White Paper

Enterprise Encryption and Key Management Strategy

The Time Is Now

By Jon Oltsik, Senior Principal Analyst

April 2012

This ESG White Paper was commissioned by Vormetric, Inc. and is distributed under license from ESG.

© 2012, The Enterprise Strategy Group, Inc. All Rights Reserved.
Contents

Executive Summary ...................................................................................................................................... 3
The Steady Increase of Data Encryption ................................................................................................. 3
Data Encryption Growing Pains ................................................................................................................. 5
Large Organizations Need an Enterprise Encryption and Key Management Strategy ....................... 6
Enterprise Encryption Architecture ........................................................................................................... 7
The Bigger Truth ........................................................................................................................................ 9
Executive Summary

When it comes to information security, large organizations tend to focus on fire fighting rather than long-term strategy. Unfortunately, this short-sighted approach has its limits—and ultimately results in high costs, disparate independent technology controls, and increased risk.

This is often the case when it comes to data encryption. This paper concludes that:

- **Encryption deployment continues to grow.** Driven by regulatory compliance requirements, highly visible publicly disclosed security breaches, sophisticated threats, and abundant technology choices, large organizations are implementing more and more encryption controls for data security. Unfortunately, most are doing so on an ad hoc basis with no central oversight or long-term strategy in place.

- **Ad hoc encryption is demonstrating growing pains.** Ad hoc encryption is based on an army of incongruent technologies, each with its own administration, key management, and auditing/reporting capabilities. These tools are often “owned” by functional IT groups rather than skilled security professionals. CISOs have to assess risk and measure IT effectiveness on a tool-by-tool basis. Even worse, ad hoc encryption leads to redundant processes, complex operations, and high costs while placing sensitive data at risk of accidental compromise or malicious insider attack.

- **Large organizations need an enterprise encryption strategy.** Before proceeding with any new encryption initiatives, CISOs must assess the existing situation and work to create an encryption strategy that works across the enterprise. This should include central command and control, distributed policy enforcement, tiered administration, and an enterprise-class key management service. The overall goal should be transparent encryption service owned by the security team but designed to support business needs without disrupting business or IT operations.

The Steady Increase of Data Encryption

Over the past few years, most large organizations have progressively increased adoption of data encryption technologies. Encryption usage is growing due to several factors, including:

- **Regulatory compliance.** Enterprises face a complex mix of federal, state, industry, and international privacy regulations which demand or recommend encryption for data security. The Payment Card Industry Data Security Standard (PCI DSS) Requirement #3 mandates protection of stored cardholder data using technical controls like encryption, masking, and hashing. For health care organizations, encryption technologies provide a “safe harbor” provision negating the need to report data breaches to patients and the Department of Health and Human Services. Privacy laws from U.S. states like Massachusetts and Nevada call for encryption of resident information, while the proposed EU Data Protection Regulation requires the appointment of a data privacy officer responsible for data security and integrity controls such as encryption and key management. Finally, South Korea’s Personal Information Protection Act explicitly calls for encryption use for protection of personally identifiable information (PII). ESG believes that privacy laws in Massachusetts, Nevada, and South Korea are a harbinger of things to come: Data encryption will become a mandate in future regulations.

- **Publicly disclosed breaches.** As of this writing, there have been a total of 126 publicly disclosed breaches exposing nearly 1.5 million personal records thus far in 2012 (source: www.privacyrights.org). These breaches cut across all industries and include organizations such as Zappos.com (24 million records exposed), New York State Electric and Gas (878,000 records exposed), and Arizona State University (300,000 records exposed). Since publicly disclosed breaches can tarnish an organization’s reputation, impact share price, and lead to costly incident response implications, many firms are implementing security countermeasures such as encryption.

- **Intellectual property protection.** CEOs have been dragged into data security due to the rise of Advanced Persistent Threats (APTs) at organizations like Lockheed Martin, RSA Security, and Sandia National Labs. Unlike past security exploits, APTs are targeted attacks with a concrete objective: intellectual property
theft. ESG research\(^1\) indicates that many enterprises are aggressively responding to APTs. For example, the recent wave of APTs led to executive-level actions at 47% of enterprises. Additionally, 77% of large organizations will increase their security budgets as a direct result of APTs. Many firms are already investing in new security technologies for APT protection. Of these new investments, ESG research discovered that 54% of organizations have deployed data encryption technologies in response to APTs (see Figure 1).

<table>
<thead>
<tr>
<th>Which of the following security technology products/solutions has your organization purchased in response to APTs? (Percent of respondents, N=95, multiple responses accepted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data encryption technologies</td>
</tr>
<tr>
<td>Web gateway for blocking suspicious URLs and web-based content</td>
</tr>
<tr>
<td>Application firewalls</td>
</tr>
<tr>
<td>Specific technology defenses designed to detect and prevent APT attacks</td>
</tr>
<tr>
<td>Database security technologies</td>
</tr>
<tr>
<td>Network behavior monitoring technologies</td>
</tr>
<tr>
<td>Managed security services</td>
</tr>
<tr>
<td>DLP (data loss prevention) technologies</td>
</tr>
<tr>
<td>New types of user authentication/access controls</td>
</tr>
<tr>
<td>Endpoint white-list/black-list enforcement technologies</td>
</tr>
<tr>
<td>Third-party penetration testing service from specialty firm</td>
</tr>
</tbody>
</table>


In aggregate, it is safe to say that data encryption evolved from a fringe military/intelligence technology to a mainstream security safeguard over the past 10 years. Traditional objections around performance impact and cost have largely been addressed by multi-core CPUs and commodity cryptographic processors. The combination of economics, technology advancement, and growing use cases has led many CEOs to deploy data encryption technologies far more liberally than in the past.

---

Data Encryption Growing Pains

Like many other initiatives, the use of data encryption has grown organically over the past few years. Driven by the trends described previously, functional storage, database, applications, and server groups often implemented data encryption technologies within their individual domains across disparate heterogeneous technologies on an ad hoc basis (see Figure 2).

Current point products do a good job of protecting private data in isolated areas, but they don’t provide a comprehensive solution to data privacy issues across the enterprise. Additionally, ad hoc encryption creates a number of increasingly troubling issues such as:

- **A lack of standards.** Ad hoc encryption is often based upon multiple “standards” and solutions across disparate functional IT groups and technical controls. In this scenario, data encryption is often poorly implemented by IT professionals who don’t really understand data security requirements. Even organizations embracing emerging industry standards like the Key Management Interoperability Protocol (KMIP) find that it is immature and thus no panacea. This general and continuous lack of standards can only lead to higher costs, redundant processes, and greater risk of a data breach.

- **No central command and control.** In a similar fashion, encryption tools provide their own management consoles for administration, monitoring/auditing, and key management. Each ad hoc solution needs to be configured separately and will provide different levels of functionality, sophistication, and certification. At the very least, this creates an operations nightmare; it also means that sensitive data is at varying degrees of risk depending upon each tool and how it is implemented. Alarmingly, CISOs have no central way to assess or address this.

- **A multitude of key management systems.** Multiple encryption technologies will each have to provision, manage, and revocate keys associated with all encrypted files. Again, with no central key management or
policies, this will have to be managed within each tool. The sheer number of key management operations only increases the risk of a mistake that could lead to a security breach or unrecoverable critical file.

- **Organizational misalignment.** Ad hoc encryption tools are often deployed in a manner where functional IT groups have access to encryption keys. This ignores a key information security principle: separation of duties. Obviously, this could expose encryption keys to numerous IT staff members and thus greatly increase the risk of an insider attack.

All of these issues create operational overhead and increased risk (see Table 1). What’s more, ad hoc encryption processes will be taxed further at companies with each new data encryption solution deployed. Without a better alternative, large firms face an unacceptable future of spiraling operating costs and ever-increasing risk.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cost</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of standards</td>
<td>Redundant processes, multiple tools and licenses, training</td>
<td>Ad hoc products may be configured, implemented, or administered poorly, increasing the risk of data loss or a security breach.</td>
</tr>
<tr>
<td>No central command and control</td>
<td>Redundant processes, multiple tools and licenses, training</td>
<td>Ad hoc products may be configured, implemented, or administered poorly, increasing the risk of data loss or a security breach. No central view for risk management or measurement of KPIs.</td>
</tr>
<tr>
<td>Multiple key management systems</td>
<td>Redundant processes, training</td>
<td>Encryption keys may be exposed increasing the risk of a data loss or a security breach.</td>
</tr>
<tr>
<td>Organizational misalignment</td>
<td>Additional and unfamiliar tasks for functional IT staff</td>
<td>Human error could leave encryption keys exposed. Increased risk of accidental or malicious security incident by an IT employee insider.</td>
</tr>
</tbody>
</table>


**Large Organizations Need an Enterprise Encryption and Key Management Strategy**

It’s time for CISOs and their peers to realize that ad hoc encryption is no longer adequate: It leads to higher costs and increased risk. So, what’s needed? An enterprise encryption and key management strategy that can extend across all sensitive data, in all formats, across the entire organization.

From an organizational perspective, an enterprise encryption strategy will only work if it:

- **Remains transparent.** Encryption cannot disrupt IT performance, place new demands on application developers, or burden functional IT professionals with unfamiliar tasks. Encryption needs to fit seamlessly and unobtrusively into systems and infrastructure.

- **Is owned by the security team.** The CISO and their staff must be responsible for encryption technology selection, policy creation (in concert with business managers), and general oversight. This is especially critical with regard to key management: Smart CISOs will train specific individuals on key management best practices and dedicate this team to all key management tasks and oversight.

- **Provides executive-level visibility into risk management.** CISOs need to be able to assess risk across the enterprise at all times and keep executive management informed of any status changes. An enterprise encryption strategy must include basic visibility tools that help improve risk management communication.
At a more fundamental level, an enterprise data security strategy must counteract the growing issues around ad hoc encryption. In other words, an enterprise encryption strategy must be designed around three objectives: streamlining operations, reducing costs, and decreasing the risk of an accidental or malicious data breach.

Enterprise Encryption Architecture

A true enterprise encryption architecture addresses each of the shortcomings associated with ad hoc encryption described above. As shown in Figure 3, it includes:

- **Central command and control.** This includes several management disciplines including policy management, configuration management, and reporting/auditing. The point here is consolidation: All of these management activities should be controllable from one central location with actual execution occurring throughout the enterprise. In the reverse direction, all management information should flow back to the centralized management repository for storage, analysis, and reporting purposes.

- **Distributed policy enforcement.** Central encryption and key management policies must be enforced on heterogeneous systems distributed throughout the enterprise. To accomplish this, central management consoles must be able to distribute agents, configure individual systems, securely manage encryption keys, and log all activities.

- **Tiered administration.** This “gotta have” functionality enables enterprises to set and enforce both enterprise and departmental policies and allows separation of duties where security administrators, not functional IT staff, control their own encryption management domains. For example, the CISO of a particular business unit may be responsible for administering his group, but he is not permitted to access other teams’ data or change universal policies. Separation of duties and transparency also frees IT personnel to do their jobs while protecting the confidentiality and integrity of sensitive data. In this way, a DBA at a financial services firm can maintain an Oracle database without accessing regulated financial data.

- **Enterprise-class key management services.** As part of an enterprise encryption architecture, key management becomes a central service for all activities, including key creation, storage, rotation, and revocation. Furthermore, key management must be designed for fault tolerance. These services must be available and consistent for heterogeneous operating systems, applications, and databases distributed across the network. Finally, key management servers should provide a demonstrable level of protection with FIPS 140 and/or Common Criteria certification.
CISOs have lots of choices with ad hoc encryption, but they will find a much shorter list of qualified vendors as they begin researching and evaluating options for an enterprise encryption and key management architecture. ESG believes that Vormetric is one vendor to consider here as it does align with encryption requirements like central command and control, distributed policy management, tiered administration, and enterprise-class key management. Additionally, Vormetric can serve as an encryption standard as it supports encryption across Linux, UNIX, and Windows servers, protecting the structured and unstructured data stored on all those systems.

The Bigger Truth

Note to large organizations: One of your most valuable assets, sensitive data, faces an increasing level of risk. Yes, you are addressing sophisticated malware threats and complying with regulations, but when it comes to data encryption, you are doing so while increasing costs and complicating IT/security operations. Oh, and by the way: If you are using ad hoc encryption tactics (and you probably are), you are exposing your sensitive data to far more risk than you think.

ESG highly recommends that CISOs develop an enterprise encryption strategy as soon as possible. To accomplish this, some simple guidelines may help:

1. **Define encryption nirvana.** Start with a clean slate and create an effective encryption and key management strategy for your company. The goals here should include transparency, ease of deployment without disruption, streamlined/central operations, and general risk management for all types of sensitive data on all types of systems.

2. **Assess what you have.** Find out what types of encryption technologies are in place, who owns them, and how they are managed on a day-to-day basis.

3. **Find gaps.** Compare what you have to your ideal solution in order to identify and prioritize the holes.

4. **Begin replacing or augmenting ad hoc solutions based upon data value.** Select a solution that adheres to the architecture defined above. Once in place, begin implementing encryption controls to systems with high value and/or lots of gaps identified above.

An enterprise encryption and key management strategy should be phased in over time with clear goals and success metrics associated with each segment of the project.

Yes, an enterprise encryption and key management strategy will require money and resources, but smart CISOs will recognize the business value and sell it to their peers. An enterprise encryption and key management strategy will enable organizations to control and share information while managing risk. This alone should provide CEOs with all the revenue and cost-saving motivation necessary to get things started.