

WHITE PAPER

Data Protection Security Best Practices

Sponsored by: Iron Mountain

Charles J. Kolodgy

Gerry Pintal

October 2008

IDC OPINION

You know that knotted feeling you get in the pit of your stomach when you realize something is dreadfully wrong? That is the way thousands of people feel each day when they realize they have lost their laptop computer. It is estimated that nearly 1,700 laptops are lost each day at airports around the country. Many more are left in taxi cabs or stolen outright. Desktops are not immune to loss as some criminals have broken into bank branches, not to take cash, but to cart off computers. Today's computers are more than productivity tools; they are huge filing cabinets with extremely valuable or irreplaceable information. A stolen laptop can contain the Social Security numbers and other personal information for millions of people, the plans to a new product, or secret military information. Whatever the situation, be it small or large, ensuring that information is protected and that it is available to the user is paramount.

These facts and many others reinforce why organizations cannot take a laissez-faire attitude toward data protection. Organizations, especially those entities entrusted with other people's personal information, must take special care of that data. Governments have realized this need and have passed data protection legislation and are promulgating data protection regulations to encourage better protection of data. IDC believes organizations of all sizes must recognize that enormous business risks are associated with the data they have and that it must be protected. Encryption is one of the most effective methods for protecting business information, personal data, and intellectual property. When coupled with other data protection security best practices, it can provide organizations with considerable benefits.

Comprehensive data protection security best practices provide for the encryption of data on a machine, using full disk or file-level encryption, and ensure that data is preserved. Through the use of backup, data is retrievable should it be corrupted or lost. The final part of the data protection strategy is to ensure that data is properly destroyed. In the physical world, you can shred or burn paper, but in the electronic world, it can be harder to ensure that data is destroyed. A number of components are associated with data protection security best practices, so it is important for enterprises to have a trusted partner that offers all aspects of a total data protection program.

Iron Mountain, a leader in data preservation, offers DataDefense in its PC backup solution. The various components of this option provide all of the features required for complete data protection capability. The suite of DataDefense services provides a broad spectrum of data protection capabilities with centralized management that allows enterprises to enforce corporate data protection policies throughout the data's life cycle.

IN THIS WHITE PAPER

In this white paper, we highlight the ever-growing need for data protection security best practices for enterprise computers. Data protection security best practices include the encryption of data to prevent it from falling into the wrong hands, the preservation of data through backups, and the destruction of data when it is no longer required. The document discusses the data and information security issues associated with personal computers, explains the overall benefits and challenges of encryption as an effective mechanism in mitigating the increasing threat of lost business and personal data, and presents the overall benefits of Iron Mountain's DataDefense offering.

INFORMATION RISKS BUSINESSES FACE

Where do the most valuable assets of a company reside? Are they stored in a bunker facility, in a safe, or in the bowels of a datacenter, protected from prying eyes? If you are Coca-Cola or KFC, you do lock down the famous recipes that provide your company's uniqueness. Colonel Sanders' handwritten recipe of 11 herbs and spices is kept in a safe, and only two executives have access to it. Coca-Cola's soda formula is also not available in digital form. However, in today's information age, the most valuable assets of most companies exist in digital form. Even for Coca-Cola, "information is the lifeblood of the company," as stated in a letter from the CEO to employees after a trusted employee tried to sell valuable trade secrets.

The information age has turned information into the new currency. Bits have as much, if not more, value than comparable assets in the physical world. Digital information is easy to create, copy, modify, replicate, and disseminate. But it is difficult to control or destroy. Information has value when it can be used for business purposes and when it can be shared among people who need it. For the information to remain valuable, it must be available to those who need it and kept away from those who would misappropriate it. Loss of data or loss of access to data puts the enterprise at risk. For this reason, the protection and preservation of data is an increasing focus.

Data Risk Environments

Technology

A number of factors are expanding the risk to enterprise data. A risk factor that might not be obvious is the growth in today's ubiquitous and indispensable business tool — the laptop computer. Nearly every employee traveling for business purposes is toting a laptop. IDC forecasts that portables will reach 68% of the total PC volume in the United States and Europe by 2011. The laptop is the information lifeline for modern corporate executives, professionals, sales staff, and service-oriented professionals. Without laptops, they would find it almost impossible to function at the levels of efficiency and effectiveness to which they and their companies have become accustomed. Laptops facilitate their ability to continue performing business activities while away from the home office and provide these "road warriors" with the connectivity, tools, and data required to do so effectively. With mobility and productivity as the principal driving forces behind laptops, we are seeing them proliferate throughout the enterprise, supplanting standard desktop computers.

Another less than obvious factor that expands the risk environment is the growth of memory. Laptop computers may now be equipped with hundreds of gigabytes of disk storage, making it feasible to carry sizable amounts of data in files and databases. In addition to large internal hard drives, removable storage in the form of USB-compatible flash memory has contributed to increased productivity. These compact memory devices are capable of storing gigabytes of data in packages not much larger than a door key. In addition, they are frequently shared with colleagues as well as outside business partners and customers.

The expansion of laptop deployment and increasing storage create risk by vastly expanding where corporate data can proliferate. People are much more mobile; they want the information wherever they are working, be it in the office, in a hotel, or at another facility. Laptops with large internal hard drives and removable storage are highly prone to being misplaced, lost, or stolen. There are numerous examples of these losses. Some of the worst cases are provided in Table 1.

TABLE 1

High-Profile Data Losses

Date	Enterprise	Impact
February 2007	U.S. government agency	A portable hard drive that contained personal information, including Social Security numbers of about 535,000 veterans, was stolen or missing.
August 2007	Financial information services agency	A laptop containing financial information on as many as 280,000 retirees was stolen from a consultant who took the computer to a restaurant.
September 2007	Major U.S. retailer	A laptop containing the personal information of approximately 800,000 people who applied online or by phone for store positions was stolen from the offices of a third-party vendor that manages job applicant data. Social Security numbers were included in the information on the laptop.
October 2007	Major U.S. retailer	A laptop computer containing about 10,000 employees' personal data was stolen from a regional manager's car. The computer contained names, home addresses, and Social Security numbers of certain employees.
January 2008	Major university	A hard drive containing the Social Security numbers of nearly 40,000 students, alumni, faculty, and staff was reported stolen from the Office of Student Affairs.
June 2008	Major university	A laptop containing personal information of up to 60,000 current or former employees was stolen.
July 2008	Communications company	12 laptops were stolen from an office. One of the laptops contained the Social Security numbers, names, and birth dates of 9,000 current and former employees.
August 2008	U.S. government agency	A laptop with the records of 33,000 individuals enrolled in a popular airport "trusted traveler" program was reported stolen. Two days later the computer was found in the same office from which it was supposedly stolen.

Source: IDC, 2008

Theft

All of the cases in Table 1 centered on the computers being stolen. Theft of data is a huge risk. Perpetrators are seeking financial gain that focuses on high-value information that companies possess. With employees roaming the world carrying laptops loaded with confidential data, criminals have become aware that laptops represent easy targets of opportunity. Initially, laptops were seen as low-hanging fruit because of their inherent street value. More recently, however, thieves have been targeting portable systems not only for the resale value of the hardware but also for the confidential personal and business data they contain. Even if the owner has taken precautions to password-protect a laptop, tech-savvy criminals who acquire the system are able to easily crack the username/password protection or simply remove the hard drive and extract the data. Armed with sophisticated software tools, they can completely bypass operating system access controls and gain full access to all the data stored on that drive.

The fear of data loss through theft or human error is top of mind for executives. IDC's 2008 *Encryption Usage Survey* asked 349 professionals to pick the top 3 threats to enterprise data. There was a clear delineation on what people saw as the top 3 threats. 66% of the respondents were concerned about defending against outside attacks to harvest data. The next most selected concern, with 60%, was protecting against exposing sensitive data or files to unauthorized users outside the organization. The third top concern was the accidental loss of devices or data by employees.

Damage/Ramifications

Laptop thefts have the potential to inflict serious deleterious effects on an enterprise's business and on the individuals whose personal information is involved. Much like a natural disaster, a lost or stolen laptop containing confidential data can be a very expensive and damaging occurrence for companies. A single laptop theft can result in:

- Significant notification costs
- Irreparable damage to the company's reputation
- Diminished brand equity
- Loss of revenue and reduced profits
- Regulatory fines
- Costly litigation
- Increased customer service and help desk activity

Protection Mandates

The threat of losing valuable data to thieves, competitors, or mischief makers should generally be incentive enough to protect data. Additional complications are not required; however, things are rarely easy. Many governments, in response to an explosion of data collection on individuals and increasing or at least highly publicized losses or thefts of personal and customer data, aggressively developed legislation directed at various industries that, because of the nature of their business, manage or process a great deal of personal, financial, and health information. Examples of such industries include financial services, healthcare, insurance, retail, business process outsourcing (BPO), and data brokering. Publicly held companies and, in some cases, privately held companies must now comply with regulations such as the Sarbanes-Oxley (SOX) Act, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Financial Institutions Examination Council (FFIEC) requirements, as well as with various state public disclosure laws. Additionally, important industry requirements such as the Payment Card Industry Data Security Standard (PCI DSS) increase compliance complexity. At a minimum, these enacted regulations require corporations to ensure the protection of consumers' personal and private information.

Privacy regulations in the United States have had a global reach, with similar regulations being put into practice on a worldwide basis. As a consequence, enterprises involved in international commerce may be subject to regulations mandated by all the countries in which they conduct business. In Europe, the Privacy and Data Protection Directive applies to all 25 member states. The Directive was enacted to allow any European citizen to be protected against misuse or abuse of personal information. For European businesses, data privacy protection is considered key for maintaining a positive reputation, and significant resources are dedicated to protecting data integrity and privacy. From healthcare to financial services, most organizations today are proactively addressing data privacy protection. Japan has its own Personal Information Protection Act and a version of SOX. There are many more instances of regulations mandating the protection of data.

The wild proliferation of these mandates raises the stakes for businesses large and small. Companies are obligated to achieve compliance with a wide range of data protection requirements. If they fail to do so, they may face business liability and the threat of criminal and/or civil penalties. Civil prosecutions can include substantial financial penalties. This requires the implementation of or the strengthening of data protection security best practices. Compliance with government regulations provides additional incentive to find the best method to prevent the disclosure of valuable information.

DATA PROTECTION SECURITY BEST PRACTICES: PEACE OF MIND

The data risk environment and protection mandates require best practices for data protection. The best technologies to achieve complete data protection are encryption and data backup.

Encryption

Encryption provides an effective technology for protecting business information, personal data, and intellectual property from disclosures due to lost or stolen computers. People don't do encryption on a whim; there have to be hard and fast reasons for taking this step, and undoubtedly, in today's environment, the justification is clear. Until very recently, encryption was primarily used to protect communications via voice, email, electronic file transfer, or remote access. As personal computers, laptops, the Internet, and wireless communications have become an integral part of our society, so too has the need for privacy and security for the vast amounts of personal data and information maintained and processed by these systems. Encryption is part of this solution. Ironically, not long ago encryption was being limited on the basis of national security, but now it is a vital building block for protecting data and provides the ability to meet the requirements of government and industry mandates. Although many regulations do not specifically mandate the use of encryption to prevent personal data disclosures, the language used in them strongly encourages encryption. Information that is lost or inappropriately acquired is not considered disclosed if it is properly encrypted. The final example in Table 1 illustrates this point. A laptop was reported stolen, but two days later it was found. A spokesperson said, "It was not in an obvious location." However, for two days, there were many concerned and anxious people. If that laptop had encryption, especially full disk encryption, the government agency's managers would have had peace of mind that the information wasn't exposed. Even after it was found, there is little to prove that the data wasn't stolen and the laptop returned.

Full Disk Encryption

There are various types of encryption and many types are required, but the form that provides the best protection for a mobile-based data risk environment is full disk encryption. Full disk encryption provides encryption of every bit of data that goes on a disk or disk volume. This includes the swap space and temporary files. With full disk encryption, the decision of which individual files to encrypt is not left to the users' discretion. It also removes human error should someone forget to encrypt sensitive files or, in the case of temporary files, not know where they are stored. Full disk encryption is more effective when it supports preboot authentication, and although it generally uses one key for the whole disk, some solutions can partition the disk to allow multiple users to "own" a part of the disk drive. When a machine is shut down, the contents of the disk are completely unreadable until authenticated again.

Data Destruction

Data protection security best practices require that data be protected throughout its life cycle, including when the data (or, in many cases, the device it is stored on) needs to be retired. As has been mentioned, destroying digital data is not that easy. There are a number of methods, including writing over a disk with 1s and 0s multiple times and physically pulverizing the disk drive, but one of the easiest methods is to utilize the capability within full disk encryption, which can provide immediate data destruction by destroying the cryptographic keys that reside in the master boot record (MBR). In this way, *all* data on that disk drive, even data that remains resident on the drive, but hidden, is also "destroyed" because it can't be accessed without the encryption key.

Characteristics of an Effective Encryption Solution

The deployment and use of an encryption solution can be difficult for organizations, so they must look for solutions that provide the best balance of security, manageability, and usability. There are many important components for organizations to consider when evaluating encryption products. IDC believes that an optimally effective encryption system should have the following characteristics:

- Provide central management and control
- Provide rapid deployment and updates
- Support an extensible key and policy management system
- Utilize a strong encryption algorithm
- Support strong/multifactor authentication
- Provide encryption for removable media
- Enable key recovery and data preservation
- Be transparent to the user
- Be able to decommission an encrypted machine

Information Backup

Backup is a key component of data protection security best practices because it ensures that data, be it critical or mundane, is preserved and recoverable in the event of physical loss of the medium holding the data, mechanical failure, or logical errors in data storage or software. For laptops, this is especially important because they are carried around, thus making them susceptible to loss or damage. Every time you drop a laptop, you pray it will still work. Backup is especially important when encryption is utilized. Should the hard disk fail, it might be impossible to recover the data, and should there be a logical error that corrupts the encryption key, the data is definitely unrecoverable. Utilizing backup with encryption is a logical and correct best practice.

THE IRON MOUNTAIN SOLUTION

For over half a century, Iron Mountain has been a leading provider of records management and data protection and recovery. Founded in 1951, Iron Mountain is a Fortune 1000 company headquartered in Boston. Its 2007 revenue was \$2.7 billion. The company has over 20,000 employees at over 1,000 facilities in 37 countries and hundreds of thousands of customer accounts worldwide. Iron Mountain started out as a physical records management company. Today, it offers records management, data protection and recovery, and information destruction for both physical and electronic data.

Over the past 10 years, Iron Mountain has invested billions of dollars to acquire 187 companies to expand its portfolio of services and global footprint. Since 2001, it has created Iron Mountain Digital (IRMD) to be the digital business unit. IRMD's service lines mirror Iron Mountain's physical business. There are tremendous opportunities associated with the explosive growth in digital content and compliance-driven information management. This business unit has more than 500 employees and more than 14,000 customers, of which 4,000 are large corporate customers. IRMD accounted for 6% of Iron Mountain's 2007 revenue, which equates to segment revenue of about \$160 million. IRMD has a much larger global presence than the company as a whole, with digital solutions deployed in 75 countries. According to IDC research, IRMD is a top 10 provider of data protection and recovery software, worldwide archiving software, and online backup services. Products from Iron Mountain Digital include Connected, LiveVault, and DataDefense.

Data Defense

DataDefense is a suite of products that offers an endpoint security solution that combines intelligent encryption with enterprise-controlled data elimination. It provides different encryption options and can also automatically eliminate specified data on lost or stolen laptops to prevent its compromise or misuse. It can effectively secure data even when the PC is offline and, most importantly, ensures organizational control of that data even when the enterprise has lost control of the device. DataDefense components include:

- DataDefense — data wiping and persistent shutdown
- DataDefense Encryption — ability to manage Microsoft's Encryption File System (EFS)
- DataDefense USB Flash — protects USB flash drives with encryption and data destruction
- DataDefense - FDE — full disk encryption

DataDefense is the perfect complement to Connected Backup for PC. Connected Backup for PC makes certain you'll always have your data; the DataDefense solution ensures no one else ever will. Customers can purchase DataDefense as a standalone solution or as a bundle with the Connected PC data protection solution.

DataDefense - FDE

Iron Mountain's DataDefense - FDE option provides enterprise-level data protection with a complete set of solutions that go beyond just encrypting every bit on a hard drive. With DataDefense - FDE, customers get a program that is reliable and easy to deploy and manage, has very low overhead, and provides robust data protection. This solution offers many useful features. The encryption utilizes the AES algorithm with a 256-bit key. It can support multiple users on one machine. Users are able to boot a computer with their own unique username and password. It also supports hardware tokens at preboot, which provides an even higher level of protection. Password changes, resets, and data recovery can all be delivered via a recovery console. Mobile media encryption is supported and the data can be shared between DataDefense - FDE users. DataDefense - FDE provides a quick and effective means of decommissioning an encrypted machine. The MBR (where the encryption key resides) can be securely wiped by an administrator. With no MBR present, there is no disk encryption key available to decrypt any of the data held on the disk. The encrypted disk is now no more useful for data harvesting than a paperweight.

A quick summary of DataDefense - FDE features is as follows:

- Complete full disk encryption
- 256-bit AES encryption
- Multiuser support at boot time
- Mobile media encryption for multiple users
- Hardware token support at preboot
- Centralized management
- Recoverable remotely via a recovery console
- MBR wipe

MARKET OPPORTUNITIES AND INSIGHTS

Are You Ready?

There are compelling reasons to incorporate encryption into your existing data protection program, including the need to protect data residing on mobile devices and the need to protect critical and valuable data from both external and internal exposure or theft and to adhere to government mandates. There are also compelling products, such as Iron Mountain's DataDefense suite, which can provide full life-cycle protection, including full disk encryption and mobile media encryption, and, when combined with Connected Backup for PC, can provide full data recovery. But are IT and business executives ready to purchase and install? The answer appears to be a resounding yes.

Many organizations are recognizing the risks associated with laptops and removable storage devices carrying valuable data. This realization has primarily been the result of high-profile front-page data losses. These news stories have elevated the issue into the public consciousness. Many people are now deeply concerned about others

losing the personal information they have. To mitigate these risks, organizations are turning to encryption, especially full disk encryption but also other forms of desktop encryption, which is designed to lock down unauthorized exposure of data, which was previously highlighted as the driving motivation for encryption deployment.

Survey results capture this trend (see Table 2). In a survey of 349 IT and business executives, desktop/laptop full disk encryption is the highest-rated product type being evaluated or presently being installed. File/folder encryption and encryption of personal computer backup are also top priorities for organizations.

In addition to this survey, other IDC research indicated that organizations that have already begun to use full disk encryption are expected to greatly expand the number of machines being protected.

TABLE 2

Encryption Usage and Plans (% of Respondents)
 Q. *Where does your organization apply or plan to apply encryption technologies in the next 12 months?*

	Evaluating/Implementing	Installed
Desktop/laptop full disk encryption	36	27
Corporate databases	33	39
Desktop/laptop file/folder	32	34
Desktop/laptop backup	30	38
Mobile device (smartphones/PDAs)	30	26
File server or network storage	29	35
USB or FireWire devices	28	26
Voice over IP (VoIP)	27	20
Tape backup or archival storage	26	42
Internally developed applications	26	26
Email at the gateway	25	42
Email at the desktop	24	38
Instant messaging	20	20
Batch file transfers or FTP	16	50

n = 349

Source: IDC's *Encryption Usage Survey*, 2008

When exploring the options available for full disk encryption and other desktop encryption capabilities, companies have a lot of products to choose from. All of the products come from security or encryption-specific vendors. These vendors have considerable experience in providing encryption, but they are generally not able to provide a full data protection security capability that incorporates data availability through managed data backup. Iron Mountain, as a data protection specialist, looks at data as something that must be preserved as well as protected. It assesses the problem through a different prism, which provides it with a unique perspective on data protection security and preservation; thus, its goal is to provide organizations with all facets of data protection security best practices. As a trusted provider and a steward to the data from thousands of organizations, Iron Mountain understands that data has intrinsic value and

that the value can be maintained only if it is available, not just locked up. Its worldwide coverage greatly enhances the ability to deliver that availability. IDC believes organizations should look at Iron Mountain because it is committed to delivering a complement of products and services that go further than just the encryption of data. The company understands how difficult it is to manage data and has incorporated this understanding into its digital solutions. It has developed a comprehensive encryption solution that satisfies all of the characteristics of effective encryption-based data protection security, as spelled out earlier in the document.

Ensuring Encrypted Data Survivability

The biggest impediment to the deployment of encryption, especially full disk encryption, is the fear that encrypted data will be unavailable or "destroyed." In IDC's surveys and interviews, the greatest encryption-related issue for IT professionals is the ability to get to encrypted data. Most IT and security personnel accept that encryption products will encrypt information. What they fear is that once encrypted, the data is at risk of not being recoverable. Most people can understand that it is relatively easy to take readable text and convert it into unintelligible gobbledygook, but it is much harder to fathom that the unreadable data can be converted back into its original form. One CTO summed it up nicely during an IDC interview: *"The two main fears we have are complications of key management and not being able to recover data. Those are exactly the problems. ... This is a really dangerous technology in that encryption is a really good way to destroy data as well as protect it."*

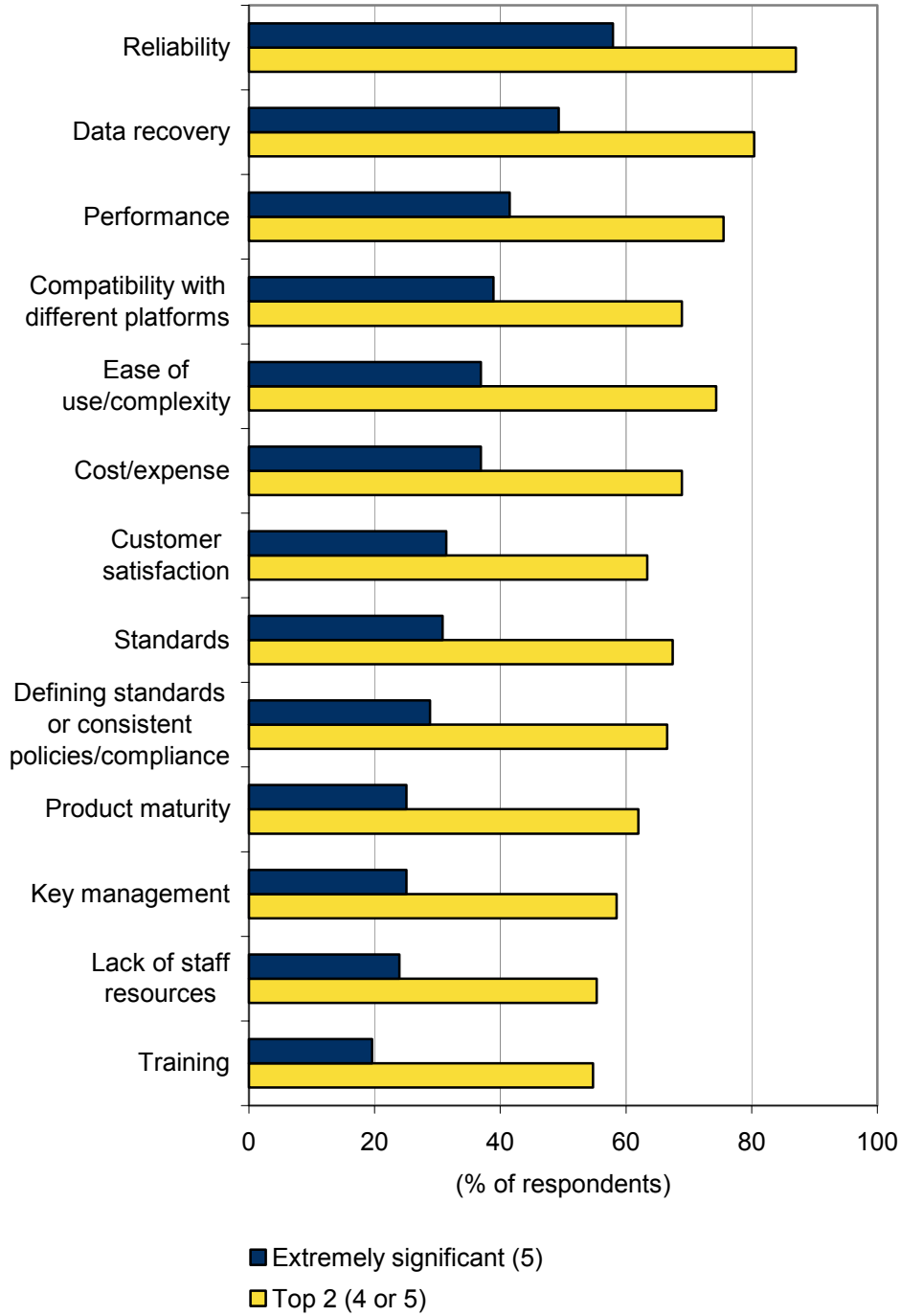
This sentiment about destroying your own data with encryption is represented in Figure 1, which illustrates how respondents rated the importance of various factors when considering the use or deployment of encryption. They didn't rate "key management" as a high concern; instead, their top concerns are "reliability" and "data recovery." They do not care so much about the "key management system"; rather, they are deeply concerned with the ability to recover encrypted information. They need to have confidence that the system is reliable — to ensure it works well in all aspects of the product and that the data is available after encryption. However, most people equate data recovery with access to the key, as was summed up in the short and sweet sentence, *"If you forget the key, you are toast."* Conventional wisdom is that key management is the problem. IDC believes this is a very narrow definition of data recovery.

Being able to get your data back is much more than just recovering data from an encrypted state. IDC believes data protection security best practices include encryption that is matched with data backup. With backup, you get another chance to have access to the data should decryption fail. Backup and encryption are especially important for laptop hard disks. Full disk encryption is used because the information is valuable and there is a risk of the computer getting into the wrong hands. Should the device be lost or stolen, encryption will ensure that the data remains secure or is even completely destroyed. However, this does nothing to get the important data back to the computer's owner. For the information to remain valuable, it must be available. Loss of data and loss of access to data put the enterprise at equal risk. Data backup allows information to be quickly restored to the rightful owner. Thus, backup provides additional data protection in the unlikely event that encryption fails or if the computer is lost or stolen and something else should happen, such as a hard drive failure.

FIGURE 1

Top Considerations for Encryption Deployment

Q. Using a 5-point scale, where 5 is critical and 1 is not at all important, please rate the importance of the following when considering use/deployment of encryption products at your organization.



n = 349

Source: IDC's Encryption Usage Survey, 2008

Challenge of Unexpected Consequences

With the implementation of any new technology or product, there are problems, or consequences, that are not readily apparent when a project begins. The deployment of full disk encryption has such unexpected consequences, but once they are identified, their impact is manageable. One of the first issues with full disk encryption installation is that fully encrypting a disk can take between two hours and five hours depending on the disk size and machine processor. This initial encryption is required only once and can be performed during some downtime, be it in the evening or at some other scheduled time. The unexpected consequence associated with implementing PC full disk encryption, as observed by IDC research, is that some machines just can't hack it. For whatever reason, it appears that on average about 5% of an organization's computers will need to be replaced. Many times, the cause is some unrealized hard drive problem that shows up during the initial encryption, or the machine doesn't have the horsepower to meet the requirement for full disk encryption. This will cost an organization a little more to replace the machines before their scheduled time, but end users will generally not complain about the encryption when they get upgraded hardware.

CONCLUSION

There is no doubt that information is the lifeblood of business. It exists nearly everywhere and, because of the value information retains, it must be protected. In the information age, the protection of data cannot be overlooked. As laptop computers proliferate, the need to protect data and mitigate the potential for system loss and theft will continue to grow in importance. Unencrypted laptops that carry confidential and/or personally identifiable information represent a significant risk to enterprises. IDC believes that organizations must have a data protection security program that adheres to accepted best practices in order to maintain the value of their proprietary data, to safeguard other's information entrusted to them, and to remain compliant with company, industry, and government policies and regulations. These best practices include the incorporation of both confidentiality (encryption) and availability (backup). Full disk encryption on all corporate computers, as part of this overall enterprise data protection security strategy, is a highly cost-effective way for enterprises and businesses to successfully maintain the confidentiality of business, employee, and personal customer data as well as intellectual property. Doing nothing can expose the enterprise to considerable risks.

IDC encourages organizations to go beyond full disk encryption and instead utilize a full data protection solution. Organizations that are serious about data confidentiality should take a close look at Iron Mountain's DataDefense suite of data protection solutions, including the full disk encryption option. The Iron Mountain solution is the only full disk encryption solution that is offered by a company whose sole business is the protection and preservation of data, be it in physical or digital form. The cost-effective and transparent solution provides a high degree of security to mitigate the theft or loss of a laptop containing confidential data. It satisfies all of the characteristics of effective encryption discussed in this document. However, due to its heritage and core business, the company also takes into consideration that the information must be available, not just confidential.

Iron Mountain offers organizations a full life-cycle data protection solution that protects information from data creation all the way to data destruction.

Iron Mountain's solution offers a "safety deposit box" for your "information currency."

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2008 IDC. Reproduction without written permission is completely forbidden.