VORMETRIC WHITE PAPER

Keeping Data Safe in an Outsourced Environment

Employing CoreGuard to Protect Non-Public Information and Intellectual Property When Outsourcing to third parties

VORMETRIC

Outsourcing is a highly attractive strategy in today's tough economy and competitive global market. Like most companies, you probably outsource some functions to third parties to reduce costs and time to market, free up resources to concentrate on your core capabilities, and gain a competitive edge in your market. Global outsourcing offers these substantial benefits, but also poses some notable challenges. The free flow of non-public information (NPI) and intellectual property (IP) in the form of digital information such as source code or engineering drawings has created a dilemma for companies that outsource -- how do you safeguard digital information and still provide the access third-party partners need to get the job done?

The Rise of Outsourcing

The ease with which companies can share information electronically across the globe and the low-cost of labor in countries such as India and China have driven today's outsourcing boom. The barriers that define what can and cannot be outsourced as well as who can outsource are disintegrating rapidly. Gartner predicts global spending on offshore outsourcing services will top $90 billion by 2007.

Outsourcing is not simply the privilege of large corporations anymore either. SMBs are now taking advantage of this new opportunity to leverage economical outsourced resources. According to a study by USA TODAY, nearly 40% of start-ups employ engineers, marketers, analysts and others in jobs created in India and other nations.

How Safe is Your Data Right Now?

The question you should be asking is: how safe is your data right now? Recent security breaches at companies like Choice Point, Wachovia, Bank of America, CitiGroup and Iron Mountain — leaving these companies with lost revenues, reduced shareholder value and lawsuits which defeat the bottom line, as well as damaged reputations — prove that even supposedly well-protected industry leaders are vulnerable.

Outsourcing to the international market makes data security an even greater concern. Many of the tasks delegated to offshore service providers require companies to entrust their outsourcing partner with sensitive data. NPI such as tax returns and credit card data tend to be top-of-mind in the public eye, but outsourcing also poses a costly threat to intellectual property. In outsourcing relationships, a company must often provide the partner with access to vital IP assets which are the key to the company's competitive edge. Exposing this valuable information to outsiders can pose huge risks.

The need to protect intellectual property isn't new — but offshore outsourcing and the evolution of IP into a digital format pose new challenges that must be addressed. No matter how thorough the outsourcing contract, it cannot prevent data theft or provide peace of mind to intellectual property owners, shareholders or service providers.

Recent major breaches in India, the largest offshore outsourcing venue, clearly demonstrate the severity of the situation. For example, call center employees at former outsourcing company Mphasis conspired to steal $350,000 from U.S. consumers' bank accounts.

"This was not a lapse of judgment or an issue of poor customer service: The incident was an organized and systematic plot to steal customers' money," said John McCarthy, Forrester Analyst. "Forrester believes that this breach, coupled with recent onshore disclosures of sensitive customer data, will have far-reaching negative connotations for the offshore BPO (business process outsourcing) space."

In another episode, employees of an Indian outsourcing service provider in the city of Pune are alleged to have used their positions to steal $426,000 from New York-based customers of Citibank. In addition, an undercover reporter from *The Sun*, a UK-based newspaper, reported that an outsource worker offered to sell as many as 200,000 account details a month, declaring that “technology is made by man and it can be broken by man.”

These are just a few examples of the prevalent threat facing companies that outsource to offshore companies and provide these contractors with access to sensitive data.

Assessing Traditional Data Protection Methods

One way companies address these threats is to employ traditional methods for protecting sensitive data, including:

Lock and Key: An acceptable method for protecting hard copy data formats, but powerless to protect digital information.

Employee Screening and Training: While finding the right employees and training them properly is essential, this method does not impose any actual controls on the people with access to data.

Corporate Policies: Written policies to define who can access specific data are important, but policies do not provide any actual protection against unauthorized access or information theft.

These outdated methods simply do not translate into the world of digital information and global outsourcing, providing no protection for data that leaves the four walls of the corporate offices –- and the recent breaches outlined above illustrate this point vividly. Written policies that define which employees can access sensitive data are barely adequate when applied to trusted employees, but they are practically useless as a means to safeguard valuable data entrusted to an outsourcing vendor. There is no way for a company to ensure that employees of the third-party contractor are properly screened and trained or will follow corporate policies.

Companies that outsource need a new way to enforce their data privacy and protection policies. As part of this data security initiative, companies must:

- Create and maintain policies locally that control outsourcing vendor access to data at their physical site.
- Deploy and enforce their local policies on a global scale.
- Prove that the policies are working as expected, and identify anyone who attempts to circumvent the policies.

Securing Data with Vormetric

CoreGuard from Vormetric is the data protection solution designed to keep your digital information safe while you are outsourcing. CoreGuard helps protect enterprise information — including IP, sensitive financial or HR data, and regulated NPI such as customer social security numbers and credit card account numbers — even in outsourcing environments.

Vormetric’s CoreGuard, a cost-effective and easy to manage solution for high-speed data encryption and policy-based user access control, is an essential data protection system for any company, especially those that outsource. It is also a great tool for outsourcing service providers that want to protect customer data. CoreGuard is ideal for outsourcing because policy management can be performed on a global scale from a single location, allowing a company to maintain centralized control over access to distributed assets and enforcement of appropriate use policy for classified information, without incurring an overwhelming management burden.

CoreGuard's policy-based management and high degree of transparency to the existing applications, business operations and IT infrastructure allow easy and economical deployment, management and scalability across a heterogeneous IT environment. In contrast to alternative data encryption solutions, CoreGuard operates seamlessly across all network, storage and data types and requires no changes to your application software.

Vormetric's patented data encryption process offers the highest performance of any data encryption product available in the market today, while the other encryption solutions consume considerable performance overhead. And unlike competitive in-line data encryption products, Vormetric customers have the option to selectively encrypt data which is most at risk, further increasing performance and reducing systems overhead.

Advantages for Companies that Outsource

Companies outsourcing or sharing data with third parties, such as offshore partners, gain the following advantages from Vormetric's CoreGuard:

Centralized Control: With CoreGuard, you manage service provider and other third party access to data with centralized control and remote enforcement of appropriate use policy across the globe.

Security Management Ownership: The system is designed to keep key management where it belongs — with you, the data owner.

Enforcement: CoreGuard empowers you to enforce your data privacy policies, even with your outsourcing vendor.

Verification: Audit logs enable you to report and verify service provider data access through CoreGuard.

Optimized Outsourcing: The power of selective data sharing through CoreGuard makes outsourcing more efficient, more feasible, and less risky, so you can feel free to outsource any tasks necessary without jeopardizing your critical data. Outsourcing more functions allows you to concentrate your resources on core value tasks such as new product innovation and customer service.

Advantages for Outsourcing Service Providers

By implementing Vormetric's CoreGuard to protect customer data, outsourcing service providers gain the following advantages:

Competitive Edge: CoreGuard enables you to promote data privacy and protection as a competitive advantage that differentiates your company in your market. If you serve multiple customers that compete against each other, CoreGuard provides demonstrable assurance that any entrusted data will be visible only on a need-to-know basis.

Secure Administration: Vormetric's ground-breaking MetaClear encryption allows management of data without visibility, so your IT administrators can still manage your customer's data, even though they are not able view it.

Access Control: Database administrator access is managed via Vormetric audit logs, providing you with even more control and accountability.

On-Demand Scalability: CoreGuard software installs and scales easily, enabling you to expand the system as your customer base grows.

Customer Confidence: CoreGuard is designed to keep security management and verification in the hands of your customer, boosting customer confidence in the safety of their data, and ultimately strengthening your customer relationship.

Improved Resource Allocation: Vormetric handles data security for you, freeing your resources to concentrate on acquiring new customers and servicing current ones — efforts that generate more revenue — rather than on securing customer data.

Additional Advantages for Auditing

CoreGuard is designed to facilitate audits relating to compliance in the areas of information security and privacy, an advantage that can be leveraged by companies that are outsourcing, as well as outsourcing service providers.

CoreGuard is ideal for audits because the system identifies who accessed what data, where, when and how — all the details an auditor needs to know. The tool provides a critical audit trail for data accessed by outsourcing partners, which would otherwise be almost impossible to track. CoreGuard's enforcement of IT governance policies and procedures significantly reduces the amount of recurrent testing required to assure auditors of system and application integrity, and comprehensive audit logs reduce the cost and time required to assess compliance with government regulations. The system is entirely auditable to comply with Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), HIPAA, CA SB 1386, the EU Data Protection Act, Visa's CISP, and other mandates regarding the handling and protection of information.

Proven Leadership with Vormetric

CoreGuard has been proven in real-world installations at many leading corporations in a variety of vertical industries that require protection for sensitive data. Vormetric's impressive customer base includes BMW, BJs Wholesale, EDS, Cadence Design Systems, Synopsys, Bank of Tokyo, Mitsubishi, Ocwen Financial Services, University of Texas Hospital, Planitax, and California Water, to name just a few.

Vormetric is the technology leader in the data protection arena, holding 13 patents and FIPS validation on all products. The company is the winner of industry acclamation such as ComputerWorld's 2004 Innovative Technology Award, and serves as a respected partner of industry giants such as IBM, Sun and Oracle.

Conclusion: Protecting Data Inside and Out with CoreGuard

This new era of digital data, outsourced tasks, and global information exchange requires a new way of thinking about securing sensitive data and information assets. Locking up the filing cabinet is no longer an adequate strategy. On the other hand, more conventional methods of data encryption consume performance overhead and do not provide a practical option for protecting data both internally and externally. The best option is to protect digital data with Vormetric's high-speed data encryption and policy-based user access control, allowing global management from a central location. CoreGuard from

Vormetric is an economical, powerful and flexible solution that keeps your data safe while giving you the freedom to outsource tasks and share information with partners that need it.

With CoreGuard, companies can outsource any tasks with worry-free protection of NPI and IP, so they can concentrate on their core competencies. Outsourcing service providers can also leverage CoreGuard to offer customers value-added protection that will heighten customer confidence and sharpen their competitive edge. All players working within the outsourcing business model can benefit from Vormetric's revolutionary technology and the versatile and reliable CoreGuard data security solution.

For more information:

Vormetric Inc
3131 Jay Street
Santa Clara, CA 95054
www.vormetric.com
+1 408 961 6100
Email: sales@vormetric.com

VORMETRIC