ENCRYPTION AS AN ENTERPRISE STRATEGY

AN IANS CUSTOM REPORT

JULY 2015

WRITTEN BY IANS FACULTY MEMBER
DAVE SHACKLEFORD

Contents

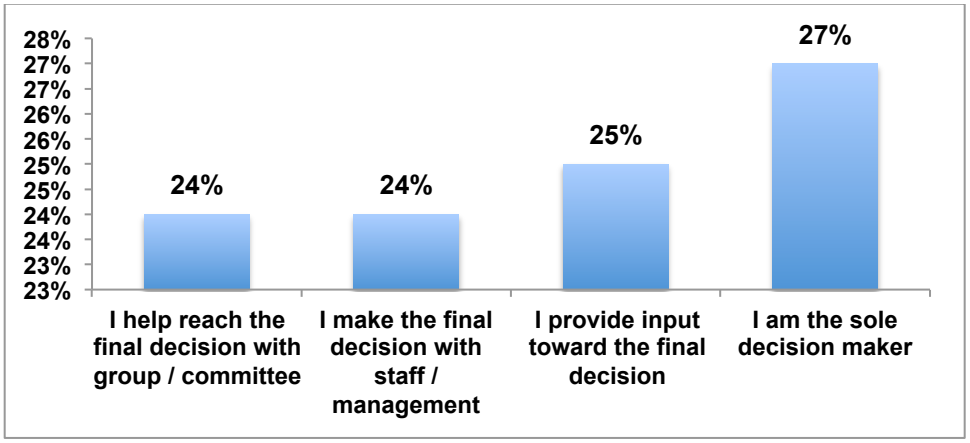
Introduction

In the last ten years, the number of data breaches and major cases involving sensitive data exposure have grown dramatically. Starting in 2005 with the ChoicePoint breach, we've seen a steady increase of data breaches that have exposed payment card information, healthcare records, personally identifiable information (PII), passwords and other authentication details, and more. Major breaches have occurred at Heartland Payments, Home Depot, Adobe, Target, Sony, Anthem and many other organizations both large and small with security teams, compliance requirements, and numerous security controls in place.

With the growing reality that breaches are not only possible but likely, how can organizations prevent attackers from gaining any useful information? In the recent hack of the United States Office of Personnel Management (OPM), Aaron Boy of The Federal Times states that "The biggest misstep in the breach of Office of Personnel Management networks was not the failure to block the initial breach but the lack of encryption, detection and other safeguards that should have prevented intruders from obtaining any useful information."[1]

For this paper, IANS conducted an independent survey of over 100 information security professionals to better understand how they are contending with more advanced attackers trying to compromise systems and steal data, all while moving into cloud and outsourced service models where they may have little, if any, control over many of the more traditional security controls we're used to implementing. 64% of the respondents indicated that they were in security management (manager and director-level positions) with the remaining group (36%) stating that they were in senior executive positions such as Vice President, CSO, CISO, CTO, and CIO. The focus of the questions was decidedly strategic in nature, and we wanted to ensure that senior influencers and decision makers were the focus of the survey.

To that effect, we asked how those responding made decisions, and the results are shown in figure 1:

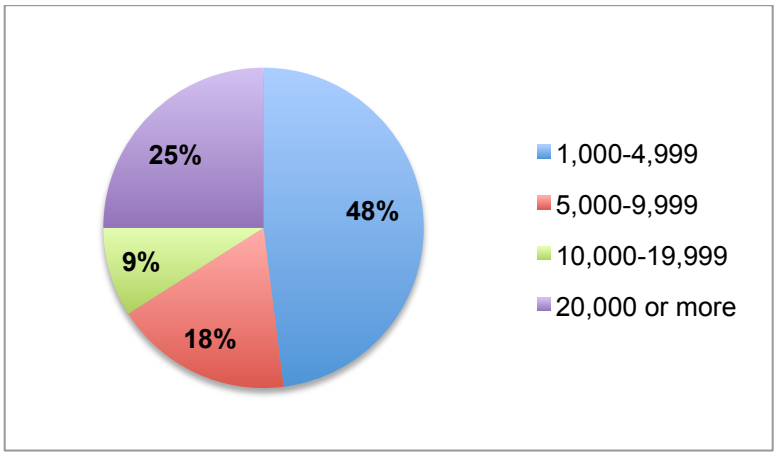


N=100

Figure 1: Respondent Decision Making Responsibilities

[1] http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/

The responses were split closely with just over half making the decision solo or with input, and the others helping make a group decision or providing input. IANS also wanted to gather input from a variety of different organizations of varying sizes, and the organization size ranges we heard from reflect this. 25% of organizations have 20,000 or more employees, the largest percentage (48%) have between 1,000 and 5,000, and the rest came in between 5,000 and 19,999, as shown in figure 2:



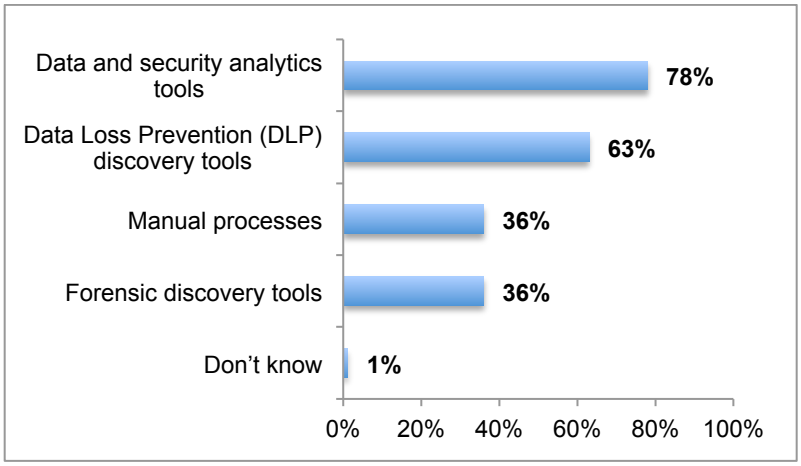
N=100

Figure 2: Size of Respondent Organizations

Security Challenges and Concerns Today

Most organizations today are becoming more and more concerned with protecting sensitive data within the organization and elsewhere. When IANS asked survey takers whether their organizations had defined data classification policies that clearly specify different data types and sensitivity levels, a whopping 95% answered in the affirmative, which was not surprising. Only four percent said “no,” with one percent indicating that they weren’t sure. Today, most enterprise security and compliance teams have a defined data classification policy that addresses data sensitivity levels, and often includes compliance specifications as well. This is a critical first step to defining the appropriate security controls needed to adequately protect the data wherever it may reside. In fact, a number of teams are readily starting to rethink the concept of the “crown jewels” in many enterprises, with emphasis on locating sensitive data within the IT infrastructure. For large (and even mid-size) organizations, this has traditionally proven to be a serious hurdle.

Fortunately, there are more tools available now than ever before that can assist teams in locating sensitive data. Figure 3 breaks down the various types of tools that survey respondents are using today to locate their “crown jewels” throughout their environments:



N=100

Figure 3: Sensitive Data Discovery Tools

IANS found the heavy use of data and security analytics tools for data discovery interesting, as this is a marked shift over the last several years. Traditionally, the use of data loss prevention (DLP) tools has been the predominant method used for discovering sensitive data in the environment, but came in second with 63%. As respondents were free to indicate multiple tools and methods when answering this question, IANS feels it's likely that some combination of these two are likely used in many environments. With more advanced SIEM and security analytics tools available today, many teams are integrate more and more data to combine and correlate than ever, and adding logs and events from many sources, including DLP tools, may be providing better and more accurate results related to sensitive data location. Manual processes and forensics tools are also proving useful, which reflects more traditional approaches to data discovery. Some teams have written custom scripts that scour data repositories and system drives for patterns, which can work well in smaller environments or those that are not highly distributed in nature. Endpoint forensics tools, as well as specialized forensic discovery tools, can also be used to match patterns of data within the environment, too.

Regardless of methods, there have traditionally been many challenges with locating sensitive data and adequately protecting it. Many teams are now starting to think carefully about the "risk window" of time that may be in place between discovery of sensitive data and application of adequate protection controls, as well as the "risk window" from not discovering the data at all or accidentally discovering the data in a location they shouldn't reside in. The typical constraints organizations have in discovering their sensitive data (let alone securing it) include lack of proper tools, not enough people to focus on data discovery and protection, and lack of budget and management support for such endeavors. IANS asked respondents how confident they were that all sensitive data stored in their organizations was adequately protected, and the answers indicate that most aren't completely sure. 37% stated that they were "very confident" their data was protected, but the majority (58%) felt only "somewhat confident". Five percent were "not at all confident" that all their data was protected currently.

In a recent survey by the Cloud Security Alliance (CSA) focused on financial organizations, 57% of financial organizations indicated that they wanted more encryption options within cloud

providers. Why such a high number? The survey also indicates that the top security concern from financial organizations is data confidentiality (60%), followed closely by loss of data control (56%) and data breaches (55%). There have been many traditional drivers for encrypting data, including the following:

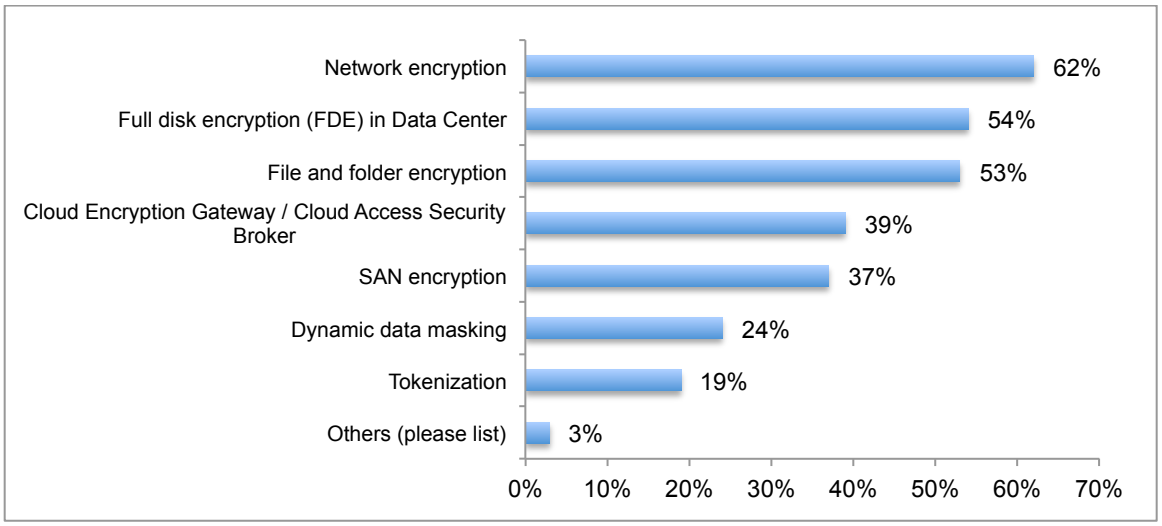
- Protection from traditional hackers that have made data exfiltration a business model, selling sensitive data on a variety of underground markets and forums.
- Protection from the insider threat (both accidental release and purposeful).
- Demonstrating compliance while also being able to remove potentially large quantities of data from compliance and regulation scope.
- Demonstrating adherence to rigorous security best practices for marketing and strengthening the organization's brand. Implementing strong security controls can demonstrate to stakeholders and customers that the organization is safe to do business with (due diligence).

To accomplish the goals of encrypting and obfuscating data, organizations have traditionally turned to a number of different approaches. In the realm of encryption, there are the following types:

- Physical (hard drive or full disk encryption): This is a common compliance requirement for certain types of users and systems that may carry sensitive data, that can be easily stolen or lost, such as laptops and mobile devices. Storage Area Network (SAN) and Network Attached Storage (NAS) full disk encryption is also common in larger enterprises, although the likelihood of these devices being stolen or incorrectly retired is usually low.
- File and folder: File and folder encryption is applied within the operating system, and can be from the OS vendor or a 3rd-party provider agent that is installed. File and folder encryption can offer much more granular access controls then full disk encryption.
- Network: Network encryption is usually applied with SSL/TLS or IPSec, and often used to create dedicated or on-demand network tunnels that protect data sent in transit.
- Application: Application encryption is usually applied within the application itself, providing encryption or tokenization of the sensitive data before it is stored within a database.
- Cloud: Cloud-based encryption can actually be implemented with any one of the aforementioned methods, and may be offered by traditional encryption vendors, with on-premises or "as-a-service" models, as well as options available from the cloud providers themselves.

Key management has also been managed and maintained in a number of ways, most often through commercial encryption solutions like PKI, Hardware Security Modules (HSMs) and key management product and service offerings from vendors. Many organizations have also embraced data manipulation and/or obfuscation techniques like tokenization and dynamic data masking. These options transform data into formats that no longer contain sensitive information, and can also be more searchable and configurable for particular applications and data usage scenarios. Tokenization can be used in a number of application scenarios, whereas dynamic data masking is often implemented in databases at the column or table levels. IANS asked survey

respondents which encryption and transformation techniques they were currently using, and the responses are shown in figure 4:

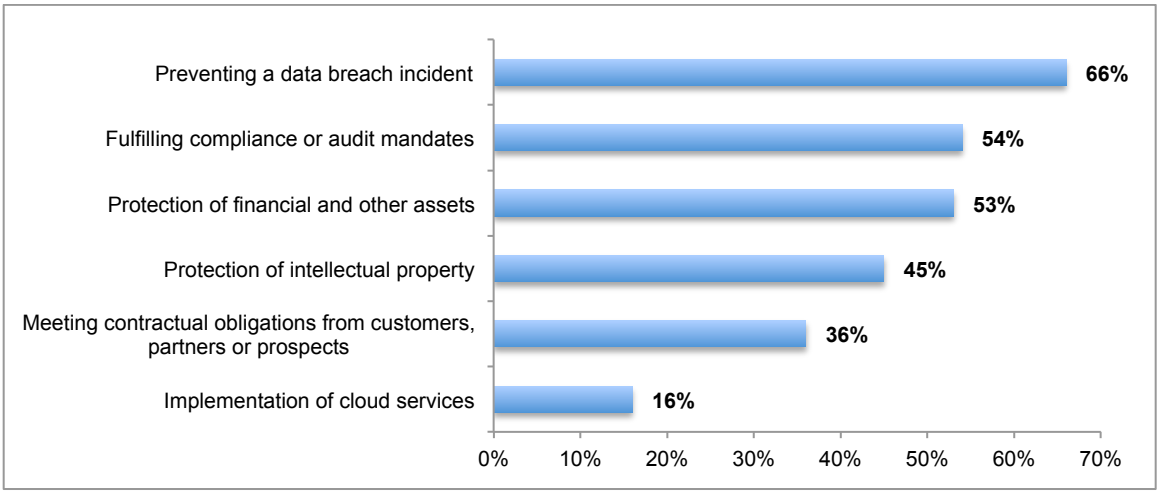


N=100

Figure 4: Data Protection Options in Use

Survey respondents were able to choose multiple responses to the question, and many chose some combinations of network encryption and encryption for data at rest and in use. Network encryption is in use by almost two-thirds of respondents (62%), while the types of encryption for data at rest varied widely, with FDE and file/folder encryption as the most popular. IANS also asked respondents whether they were using commercial and/or open-source or free encryption options. Most stated that they were using commercial encryption explicitly (45%) with 18% only using open source technology. A third (33%) are using both, and only four percent are not using either commercial or open source technology. Based on these responses, it appears that encryption is a popular option for data protection in many enterprises, and many organizations feel that it is a highly effective method for protecting data.

Most organizations have significant business drivers for implementing encryption. In figure 5, the top reasons people are encrypting data are shown:

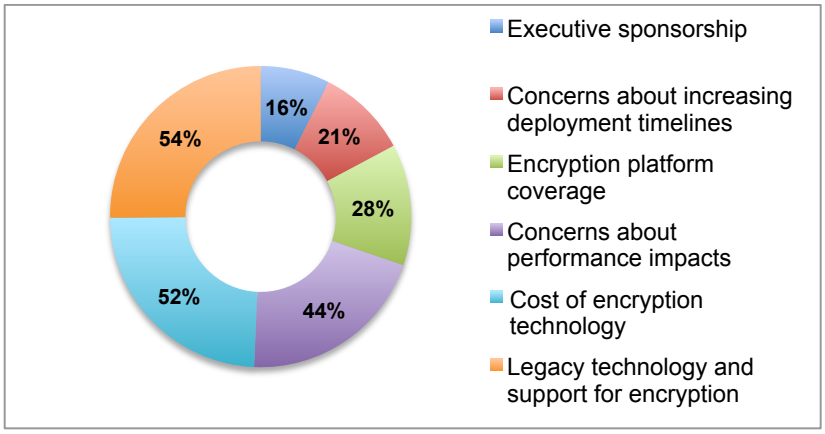


N=100

Figure 5: Primary Drivers for Encrypting Data

A full two-thirds of respondents stated that preventing data breaches is a key driver for encryption implementation. This makes sense, as encryption is likely one of the only technologies that, when properly implemented, could thwart a data breach or exposure scenario. Meeting compliance and regulatory concerns that mandate encryption of sensitive data is a top requirement for over half of respondents, along with general concerns in protecting financial and other assets (driven by internal requirements). Protection of intellectual property is another major driver that falls in line with the other top priorities, but indicates that organizations are branching out *beyond the traditional data types covered by compliance*, and are starting to protect more and more of their data in general. Encrypting data to meet customer and partner requirements, or to protect data in cloud environments, also points to encryption taking more of a central role in data protection strategies.

So today, one of the big questions is: Why have more security and infrastructure operations teams not deployed encryption to protect their data? What challenges are they running into? Figure 6 shows the major challenges respondents provided when trying to implement encryption:



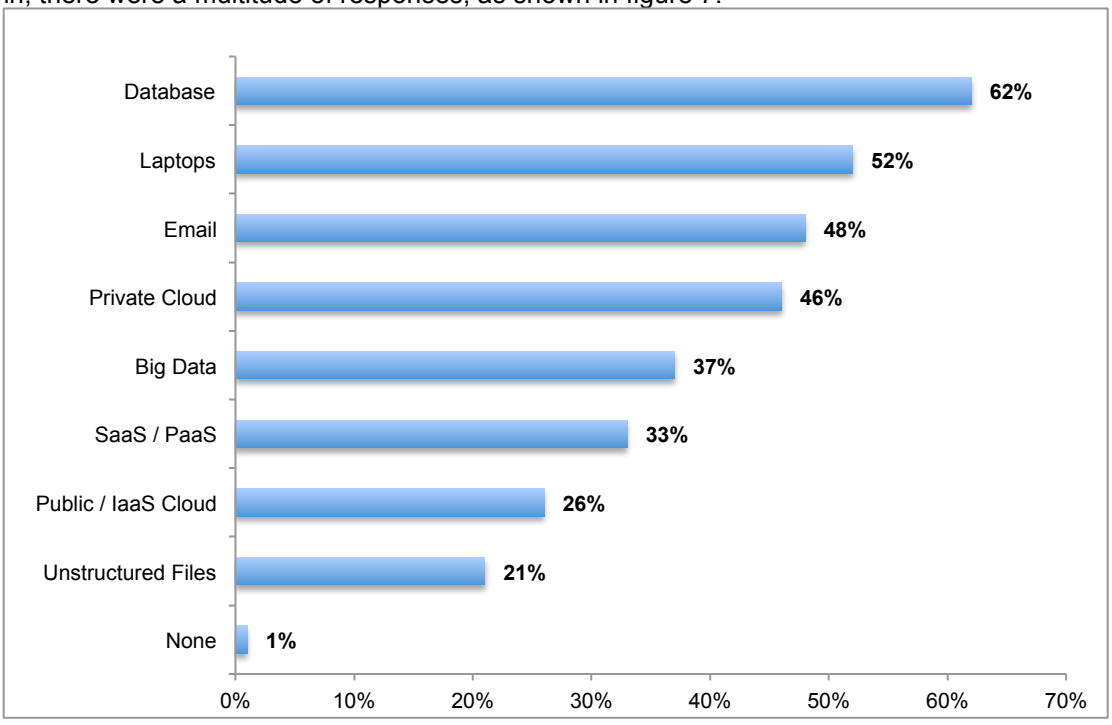
N=100

Figure 6: Top Challenges with Encryption Implementation

The top concern when implementing encryption is legacy technology and support for encryption. For these scenarios, tokenization and data masking are likely more viable options, and can often work with technology that does not support encryption application. Cost and performance impacts were also cited commonly, but there are many options now available that can help overcome these issues. More and more commercial encryption vendors have a wide range of packages and cost models that support enterprises and smaller organizations alike. Performance impacts can also be mitigated in some cases with specialized approaches and hardware encryption support like AES-NI (AES New Instructions), which are often implemented in chipsets from Intel, AMD, and others to accelerate the rate of encryption in hardware, thus offloading the encryption operations from the operating systems and applications. Coverage of encryption was cited as a concern by 28% of organizations, too. Fortunately, new options are becoming readily available as some vendors offer platforms that cover a large range of use cases and environments that can simplify key management and operations (often the most complicated aspect of encryption, as well as an Achilles Heel of coverage). Some of these include the Key Management Interoperability Protocol (KMIP) from OASIS, Transparent Data Encryption (TDE), and others.

Encryption Implementation

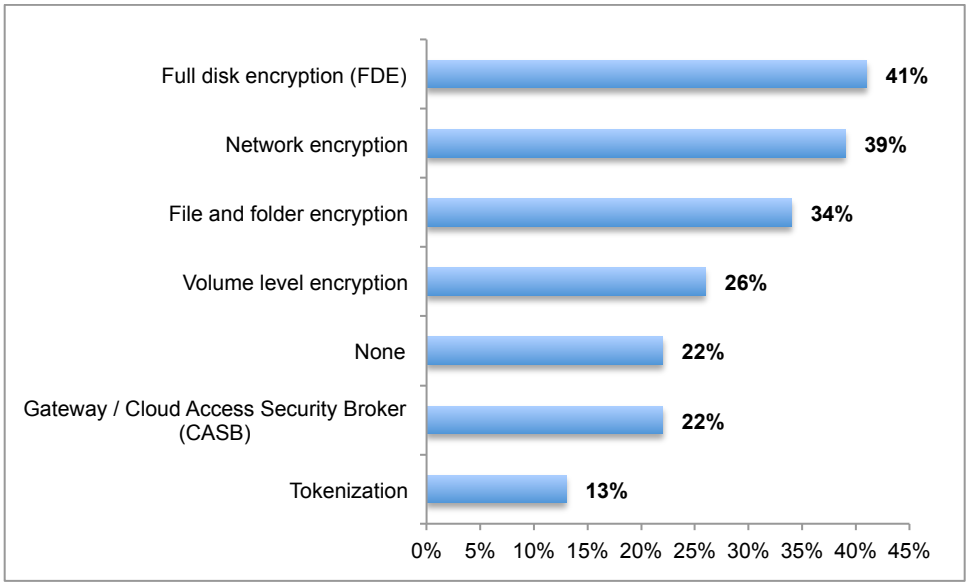
When we asked organizations what types of environments they were implementing encryption in, there were a multitude of responses, as shown in figure 7:



N=100

Figure 7: Encryption Options in Use

The sheer breadth of responses implies that there are readily available options in encryption products that can be implemented within environments of any type. Database encryption, laptop encryption, and email encryption are the most common, followed closely by "private cloud" encryption, where the infrastructure and systems running in the cloud are largely or completely controlled by the consumers. This could include disk encryption, file/folder encryption, or other types, as discussed earlier. However, more encryption is now being applied for newer technologies like "big data" and unstructured files, along with numerous types of cloud service models (Infrastructure, Platform, and Software as a Service). To that end, we asked respondents what types of encryption they were currently applying within their cloud implementations. The majority is still using full disk encryption (FDE), which implies concerns about the physical security of their backups and data stored in external environments or that FDE qualifies for a compliance checkmark. Network encryption is common (39%), as is file and folder encryption (34%) and volume encryption (26%). The full results are shown in figure 8:



N=100

Figure 8: Cloud Encryption Types in Use

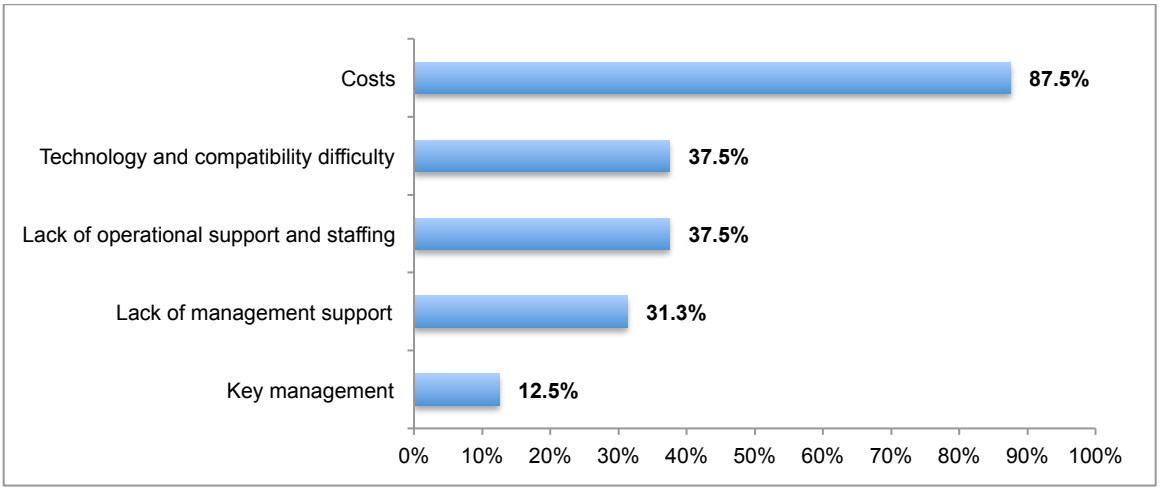
Encryption in cloud and hybrid architectures can be somewhat challenging for organizations who are trying to manage keys and operational processes, which may explain why 22% of respondents stated that they were not currently using any encryption in the cloud (this may also be due to the types of data and cloud assets deployed). Nonetheless, newer techniques like tokenization and cloud security and encryption gateways, as well as Cloud Access Security Brokers (CASBs) are gaining more traction all the time. As these types of options mature and become more accessible, many teams may find that encryption for all cloud data becomes a potential simplification mechanism, enabling business initiatives to get there faster with less risk. To that end, SaaS and PaaS leader Salesforce.com recently announced that they were implementing a new security-focused service for their platform called Salesforce Shield that includes platform and specific field-level encryption.[2] A built-in encryption offering from a leading provider of Salesforce.com's size definitely indicates the market demand for this type of protection. When encryption can be managed with a single tool or vendor, this can also make the process much easier, but that has been a challenge across both internal and external cloud infrastructure, especially when multiple cloud providers are in use.

Could that strategy be shifting, though? Could security leaders be considering the concept of encrypting everything? As a matter of fact, the answer is a resounding "yes"! 84% of respondents indicated that they had considered implementing a security strategy of encrypting all sensitive data. What would this mean? First, this may not mean, "encrypt all data", but would instead imply that only "internal" data be encrypted. Encrypting data that is meant to be public, like websites and knowledge bases doesn't make sense. However, creating a strategy where all sensitive data was discovered and encrypted could be a significant strategy for ensuring protection of the data whether within the data center or moving to cloud environments. However, we know that

[2] http://www.salesforce.com/company/news-press/press-releases/2015/07/150714.jsp

discovering “all” sensitive data is a very expensive, time consuming, and imperfect science. Therefore, a policy of encrypting all data that is meant for “internal use” by a default policy can significantly reduce risk immediately.

What would hold enterprise teams back from implementing an “encrypt all the internal data” strategy? By an overwhelming margin (87.5%), respondents stated that cost was the biggest issue, as shown in figure 9:



N=100

Figure 9: Perceived Issues with an “Encrypt Everything” Strategy

From there, the usual suspects of compatibility, lack of operational support, and lack of management support are listed as possible factors, with key management coming in last with 12.5% of respondents (surprising given that key management is usually listed as one of the top challenges or headaches in implementing widespread encryption).

Despite the challenges with encrypting everything (real or perceived), the idea nonetheless remains compelling, as this type of security architecture could significantly reduce risk of sensitive data theft and exposure.

Conclusion

It’s obvious that organizations consider data encryption and obfuscation mainstays of sound data protection requirements. Many organizations have compliance requirements that mandate encryption, but it seems that more are branching out to encrypt and mask many other data types, as well. Applying a strategic security policy of encryption and key management across the enterprise could certainly bring many benefits, as long as the challenges and perceived drawbacks can be overcome.

In fact, IANS is seeing a definitive shift toward encryption as a strategic activity versus a tactical one, with many defining and applying widespread and far-reaching encryption policies for the entire organization. Many organizations we work with are seeing shifts in drivers for encryption

overall, as well - encryption is rapidly going from a “security checkbox” to a technology that can address specific and advanced security threats, as well as help to reduce compliance scope for many businesses, which turns encryption into an immediate business advantage. While laws vary between states and countries, encryption may help with data breach notification requirements, potentially removing the need for disclosure altogether if encryption can be shown to be implemented and in place properly.

IANS also sees organizations working steadily to implement new technologies and services in the areas of disk encryption, file and folder encryption, and key management when deploying cloud services. Many cloud service providers readily support encryption technologies, or even offer in-house hardware security modules (HSMs) for key storage and management, which can help to alleviate one of the biggest pain points many organizations have traditionally cited when implementing large-scale encryption projects. NIST has also published a best practices guide for addressing key management in cloud environments (NISTIR 7956).

Could encrypting everything result in a more simplified strategy for security technology, saving costs and improving security posture now and in the future? The idea is compelling, and the majority of security leaders we questioned felt that this could be a good idea. Currently, IANS recommends that organizations look at encryption more strategically, potentially exploring an “encrypt everything” approach now or in the near future. With the various business and security benefits that encryption technology and services can offer (especially with more widespread adoption of cloud services), the value and return on investment with encryption technology likely makes a lot of sense for organizations both large and small.

About Vormetric

Vormetric is the industry leader in data security solutions that protect data-at-rest across physical, big data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters – their sensitive data – from both internal and external threats. The company’s scalable Vormetric Data Security Platform protects any file, any database and any application’s data —anywhere it resides — with a high performance, market-leading solution set. For more information, please visit: www.vormetric.com.

About IANS

IANS is the leading provider of in-depth security insights and decision support delivered through research, community, and consulting. Fueled by interactions among IANS Faculty and information security practitioners, IANS’ experience-driven advice helps IT security, risk management, and compliance executives make better, faster technical and managerial decisions. IANS was founded in 2001 as the Institute for Applied Network Security. Inspired by the Harvard Business School experience of interactive discussions driving collective insights, IANS adapted that format to fit the needs of the information security community.