IDC
Analyze the Future

WHITE PAPER

Addressing the Growth and Complexity of Information Security Concerns

Sponsored by: Kaspersky Lab

Kevin Bailey
February 2013

IDC OPINION

The relevance of security as one of the major contributors to an effective operational infrastructure has been growing in importance over the past 3-5 years, and today it resides as one of the two top investment priorities for senior management (the other one being critical server virtualization). Effective management by organizations when dealing with targeted and multiple parallel attacks comes down to recovery within a matter of minutes and hours or their businesses may not survive. A single integrated policy for managing all these aspects of security is growing in importance as a result.

At the heart of a security strategy are requirements to appreciate the data protection features of encryption, and the effect that mobile security is having on operations and planning.

- IDC believes that encryption is sporadic in its implementation, with only 30-40% of SMB organizations implementing enforcement consistent with internal policy standards, partially due to the misnomer that their data does not warrant such security measures and also the [assumed] costs involved for implementation and management. In contrast, enterprise organizations have a higher implementation at approximately 70% due to the increased budgets and [assumed] criticality of the data that they retain and communicate.

- Targeted attacks on enterprises of all sizes, as well as individuals inside organizations, are now primarily aimed at stealing sensitive information from individuals' machines or infiltrating networks for deeper data-theft purposes. According to IDC's 2012 *Security Survey,* these three issues — preventing exposure of confidential information, increasing sophistication of attacks, and mobile clients and unmanaged devices — were cited as the top 3 challenges over the next 12 months.

- IDC predicts that 2013 will be the year that Mobile Device Management will be redefined. The mobile category will establish clear functional definitions for application management (MAM), enterprise management (MEM) and also data and device management (MDM). Many features within the original MDM definition, including device lock/wipe, will become commoditized and provided by device and operating system organizations as integral components of their offerings as consumers and businesses expect these functions to secure their personal and business data.

IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

METHODOLOGY

The information contained within this white paper is a combination of IDC's worldwide primary research surveys, reinforced with the research documents and security analysts responsible to deliver forecasts, trends and strategic plans to the mixture of IDC's enterprise, SMB, and consumer clients (vendors, channel, and end users).

IN THIS WHITE PAPER

This white paper will outline the reasons why security has increased in importance over other essential infrastructure architectures, diverting budget and resources to ensure that organization information is protected with the necessary required secure levels. In parallel we will outline the reality behind the costs in physical, operational, and reputational damage that could arise if device loss is encountered without integrating the various security elements of Mobile Device Management (MDM), as employers allow mobile devices to become a primary engagement platform.

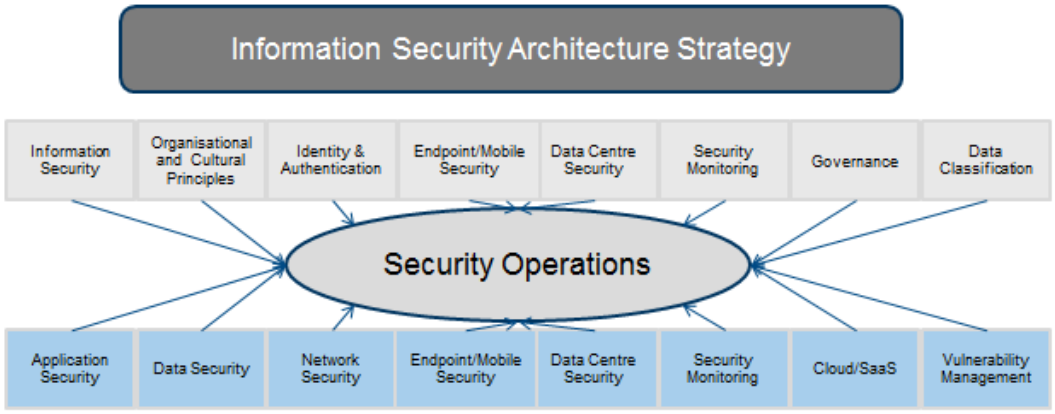
SITUATION OVERVIEW

As the growth of information increases in size, complexity, and relevance, the need to ensure that the highest level of required security is applied to the information, associated to its use, transportation, and sensitivity to businesses, consumers, and authorized third parties is growing in importance. The relevance of security as one of the major contributors to an effective operational infrastructure has been growing in importance over the past 3-5 years, and today it resides as one of the two top investment priorities for senior management (the other one being critical server virtualization).

Structured organizations have started to implement an Information Security Strategy (ISS) (Figure 1) to ensure a full appreciation of the many disciplines around building an appropriate security posture relevant to the business and operational needs of organizations. Budget resources are being diverted to encryption as a complimentary implementation strategy, with focus on integration into many of the Data, Information, and Device components of the ISS.

FIGURE 1

Information Security Architecture Strategy



Source: IDC, 2012 not for reproduction without permission

Why Has Security Grown in Importance?

The security market is evolving from a reactive antimalware execution-based implementation into a complex context-aware protection mechanism. Spanning wider than the corporate network, IT security coverage is becoming more complex as mobile and cloud computing become key variables that contribute toward operational efficiency and delivery, whilst the increased risks associated with the information sprawl related to these and existing infrastructure components puts organizations at financial and reputational danger.

The new challenge facing IT security is the need to control sensitive data in un-trusted environments not necessarily designed for enterprises (e.g. consumer-focused devices, cloud services, and apps). Combined with this is the awareness from organizations that they need to protect cyber activity from both internal and external threats. As Figure 2 shows, a recent IDC survey highlighted the top challenges that organizations believe are their highest priority in the next 12 months.

Addressing the top 5 priorities:

Employees underestimate importance of following security policy: It is essential that all employees, immaterial of status in a company, understand how their misguided actions (innocent or unintended) can impact their organization. Policies that control access, movement, and communication of data in a secure and understood manner will be needed by organizations.

Increasing sophistication of attacks: Attackers are increasing the amount of advanced malware they are driving to the endpoint. The sophistication and complexity of the attacks increase the need for advanced antimalware offerings that appreciate the multiple attack points (web, network, device, etc.) used to infiltrate the endpoint

and minimize the resources needed to thwart these attacks and protect the asset (device and data).

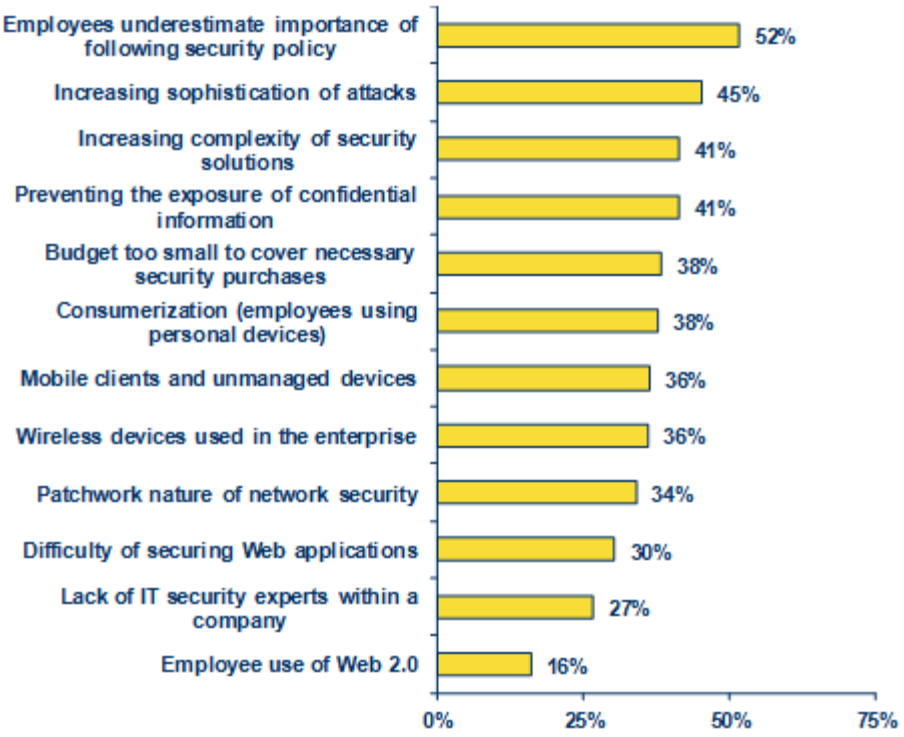
Increasing complexity of security solutions: Organizations appreciate the need to defend their endpoints across the disappearing perimeter, but cannot maintain multiple skill sets, management portals, policy engines, etc. in order to keep to their desired security posture. Vendors need to maximize their architectures, to be managed in a single, consistent, and intelligent manner, providing a faster response time and minimizing any drop in their security levels.

Preventing the exposure of confidential information: Every organization knows that information differentiates their business. Minimizing collateral damage when a system or individual communicates the information to an un-trusted party requires the use of encryption technologies, to maintain a level of appropriate security. Procedural and education adjustments should then be executed to minimize further incidents.

Budget too small to cover necessary security purchases: With many of the concerns in the previous four priorities addressed, organizations, typically in the SMB sector, will realize that they can afford an enterprise class endpoint security offering within their scope of budget. There is no need to buy 'good enough' antimalware and data protection offerings anymore, when organizations are able to choose the right class of product appropriate to the desired security posture.

FIGURE 2

Top Challenges over the Next 12 Months

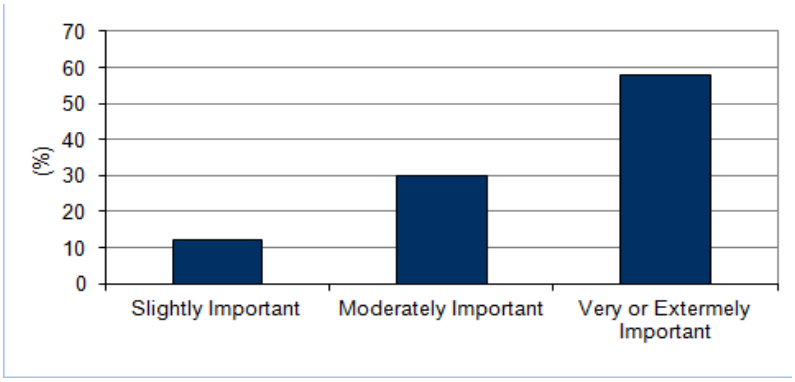


Source: IDC Market Analysis Perspective: Worldwide Security Products, Dec 2012

Figure 3 indicates that only 11% of respondents from the IDC end user survey in 2012 deemed that security was only slightly important, whereas 30% regard security as moderately important and an overwhelming 59% see security as very important.

FIGURE 3

Q: Indicate the level of importance for security

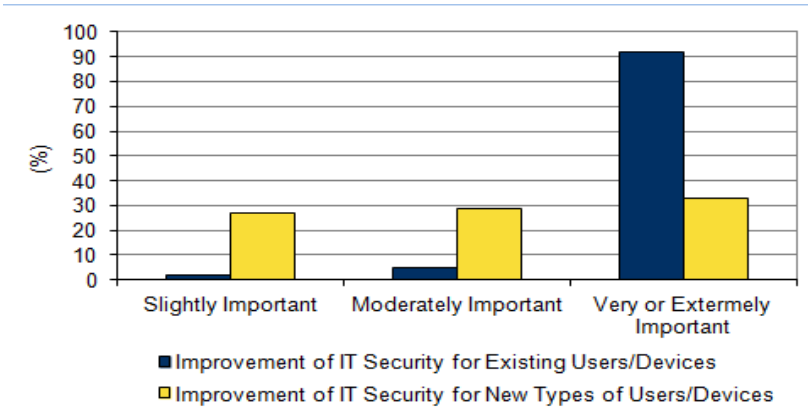


Source: Western Europe End User Survey, Feb 2012

Figure 4 explores the relevance of security upon the respondents existing and new users/devices. All respondents share an equal view as to the importance of securing new users and devices, whereas the respondents who believe that security is very important to them may have a strategic approach to security within their organizations.

FIGURE 4

Improvement of Security for New and Existing Users/Devices



Source: Western Europe End User Survey, Feb 2012

Best Practices to Secure Information

Organizations spanning enterprise and small medium businesses (SMB) have many comparative methods to secure their information, whether the information is active, at rest, or archived.

ISO 27000 is often used as a generic term to describe a series of documents: but primarily ISO 27002 (aka ISO 17799) is a set of security controls (a code of practice), and ISO 27001 (formerly BS7799-2) is a standard 'specification' for an Information Security Management System (ISMS).

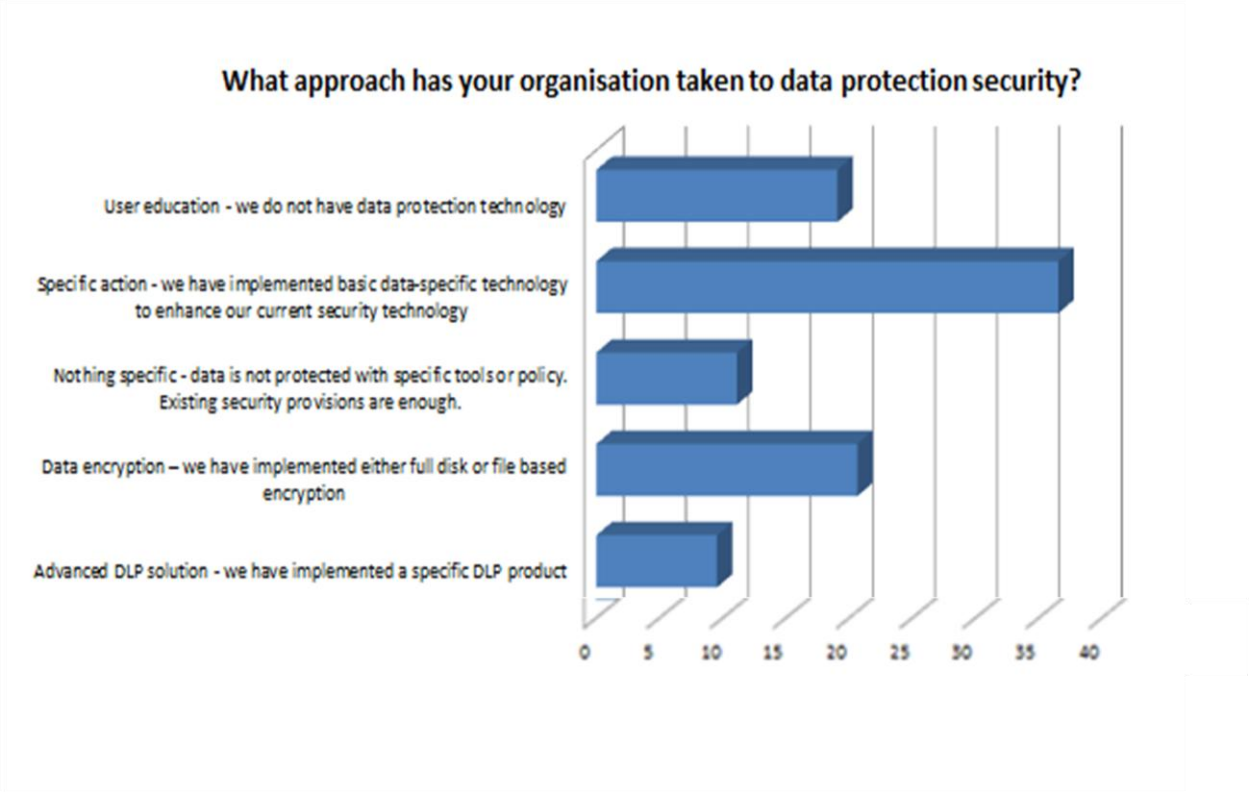
Once organizations have reviewed the applicability of key areas such as data classification and have a full topology of the infrastructure and individuals that constitute the environment and that the information is active, a review of many technologies and methodologies that can be implemented to physically secure the information is undertaken.

Within this paper we will be focusing on the areas that are witnessing a great deal of noise from end users, as well as governments and policy makers.

Figure 5 provides guidance on how organizations are implementing data protection, providing a mixed response of implementation, awareness, and exposure.

FIGURE 5

Q: What approach has your organization taken to data protection security?



Source: IDC IT Security Conference, Sept 2012

TO ENCRYPT OR NOT TO ENCRYPT

The Evolution of Encryption

Until the 1970s, all encryption was symmetric: anyone who knew how to encrypt a message could work out how to decrypt it. This was adequate for communication between a small number of trusted people sharing a secret encryption key. However, in a situation where large numbers of people want to communicate securely (like modern ecommerce) it is impossible for everyone to share a 'secret' key. This problem was solved by the advent of asymmetric or public key cryptography (PKC). PKC involves pairs of keys: a 'public' key which can be made openly available, and a 'private' key.

The IT industry has embarked on a very lengthy debate via the media on the appropriateness of information encryption, with one side endorsing the use of encryption for all data that is transmitted, and the other – many authorities and government organizations – requiring a less 'blanket' approach enabling access to data for legal and national security concerns.

IDC estimates that data protection (endpoint encryption and data leak prevention) features will become a necessity for all segments of the market. IDC believes that encryption is sporadic in its implementation, with only 25-30% of SMB organizations implementing enforcement consistent with internal policy standards, partially due to the misnomer that their data does not warrant such security measures and also the [assumed] costs involved for implementation and management. In contrast, enterprise organizations have a higher implementation at approximately 70% due to the increased budgets and [assumed] criticality of the data that they retain and communicate.

Many organizations would benefit from an understanding of best practices around the concerns that they may encounter when dealing with the appropriateness of encryption. Table 1 outlines a simple but effective set of 'Actions' that would help to determine the use and type of encryption those organizations may be considering.

TABLE 1

Encryption Concerns and Actions

Information Concerns	Information Action
Weak administration and procedures surrounding the all-important encryption keys can limit the effectiveness of this security measure.	Document all procedures carefully. Keep public/private encryption keys safe.
Encrypted information may be secure, but it may also prove to be inaccessible, even to authorized persons, where keys are poorly managed.	The keys used to encrypt and decrypt must be held securely, but they must also be accessible when required. Introduce procedures which ensure the availability of the data when required by those authorized.
Processor capacity (overhead) is used by the process of encryption and decryption. Lack of available capacity could lead to the data being effectively 'unavailable' when actually needed.	Only employ large scale encryption across entire systems where necessary. Determine which information is classified as sensitive, and whether it needs to be transmitted over insecure networks, such as the Internet. See Classifying Information and Data. Once the information has been encrypted, transmitted to its destination, and then decrypted, consider how the information should then be stored securely.
In some countries, it is illegal to use ciphers; or the type of permissible cipher may be strongly regulated. This could result in unintentionally breaking the law where encrypted data is sent to such a country.	Where necessary, seek legal opinion to confirm that the proposed encryption technique may be used between the organizations and countries in question.

Source: IDC, January 2013

Implementation Challenges of FDE and FLE

A security system is only as good as its weakest link, and the weakest link of most good security systems is the user. Systems should be designed so that they are used, and are also easy to use. Full Disk Encryption (FDE) solutions offer the

advantage of being transparent to the user, and providing mandatory security. File Level Encryption (FLE) does not offer mandatory security, as each new folder is required to be marked for encryption. Additionally, users are required to remember to save sensitive data to the correct folder.

In summary: FLE products are partially dependent upon the nature of the operating system and the applications with which they interact. For FDEs, there are no such dependencies. If an FDE has been implemented correctly, the security of the product is dependent upon the security of the algorithm used. Thus, data recovery by an attacker can take in the order of thousands of years.

Advantages and disadvantages of FLE and FDE

Table 2 and Table 3 outline some of the common concerns when deploying FLE and FDE offering.

TABLE 2

File Level Encryption Advantages and Disadvantages

FLE Advantage	FLE Disadvantage
Advantage One - is that in a system using FLE, since only sensitive files are encrypted, the system performance is faster than in a software based FDE system. This is because the CPU is not impacted by constantly encrypting and decrypting system or other files that do not require protection. While this is not usually an issue for hardware-based encryption solutions, it can be a significant matter for software-based solutions. FLE systems are faster than FDE systems.	**Disadvantage One -** FLE can be very difficult to deploy and manage from a policy point of view. Organizations need to first determine what data needs to be encrypted and that is not a trivial exercise. Determining what is sensitive or not is not as easy as it sounds, and getting the whole organization to agree on and enforce the resulting policy can be even more difficult. Furthermore, a document initially classified as non-sensitive might have sensitive data added later, so monitoring all documents becomes an on-going discipline.
Advantage Two - The installation process. An FLE solution allows users to back up and apply encryption to just a few files until they gain confidence that either an operator error or technology problem will not destroy their data. In contrast, an FDE system encrypts everything at installation time. It is important to note that not all FDE solutions suffer from these installation issues — this does not apply to FDE solutions that are built-in at the factory. However, for add-on software FDE solutions, the installation concerns can be a significant disadvantage. FDE may destroy all user data in case of operating error or technical problem, whereas FLE does not.	**Disadvantage Two -** The dependence on user action. Since users can inadvertently forget to encrypt a file that should be encrypted, or intentionally choose not to, the whole security system is very prone to human weaknesses. One of the underlying principles of effective security is that it must be provable security. If management cannot prove that all sensitive data is encrypted at all times, the security will generally not be in compliance with federal and or other regulations and management can be held accountable.
Advantage Three - is an attribute called "persistent encryption". Protected files remain encrypted until an authorized application or application plug-in opens them. The data can only be obtained in clear, unencrypted format through an authorized application that authenticates the user. This means that a protected file can be sent via ftp, instant messenger, attached to an email, backed up, copied to a USB drive or other	**Disadvantage Three** - It is sometimes impossible, or at least impractical to encrypt specific bits of sensitive data within an application. For example, there is no way in Microsoft Outlook to encrypt specific fields or a specific record within the Contacts database. The only option is to encrypt all the Outlook database files which can significantly degrade performance.

TABLE 2

File Level Encryption Advantages and Disadvantages

FLE Advantage	FLE Disadvantage
removable media and the protection remains intact. FLE data encryption is persistent and is not dependant on any particular device or location for its protection.	

Source: IDC, January 2013

TABLE 3

Full Disk Encryption Advantages and Disadvantages

FDE Advantage	FDE Disadvantage
Advantage 1 - once installed, FDE-based solutions are completely automatic and transparent. There are no burdensome administrative policies to establish or enforce because everything is protected, even isolated records or fields within database applications. The security is provable in an audit and it will hold up in court because it is not subject to human weaknesses. While organizations still need a method to recover data on a user's disk drive, the overall key management effort is a fraction of that required in FLE solutions.	**Disadvantage 1 -** They do an excellent job of protecting data on a system that has been shut down because an attacker cannot start the system and obtain any data. However, once an authorized user has started a system and it is up and running, the effect is as if no encryption were in place. Every read from the disk drive automatically decrypts data for any process that requests the data. If a machine becomes infected with spyware, the ill-intended software can obtain any data on the drive. If a machine is left unattended and unlocked, an attacker who has physical access, even momentarily, can also obtain any and all data.
Advantage 2 - is that they have been around since the 1990s. The solutions are solid and very mature and are in use by large organizations the world over. Their simplicity means a lot fewer problems to deploy and manage.	**Disadvantage 2 -** FDE systems are designed to protect data on the disk drive. They do not protect data anywhere else. Data that is encrypted on a hard disk is automatically decrypted when it is read. If that data is copied and pasted as an attachment, the attachment is in the clear, unencrypted unless some other process later encrypts it such as SSL or a VPN. If data is copied from the drive and burned to a CD, or copied to a USB drive, that data is decrypted by the FDE system and will be in the clear. It will not be protected by the FDE system, so unless some other protection mechanism is in place to re-encrypt the data, it will be unprotected.
Advantage 3 - hardware solutions have additional advantages. For instance, since all of the cryptographic functions are performed within secure hardware, encryption keys are never vulnerable to capture. Currently, there are no real hardware-based FLE solutions for enterprises. All FLE solutions use the CPU to encrypt and decrypt the data, which means spyware could potentially capture the encryption keys used within an enterprise as the process executes.	

Source: IDC, January 2013

Reasons for selecting FDE and FLE

FDE is the best approach for solid protection of data stored on disk drives. However, FLE protection is better suited for providing persistent protection of files that are moving from device to device. Since both technologies serve different needs, most organizations will ultimately end up deploying both solutions at some point. The questions are, where does one start today and why should I widen my implementation?

- Complying with data protection and privacy regulations is becoming the primary reason behind organizations' use of encryption.
- Protecting against malicious cyber attacks is the top overall enterprise data protection priority for organizations.
- Data breaches continue to become more common and more severe: companies are experiencing greater numbers of more severe cyber attacks that lead to data breaches.
- Data protection is increasingly viewed as a mission-critical element of an organization's risk management efforts: in IDC's 2012 IT Security Conference, only 20% of respondents had implemented FLE/FDE, whilst 28% had not implemented any data protection security.
- Encryption is not the technology with the highest level of importance or awareness in the IT budgets of organizations, but IDC believes it will become one of the fastest growing among them.

If your organization already has FDE deployed, then rolling out an FLE solution is a natural extension of your security and good next step. However, if you do not have any protection for stored data, starting with FLE and its added complexity may be overwhelming. The added security available with FDE solutions is another major consideration. If your organization requires the utmost in security, make sure you understand the potential of capturing the encryption keys during the execution of FLE systems.

Encryption Forecast and Assumptions

The Encryption market is classified within the Information Protection and Control (IPC) market by IDC and its levels of differing options makes a forecast of the market complex. Table 4 shows the revenue for key encryption (IPC) markets, respectively, by segment.

TABLE 4

Worldwide Information Protection and Control Revenue by Segment, 2010–2016 ($M)

	2010	2011	2012	2013	2014	2015	2016	2010 Share (%)	2016 Share (%)	2011–2016 CAGR (%)
Endpoint encryption	403	482	556	632	710	794	866	29.5	27.8	12.4
Secure messaging (encryption)	390	455	525	588	647	714	778	28.6	25	11.3
Other	572	739	895	1046	1200	1335	1473	41.9	47.2	14.8
Total	1364	1676	1977	2265	2556	2843	3116	100.0	100.0	13.2

Source: IDC, 2012

MOBILE DEVICE & DATA MANAGEMENT

The Cost of Losing [Control of] Your Mobile Device

'It takes the average person 30 minutes to realize they have lost their wallet or purse, whereas it only takes 3 minutes to realize you have lost your phone'.

Many people continue to have a naïve view that mobile devices are consumable units that when lost have little or no impact, apart from the cost of buying a replacement. If the device has no business value, there is the immediacy of fraudulent use of the device by the thief, as was seen in the UK in 2012 when a woman had her phone stolen and the thief ran up a £8,200 bill. Whereas banks carefully monitor accounts, block cards, and contact customers when spending patterns change and they suspect fraudulent use, the same protection is not afforded to mobile phone users.

In a business environment, the physical or technical loss of control of your mobile device and its data can be devastating. No longer does a criminal need to have physical control of you device to initiate their activity, but can utilize anyone of thousands of malware applications to execute the criminal activity. As BYOD extends its adoption across the world, IDC's EMEA Enterprise Mobility team surveyed 1,391 respondents, confirming that 28% of all the firms surveyed claim BYOD is already happening informally and the potential for data leakage was selected as the top concern for BYOD deployment, listed by 50% of companies across the region.

- A recent survey of more than 300 U.S. businesses and organizations found that they lost 86,000 laptops resulting in $2.1 billion in damage. The losses resulted

from data breach, lost intellectual property, reduced productivity, and legal and regulatory charges.

- Smartphones are sharing personal data widely and regularly, a Wall Street Journal investigation in late 2011 found. Out of 101 popular apps – games and other software applications for iPhone and Android phones – 56 transmitted the phone's unique device identification to other companies without users' awareness or consent.

- Top financial services institutions including Wells Fargo, Bank of America, and USAA rushed to fix security flaws in wireless banking applications that could allow a criminal to obtain sensitive data like usernames, passwords, and financial information.

Mobile Device Management Security Components

Mobile Device Management (MDM) is an essential function for the 'hyper-mobile' workforce, protecting them against loss and theft, and providing OS level maintenance, etc. As the relevance of mobile devices increases with users as a replacement for all or some of the functions that traditional PCs performed, it is essential that these following mobile security categories become part of the vocabulary of managers, technicians, and administrators.

Mobile secure content and threat management (MSCTM) is broken into three functional categories

- **Mobile threat management (MTM)**. Antimalware (which includes antivirus and antispyware), anti-spam, intrusion prevention, and firewalls for mobile devices.

- **Mobile information protection and control (MIPC).** File, full disk, or application encryption for mobile devices; also includes data loss prevention technologies. (Virtual data partitioning, either by hypervisor or by container, is also included in this category.)

- **Mobile VPN (MVPN).** VPN clients and infrastructure for mobile devices.

In addition, there are three other categories to complete the security components of MDM:

- **Mobile security and vulnerability management (MSVM)** solutions provide device wipe, device lockdown, configuration settings, vulnerability status (e.g., is the device jail-broken?), and patching for mobile devices. They also include mobile security, policy, and compliance management. Application vulnerability assessment scanning falls within this category.

- **Mobile identity and access management (MIAM)** solutions provide authentication and authorization technologies (such as PKI and SSL certificates) for transactions conducted from mobile devices that support network access for mobile devices.

- **Mobile other security (MOS)** covers emerging security functions, such as antitheft/antifraud.

There has been a substantial need in the last 3-4 years to provide more granular management for secure corporate applications on employee-owned devices; vendors are now offering solutions that allow companies to provide flexible secure management policies for individual applications.

- **Mobile Application Management (MAM)** sometimes described as "app wrapping." Companies can apply very specific policies to individual applications such as password protection, VPN tunneling, geo-fencing, and advanced encryption, among others.

Encryption for Mobiles

One of the most vulnerable groups to outside interference is the mobile device user. Encryption of information on a mobile device has been a topic for a good few years now. No organization wants their data in the wrong hands and when talking about mobile devices that are not behind a secure door then this is all the more likely.

This means that people who manage to get hold of a smartphone, tablet, laptop, etc. will not be able to get access to your corporate data even if they open up the machine, take out the hard disk and load it as a secondary drive in a different machine.

Encryption for mobile devices, as referenced previously within IDC's MIPC sub-category can be deployed at file, full disk, or application encryption levels and is an important aspect of deploying a mobile solution.

Moreover, the likelihood of your organization experiencing a breach is greatly reduced by the implementation of encryption. A recent study by the U.S. Department of Health and Human Services (HHS) found that almost 40% of “large breaches” resulted from “lost or stolen devices.” If the information on the devices had been encrypted, the data would have been secure and no breach would have occurred. The increasing prevalence of mobile devices will make this likelihood even higher.

MDM Drivers and Inhibitors

The explosion of mobile device usage has been driven by the advances in connectivity (WiFi and 3g/4g) coupled with the increased functionality (applications and messaging) and device technology packaging that connect an individual's business, personal, and social personas.

Drivers

The MDM category is gaining adoption by many macro level drivers that attest to mitigate device and data loss, enforcing a strict rule of policies dependent on the individual and their role within the organization.

- The diversity of unique operating system and mobile device types, increase the need for single MDM offerings
- The convergence of social and business application usage on a single device, but which can be downloaded onto another individually owned 2nd/3rd device
- Processing and sharing of company data on a corporate or BYOD device
- Mitigating the increased threats, primarily against Android devices from malware
- Physical loss and theft of mobile devices require device lock and/or wipe

Inhibitors

The MDM category is currently enshrined in complexity, minimizing the ability for organizations to identify the functionality within the category that would address their concerns.

- Lack of clarity from MDM providers on the features and issue resolution
- Integration of MDM as part of organizations security platform architecture
- Lack of awareness and education within organizations
- Lack of mobile management policies that can be implemented in parallel

FUTURE OUTLOOK

Security

Security was identified in the *2012 Western European End User Survey* as #2 in importance for IT and functional decision makers. IDC expects the level of importance and integration with traditional infrastructure architectures to continue on an upward spiral as cyber attacks target a mixture of reputational, financial, and political gains.

The evolutionary transition for vendors is to develop and offer end user requirements within the next 6-18 months around flexible security architectures, balanced with ease of use and automated functionality to address protection of data at rest, in-motion and in-use, whether on an active or secondary device outside of the traditional network perimeter or located within a centralized datacenter or remote office location.

The collaboration of security vendor to security vendor will increase with a mixture of co-developed architectures, APIs, and open standards and will provide end users with more [relative] differentiated security offerings across vertical and horizontal segments, appreciating the economic and threat attack vectors for specific markets.

Encryption

If your organization already has FDE deployed, then rolling out an FLE solution is a natural extension of your security and good next step. However, if you do not have any protection for stored data, starting with FLE and its added complexity may be

overwhelming. IDC believes that unless you can make a good case that it is more important to protect data moving from device to device than it is to protect data on your organization's disk drives, you are probably better off starting with FDE. It is simpler, more mature, and gives you provable security.

IDC regards the added security available with FDE solutions to be another major consideration. If your organization requires the utmost in security, make sure you understand the potential of capturing the encryption keys during the execution of FLE systems.

Mobile Device Management

IDC has predicted that 2013 will be the year that Mobile Device Management will be redefined. The mobile category will establish clear functional definitions for application management (MAM), enterprise management (MEM), and also data and device management (MDM). Many features within the original MDM definition, including device lock/wipe, will become commoditized and provided by device and operating system organizations as integral components of their offerings as consumers and businesses expect these functions to secure their personal and business data. As security continues to raise its importance in the protection of personal identifiable information (PII) and corporate intellectual property (IP) and mitigation of the greater targeted threat landscape, all the features covering identity, anti-malware, encryption, data loss, and application security will be delivered via a single integrated mobile security platform offering.

CONCLUSION

The security landscape is rapidly raising concerns as more publicized attacks are becoming visible to consumers and organizations of all segments. Organizations need to improve their security posture to ensure that the information and systems/devices that they use for operations and commercial outreach protect the individual from malicious and unintentional breaches.

The inclusion of features such as encryption will protect the information from unintentional access. A collaborative planning and implementation strategy should be applied with all organizational stakeholders' involvement, utilizing the skill and market understanding from the vendor community.

FURTHER READING

- 2012 End-User Software Trends in Europe (#LC53U, Mar 2012)
- EMEA Mobile Security Market 2011-2016 Forecast and Analysis (#LM56U, Nov 2012)
- Worldwide Endpoint Security 2012-2016 Forecast and 2011 Vendor Shares, (#235930, Jul 2012)
- IDC's Worldwide Security Products Taxonomy, 2012 (#235288, Jun 2012)

- IDC Market Analysis Perspective: Worldwide Security Products (#238720, Dec 2012)
- EMEA Enterprise Mobility Survey 2012: Comparison Results between Regions (#LM03U, Oct 2012)