IRONKEY™

Moving Beyond Compliance: Why 'Secure Enough' Isn't Enough

CONTENTS

INTRODUCTION

Moving beyond compliance: Why 'secure enough' isn't enough. Defining the difference between compliance and protection – and what it means for your organization's USB data storage strategy.

Organizations and agencies struggle to remain ahead of constantly evolving threats to the security of their data. Not only is news of data breaches increasingly being reported; the threats are escalating and the risks are many:

- Intellectual property representing years of R&D falling into the hands of competitors
- Sensitive corporate records leaked to hackers, hacktivists and malicious governments
- Data breaches involving customers' personally identifiable information about health records or finances, and the resulting damage to brands and customer loyalty
- Fines and other costs associated with failure to comply with data security mandates
- Pre-release of product, content or trade secrets spoiling market opportunity

Many organizations in healthcare, financial services, government and other regulated industries must comply with privacy and data protection laws, regulations and policies designed to protect sensitive and confidential information. And as a result, they often implement data security policies simply because it is required. Meeting compliance regulations is important, but even the strictest compliance requirements still can leave sensitive data vulnerable to malicious parties capable of breaking into encrypted USB storage devices and extracting confidential data from them.

Now more than ever, the need to move beyond just compliance should be on the forefront of an organizations' data security and protection strategy. To help organizations and agencies answer the question, "is 'secure enough', really enough?", this paper from IronKey explains when compliance alone may not offer the protection needed to prevent data breaches that can cost millions of dollars, inflict untold damage to corporate brands and customer relationships, and invite weeks or months of negative publicity.

The paper pays special attention to the Federal Information Processing Standards (FIPS) 140-2 Level 3, a U.S. Government standard for information technology and computer security that offers a high level of protection designed to put sensitive data beyond the reach of a much larger population of hackers and thieves.

The paper also reviews the benefit to making the incremental added investment in solutions that work harder to protect a secure USB device’s encryption keys.

Preventing a $5.9 Million Mistake

Securing data involves a seemingly infinite menu of carefully layered systems, technologies, strategies and methods. Costs range from free to jaw-dropping. Deployments can be simple or sophisticated. Management requirements can vary widely.

As there is a lot of complexity, it is no wonder many organizations gravitate towards the most common data protection strategies and visible compliance documentation such as HIPAA as good enough, but compliance and security are not the same thing. Simply aiming for compliance alone can be a costly strategy. Just because compliance requirements are met does not mean your organization will attain the appropriate level of protection. According to a 2014 Ponemon Institute study, a data breach in the U.S. comes with an average price tag of $5.9 million. The study continues to note that the cost of lost business resulting from a data breach increased to $3.2 million.

When you are looking to secure mobile data, either on a USB stick, hard drive or Windows To Go device, it’s worth your time to understand how the levels of mobile security stack up.

> Compliance and security are not the same thing and simply aiming for compliance alone can be a costly strategy.

Defining the Levels of Security

When evaluating security options, it is important to identify the impact to your business associated with the information you are protecting and the threats from which you are protecting them. Remember, too, that security is a moving target and the threats continue to escalate to both the data and the device itself. As revealed at Black Hat 2014, BadUSB is the first USB malware designed to attack the device itself instead of attacking the data on the device. The attack changes the firmware that controls the behavior of the USB hardware, allowing the USB device to become a host that can subsequently infect other computers and USB devices.

> The best protection against BADUSB is to use code signing for firmware updates. If the signed firmware is modified, the device cannot authenticate the firmware and simply will not operate. IronKey’s secure USB devices protect against BadUSB malware. Our leadership in security, including our use of digital signatures in all controller firmware, makes IronKey products immune to this threat.

Compliance vs. Security.

Security levels for storage devices can be described as "compliant," "more secure," and "most secure." To understand the level of security your organization needs, you first must take inventory of your reasons for implementing a secure data strategy. You must also always evaluate the need to move beyond compliance.

IT managers frequently cite one of three primary drivers:

1. **We only need to be compliant with data security requirements.** When compelled to implement a data security strategy, organizations frequently fail to see a direct relationship between adding security and achieving improved efficiencies across their operations. Their goal is to simply be secure enough that if a breach occurs, they can show that they followed "industry standard and best practice," thus avoiding the cost of fines from government oversight bodies. In other words, the organization needs to get a passing grade in a security audit but does not see any pressing reason for security investments outside of this objective.

2. **Our workforce deals with information that is highly sensitive and cannot fall into the wrong hands.** In this case, a loss of critical proprietary or confidential information could have severe or even catastrophic consequences to a business; organizations and agencies tend to choose a security level that keeps the data secure from even the most aggressive and well-capitalized hackers, such as foreign governments and identity theft cartels.

3. **The storage device must survive the harshest of environments while being secure and accessible for long periods of time.** For organizations or agencies that subject their data devices to challenging physical conditions – including government, military, first responders, and hospital workers in sterilized environments – keeping data secure is a matter of more than data security. It can be a matter of national security or public safety. And for organizations that don't necessarily work in the harshest environments, the devices can still be subject to harsh environments simply by human error – accidentally dropping the device in a washing machine, leaving in the hot sun etc. – exposing risk to the data on drive.

Understanding your needs and the potential impact that exposures may have on your organization or business will help pinpoint your tolerance for data breaches. The greater the potential damage, the greater the need for the highest levels of security. With all the security breaches today, being good enough isn't often suitable.

> With all the security breaches today, being good enough isn't suitable.

Understanding What Keeps Data Safe

It's one thing to pinpoint why you need security. It's another to understand the options available to you to help you meet those needs. This requires digging into the technology, architecture, physical composition, and management of storage devices. The more you know, the more it becomes clear why some solutions protect data more persistently than others, and why those solutions can cost more.

Encryption and authentication. These are the common denominators for all systems regardless of the security level.

- **Encryption** transforms the data on the storage device so that an intruder cannot decipher the information.
- **Authentication** controls access to the information by requiring users to provide passwords or biometric identification (such as a fingerprint). Some devices require multiple forms of authentication.

Encryption comes in many forms and different algorithms, but all are designed around a fundamental premise: To create an algorithm with so many permutations that it would take thousands of years to solve them, even when using the most advanced current computing power. To ensure that this is true, current encryption algorithms use long encryption (or crypto) keys that make them exponentially more difficult to crack than shorter ones.

Hardware design. The way a device's security is implemented is just as important as the encryption technology utilized within it. Some devices store the crypto key in clear readable text in the flash memory itself such as when BitLocker encrypts a USB key, while others store the crypto key on a separate secure cryptographic module.

- **Readable clear text in the flash.** This means the crypto key is stored in the flash memory or hard drive built into the device, which makes it easier to read by people trying to get to the stored data. **Many devices that meet the FIPS 140-2 Level 2 security standard store their crypto key in this manner, or they obfuscate it using a key derived from the password.** In either case, the key is usually stored in the same memory area as the rest of the data. It is a lower-cost approach that offers less protection than devices with a cryptographic module. (See Figure 1.)

- **On a chip.** More secure systems keep the data encryption key out of the main device memory and store it on a separate cryptographic module, commonly used in smart cards. The chip is shielded in a tamper-resistant environment. **Devices that meet the more stringent FIPS 140-2 Level 3 security standard store their encryption key on a cryptographic module in this manner.** (See Figure 2.)

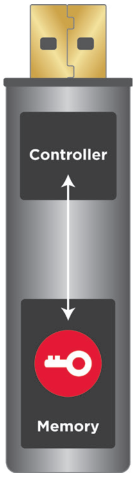

Figure 1.
Drives that store encryption keys in the clear make it easier for hackers to read the key and steal the data stored on the device.

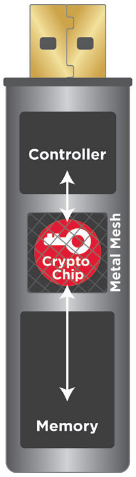

Figure 2.
Drives that store encryption keys in a separate tamper-resistant cryptochip module are significantly more difficult to compromise. They tend to feature unique defenses, such as a metal mesh cladding and self-destruct function in case of physical attacks.

When 'Secure Enough' Isn't Secure Enough

If a device uses a well-formed long key such as AES 256, most thieves and hackers have slim hope of accessing encrypted data. The "man on the street" with rudimentary hacking skills will likely be foiled by 128-bit or 256-bit encryption, even on devices that store encryption keys in a clear readable form in the flash drive.

The man on the street, however, is not an organization's most serious threat. Researchers have recently seen an increase in incidents that suggest a precipitous rise in the sophistication of data thieves. State-supported corporate espionage, identity theft cartel activity and highly organized hactivism are just three examples of more serious threats to valuable corporate or customer data. These are not individuals who will lamely guess at passwords until they get lucky. They have the resources to outsmart all but the strongest security protections. In fact, given enough time, money and expertise, it's possible for hackers, identity thieves and corporate spies to access data protected by AES 256-bit encryption. This could occur in many ways including these two examples: either accessing the encryption key by opening the drive and attempting to physically read the key directly from the flash memory chip on which it is stored, or accessing the encrypted data by deriving the password used to protect the crypto key.

Protecting against physical access. With the right equipment and know-how, hackers can read the encryption key directly from memory by physically opening up the device to access the components on which the encryption key is stored. This could be compared to storing the encryption key on the hard drive in a PC. This is where the difference between devices using a dedicated secure cryptographic chip to protect the crypto keys, compared to just using the unsecured flash memory. For example, some cryptographic chips use a metal mesh cladding that acts as both protector and sensor, and an automatic self-destruct function that is set in motion whenever the mesh senses it has been compromised. Within those drives, if a hacker tries to physically open up the device and peel off the epoxy coating to get to the semiconductor die directly and read the memory inside the smart card chip, the chip when powered up, will sense that the surrounding metal mesh has been tampered with and will render the chip non-functional. Successfully hacking these devices is no simple feat, if it's possible at all. Several research papers describe the costly equipment required to attempt such a hack, though the results they describe are more academic than actionable. Devices that simply store the password hash and crypto keys in the storage flash memory lack this protection.

Protecting against password attacks. Hackers attack passwords because there will be fewer possible password permutations than encryption key permutations. For this reason, figuring out the password for a device is much faster than directly going after the data encryption key. Devices that store the password hash and encryption keys in the same memory as the rest of the data, offer an opportunity for knowledgeable hackers to mount a so-called "brute force attack" or "dictionary attack." In a brute force attack the attacker would try every permutation of characters until the password is found, while in a dictionary attack the hacker would use permutations of likely character combinations a user would use in order to guess the password.

Hackers know that most password-protected devices defend themselves from password guessing by allowing only a limited number of wrong password attempts before locking the device – a reliable defense against the man on the street. But hackers also know that the device stores a "one way hash" of the correct password somewhere in the storage area. (See Figure 3.) This knowledge gives hackers an opportunity to make as many password guesses as they like.

To achieve this, hackers create a "development rig" – an environment in which the raw storage device is hooked up to components that allow hackers to bypass any security that exists in the device's USB controller. In doing so, they can take full control over the storage memory and mount their dictionary attack on the hash of the password at their leisure. In most cases, they will be able to ascertain the correct password in a matter of days. Or they could mount a so-called "brute force attack" in which software systematically checks all number combinations until the password is found. A brute force attack set for a six-digit password can be mounted in seconds.

In addition, if a device has no physical access defense, the data can be copied allowing for 1000's of identical attacks to be mounted simultaneously greatly reducing the potential time to crack – this is happening today.

Due to these risks thousands of corporations, government agencies and intelligence operations rely on storage devices that meet the more stringent FIPS 140-2 Level 3 standard – devices that store passwords and encryption keys in a tamper-resistant cryptographic module that is separate from the memory component. In addition, the strongest of these tamper-resistant cryptographic modules "count" the number of times an attacker tries to apply a password guess derived in a brute force attack before destroying the data on the device, reducing even more the possibility of successful access to the devices data.

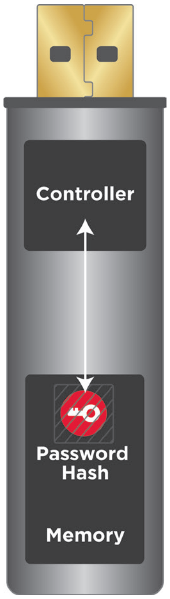

Figure 3.
FIPS 140-2 Level 2 devices are more likely to be hacked by mounting a password attack on the hash of the password, which is stored in the same memory as the encryption keys and the encrypted data.

The Value of Stronger Protection

Of course, it's the job of IT security professionals to make these attacks as difficult as possible. Only if the compromised data has no impact on the organization– which is rarely the case– should an organization's sole objective only to be compliant with the regulations it is obliged to follow. If that is the case, and all possible scenarios of potential risk have been thoroughly vetted, then virtually any device that uses industrial strength security is good enough.

Ruggedized devices. For most storage devices, ruggedizing is more of a packaging and marketing exercise than a true value-add. In most cases, the worst-case scenario these drives will face is being dropped in the sink. Truly ruggedized drives, however, are resistant to shock, dust and an accidental trip through the washing machine. For military and intelligence users, the ability to withstand these mishaps could mean the difference between lives and identities lost or saved.

Internal threats. Not all threats to data security come from outside the organization. Most data leaks are actually caused by employees – either through their own carelessness or by knowingly sharing confidential information for money or to cause the organization harm. For security conscious organizations, these devices need to have the capability to be remotely managed. When they suspect a device has gone "rogue," the organization must be able to remotely disable or destroy the device, thus rendering the content inaccessible and deleted.

Here, devices with "good enough" security offer little value and very limited capability. More secure devices, however, provide an array of management capabilities, and even the choice of managing via a cloud-based solution or on-premises management platform.

Deciding What’s Right For You

Understanding your business needs and goals – and how today’s range of storage devices helps you meet them – are essential to determining what’s right for you.

- **Compliance is everything.** It’s possible that your mobile storage security needs are basic, and that simply complying with data security regulations is your overriding concern in choosing your storage platform. In these cases, losing data would be inconvenient but not damaging, and central management of storage devices is not essential to maintaining the integrity of your operations. If this describes your organization, you would be wise to invest in the least expensive option that enables you to reach the compliance level you’re obliged to meet. In most cases, a drive with FIPS 140-2 Level 2 may be sufficient.
    - It’s important to note again that if you decide on this level, you should vet all possible data breach and data loss scenarios and the toll it would take on your organization. With all the security breaches today, being good enough isn’t often suitable for enterprises or agencies.
- **Security is vital.** If your mobile workers carry data that would prove costly or otherwise disastrous if lost – customer data, intellectual property, passwords to enterprise systems and databases, corporate plans and documents – then it’s advisable for you to invest in solutions designed to defend against sophisticated, knowledgeable and well-financed intruders. In these cases, a FIPS 140-2 Level 3 certified device equipped with a tamper-resistant, self-defending cryptographic module offers your best defense. It is also advisable to choose a device that comes with a centralized device management platform that allows you to keep control of usage and access policies, and even remotely disable or destroy lost or stolen drives.
- **Secure, rugged and reliable are all essential.** Some organizations – such as military and intelligence groups, in addition to industries like oil and gas exploration and sterile healthcare environments – subject their devices to more than just an unanticipated wash cycle. Here, an encrypted device whose components are sealed in epoxy and tested to withstand harsh conditions is a must.

The World's Most Secure USB Devices

Organizations the world over turn to IronKey for USB storage solutions that provide persistent protection – on secure flash drives, hard drives, Windows To Go devices and through an advanced cloud-based or on-premises device and policy administration platforms.

With IronKey solutions, you can not only meet rapidly expanding compliance requirements, but confidently move beyond to safeguard and control confidential enterprise and agency data thanks to some of the most advanced authentication and encryption technologies available. Key security features of IronKey solutions available for secure USB include:

- Secure, military-grade hardware encryption
- FIPS 140-2 Level 3 validation
- Centralized management supporting remote wipe/disable of lost or stolen drives
- Multifactor authentication including biometric
- Built-in password protection policies
- Ruggedized, waterproof enclosures that resist physical break-ins and are tamper-evident
- Virus/malware protection

For more information about FIPS 140-2 Level 3 certified USB storage solutions from IronKey, ironkey.com

Summary

In most cases, secure enough for compliance just isn't secure enough to protect valuable assets like corporate or customer data. Once your organization assesses the real cost of data loss to your business and your future, then you may well realize that compliance alone is no longer your primary concern. And if the price of data loss is significant – in dollars, intellectual property, or reputation – the added investment of a stronger USB device easily makes sense.