The Hidden Costs of Microsoft® BitLocker®

White Paper

By: Kevin Beaver, CISSP

August 2011

WINMAGIC®
DATA SECURITY

Contents

Summary

This whitepaper discusses the known issues with Microsoft BitLocker that you need to consider before deploying it.

It's hard for one vendor to be everything to everyone. The vendor with the best operating system or most powerful directory service may not be the vendor with the best security options for your business needs. Sure, it's wise to use what you already have at your disposal – i.e. BitLocker with Windows 7 Ultimate and Enterprise. But is putting all of your eggs into one basket and relying on a single vendor the best approach?

BitLocker could require changes in your mobile computing environment, not to mention a full-time employee to support. Furthermore, known security weaknesses with BitLocker can put sensitive business information at risk. Even with BitLocker's recent and forthcoming improvements there are some things you need to think about.

Read on for some things you may not have known about BitLocker as well as some enterprise mobile security considerations that will help you make educated decisions on what's best for your business.

Introduction

The case for mobile computing has been made. There's no refuting the value of a mobile workforce and all the gadgets that go along with it. The benefits to users and the business as a whole outweigh the costs – that is with one exception: information security. Protecting sensitive information on laptops, netbooks and mobile storage devices is a huge concern that many businesses are either ignoring or they've yet to get their arms around.

The desire for mobile computing often outweighs the perceived risks. Consequently, when laptops and mobile devices are lost, stolen or otherwise mishandled, businesses have security incidents and data breaches to contend with.

Mobile computing has created one of the greatest information risks for businesses today. Rather than having sensitive information protected behind the traditional four walls of the building, there are literally hundreds, if not thousands (or more), of "islands" of information scattered about on laptops and mobile storage devices.

Regardless of the configuration, it's virtually guaranteed that any given laptop contains sensitive information such as those shown in Figure 1:

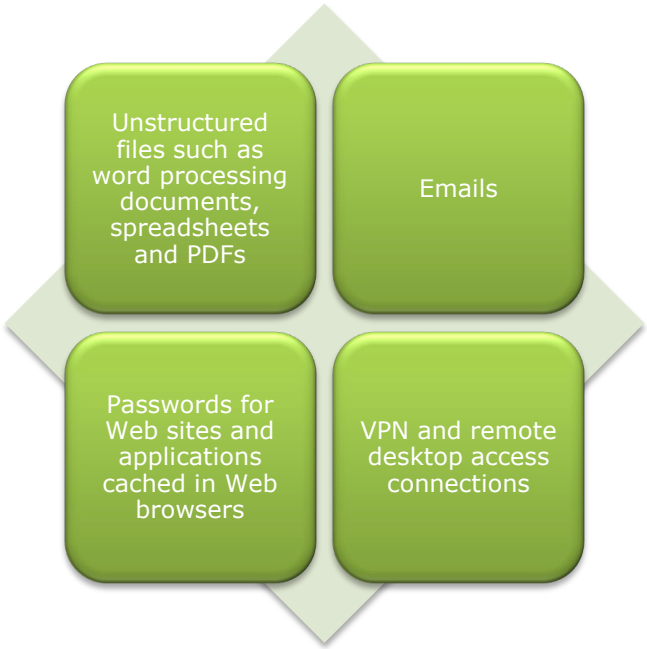

Figure 1 – Sensitive information present on many laptops

Likewise, anything goes when it comes to mobile storage devices such as thumb drives and external hard drives.

Unless and until these systems are *properly* encrypted, all of this sensitive information can be put at risk in the event of loss, theft or improper disposal. So, what's such an incident going to cost your organization? According to the Ponemon Institute's study *The Cost of a Lost Laptop*, the average value of a single lost laptop is $49,246 – a considerable sum given the number of mobile systems and likelihood of an incident occurring.

Another thing that's often overlooked is the fact that no magical hacking skills are required for someone to be able to gain access to this information when it's not properly encrypted on a mobile system. Even with password protection on Windows-based systems, there are free and commercial software tools that can easily bypass such controls. Power-on passwords in the system BIOS are equally ineffective in most cases. When you add consumerization of IT and internal politics into the equation, it becomes clear that mobile security is a huge business challenge that must be dealt with, now.

So what are businesses doing about information risks on mobile systems? Many are turning to Microsoft's free BitLocker disk encryption software. However, as many people are finding out with BitLocker, "free" solutions are hardly ever free.

Getting to Know BitLocker

Microsoft BitLocker offers a full disk encryption (FDE) solution for Windows Vista and Windows 7 workstation operating systems. BitLocker also supports FDE on Windows Server 2008 and Windows Server 2008 R2. Encryption capabilities are extended to mobile storage devices such as thumb drives and external hard drives via Microsoft's BitLocker To Go®.

Available since 2007, BitLocker originally supported FDE only on the boot partition of the computer. This meant that data drives and external media weren't supported. Enterprise features were limited as well. However, BitLocker has undergone several improvements including the new Microsoft BitLocker Administration and Monitoring (MBAM) for centralized administration which is currently in beta and slated to be available in Q3 2011. Pricing is unknown at this time. Notable features in MBAM include the ability for users to be able to start the encryption process, being able to prove a systems encryption status at the time of an incident and a key recovery portal for users. -

When it comes to providing user access to an encrypted system, BitLocker has two types of authentication: 1) *transparent* and 2) *user*. Transparent authentication stores the encryption key in memory. Users aren't even aware that this method of authentication is taking place when the system boots. Unfortunately, this method of authentication is less secure and prone to attack. On the other hand, user authentication requires that users either enter a PIN via the function keys on the keyboard or plug in a USB thumb drive or similar device holding the encryption key every time the computer boots. Unfortunately, both of these methods can be cumbersome to users.

BitLocker – The Rest of the Story

We've all learned the hard way at some point that "free" is not always free. In the context of IT, administrators and managers who have performed a total cost of ownership (TCO) analysis for certain technologies are sure to admit that the devil is in the details. In fact, many issues don't reveal themselves until you're well into the implementation.

When procuring Windows 7 Ultimate or Enterprise licenses, you're already paying for BitLocker since it's one of the main differentiators between these versions of Windows and the next version down – Windows 7 Professional. Interestingly, this is often how BitLocker makes its way into the enterprise. The thought is "We have it so we might as well use it." Or, as the people in charge of the budgets might see it: "We've already paid for it so let's try it out. What is there to lose?"

Being a strong proponent of spending your IT dollars wisely, this mindset is hard to argue against. That is until you start thinking long term about all the *other* issues that go along with BitLocker such as:

Perceived price doesn't paint the entire picture for enterprise networks

Perhaps the most appealing aspect of Microsoft BitLocker is its price: $0. For organizations with hundreds or thousands of workstations, the price seems right as BitLocker is included with the Ultimate and Enterprise editions of Windows 7.

If you're considering deploying BitLocker in an enterprise setting with the need to protect hundreds, thousands or tens of thousands of computers, the extra cost of Windows Ultimate and Enterprise– up to $20 more per computer depending on discounts and volume pricing – can add up quickly. Assuming you have a thousand desktops and no use for other features in Windows 7 Ultimate or Enterprise, you may be hard-pressed to justify an extra $10,000+ for BitLocker protection.

If you're like many organizations and currently moving towards Windows 7, now is the time to be thinking about which licensing model is the best fit for your business.

1. Each computer needs to have a Trusted Platform Module (TPM) version 1.2 chip in order to access all of BitLocker's features. Furthermore, every computer with a TPM chip may have to be touched so the chip can be enabled and configured for the first time. Do you have the budget and the IT resources to support this?

   What's the real cost in terms of time, effort and money to spend, at a minimum, a minute or two at each computer that needs its TPM enabled and configured? In addition to hardware procurement costs, it's not unreasonable to factor in up to 2-3 minutes or more of IT staff time configuring each system which could result in the following scenario:

   $50/hour or $0.83/minute (reasonable cost to employee an IT professional)
   x 2 minutes (time spent per computer)

   = $1.66 per computer just to get rolling with TPM enablement/configuration

   If you have, for instance, 500 computers, you're already $830 in the hole before procuring or installing any FDE software. Is this really money well spent?

2. Computers that *do not* have a TPM chip will have to be booted with the encryption key accessible on a storage device such as a USB thumb drive. Loss of the thumb drive or the fact that users will likely storing the thumb drive with their laptops can completely negate any benefits of FDE. Are you willing to take on the realities associated with users being responsible for yet another facet of information security?

What's the real cost when something goes awry and a breach occurs because thumb drives were mismanaged? What's the cost in productivity by users having to fumble around to find their storage devices every time their computer boots?

3. BitLocker doesn't support workstations running Linux, Mac OS X or older versions of Windows such as Windows XP or Windows 2000. Even if your enterprise is moving toward – or has already deployed – Windows 7, the odds are good that older systems running Windows XP still exist and will continue to be used indefinitely. Are you willing to take the chance on a single system that's not protected by BitLocker negating all your other efforts for FDE?

   What's the real cost of lingering legacy systems that go unprotected?

4. Consumerization is no doubt affecting the procurement and computers and security on the data they process and store. How is this additional complexity going to affect your rollout and support of BitLocker?

   What's the real cost to oversee and manage the security of such a diverse set of computers within the confines of BitLocker's minimum requirements? It's not unreasonable to factor in several minutes per machine – arguably hours or days overall – just to determine which systems are going to be able to run BitLocker. Can you justify spending thousands of dollars justifying whether or not something is a good fit in your enterprise environment before you ever receive any tangible payoffs?

5. There's no reasonable way to enforce encryption on storage devices such as thumb drives and external hard drives. Furthermore, BitLocker doesn't support the encryption of CDs and DVDs. How is this going to impact your security and compliance requirements?

   What's the real cost when personally-identifiable information or intellectual property is unprotected and ultimately breached due to a lack of mobile storage protection? Many businesses, especially those in the healthcare industry, rely heavily on optical media for transferring and sharing sensitive information. Even if you go as far as paying more for self-encrypting drives (SEDs) based on the Trusted Computing Group's Opal specification, a single unencrypted CD or DVD containing sensitive information can bypass any such benefits.

6. BitLocker only supports a single TPM PIN for initial system authentication. Do you have shared computers in your environment? If so, will sharing PINs increase your risk or affect compliance status?

   What's the real cost when a lack of accountability impedes an analysis of insider abuse or a formal breach investigation? What's the productivity cost to users when multiple people have to be involved in the authentication process?

7. Without MBAM, BitLocker stores encryption keys in Active Directory that domain admins can access. Are you going to have problems with not being able to reasonably enforce the principles of *separation of duties* and *business need to know*?

   What's the real cost if you end up on the wrong side of a data breach situation or lawsuit and it can be shown that certain fundamental security principles were overlooked, bypassed or ignored altogether?

8. There are commercial tools such as Passware Kit Forensic ($795 U.S. at www.lostpassword.com) for compromising BitLocker-protected systems that can negate any

benefits of FDE. How are you going to respond to a situation where a BitLocker-protected system is lost, stolen or otherwise mishandled?

What's the real cost if sensitive data is ever recovered from a system that you knew was vulnerable to compromise? Fines, legal fees and related costs can be astronomical.

The business and technical complexities associated with mobile computing are enough of a burden. You have to ask yourself if these additional issues are going to help or hinder your move towards improved security.

One thing's for sure: complexity is the enemy of security. The more complexities you have in your mobile computing environment the greater the chances of things going awry.

BitLocker may seem to be a good deal now, but based on how these issues may impact your environment, BitLocker's true cost of ownership may not be realized until months or years into your deployment. Again, only you will know. The important thing is to acknowledge potential hurdles you may face, perform your own calculations and think long term about the impact to your business.

Conclusion

The moral of the story is that you have to do your homework. You're at a crossroads and the choices are clear:

Option 1

•Go the BitLocker path that many others are considering

Option 2

•Go with a commercial FDE alternative from a third-party vendor

Option 3

•Wait and see how BitLocker and MBAM improve and eventually jump on board

The benefits of an FDE solution – arguably *any* FDE solution – are worth much more than the purchase price. BitLocker may be a good fit; perhaps it's not. The important thing is to look at the big picture. Potential costs brought about by BitLocker in the enterprise include:

- Deployment including complexities brought about by IT consumerization
- Hardware such as TPM support (easily $2 per computer just to enable or configure the TPM), removable media and so on
- Software including Windows 7 Ultimate and Enterprise licenses (up to $20 per computer) as well as third-party management tools such as Wave for BitLocker® Management Administration including complexities brought about by CDs and DVDs needing to be encrypted

Breaches brought about by hacking tools that can negate BitLo[c]ker disk encryption altogether.

These costs could vary anywhere from several hundred dollars to several hundred thousand dollars – or more. What can your budget handle?

In the end, you cannot secure what you don't acknowledge nor can you change what you tolerate in IT. Determining how to manage FDE is not something you should take lightly. Time is of the essence. Get started now by determining what your business's specific needs are, what your compliance requirements are, what your business's risk tolerance is and what FDE technology will be best for keeping your laptops, netbooks and mobile storage devices in check. Make sure the right people are involved and the team really thinks through what's best for your business. BitLocker or not, any time you spend up front understanding the facts and planning things out will pay for itself over and over again moving forward.

About the Author

Kevin Beaver, CISSP, is an independent information security consultant, author, expert witness and professional speaker with Atlanta, GA-based Principle Logic, LLC. He has over two decades of experience in IT and specializes in performing information security assessments revolving around compliance and minimizing business risks. Kevin has authored/co-authored 10 books including one of the all-time best-selling information security books Hacking For Dummies (Wiley) as well as Implementation Strategies for Fulfilling and Maintaining IT Compliance (Realtimepublishers.com) and The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach). He is also the creator and producer of the Security On Wheels audio programs providing security learning for IT professionals on the go (securityonwheels.com). Kevin can be reached at his website www.principlelogic.com and you can follow him on Twitter at @kevinbeaver.