Whitepaper

PC Encryption: A Practical Guide for MSPs

WHY your clients need it and HOW you can offer it

March 2017

Introduction

Any company or organization that holds sensitive data has a critical need to ensure that the information stored is properly protected. Businesses that collect personal, private information – data that is used to deliver superior service and make customers' lives that much easier – nevertheless enter into a trust with consumers. In all-too-common cases when data breaches occur and make headlines, reputational damage ensues. And, when data breaches occur in industries where governmental regulations are involved, organizations found to be careless in safeguarding data can also face substantial fines. In other cases the issue is not customer data but sensitive intellectual property belonging to a company, the secrecy of which is essential to that business' competitive advantage. Proper protection of data can also open the door to new business relationships, especially with institutions that have policies of exclusively selecting vendors and partners that meet certain careful criteria when it comes to data security practices. But in all these cases – whether an organization is incentivized to invest in data security in order to protect their reputation, to meet regulatory requirements, to safeguard intellectual property, to prepare for new business relationships, or for any other reason – data encryption is the first and most critical tool in the data security playbook. Importantly, implementing encryption does not have to be difficult or cumbersome to an organization's operations. In fact, encryption functions best when it is unobtrusive and when it is, more or less, invisible to users.

Data Breaches

The news is rife with high-profile examples of these data breaches. While the press gives the most coverage to black hat breaches stemming from hacking and malware intrusion, in truth, data from Privacy Rights Clearinghouse finds that since 2005, a full two-thirds of breaches have resulted from user/employee oversight or malfeasance including lost and stolen PCs, mobile devices and electronic storage.

In such incidents from 2016 alone:

- The NFL notified thousands of players whose medical records may have been exposed after an unencrypted laptop and electronic storage device was stolen.
- The FDIC reported that an outgoing employee breached the data of 44,000 customers by downloading it to a personal storage device.
- Healthcare provider Premier Healthcare reported the theft of a laptop containing the sensitive personal and clinical information of over 200,000 patients.

These exposed records might consist of social security numbers, usernames and passwords, financial or medical information, corporate intellectual property or client lists, and other digital information that amounts to a violation of privacy and puts individuals and organizations at risk for identity fraud and losses.

However, it's important to know that while data breaches of larger magnitudes grab headlines, it's actually small and medium-sized businesses that can suffer the most harm from them. For SMBs with less capacity to absorb hardships than larger enterprises, the reputational damage, financial pressure of a large regulatory fine, or loss of intellectual property from a data breach can be a devastating – and sometimes fatal – blow.

Keeping Criminals Away from Our Data

SMBs can often have the most to gain from implementing data security measures like encryption. The goal of data security is to keep criminals, corporate spies, disgruntled ex-employees, insider threats, and anyone else with bad intentions from accessing sensitive information. Encryption is a highly effective measure because it renders data such that even if it falls into a criminal's hands, they can't read it.

Other measures working in tandem with encryption are important to robust data security as well. While encryption is a powerful tool, the practices of an organization's employees and the safety with which they handle data and minimize threats are just as important. Keeping employees well trained and aware of their responsibilities with data – such that they do not put their systems and devices at risk – are key components to achieving effective data security.

For the purposes of this white paper we'll focus on data residing on devices – hard drives, smartphones, tablets, external drives – where it ought to be encrypted in case those devices become lost, stolen or otherwise accessible.

The "Nuts and Bolts" Of Encryption

Encryption is a powerful defense for data at rest when a device's power is off, and the password to bypass it is secure. The Department of Health and Human Services offers a useful definition of satisfactory encryption with its HIPAA security rule, describing it as "an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key...and such confidential process or key that might enable decryption has not been breached." In short, encryption is essential to data protection and rendering private information unreadable, but it has limits. If a device is stolen or left unattended with the power on and login credentials entered (or if the password is known or can be learned), then encryption is no longer an effective defense.

Employees will always seek out ways to be their most productive, and this means that thoughtful training in best practices and the importance of data security is needed in order for most encryption regimens to be truly effective. Bad passwords effectively negate encryption; too often employees will write down their passwords in close proximity to the device they need to authenticate, or have passwords written on the surface of the USB devices they need to read. Devices left unattended during open sessions leave data fully exposed. In some scenarios, formerly authorized users become unauthorized (ex-employees, for example), but their access is not revoked as it ought to be. There are also cases like the one last year at Coca-Cola, which suffered a data breach when an employee took home 55 work laptops – likely with intentions beyond just getting some work done over the weekend. Employees should be trained in proper password security and vigilance over their credentialed sessions, and organizations should demonstrate proper diligence in managing access controls, as well as keeping track of all of the company or employee devices with access to sensitive information.

However, in the end it is most effective for organizations to support workers by taking the responsibility for data security out of their hands as much as possible. Data controls than can be implemented remotely are able to provide organizations with the capabilities they need to delete sensitive data from compromised devices and to revoke access to users in the case that credentials are compromised (either because login information has been stolen or because an employee has gone rogue.) It's a best practice to remove access for employees and contractors when they leave the company for whatever reason - companies need the tools to cut off access and remove company data from ex-employees' own personal devices as well. The right way to reconcile the need for data security with the needs of employees is to implement security that steps so lightly that workers forget it is there while ensuring it is powerful enough to be effective – and also training employees to understand why data security is so critically important.

Who Is Buying Encryption?

So, which organizations are investing in encryption? Let's take a look at some of the primary motivations:

When encryption is necessary (or all but necessary) to meet compliance regulations

Organizations subject to regulation – such as those in the healthcare industry covered by HIPAA, the financial industry covered by FINRA, or even the land title insurance industry where ALTA compliance is key – most often must implement data encryption in order to be in good standing. Regulators and agencies in certain industries that deal with private information have recognized that data breaches continue to occur and to carry the risk of devastating harm to customers, and as a result have adjusted required practices and regulatory audits to specify encryption as a solution. Again, the fact that some organizations are compelled to invest it data security solutions due to a begrudged necessity to follow legal compliance requirements is unfortunate, because a mindset that doesn't also encourage employee training and a valuing of data safety can certainly reduce the effectiveness of any measures put in place.

HIPAA

HIPAA, the Health Insurance Portability and Accountability Act that legally requires the personal health information (PHI) of patients to be secured, means that unencrypted data represents a large risk for both medical facilities and the MSPs that serve them in a data security role. PHI holders – medical practices, pharmacies, labs, MSPs serving them, etc. – are not directly mandated by HIPAA to encrypt data, but they must take "reasonable measures" toward data security, and encryption is established as such a measure. In the event that PHI is lost, failure to report the data breach to authorities is potentially a criminal event. If authorities discover non-compliance, such as lost medical records going unreported, it's possible for the case to be referred to the Department of Justice for prosecution. When a medical facility is found to have a data breach, the MSP it works with is certain to be brought into any regulatory audit to explain the technical aspects – not a desirable situation. For the government, HIPAA enforcement is a priority (and, frankly, a revenue stream). Even small organizations need to be protected. One frightening story that illustrates this is the $50,000 HIPAA breach settlement by Hospice of North Idaho, a respected non-profit that suffered the theft of a single unencrypted laptop containing patient information. This enforcement event proves the importance of protecting PHI and the risk to any organization – no matter how small or sympathetic – if they fail to do so.

Penalties for failing to properly safeguard PHI are known to reach into the mid-five figures for each offense, whereas effective encryption products like SimplySecure carry a relatively low monthly fee, making going without proper protections a penny-wise but pound-foolish proposition. Because regulations included in the related Health Information Technology for Economic and Clinical Health (HITECH) Act put legal responsibility on an MSP whenever PHI or a device with PHI is in their care, MSPs would be wise in taking prior steps to encrypt any data that could transfer to their possession in order to ensure against regulatory action, regard- less of the client's position on the matter. In fact, a good number of MSPs providing SimplySecure make it a mandatory part of their service packages in order to cover this risk of fines.

HIPAA and the importance of the Business Associate Agreement

HIPAA's complexities even amount to a paradox for MSPs when it comes to this fact: an MSP that has access to a HIPAA Covered Entities (CE) PHI is required to be HIPAA compliant as well. However, this is a Catch-22: how can a business that hires an MSP to handle its data security and implement HIPAA compliance possibly have the expertise to judge whether the MSP's own practices around HIPAA are adequate? Given this situation, the best way forward is for MSPs to ensure their own HIPAA compliance on behalf of the organizations they serve by making it part of their service duties. What HIPAA requires of a business is that any "business associate" – meaning any entity that has or has had access to PHI entrusted to a HIPAA-covered business – must do its work under a business associate agreement (BAA). This BAA requires the business associate to work within data security requirements delineated by the HIPAA-covered organization. It also calls for the implementation of technology measures such as encryption to secure PHI in accordance with certain provisions of HIPAA's security rules. The kinds of business associates who must operate under such as agreement can include all types of MSPs, from technology providers to medical claims processors, data analysts, providers of quality assurance, billing and collections, practice management, legal services, accounting, and consulting.

The BAA establishes the legal responsibilities of the involved parties and gets specific about how PHI may be used and handled. It also touches on breach-preventing data protections that the business associate is required to have in place. Per HIPAA requirements, the BAA must also legally require the following: that the business associate report breaches or unauthorized uses of PHI, that any subcontractor used by the business associate is also legally bound by the BAA, and that the business associate must return or destroy all PHI when the BAA is terminated.

As a best practice, MSPs should proactively offer and commit to BAAs when dealing with any client covered by HIPAA, both for the client's benefit and their own. As the more knowledgeable member of the relationship, MSPs must be responsible for making sure both themselves and their clients conform to HIPAA's strict guidelines. MSPs must understand that failing to fulfill HIPAA's BAA requirements means exposure to fines and penalties as severe as those they've been hired to protect their clients from. HIPAA enforcement fines are often in the five figures for a single violation, plenty large enough to act as a knock out punch for many small or medium-sized businesses.

MSPs should explain the HIPAA paradox to clients and demonstrate how they resolve it by offering an airtight BAA. They should consider it just another part of delivering fully HIPAA-compliant data protection. MSPs that take this tact can carve out an important competitive differentiator in the marketplace. Providing a seamless solution that showcases their professional knowledge and worthiness of trust, one that their clients might not have even know they were legally obligated to have.

FINRA

Similar to HIPAA, the Financial Industry Regulatory Authority (FINRA), has indicated that firms in the financial industry that deal with sensitive personal data must take steps to effectively secure that data, or else face substantial fines and criminal punishments as a means of enforcement. As an example proving this point, in 2015 FINRA reached a settlement (that included a public censure and $225,000 fine) with Sterne Agee, stemming from the loss of a company laptop containing the unencrypted confidential financial and personal information of more than 350,000 customers.

A definitive FINRA report on data security practices lays out in no uncertain terms that the organization is and will be active in carrying out enforcement actions against firms. (And executives themselves aren't immune from being found personally responsible in cases where customer data is poorly handled or

breached.) As it appears that FINRA is looking to take a harder line in response to the fact that breaches of this nature continue to occur, it would follow that prudent financial firms ought to take a harder look at their data security strategy and ensure their houses are in order when it comes to acting in line with FINRA's recommendations.

FINRA's report does offer principles and practices for firms to follow, the result of a year-long study of cybersecurity programs across a cross-section of financial firms – including large investment banks, clearing firms, online brokerages, high-frequency traders, and independent dealers. FINRA demonstrates an accurate understanding that data security is not one-size-fits-all, and that every firm requires a program custom-fit for their functions and internal structure. In an example case study, the report details an enforcement action against a firm involved with a data breach and theft of around 200,000 customer profiles, including names, bank account numbers, Social Security information, dates of birth, etc. The firm had done penetration testing of its systems, but FINRA determined that the scope of their tests did not adequately detect vulnerabilities in their password management and encryption procedures, which allowed for a database of customer data to remain unencrypted and contributed to the breach. Making a good-faith effort isn't good enough; the firm was fined $375,000.

In other case studies, FINRA cited these factors as reasons for enforcement actions: "failure to safeguard confidential customer information," "inadequate user access restriction," and "failure to rapidly remediate a device the firm knew was exposing customer information to unauthorized users." For firms looking to remedy deficiencies in these areas and avoid similar enforcement actions, FINRA recommends implementing powerful technical controls over data, as well as putting in place policies and procedures that support these data security efforts. Financial entities need the ability to remotely monitor sensitive electronic data across all employee and partner devices that have access, and to promptly terminate access when a device is compromised – as was the case with Sterne Agee and the missing, data-laden laptop.

FINRA notes the central importance of encryption in protecting data, and recommends encrypting both data at rest and data in transit. Properly training staff is noted as a key feature for a successful cybersecurity program as well, as employees are indeed walking security risks if not made to understand proper procedures for handling sensitive customer data (and information such as passwords). In today's bring-your-own-device world, employees may be working with the firm's sensitive customer data on their own laptops, phones, or tablets, and it's critical that they know how to handle that access responsibly. Just as importantly, the firm must also have data controls with the ability to revoke access and protect that data remotely if the potential for a data breach arises. Avoiding enforcement actions and securing customer data must now be a top concern of financial firms, not only to avoid steep fines but also to avoid the reputational damage that comes with a public declaration that a firm cannot protect their customers' private data.

Other compliance regulations

Many other industries and localities have specific requirements around data security that are enforced by various industry associations or governmental agencies, and organizations must be careful to maintain an awareness of those compliance regulations which apply.

Retail merchants touch upon a high volume of sensitive data as customers make payment transactions, and must follow strict rules to keep this customer information safe. To govern the practices of merchants and any processors of payment card data, the payment card industry's Security Standards Council, founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., has implemented the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS delineates requirements by which cardholder data must be stored, processed and

transmitted, specifying strong access control measures, password safety practices, and an emphasis on robust encryption.

In the land title insurance industry, the American Land Title Association (ALTA) – the key trade association for businesses in the industry to which almost all title insurers belong – has recognized the need for precise data security standards governing practices at these companies. ALTA has begun making membership contingent on adhering to more specified guidelines, and has adopted standards requiring that businesses have enforceable, auditable, and persistent plans for making sure that sensitive data is either completely absent from devices that are at risk, or that such data can be made unreadable, inaccessible, or indiscernible – all but requiring that encryption be in place.

At the state government level, 46 US states as well as the District of Columbia have enacted breach disclosure laws which mandate the protection of consumer data, permitting customers injured by a violation of the law to recover damages. States such as Massachusetts and Nevada have laws even more aggressive in protecting citizens' personal information, explicitly requiring that any organization conducting business in-state must encrypt sensitive personal data. As more states consider and enact similar legislation, organizations must be careful to understand the laws and requirements that pertain to their practices, in order to avoid both hefty fines and harmful reputational damage.

When encryption is good for business

One segment of the organizations investing in encryption includes those motivated by the importance of protecting data as a positive business practice. Data security is in fact a valuable and cost-effective business asset.

Here's an example of this: a business in the chemical industry, now using an MSP providing the SimplySecure service was concerned with protecting its intellectual property (which employees would carry on portable devices). These included laptops and smartphones used by traveling salespeople and workers in the field, devices holding proprietary chemical formulas, client lists, and other sensitive data. Leveraging cloud-based SimplySecure, the MSP was able to protect the firm's proprietary data through encryption and the ability to remotely lock and wipe data from compromised devices. In this case, implementing data security has provided more than just peace of mind – it has saved the company from major breaches a few times. Devices containing sensitive data have been left behind in taxis and airplanes, and, in every instance, the data encryption and data wiping capabilities in place have prevented leaks that could have done untold damage to their business. The company's data security strategy helps shield it from insider threats as well, protecting each device with encryption at the user level. This means that an employee (e.g. domain administrator) with credentials and bad intentions could enter the CFO's office, and authenticate (or get access to) their laptop but not have access to the sensitive data. (If they could see that protected financial information, they might discover how the company's investment in data security has paid for itself by keeping company secrets secure.)

Many businesses find that implementing encryption opens the doors to new business partnerships and opportunities as well. For example, a company serving clients in the financial field found that, in the aftermath of the JPMorgan Chase hack and other similar incidents last year, many large financial institutions adopted a policy of strict data security guidelines – not only for themselves but for any vendors they do business with. In this case, the company in question began using SimplySecure to fulfill this business development requirement, and in turn was able to secure valuable relationships because they could secure valuable data.

MSPs should recognize the positive reputational advantages of encryption and data security for their customers. SimplySecure helps avoid data breach incidents that can devastate reputations and customer trust. Wise customers will count these solutions as important business investments as well. Unfortunately, the reality is that this customer segment is only starting to grow, and the syndrome of

believing “it’s never going to happen to me” about data security issues has ruled the day. MSPs should educate their customers about not only the importance of meeting any pertinent compliance mandates, but also about the opportunities that may become available when implementing data security practices that achieve a level of competitive differentiation.

The challenges of supporting or offering encryption (…until now)

So why is encryption not enforced on every PC, Mac, iPhone and iPad, Android, and USB storage device? Unfortunately, in going about the task of crafting data security strategies to fit our brave new device world, companies often gravitate toward one of two extremes. Many companies tend to overlook or ignore the need to comply with regulations, overwhelmed at what seems like a monumental chore. This approach seems perfectly reasonable, of course – until a data breach occurs.

Others, meanwhile, overestimate the complexity of the issue. They impose a tangled mesh of measures that prove costly and difficult to implement – developing a separate security program for each platform or operating system in use, for instance. These security provisions can hinder the rich user experience afforded by the new generation of mobile devices, and can in the end undercut many of the advantages that led the company to adopt a more flexible, device-diverse work environment in the first place.

Poorly implemented and cumbersome solutions that make data security and encryption difficult for users certainly do not help matters. Some solutions require that users remember and follow certain procedures, such as remembering to put sensitive data in particular file locations, or using secondary authentication methods. With some less user-friendly solutions, the first pass at implementing encryption can take many hours. Some solutions may require internet connectivity in order to work properly, and deny users important access when not online. Some may increase system latency to a frustrating degree. Unfortunately, these difficult solutions have earned encryption a bad reputation for generally hindering usability and user productivity – and being a pain to manage on the IT side as well. But the truth is this doesn’t have to be the case.

Issues with full disk encryption

For MSPs, software-based full disk encryption (FDE) – the traditional de facto method of implementing encryption – doesn’t readily lend itself to remote system management (pre-boot), making it incongruent with how MSPs provide value to their customers. The encryption wrapper of FDE means that MSPs cannot access or troubleshoot issues with the solution without using special tools or resorting to remediation at the hardware level. It is not possible to execute important remote management functions without user or administrator assistance either, limiting virtually any activities an MSP might provide: remote powering on, logging in to perform updates, patches, diagnostics, reporting, etc. FDE also introduces compatibility issues for MSPs, with the encryption essentially locking in whatever operating system is in place on a machine, and leaving no room to maneuver if that OS isn’t compatible with the MSPs other solutions. Finally, FDE usually consists of purchasing software to be installed on machines, and sometimes on the server-side as well. However, this upfront payment model is a poor fit for the way MSPs do business and how MSP customers consume services.

The solution: Beachhead's SimplySecure

There is a better solution for MSPs looking to provide data security and encryption: cloud-based SimplySecure. Beachhead's SimplySecure offers unobtrusive web-managed encryption and data security for all company and employee-owned devices in use within an organization, including PCs, laptops, phones, tablets, and USB storage devices. MSPs can provide SimplySecure as a monthly-managed service, with no hardware or software purchases or long-term commitment required. SimplySecure fits within an MSP's monthly pay-as-you-go programs as well, and allows MSPs to completely handle every aspect of the solution on behalf of clients, from deployment to management. SimplySecure's remote cloud-based management means MSPs can handle troubleshooting and remediation remotely as well, translating into less downtime and maximizing employee productivity for clients. Importantly, the SimplySecure platform plays nice with other services that MSPs may provide.

Using SimplySecure, an MSP can provide protection for mobile devices, all under the same management console, and with the same inherent security benefits. The worry and hassle-free SimplySecure service is the only monthly pay-as-you-go service that not only encrypts data, but can also give you the ability to lock out a user or kill a device completely in the event that this becomes necessary. For those unfortunate scenarios where encryption is not enough – when a password is compromised, when devices have open sessions with credentials entered and fall into the wrong hands, when malicious former employees have access via their devices – SimplySecure can be thought of as encryption plus, delivering the means to cut off these avenues that would otherwise result in data breaches. Having proof-positive evidence to show your customer that a computer was wiped under one of these circumstances will establish you as a savior with which they will want to maintain a lifelong relationship. SimplySecure also offers full reporting, with read-access to the console, which you have the option of providing. While encryption alone may seem like a passive technology, the SimplySecure platform allows an MSP to continually provide demonstrable value in the form of superior data protection, and that helps MSPs and their clients sleep better at night.

Questions, comments? Write Cam Roberson
croberson@beachheadsolutions.com
408.496.6936 x6866