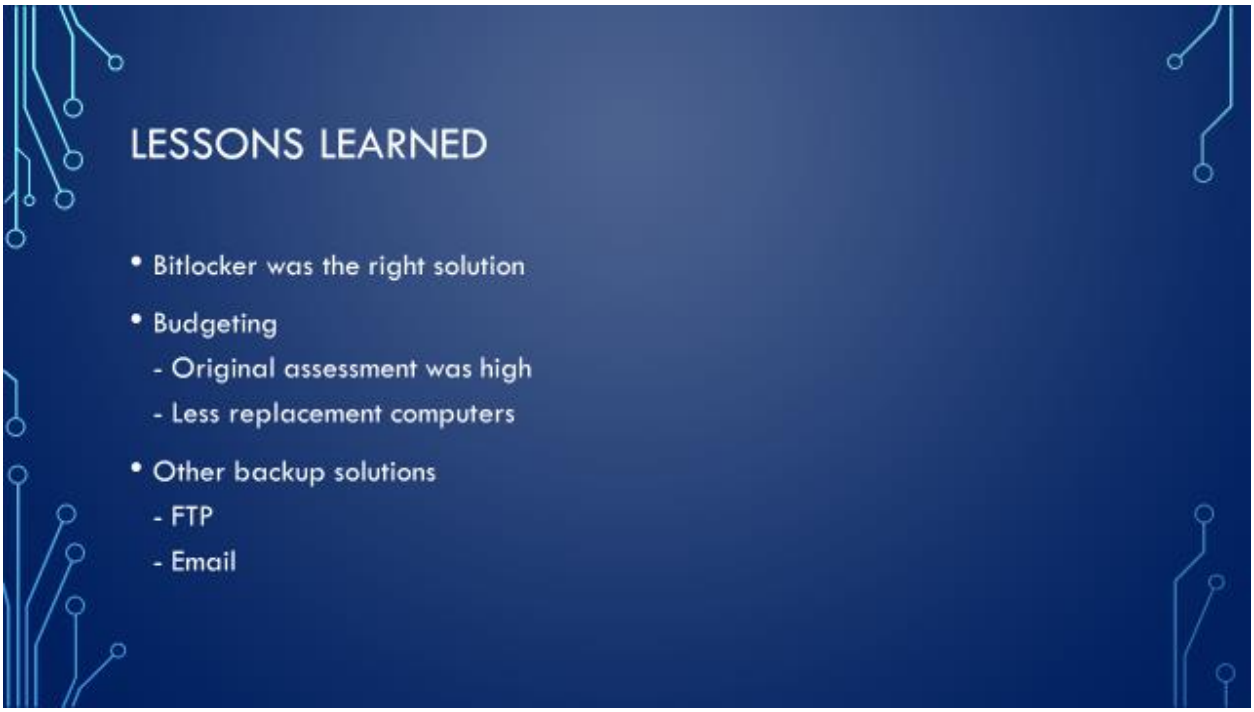
BITLOCKER COMPLIANCE




BITLOCKER BACKUP
report_final.txt - Notepad
File Edit Format View Help
Test-2205,<not set>
Test-1284,089886-583693-820417-824008-670538-348402-150887-247643
Test-3318,186389-855301-682718-884420-871391-487299-178255-596629
Test-3246,<not set>
Test-2206,324698-388086-449515-456357-369886-360569-531729-339889
Test-2300,336182-834079-817842-084381-242813-586880-559097-666853
Test-3150,<not set>
Test-3258,048388-834486-026037-482476-538142-869510-818645-183051


BITLOCKER SUPPORT TOOL
Enter Computer Name:
1
Recovery Password: 565895-565895-565895-565895-678876-320980-218614-438460
Press any key to continue . . .
2


END GOALS MET
• Enabled TPM Chips
• Imported the recovery information
• Fulfilled the compliance need
• Created a disaster recovery backup
• Created tool for support staff


LESSONS LEARNED
• Bitlocker was the right solution
• Budgeting
- Original assessment was high
- Less replacement computers
• Other backup solutions
- FTP
- Email

* Videos have also been prepared detailing the project, the challenges, and the implemented solutions.

Technical Documentation

Preface

This documentation is setup in the form of Problem and Solution; the Problem being a Bitlocker reporting or maintenance need, and the Solution being a script that has been developed and implemented in a production environment. Because this particular implementation of Bitlocker is not utilizing MBAM, MDOP, SQL, or any other reporting/compliance solution, customized scripts were created to fulfil the needs of Company X. The business requirements include reporting the current status of the TPM chip, enabling the TPM chip, importing critical Bitlocker recovery information into Active Directory and LANDesk, and designing other miscellaneous support tools. The primary reason these scripts were engineered were to avoid current and future costs related to owning and operating a Microsoft-based or third party Bitlocker management solution, which would include licensing and software support fees. Although every effort has been made to ensure the reliability and efficiency of the scripts, all the code should be tested in a lab before being introduced into a production environment. The documentation includes scripts coded in PowerShell, batch shell, and VBScript. It is also important to note, all the scripts where compiled into secure EXE files before entering a live environment.

Bitlocker Coding

Check TPM Status

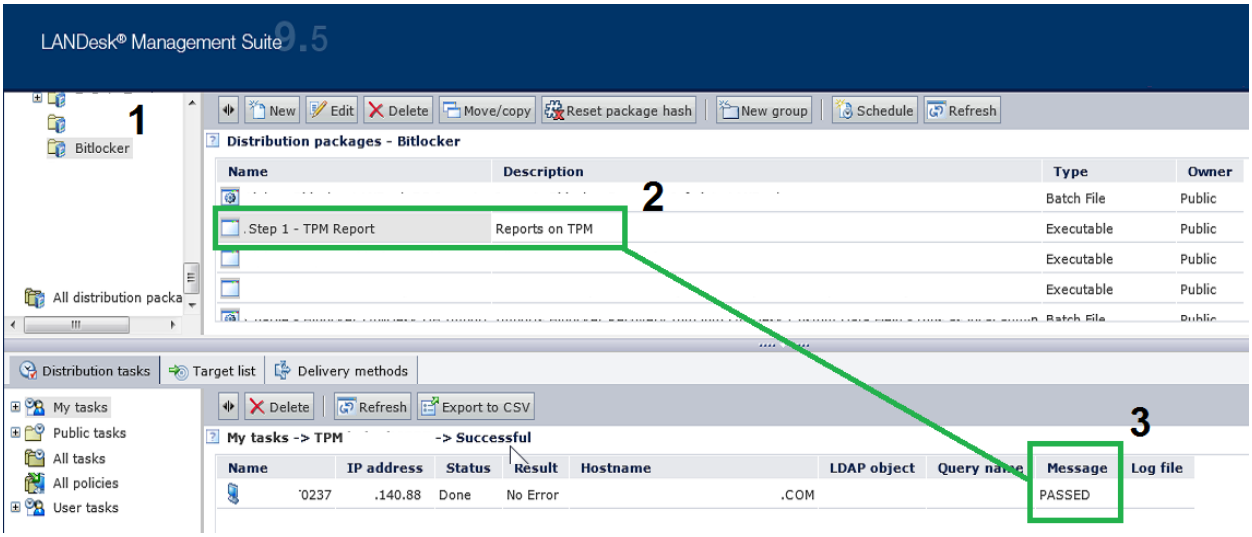
Problem

Before starting the Bitlocker encryption process, a workstation must first have a working and enabled TPM chip. The TPM chip is used to securely store Bitlocker recovery information. So, the question is: How can the status of the TPM be checked to verify that it is indeed on? Also, if the TPM status is disabled, steps should be taken to attempt to enable the chip, as well as a 'FAILED' status should be reported to LANDesk. If the chip is enabled, a 'PASSED' status should be reported to LANDesk.

Solution

Create a batch script that uses *manage-bde.exe* to output the status of Bitlocker; that output will be scanned for specific a specific keyword: 'not' (as in TPM *not* found). If 'not' is found, the script uses the HP BIOS Utility *BIOSConfigUtility.exe* to set a BIOS password, which is required by some computer models to enable the TPM Chip. Next, the script runs the Microsoft VBScript *EnableBitlocker.vbs* to enable the TPM. The 'FAILED' status of the TPM is sent back to LANDesk and is also stamped in the registry. Now, if 'not' cannot be found, it is assumed that the TPM is enabled. Consequently, a 'PASSED' status will be returned to LANDesk as well as being stamped in the registry. This batch script was created to run from LANDesk *before* continuing to the Bitlocker recovery key import stage. By first ensuring that TPM chips are enabled, the import process will go much smoother. A TPM Status Check can be observed in Figure 11.

■ **Figure 11 TPM Status Check in LANDesk**



The Script

```
@ECHO ON
:: CHECK TPM STATUS - IF TPM 'NOT' FOUND IS RETURNED, GOTO FAILED ELSE GOTO PASSED
C:\windows\system32\manage-bde -tpm -TurnOn | findstr /f "not" && GOTO :FAILED
GOTO :PASSED

:FAILED
CLS
COLOR 0c
ECHO ERROR: A compatible Trusted Platform Module (TPM) was not detected.
ECHO.

:: SEND FAILED TO LANDESK
IF EXIST "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files
(x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg="FAILED"
IF EXIST "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program
Files\LANDesk\LDClient\SDCLIENT.EXE" /msg="FAILED"
ECHO %DATE% %TIME% Sent FAILED message to LANDesk>>C:\Bitlocker\log.dat
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM_Status /d FAILED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "%DATE% %TIME%" /t REG_SZ
/f


:: IF TPM ENABLER IS FOUND (A SCRIPT FROM MICROSOFT), RUN SCRIPT WITH 'ON' OPTION AND SET
BIOS PASSWORD USING SETPW.EXE

:: WIN7
IF EXIST "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\\enablebitlocker.vbs" (

:: HP BIOS CONFIGURATION UTILITY - SET BIOS PASSWORD - REQUIRED TO ENABLE SOME TPM CHIPS
"C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\BIOSConfigUtility.exe" /nspwdfile:""C:\Program
Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\password.bin"

:: ENABLE TPM
```

```
"C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" /on:tpm
/l:c:\setup\bitlocker.log
)

:: XP
IF EXIST "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" (

:: SET BIOS PASSWORD - REQUIRED TO ENABLE SOME TPM CHIPS
"C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\BIOSConfigUtility.exe" /nspwdfile:""C:\Program
Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\password.bin"

:: ENABLE TPM
"C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\enablebitlocker.vbs" /on:tpm /l:c:\setup\bitlocker.log
)

:: LAUNCH RESTART COMPUTER PROMPT - SIMPLE EMPTY REBOOT HTA
IF EXIST "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta" (
start "" "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta"
)
IF EXIST "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta" (
start "" "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\RESTART.hta"
)
EXIT /B 0

:PASSED

:: SEND PASSED TO LANDESK
IF EXIST "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files
(x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
IF EXIST "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program
Files\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
ECHO %DATE% %TIME% Sent PASSED message to LANDesk>>C:\Bitlocker\log.dat

:: WRITE PASSED STATUS TO REGISTRY
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM_Status /d PASSED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "%DATE% %TIME%" /t REG_SZ
/f
EXIT /B 0
```

* PowerShell and VBScripts were also coded, however due to their length in routines, were not selected.

TPM Management

Problem

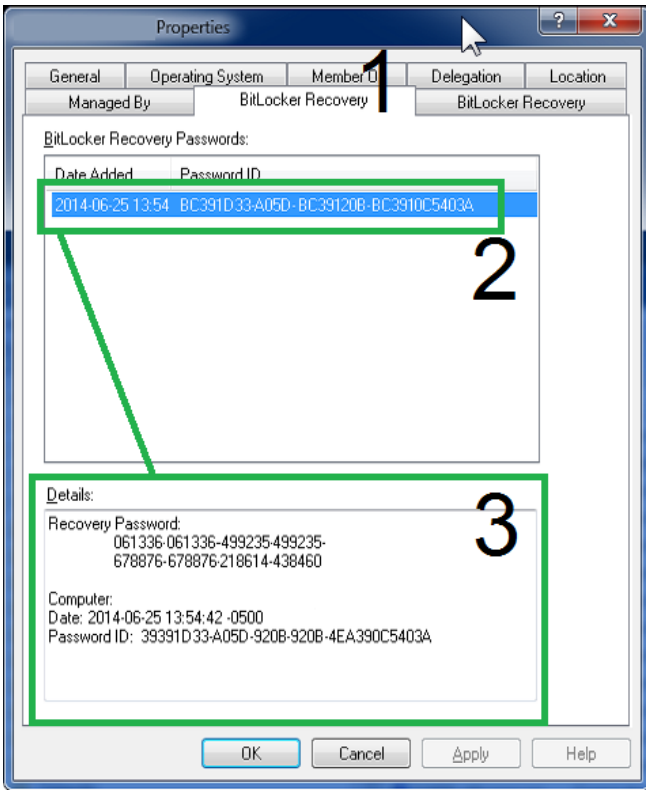
Once the TPM chip have been enabled, the next stage is to perform TPM management. Managing the TPM includes taking ownership of the TPM chip, adding protectors to the TPM, and importing the Bitlocker recovery information into Active Directory and LANDesk. Before starting the actual Bitlocker encryption process, it is critical that the recovery information be stored in central repositories (such as Active Directory). The consequence of not storing recovery information could

prove disastrous, as Bitlocker requires a 48-digit recovery password to be entered under certain recovery circumstances (such as hard drive restoration and partition access from WinPE). The 48-digit recovery password will look something like this: 749474-424079-255893-309697-487611-671444-219460-369961.

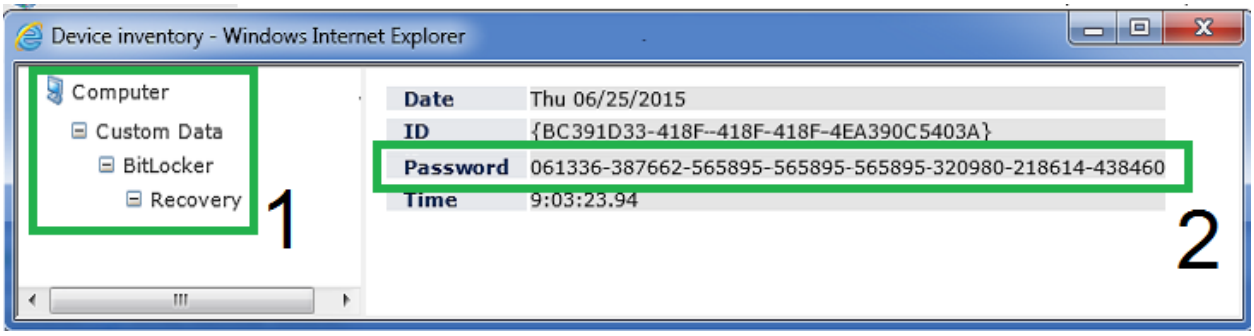
Solution

To address each of the management requirements, a batch file was created that uses manage-bde, along with some branch logic. The script works by being deployed from LANDesk, and then is executed in the computer's system account. Upon execution, it verifies the machine is online, and if so, takes ownership of the TPM, adds protectors to the TPM, and then proceeds to import the Bitlocker recovery information into Active Directory and LANDesk. Successful imports can be seen in Figure 12 and Figure 13.

■ **Figure 12 Successful Active Director Import**



■ **Figure 13 Successful LANDesk Import**



The Script

```
@ECHO OFF
CLS
TITLE TPM Management
COLOR 0E
SET MyVar0=
SET MyVar1=
SET MyVar2=
SET FOUND=FALSE
SET CurDir=%CD%

SETLOCAL ENABLEDELAYEDEXPANSION

:: EXTRACTS FILES - CONTAINS ALL SOURCE FILES
if exist "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" "C:\Program Files
(x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe"
if exist "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" "C:\Program
Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe"

:: PRIMARY PATH CHANGE
Set CurDir=C:\Bitlocker
:: SECONDARY PATH CHANGE
C:
CD C:\Bitlocker


:: TEST FOR ONLINE STATUS
:VERIFYCOM
CLS
ECHO Detecting Internet connectivity...
ping -n 4 127.0.0.1>nul
:: CHECK ONLINE STATUS - google.com
ping www.google.com -n 1 | find "Reply" && SET FOUND=TRUE
IF [%FOUND%] EQU [TRUE] GOTO :FOUND ELSE
CLS
COLOR 0C
Echo No Internet Connection Found. Exiting now...
ping -n 10 127.0.0.1>nul
exit /b 1
```

```
:FOUND
CLS
COLOR 0A
ECHO Internet Connection Found. Loading TPM Management...
ping -n 10 127.0.0.1>nul

CLS
COLOR 0B
ECHO Checking TPM Compliance...started
ECHO Taking Ownership of TPM...pending
ECHO Adding TPM Protector...pending
ECHO Adding TPM Recovery Password Protector...pending
ECHO Importing recovery information into Active Directory...pending
ECHO Importing recovery information into LANDesk...pending

:: CHECKS TO SEE IF TPM HAS ALREADY BEEN SETUP...IF YES, SKIP TO END, IF NO, CONTINUE TO
CHECK1
FOR /f "tokens=1" %%f in ('"C:\windows\system32\manage-bde.exe -status"') DO SET MyVar0=%%f
IF ["%MyVar0%"] EQU ["Numerical"] GOTO :PASSED2

IF NOT EXIST C:\Bitlocker (
MD C:\Bitlocker
ECHO %DATE% %TIME% Created C:\Bitlocker folder.>>C:\Bitlocker\log.dat
)


:CHECK1
:: TAKE OWNERSHIP
C:\windows\system32\manage-bde -tpm -takeownership AddYourPasswordHere

:: CHECK TO SEE IF TPM HAS NO PROTECTORS
for /f "skip=4 tokens=2 delims=:" %%g in ('"C:\windows\system32\manage-bde.exe -protectors -get c:"') do set
MyVar1=%%g
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul
IF ["%MyVar1%"] EQU [" No key protectors found."] GOTO :TPMMGN
GOTO :ADIMP

:TPMMGN
ECHO %DATE% %TIME% No Key Protectors Found.>>C:\Bitlocker\log.dat
ECHO %DATE% %TIME% Starting TPM Management.>>C:\Bitlocker\log.dat
:: THIS IS THE TPM MANAGEMENT ROUTINE
CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...started
ECHO Adding TPM Protector...pending
ECHO Adding TPM Recovery Password Protector...pending
ECHO Importing recovery information into Active Directory...pending
ECHO Importing recovery information into LANDesk...pending
ECHO.
ECHO.
C:\windows\system32\manage-bde -tpm -takeownership AddYourPasswordHere
ECHO %DATE% %TIME% Taking Ownership of TPM.>>C:\Bitlocker\log.dat

CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...started
ECHO Adding TPM Recovery Password Protector...pending
ECHO Importing recovery information into Active Directory...pending
ECHO Importing recovery information into LANDesk...pending
ECHO.
```

```
ECHO.
ECHO %DATE% %TIME% Adding TPM Protector.>>C:\Bitlocker\log.dat
C:\windows\system32\manage-bde.exe -protectors -add C: -tpm

CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...DONE.
ECHO Adding TPM Recovery Password Protector...started
ECHO Importing recovery information into Active Directory...pending
ECHO Importing recovery information into LANDesk...pending
ECHO.
ECHO.
ECHO %DATE% %TIME% Adding Recovery Password Protector.>>C:\Bitlocker\log.dat
C:\windows\system32\manage-bde.exe -protectors -add C: -recoverypassword
GOTO :CHECK2

:CHECK2
for /f "skip=4 tokens=2 delims=:" %%h in ('"C:\windows\system32\manage-bde.exe -protectors -get c:"') do set
MyVar2=%%h
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul
IF ["%MyVar2%"] NEQ [" No key protectors found."] GOTO :ADIMP
ECHO %DATE% %TIME% Adding Protectors failed. TPM has not been enabled.>>C:\Bitlocker\log.dat
GOTO :FAILED

:ADIMP
:: IMPORT RECOVERY INFO INTO AD
CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...DONE.
ECHO Adding TPM Recovery Password Protector...DONE.
ECHO Importing recovery information into Active Directory...started
ECHO Importing recovery information into LANDesk...pending
ECHO.
ECHO.
ECHO %DATE% %TIME% Starting AD Recovery Import.>>C:\Bitlocker\log.dat
C:\windows\system32\manage-bde.exe -protectors -adbackup c: -id%MyVar2% && GOTO :LDIMP

:: LOG
ECHO %DATE% %TIME% AD Recovery Import failed>>C:\Bitlocker\log.dat

:: STAMP REGISTRY
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v AD_Import /d FAILED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v LD_Import /d FAILED /t REG_SZ /f
GOTO :FAILED

:LDIMP
:: LOG
ECHO %DATE% %TIME% AD Recovery Import was successful.>>C:\Bitlocker\log.dat

:: STAMP REGISTRY
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v AD_Import /d PASSED /t REG_SZ /f

:: IMPORT RECOVERY INFO INTO LANDESK
CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...DONE.
ECHO Adding TPM Recovery Password Protector...DONE.
ECHO Importing recovery information into Active Directory...DONE.
ECHO Importing recovery information into LANDesk...started
```

```
ECHO.
ECHO.
ECHO %DATE% %TIME% Starting LANDesk Recovery Import.>>C:\Bitlocker\log.dat
if exist "C:\Program Files (x86)\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" call
"c:\Bitlocker\LDCustom64.cmd"
if exist "C:\Program Files\LANDesk\LDClient\sdmcache\apps\Bitlocker\tpmman.exe" call
"c:\Bitlocker\LDCustom32.cmd"
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul

:: ADD TEST FOR LD STILL HAVE TO DO THIS VERIFICATION ROUTINE
:: LOG
ECHO %DATE% %TIME% LANDesk Recovery Import was successful.>>C:\Bitlocker\log.dat
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v LD_Import /d PASSED /t REG_SZ /f
GOTO :PASSED

:PASSED
:: THIS IS FOR 1st PASS
ECHO %DATE% %TIME% TPM Compliance PASSED. Numerical ID was created.>>C:\Bitlocker\log.dat
CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...DONE.
ECHO Adding TPM Recovery Password Protector...DONE.
ECHO Importing recovery information into Active Directory...DONE.
ECHO Importing recovery information into LANDesk...DONE.
ECHO.
ECHO Computer meets TPM Compliance.
ECHO.

:: STAMP REGISTRY
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM_Status /d PASSED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "%DATE% %TIME%" /t REG_SZ
/f

:: SEND MESSAGE TO LANDESK
if exist "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files
(x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
if exist "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program
Files\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
ECHO %DATE% %TIME% Sent PASSED message to LANDesk.>>C:\Bitlocker\log.dat
manage-bde -on c: -s
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul
manage-bde -pause c:
CLS
ECHO Passed.
C:\windows\system32\ping.exe -n 6 127.0.0.1>nul
GOTO :END

:PASSED2
:: THIS IS FOR 2nd PASS
ECHO %DATE% %TIME% TPM Compliance PASSED. Found Numerical ID.>>C:\Bitlocker\log.dat
CLS
ECHO Checking TPM Compliance...DONE.
ECHO Taking Ownership of TPM...DONE.
ECHO Adding TPM Protector...DONE.
ECHO Adding TPM Recovery Password Protector...DONE.
ECHO Importing recovery information into Active Directory...DONE.
ECHO Importing recovery information into LANDesk...DONE.
ECHO.
ECHO Computer meets TPM Compliance.
ECHO.
```

```
:: SEND MESSAGE TO LANDESK
if exist "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files
(x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
if exist "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program
Files\LANDesk\LDClient\SDCLIENT.EXE" /msg="PASSED"
ECHO %DATE% %TIME% Sent PASSED message to LANDesk.>>C:\Bitlocker\log.dat
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM_Status /d PASSED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "%DATE% %TIME%" /t REG_SZ
/f
manage-bde -on c: -s
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul
manage-bde -pause c:
ECHO Passed.
C:\windows\system32\ping.exe -n 6 127.0.0.1>nul
GOTO :END

:FAILED
manage-bde -protectors -delete c:
ECHO %DATE% %TIME% TPM Compliance FAILED. Check TPM.>>C:\Bitlocker\log.dat
ECHO %DATE% %TIME% Deleted Recovery Info to start over>>C:\Bitlocker\log.dat
CLS
ECHO FAILED!
:: SEND MESSAGE TO LANDESK
if exist "C:\Program Files (x86)\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program Files
(x86)\LANDesk\LDClient\SDCLIENT.EXE" /msg="FAILED"
if exist "C:\Program Files\LANDesk\LDClient\SDCLIENT.EXE" "C:\Program
Files\LANDesk\LDClient\SDCLIENT.EXE" /msg="FAILED"
ECHO %DATE% %TIME% Sent FAILED message to LANDesk>>C:\Bitlocker\log.dat
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v TPM_Status /d FAILED /t REG_SZ /f
C:\windows\system32\REG.exe ADD HKLM\SOFTWARE\Bitlocker /v Timestamp /d "%DATE% %TIME%" /t REG_SZ
/f
C:\windows\system32\ping.exe -n 10 127.0.0.1>nul
ECHO Failed.
C:\windows\system32\ping.exe -n 6 127.0.0.1>nul
GOTO :END
exit /b 0

:END
:: PERFORM CLEANUP
IF EXIST c:\bitlocker\LDCustom32.cmd DEL /Q c:\bitlocker\LDCustom32.cmd
IF EXIST c:\bitlocker\LDCustom64.cmd DEL /Q c:\bitlocker\LDCustom64.cmd
IF EXIST c:\bitlocker\LDSCNHLP32.INI DEL /Q c:\bitlocker\LDSCNHLP32.INI
IF EXIST c:\bitlocker\LDSCNHLP64.INI DEL /Q c:\bitlocker\LDSCNHLP64.INI
EXIT /B 0
```

Active Directory Bitlocker Compliance Report

Problem

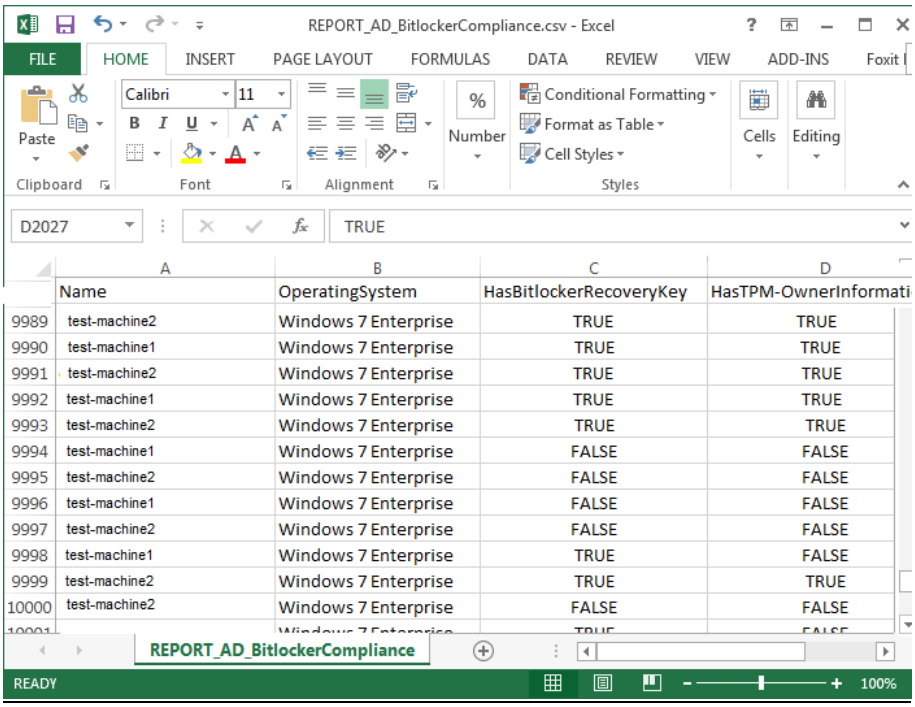
Once TPM Chips have been enabled, and TPM Management has been carried out, Bitlocker encryption can be started. Although the Bitlocker recovery information is being stored in Active Directory, there is no built-in way to audit and report on Bitlocker compliance throughout the

enterprise. Thus, steps must be taken to create an automated method of reporting Bitlocker compliance.

Solution

To address the Active Directory Bitlocker compliance request, a PowerShell script was created to scan computer objects in Active Directory, and return ‘true’ or ‘false’ on the status of Bitlocker. The recovery key and owner information are returned and outputted to a CSV file. This script is meant to be ran by the compliance officer or Bitlocker administrator. The compliance report can be seen in Figure 14.

■ Figure 14 Active Directory Bitlocker Compliance Report



	Name	OperatingSystem	HasBitlockerRecoveryKey	HasTPM-OwnerInformati
9989	test-machine2	Windows 7 Enterprise	TRUE	TRUE
9990	test-machine1	Windows 7 Enterprise	TRUE	TRUE
9991	test-machine2	Windows 7 Enterprise	TRUE	TRUE
9992	test-machine1	Windows 7 Enterprise	TRUE	TRUE
9993	test-machine2	Windows 7 Enterprise	TRUE	TRUE
9994	test-machine1	Windows 7 Enterprise	FALSE	FALSE
9995	test-machine2	Windows 7 Enterprise	FALSE	FALSE
9996	test-machine1	Windows 7 Enterprise	FALSE	FALSE
9997	test-machine2	Windows 7 Enterprise	FALSE	FALSE
9998	test-machine1	Windows 7 Enterprise	TRUE	FALSE
9999	test-machine2	Windows 7 Enterprise	TRUE	TRUE
10000	test-machine2	Windows 7 Enterprise	FALSE	FALSE

The Script

```
#SET REPORT NAME
```

```
$CsvFilePath = "REPORT_AD_BitLockerCompliance.csv"

#LOAD COMPUTER OBJECTS BASED ON OBJECT PROPERTIES
$BitLockerEnabled = Get-QADObject -SizeLimit 0 -IncludedProperties Name,ParentContainer | Where-Object
{$_.type -eq "msFVE-RecoveryInformation"} | Foreach-Object {Split-Path -Path $_.ParentContainer -Leaf} | Select-
Object -Unique
$strComputers = Get-QADComputer -SizeLimit 0 -IncludedProperties Name,OperatingSystem,msTPM-
OwnerInformation | Where-Object {$_.operatingsystem -like "Windows 7*" -or $_.operatingsystem -like "Windows
Vista*"} | Sort-Object Name

#CREATE ARRAY TO HOLD COMPUTER INFORMATION
$ExportToArray = @()

foreach ($strComputer in $strComputers)
 {

   #Create object for each computer
   $strComputerObj = New-Object -TypeName psobject
   $HOST.UI.RawUI.ReadKey("NoECHO,IncludeKeyDown") | OUT-NULL
   $HOST.UI.RawUI.Flushinputbuffer()


   #Add name and OS
   $strComputerObj | Add-Member -MemberType NoteProperty -Name Name -Value $strComputer.Name
   $strComputerObj | Add-Member -MemberType NoteProperty -Name OperatingSystem -Value
$strComputer.operatingsystem

   #SET HasBitlockerRecoveryKey to true or false
   if ($strComputer.name -match ('(' + [string]::Join('|(', $bitlockerenabled) + ')')) {
   $strComputerObj | Add-Member -MemberType NoteProperty -Name HasBitlockerRecoveryKey -Value $true
   }
   else
   {
   $strComputerObj | Add-Member -MemberType NoteProperty -Name HasBitlockerRecoveryKey -Value $false
   }

   #SET HasTPM-OwnerInformation to true or false
    if ($strComputer."msTPM-OwnerInformation") {
   $strComputerObj | Add-Member -MemberType NoteProperty -Name HasTPM-OwnerInformation -Value $true
   }
   else
   {
   $strComputerObj | Add-Member -MemberType NoteProperty -Name HasTPM-OwnerInformation -Value $false
   }

#Add the computer object to the array
$ExportToArray += $strComputerObj

 }

#Export the array with computer information
$ExportToArray | Export-Csv -Path $CsvFilePath -NoTypeInformation
```

Helpdesk Support/Tech Support

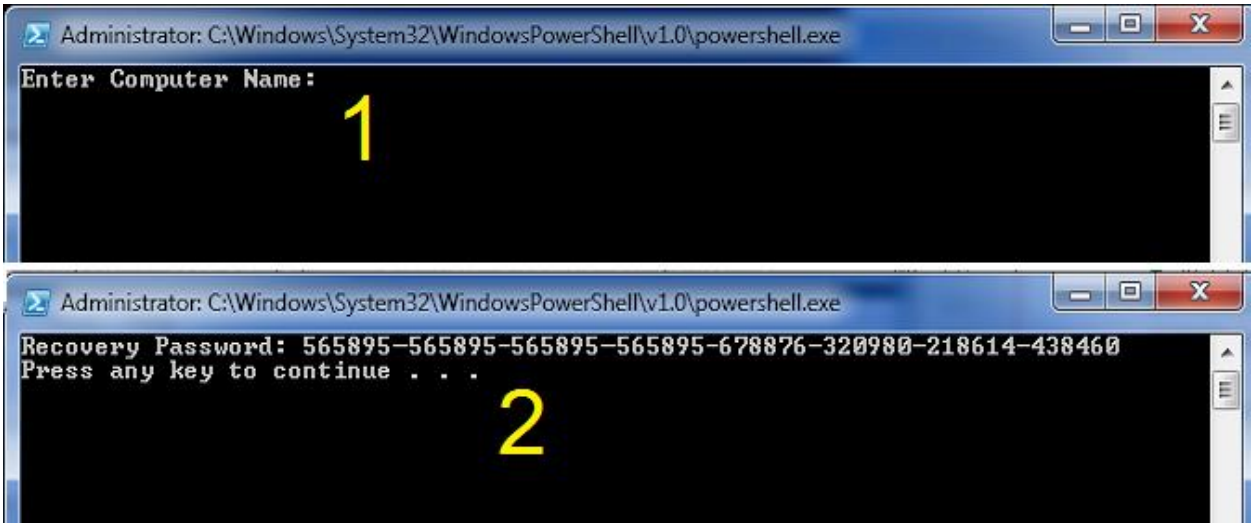
Problem

Although the Bitlocker recovery information is in Active Directory, not everyone will have the Active Directory User console installed on their machines. This presents a support challenge in the scenario that helpdesk or other support personnel need access to the 48-digit Bitlocker password.

Solution

To address this ease of access issue, a PowerShell script has been created to allow support staff to enter a specific computer name and the Bitlocker recovery password will be returned. The scripting input and output can be seen in Figure 15.

■ Figure 15 Support Staff Recovery Script



The Script

```
clear
#Retrieve user input
$strComputer = Read-Host 'Enter Computer Name'

#Import AD commands
Import-Module ActiveDirectory

#Check AD Object
$strComputerObject = Get-ADComputer -Filter {cn -eq $strComputer} -Property msTPM-OwnerInformation, msTPM-TpmInformationForComputer
```

```
if($strComputerObject -eq $null){
    Write-Host "Computer object not found.  EXITing the script..."
    %compspec% /c PAUSE
    EXIT
}

#msTPM-OwnerInformation attribute
if($strComputerObject.'msTPM-OwnerInformation' -eq $null){
    #Check TPM info is backed up to AD
    if($strComputerObject.'msTPM-TpmInformationForComputer' -ne $null){
        # Retrieve TPM Owner Password
        $TPMObject = Get-ADObject -Identity $strComputerObject.'msTPM-TpmInformationForComputer' -Properties
msTPM-OwnerInformation
        $TPMKey = $TPMObject.'msTPM-OwnerInformation'
    }else{
        $TPMKey = '<not SET>'
    }
}else{
    #TPM Owner Password
    $TPMKey = $strComputerObject.'msTPM-OwnerInformation'
}

#Check computer object AD BitLocker Recovery Password
$BitLockerObject = Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -SearchBase
$strComputerObject.DistinguishedName -Properties 'msFVE-RecoveryPassword' | Select-Object -Last 1
if($BitLockerObject.'msFVE-RecoveryPassword'){
    $BitLockerKey = $BitLockerObject.'msFVE-RecoveryPassword'
}else{
    $BitLockerKey = '<not SET>'
}

#Return Info to screen
clear
Write-Host 'Recovery Password:' $BitLockerKey

#Export TPM Owner Password File
if($strComputerObject.'msTPM-TpmInformationForComputer' -ne $null){
    $ExportToArrayToFile = Read-Host 'Would you like to export the recovery key [y or n]'
    if($ExportToArrayToFile -ne 'y'){
        EXIT
    }

    $TPMFile = '<?xml version="1.0" encoding="UTF-8"?><ownerAuth>' + $TPMKey + '</ownerAuth>'
    $TPMFile | Out-File "TPMOwnerPasswordFile.tpm"
}else{
    Cmd /c PAUSE

}
```

Backup Bitlocker Passwords

Problem

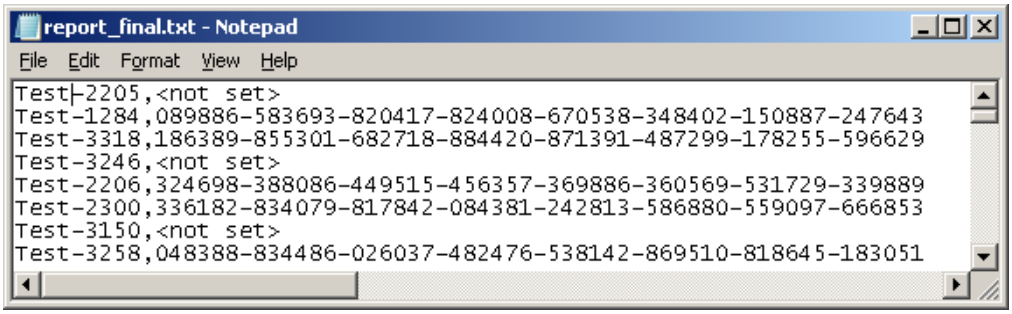
The Bitlocker recovery information is in Active Directory and in LANDesk, however there may be need to export or backup the Bitlocker passwords. This will useful for disaster recovery, and is

considered best practice to maintain a secondary or even tertiary copy of the Bitlocker passwords. Thus, measures should be taken to back up the passwords to a text or CSV file.

Solution

To address the backup requirement, a PowerShell script was written which uses the Import-Module ActiveDirectory cmdlet. A sample report can be observed in Figure 16. Note, this text file is comma delimited, which can be easily converted to an Excel spreadsheet or CSV report.

■ **Figure 16 Backup of Bitlocker Passwords**



The Script

```
Import-Module ActiveDirectory

$ou = Get-ADObject -Filter { ObjectClass -eq 'organizationalunit' } -SearchBase "OU=Workstations,,DC=
YourDomainName,DC=com"

foreach ($obj in $ou) {
Get-ADComputer -Filter 'ObjectClass -eq "computer"' -SearchBase $obj -ErrorAction SilentlyContinue -
ResultPageSize 2000 | foreach-object {
$Computer = $_.name


#Check if the Computer Object exists
$Computer_Object = Get-ADComputer -Filter {cn -eq $Computer} -Property msTPM-OwnerInformation, msTPM-
TpmInformationForComputer

#Check if the computer object has had a BitLocker Recovery Password
$Bitlocker_Object = Get-ADObject -Filter {objectclass -eq 'msFVE-RecoveryInformation'} -SearchBase
$Computer_Object.DistinguishedName -Properties 'msFVE-RecoveryPassword' | Select-Object -Last 1
if($Bitlocker_Object.'msFVE-RecoveryPassword'){
   $Bitlocker_Key = $Bitlocker_Object.'msFVE-RecoveryPassword'
}else{
   $Bitlocker_Key = '<not set>'
}
```

```
#Display Output
$strToReport = $Computer + "," + $Bitlocker_Key
Write-Host $strToReport

#Save to Report
$strToReport | Out-File Report.txt -append
    } # end for-each
} # end for-each
```

Appendix

SDLC

When installing any IT-based system, there should be a strategic approach taken in the design and implementation of that system. A system could refer to a full-fledged enterprise system, such as an ERP or MIS, a new software application, or even a software or hardware service. Without an official business strategy, there is a good chance that the system will take longer to implement and be riddled with problems all along the way. To reduce problems associated with the setup of a new system, it is common (and best practice) that an IT specialist will use a standardized, proven methodology. One of these methodologies is known as SDLC. SDLC, or systems development life cycle, is a phased approach to system design, which includes three main levels or phases that can be further broken down into eight individual steps (Brown, Dehays, Hoffer, Martin, & Perkins, 2012).

The primary phases of the SDLC are (1) Definition, (2) Construction, and (3) Implementation. In the Definition phase, there are two steps (1) feasibility analysis and requirements definition (Brown, et al., 2012). In the *feasibility step*, the person leading the systems project will determine the economic, operational, and technical requirements of the system. Of course this person will not work alone; they will meet with a sponsoring manager, the technical people that will be involved with the project, and any other personnel that may have input on the system's feasibility. The feasibility analysis step is essential to designing and building a new system, in that, this is the step where project leaders and business managers will work together to commit to project resources. The second step in the Definition phase is the *requirements definition*. In the requirements definition step, an official document is drawn up, known as the system requirements document. In the systems requirement document, there will be

detailed descriptions of the new system's input and output, a refined budget sheet, and an updated plan that will be used for project development.

In the second phase of the SDLC methodology, the Construction phase, there are three separate steps (1) systems design, (2) system building, and (1) system testing (Brown, et al., 2012). The *systems design* step is just how it sounds; this is where IT specialists design the system, or create a plan for implementing a form of hardware or software. The next step is *system building*. System building is where the code is developed, the hardware is acquired, or the software is built. Once the system building step is complete, the system will need to be tested. In *system testing*, the new system is tested in segments, and then in full. The point of this step is for all those involved in the project to sign-off on a "working" system, and for relative documentation to be created.

In the third phase of the SDLC methodology, the Implementation phase, there are three steps (1) installation, (2) operations, and (3) maintenance (Brown, et al., 2012). The *installation* step is where IT specialists and supporting personnel will begin updating older systems, create databases, prepare the environment for the system, and train employees how to use the new system (if applicable). The second step is *operations*. In operations, the "system" is close to production; development, test versions, and production versions will be turned over to the proper teams and employees. Documentation will be reviewed, and any updates will be added to these final documents. If everything is satisfactory, the new system will be deemed acceptable, closing procedures will be concluded to make the new system is fully operational, and the system will now be considered "in production." The third and final step in the Implementation phase—as well as in the SDLC methodology—is *maintenance*. In the maintenance step, when the system needs updates, patches, and upgrades, these tasks must be scheduled, and the changes made

accordingly. Likewise, this is the step where improvements can be applied, and user interfaces and user experience can be updated. The maintenance step is an important step in the SDLC methodology, and should be incorporated into the overall business strategy.

Project Management Life Cycle

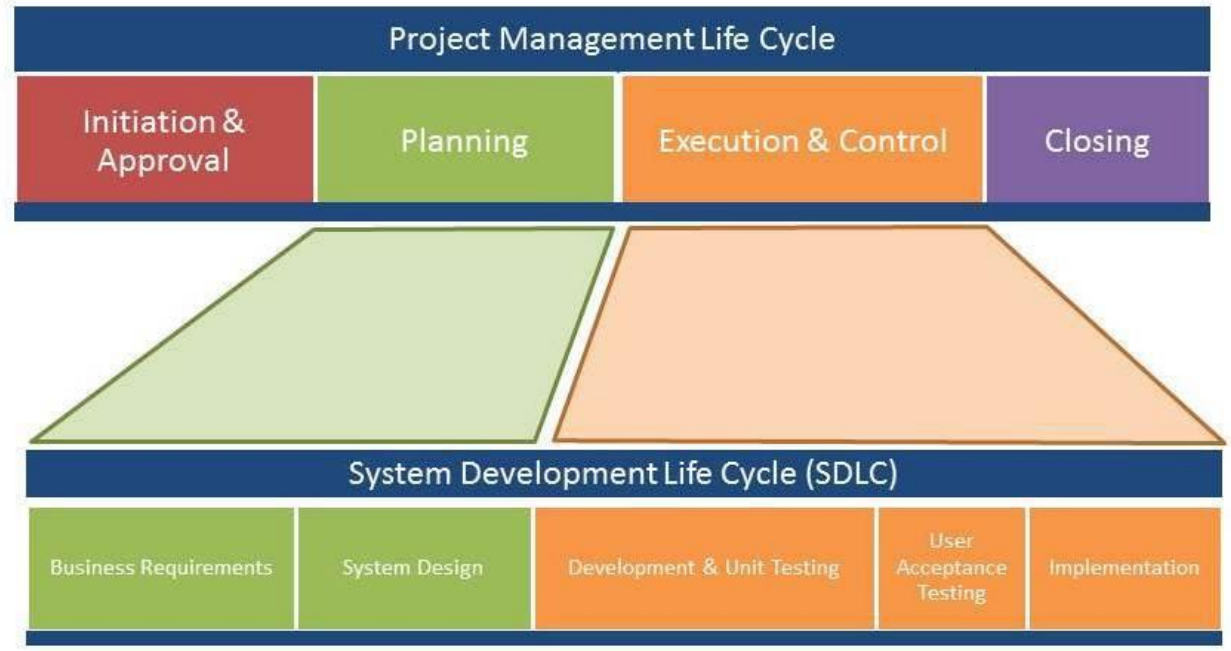
Of course, as an even better systems management strategy, SDLC may be paired with other best practices management techniques. These techniques should encompass the project life cycle. Understanding the project life cycle will enhance the processes used in the SDLC methodology by adding even more structure to the system design and implementation. The project life cycle is a collection of phases which include initiation, planning, implementation (commonly referred to as execution and control), and closing phases (Watt, 2014). In the *Implementation* phase, a business case is prepared which includes details such as business need, proposed solutions, and any solutions are reviewed and investigated for viability. The next project life cycle phase is the *Planning* phase. The Planning phase is where ideas begin to be developed, and the appropriate resources, personnel, and scope are identified. Additionally, tasks and timelines will be discussed, and scheduled will be created. The third phase in the project management life cycle is the *Implementation* phase. In the Implementation phase, everything comes together; meetings are held, the pieces of the system start to be completed, reporting is done (this includes status reports), and team members work together in testing and implementing the system (pre-production and into production). In the final phase, the *Closing* phase, the responsibility of the system is transferred to the customer, documentation is handed over, and lessons learned are discussed.

(Watt, 2014)

Synthesis

A best practice approach to implementing a new system is to use SDLC and the project management life cycle. A successful adaption of SDLC and the project life cycle is to first understand how they align. If the phases of each methodology was divided up and matched respectively (using a simple, condensed chart), both approaches could be added to a single project strategy. This can be seen in Figure 17.

■ **Figure 17 SDLC and Project Life Cycles**



SOURCE: http://www.thinkforachange.com

It is evident, that planning, business requirements, and system design are all closely related. Likewise, execution and control, development, UaT, and implementation can be considered essential to creating the system and then testing a new system.

Real World Example

As a real world example of SDLC and the project management life cycle, a brief scenario has been prepared for review. In this example, a company is rolling out a new enterprise email

system. The company is currently using Google's Gmail, and requires something more robust that does not have restrictions in storage and transmission capabilities. An IT specialist is assigned the project by the CIO, and begins the *Initiation and Approval* steps, and starts *Planning* the project. These first steps include holding a few meetings and drafting a project charter. A project charter is an official document that lists details such as project goal, the personnel involved in the project, the stakeholders of the project, and any requirements and constraints that will be essential to the overall project (Rouse, 2012). Additionally, the project charter will discuss milestones and deliverables. Furthermore, business requirements will be considered, such as how many clients need to be upgraded, the cost associated with the project, as well as the scope of the project. These steps are connected to the SDLC *Business Requirements and System Design* phases, and the *Initiation* and *Planning* phases of the project management life cycle.

Referencing the chart in Figure 1, the new email system is to be developed and modular testing is to be performed. The system is installed, sample users are created, and the system is tested in a non-production environment. Once the email system is setup, UaT is completed, and the system is implemented. These steps are part of the *Development and Unit Testing*, *UaT*, and *Implementation* phases in SDLC, and *Execution and Control* phase in the project management life cycle. The email system is nearly complete, documentation is updated (where applicable), and the administration of the new email system is turned over to the appropriate IT personnel. These steps are linked to the *Maintenance* phase of SDLC and the *Closing* phase of the project management life cycle. Note, by this point, the email system is live, the documentation has been completed, personnel have been trained, and the technical administration of the email system has been turned over; lessons learned may be discussed at this time.

SDLC Summary

SDLC and the project management life cycle create a framework which provides structure and organization to a project. SDLC is a phased approach to system design, which has three main phases (1) Definition, (2) Construction, and (3) Implementation. The project life cycle also uses three primary phases or stages to organize system design (1) Planning, (2) Implementation, and (3) Closing. The importance of using a methodology cannot be understated nor undervalued; there are numerous advantages that all lead to the successful implementation of a new system. Thus, learning the utility aspects of SDLC and the project management life cycle will become essential to controlling project timelines, understanding the scope of the project, keeping the project within budget, and maintaining clear lines of communication with all appropriate personnel, including developers, testers, and project stakeholders. Thus, applying these methodologies is not only a good idea, it is a necessity.

Ethical, Legal, and Social Implications

Ethical

This week's part 2 assignment is to provide some information about the ethical, legal, and social ramifications of using Bitlocker (or any encryption technology for that matter) on company computers. Due to most company computers containing customer and company data, it would be highly unethical for that data not to be protected at all times. Thus, once Bitlocker has been installed on all computers, encryption compliance will be enforced by using the scripts created for LANDesk. While encrypting data seems like an obvious solution to a serious risk, i.e. unauthorized access to data recovered from stolen or lost hard drives, Bitlocker can be influenced by cultures in other countries. Because Company X employees do occasionally travel outside the country, it is imperative that all company personnel familiarize themselves with the international laws that govern encryption, as it specifically impacts how encryption may and may not be used outside the country. There will be scenarios where encryption must be temporarily disabled when traveling abroad.

Legal

When it comes to encryption legislation on a global scale, numerous countries have laws *against* encryption, this would include having computers imported or exported with the recently implemented Bitlocker. For example, a short list of countries has been compiled with certain countries and what actions must be taken when encryption enters that country. These can be seen in the chart below (Brown University, 2015):

Country	Action
Burma	A license is required
Belarus	Restricted initially until license is approved
China	A permit is required from the Beijing Office of State Encryption Administrative Bureau
Hungary	Has laws that foreigners must adhere to
Iran	Has laws that all people must adhere to
Israel	You can have encryption, but the password must be provided to officials
Morocco	Has strict laws against all encryption
Russia	A license is required
Saudi Arabia	Encryption is normally banned everywhere
Tunisia	Importing encryption is restricted
Ukraine	Has strict laws against all encryption

Note, this is only a small portion of the actual list. To see more, the U.S. State Department's website may be referenced. Additionally, the Electronic Code of Federal Regulations, or e-CFR, outlines laws and regulation surrounding encryption commodities, software and technology (U.S. Government Publishing Office, 2015).

Social

The social implications of using encryption encompass three primary schools of thought: (1) encryption should be available to everyone, for any kind data that is deemed sensitive; (2) encryption can be employed, but the recovery passwords must be accessible by the government; and (3) no encryption is allowed. In the first approach to encryption, all sensitive, private data should be protected from unauthorized access, this would include encrypting data to protect it against offline attacks. It is important to clarify, even the local and federal government will not

have access to view this particular type of encrypted data.

In the second approach, sensitive, private data can be encrypted, however the local and national authorities must have access to view the content, and in most scenarios, special permits and official documentation must be acquired *prior* to implementing encryption. Why would this be necessary? Why would law enforcement and government officials require access to encrypted data? In some cases, criminals and terrorists use encryption to hide their criminal activity. Likewise, encryption could be used to steal company data, or commit corporate and government espionage. It is understandable, if everyone is allowed full access to and usage of encryption, the social implications could be severe in the hands of a criminal. If the government had the ability to regulate encryption, they could monitor it for criminal-like activity, thus preventing certain crimes.

The third outlook towards encryption is that encrypted data is a national or state security risk, and that it should be denied completely. As referenced in the legal aspects of encryption on a global scale, not all countries share the ideology that encryption is good, and as such, heavy restrictions will apply. In fact, numerous countries have laws *against* enabling any form of encryption on computers, this includes importing, exporting, and domestic forms of encryption.

Lessons Learned

As the IT Specialist in my project, I was responsible for the entire project. I did have a few local site technicians assisting with me “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 practical risk analysis.

For scope, I wanted 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 ten thousand computers, which were added to the project’s scope and became the targeted list. This was specifically added to lessons learned because there were several ideas that came up on how to retrieve this target list. For example, it was suggested we use our inventory software, except the inventory software could not return machines that were currently online. 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 and query online machines.

Next in lessons learned, I spent some time trying to figure out exactly what the budget was for this project. There were 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 difficult to create a solid budget around the numerous tasks I

would be completing during the project. 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 five of the twenty 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 a 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, leading to the purchase of twenty new computers. We ended up using only five of those computers, which I thought was not a bad estimate. However, I think a better solution would have been to order ten computers, and then on a case by case basis order extra computers as needed; this would have saved us $10,000. One last afterthought was retrieving and storing the Bitlocker recovery passwords using different methods. Although we did have the Bitlocker information in Active Directory and LANDesk, additional options, such as secure FTP and email, could have been used to store the recovery data. But I would say, overall, the project went as intended, and the company and the customers were pleased to now have secured data on hard drives.

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.

Brown University. (2015). Learn about BitLocker (encryption for Windows). Retrieved from http://www.brown.edu/information-technology/knowledge-base/article/1254

Dalechek Technology Group. (2014). Recovery keys to the kingdom: How an enterprise IT guy learned to love Bitlocker. Retrieved from http://www.dalechek.com/2014/02/recovery-keys-to-the-kingdom-how-an-enterprise-it-guy-learned-to-love-bitlocker/

Hardekopf, Bill. (2015). The big data breaches of 2014. Retrieved from http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/

Northern Ireland Business. (n.d.). The advantages of project management and how it can help your business. Retrieved from https://www.nibusinessinfo.co.uk/content/advantages-project-management-and-how-it-can-help-your-business

Rouse, Margaret. (2012). Project charter (PC). Retrieved from http://searchcio.techtarget.com/definition/project-charter-PC

U.S. Government Publishing Office. (2015). Electronic code of federal regulations. Retrieved from http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=f69a12e71396cdb0037d905024c2eca2&rgn=div8&view=text&node=15:2.1.3.4.25.0.1.17&idno=15

Venkata. (2012). What is SDLC? Retrieved from http://www.sdlc.ws/what-is-sdlc/

Watt, Adrienne. (2014). The project life cycle (phases). Retrieved from http://opentextbc.ca/projectmanagement/chapter/chapter-3-the-project-life-cycle-phases-project-management/