Increasing the Return on Investment of Your Hardware Security Module

Organizations often purchase security technology to satisfy specific industry regulations, however, these regulations are only the bare minimum of requirements to ensure the safety of your data and your customers' information.

When developing a strategy for your core cryptographic infrastructure, it's important to consider a holistic plan for how hardware security modules (HSM) will be integrated into your existing infrastructure; establishing a security framework by implementing a system of procedures to complement your hardware security solutions; and what other applications you might find for your hardware security module in your organization.

Viewed from this frame of reference, you begin to unlock the true value of a hardware security module and how it can protect your organization and its sensitive data. This whitepaper discusses common dangers enterprises face and the multifaceted advantages of hardware-based data security solutions.

Compliance: More than a Checkbox

Every industry has its regulatory requirements which, by nature, assign responsibility to certain entities to ensure best practices are followed and protections are enforced. The specifics of these regulations vary from industry to industry, but with the growing confluence of Big Data and the collection of sensitive customer information, one thing has become increasingly common: regulations have been adapting to a growing need for standardization and the development of procedures for securing personal information.

In short, enterprises have a responsibility to safeguard the information they protect and prevent it from falling into the wrong hands. When sensitive information is accessed by unauthorized parties, or data is unintentionally released, it is known as a data breach. The motives for these breaches run the gamut from fraud, to corporate espionage, to state-sponsored espionage or activism, to less intentional breaches involving employee negligence.

> "Personally Identifiable Information is defined as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
>
> ***"NIST Guide to Protecting the Confidentiality of Personally Identifiable Information."***
> ***NIST SP 800-122***

Enterprises spend a significant amount of time, money, and energy complying with industry regulations mandating the protection of sensitive information. In reality, these regulations are only the beginning of the measures an organization must take to properly secure their sensitive information from possible breach. What's more, the regulatory landscape is constantly shifting. Extra measures that organizations currently take to secure their data may someday become mandatory as regulatory requirements evolve. Thus, while regulations are necessary protections for enterprises and their customers, compliance does not ensure complete safety from data breaches.

While much fear is circulating about the prevalence of breaches and the release of customer data, proper planning and consideration of security options can greatly mitigate the risk and help organizations navigate the waters in an increasingly complex regulatory world and avoid costly breaches.

Threats to Enterprise Security

Threats to enterprise security are numerous and well-documented by the media. Hardly a week goes by without reports of large-scale compromises of records, with many of these breaches occurring at large, Tier One organizations. If you are a systems administrator, it may seem like breaches can come from anywhere—and you would be correct in that assumption, based on several studies released in 2013.

According to the findings from Verizon's annual Data Breach Investigations Report, 621 confirmed data breaches with 47,000 reported security incidents were identified in 2012.[2] Among the breaches, 24% came from the retail environment or food services industry. These industries face higher incidents of breaches in part because of the vulnerability of their electronic payment terminals. Credit, debit, and prepaid card terminals are often situated in publicly accessed areas and connected to less secure, public networks, placing them at greater risk for criminals to install malware to intercept cardholder information.[3]

These statistics are consistent with the longer-term data collected by the Privacy Rights Clearinghouse (PRC) which began tracking breaches in 2005. Since then, PRC estimates place the number of records compromised at more than 606 million.[4]

Organizations across multiple industry verticals share this risk. Education (schools and colleges) represented 15% of the incidents, government agencies for 18%, healthcare providers for 16%, and businesses for 52%. The most prevalent cause of breaches: 25% from hackers, 13% from stolen endpoint devices such as tablets, laptops and smartphones, and 56% of all breaches were from outside perpetrators.[4]

What is evident from these numbers is the diversity of entry points which attackers can and do exploit. According to the Verizon Data Breach Investigations Report, 72% of attacks on organizations originate as outsider attacks: including hackers or others without authorized access to network systems and data.[2]

Worrying still, is the threat of a breach caused by a rogue, or simply negligent, employee. Breaches of this type range in type from the lost device like a cellphone or tablet to an orchestrated attack. When industry best practices are not integrated into an organization's policies, or are ignored altogether, the stage is set for an internally driven breach.

Trends in technological development, while they are revolutionizing the way data is stored, accessed, and used, should give organizations pause. Information stored in vast, cloud-based repositories or on unencrypted servers are ripe for a data breach. Additional steps must be taken in order for employees or outside attackers to access the information beyond simple password protection, and limitations must be placed on the ability to transfer large chunks of data using a USB thumb drive or other storage device.

Outsiders have become ever more resourceful in their attacks on organizations. In 2012, a report surfaced describing a website which has commodified access to hacked corporate systems worldwide. An Eastern European-based site sold access to more than 17,000 computers compromised through Microsoft's Remote Desktop Protocol for as little as a $20 registration fee.[5]

To mitigate these risks, organizations are taking a varied approach to data security. A mix of policy-based security procedures and hardware-based security systems with a foundation in data encryption are proving effective in preventing both insider and outsider attacks.

Costs of a Breach

Breached organizations experience a number of negative consequences, which ultimately include financial losses, but also less direct losses including a decline in their brand value and potentially a loss of customers. Total estimated costs from data breaches worldwide in 2012 are cited at an estimated $8.1 billion dollars, with an average of $194 per record.[6]

Data breaches are not isolated events exclusive to large organizations, and the impact to a small company can have devastating effects. According to a study released in 2011, nearly 72% of breaches involved organizations with 100 or fewer employees. The median cost for downtime associated with a breach was $12,500 per day.[7]

Beyond the punitive costs of violating regulations, if an organization is proven negligent, a breach can have far-reaching effects. Risks associated with a breach include:[6]

- Loss of customers and revenue
- Negative publicity in the blogosphere and through media outlets
- Release of personal private information
- Diminishment of customers' and business partners' trust and confidence
- Lawsuits by affected parties and regulatory fines resulting in severe financial losses
- Exposure of confidential proprietary information

Organizations pay a steep price in the wake of a breach. Some regulatory bodies mandate breached organizations undergo a lengthy audit process to determine if proper measures have been instituted to prevent another breach. If the compromised data is related to personally identifiable information, organizations may choose to cover the costs of personal credit counseling or monitoring in an effort to minimize the effects of identity fraud or theft related to the breach.

Benefits of Hardware-Based Security Solutions

Hardware security modules implemented in an enterprise's security infrastructure are dedicated devices built to protect data using physical, logical, and encryption-based security features. HSMs are versatile solutions which can perform a wide array of functions across multiple industry verticals.

Encrypting and authenticating sensitive data using a secure cryptographic device offers unparalleled benefits for maintaining security, preventing fraud, and ensuring regulatory compliance. Breaches from both insiders and outsiders are valid worries for system administrators, but hardware security modules provide an unrivaled form of protection to defend against these vulnerabilities. These tamper-responsive devices are designed to house encryption keys within a secure boundary, eliminating risks commonly associated with software data security tools.

Furthermore, attackers are unable to access the clear encryption keys contained within the HSM, even when they physically tamper with the device, whereas a simple keylogger can often prove the downfall of software-based tools. HSMs, however, are capable of identifying unauthorized access or attempted attacks. Attempts at tampering with the hardware will cause the device to immediately erase all sensitive data, providing an additional layer of protection preventing the attacker from acquiring that information.

Additionally, hardware security technology can offer advanced disaster recovery and redundancy features — functions that guarantee continued operation in the event of an unplanned outage. For global organizations with a vast array of mission-critical data in widespread use on a 24x7x365 basis, this reliability is a necessity.

One Device, Many Applications

**Some functionalities of a hardware security module, such as PIN printing and 3-D Secure, must be carried out on a dedicated device.*

Historically, hardware security modules most commonly have applications in the financial and banking industries for use in debit transactions where the PIN is being encrypted and an exchange of encryption keys occurs for the transactions to be processed. However, an HSM is a far more versatile solution which can serve as an important facet of an organization's data security infrastructure.

Point-to-Point Encryption

Point-to-Point Encryption, also known as P2PE, is a robust technique for encrypting data from the moment which cardholder data is captured until it has entered the secure network of the transaction processor. Sensitive cardholder data, which includes the Primary Account Number (PAN), is initially encrypted at the point of interaction. The encrypted data is sent to the transaction processor, where it is decrypted within the confines of a hardware security module, and then is sent to the card issuer for validation.

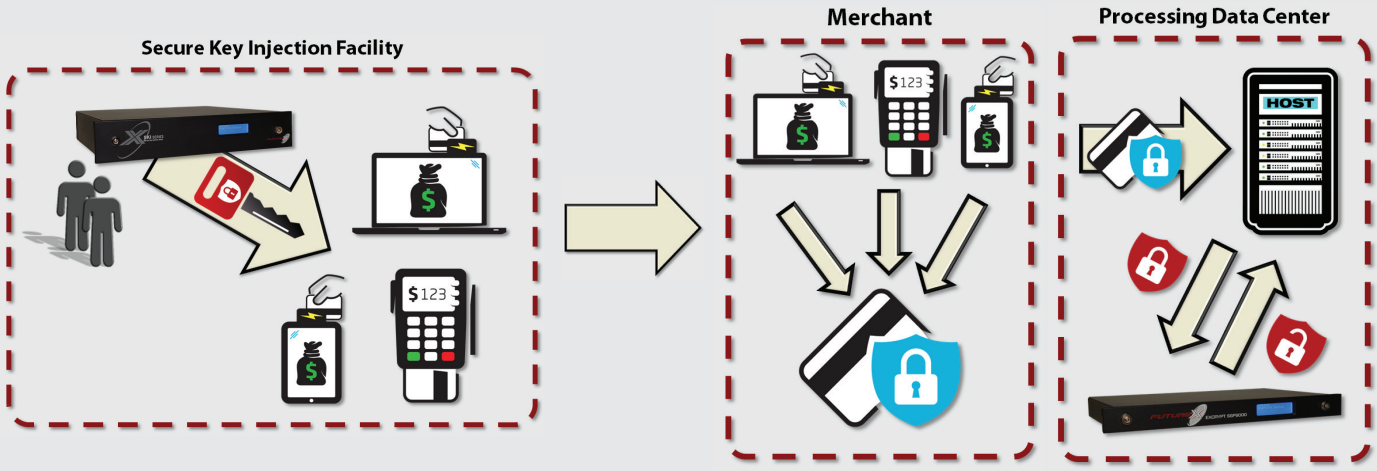
What is an HSM?

A hardware security module, or HSM, is a dedicated, standards-compliant cryptographic appliance designed to protect sensitive data in transit, in use, and at rest through the use of physical security measures, logical security controls, and strong encryption.

P2PE is advantageous because it eliminates clear text PAN data from unsecured communication lines, reducing the scope and cost of PCI DSS compliance and providing a high level of security for organizations transmitting cardholder data. Conventionally, organizations have secured their infrastructure behind their firewall between the host and acquirer but this method does not do enough to protect cardholder information in transit. Without P2PE, sensitive cardholder data is often transmitted in clear text format.

Point-to-Point Encryption: How Does it Work?

1. Cardholder data encryption keys are injected within a secure facility.
2. Payment terminals, deployed at merchant sites, encrypt cardholder data at the point of interaction.
3. Encrypted cardholder data is securely decrypted by the hardware security module.



Tokenization

Tokenization, a technique for reducing the scope and cost of PCI DSS requirements, is a process by which a token, or a string of characters that represent sensitive data, is generated using a mathematical function. The token then replaces all, or nearly all, instances of sensitive data stored within the merchant system, thereby limiting the risk of data breach while retaining the functionality needed by a variety of business processes. Two common methods to achieve this end include using a hash-based Message Authentication Code (HMAC) or encrypting the data directly.

In a hash-based MAC approach, data is put through a hashing algorithm, resulting in a string of identifying information used to verify the integrity and authenticity of data. These tokens are used by both the merchant and the host in the place of the original sensitive data. Both the clear cardholder data and the matching HMAC-derived tokens are stored in the host's secure database for recall in case they are needed, such as for returns or refunds. The merchant only stores, and has access to, the tokens, which cannot be reversed to derive the original cardholder data.

For the encryption method of tokenization, the host and the merchant are completely removed from the burden of storing cardholder data in the clear. All sensitive data is processed inside the hardware security module. Unlike the HMAC-derived tokens, the encryption-created tokens can be decrypted and detokenized.

Data Encryption

The greatest area of risk when trying to protect sensitive data is when it exists in a clear text format. This opens up enterprises not only to the risk of systems being compromised by attackers, but by negligence on the part of employees or other accidental disclosures of data.

For this reason, it is important to keep the idea of data encryption in mind. An HSM can encrypt any set of data using various techniques specifically tailored to achieve any end. It's best to first classify data based on its state, either at rest, in use, or in transit, and then determine how best to encrypt it. Each of these states comes with its own security challenges and techniques for securing data.

One-time Password Generation for Online Security

An organization's online presence can be a particularly vulnerable point for an attacker. Many attacks involve targeting the password validation process, using a replay attack or keylogging to gain knowledge of the user's password, using it at a later point to gain access to systems. A one-time password mitigates this risk by generating a random sequence of characters, so a password that is generated is only valid for a single use.

A hardware security module can be used to generate random numbers used in the generation of passwords. Because these values are generated inside the HSM, they cannot be hacked or tampered with, ensuring the integrity of the access control systems that use them.

Message Authentication and Data Integrity

Message authentication and data integrity are two interrelated yet different concepts, each with the goal of preventing man-in-the-middle attacks. Message authentication is a method to ensure the origin and identity of the sender, whereas data integrity applies to the contents of the message and whether it has been altered. This can be achieved through digitally signing data, or creating a HMAC. The objective of these operations is to verify the authenticity and integrity of the data.

Digitally Signing Documents

With the increasing prevalence of eGovernment around the world, electronic signatures have become increasingly important in the way business is conducted internationally. Many countries have established regulatory requirements mandating the transmission of invoices and tax documents online, and for enterprises doing business in these countries, it is important to ensure the integrity and authenticity of the messages being transmitted.

Using the RSA algorithm, an HSM can send messages encrypted under a public key infrastructure (PKI). A document is digitally signed using the originating organization's private key, and then encrypted with the destination entity's public key. This signature ensures the recipient can authenticate the source of the message. The document is then sent to its intended destination where it can be validated using the originating organization's public key, and subsequently decrypted by the destination's private key. Following this, the message can then be read or validated as intended.

Digitally Signing E-mails

Modern enterprises are often almost entirely dependent upon electronic means of communication. Some of an organization's most sensitive information is transferred daily through its various e-mail channels. What is preventing this e-mail from being intercepted and read or altered in some way? In many enterprises: nothing. A hardware security module can be used to digitally sign e-mails, ensuring the integrity and authenticity of the message have been maintained. This is achieved through a similar method of signing the documents mentioned in the previous section, with the signing of the e-mail and attachments using the sender's private key and verified using their public key.

Generation of Identification Cards

In any enterprise, identification for employees, vendors, and customers is an important part of not only maintaining a sound physical security plan, but also ensuring the safety of an organization's sensitive data. These credentials can be used to limit access to physical spaces as well as information systems. The cryptographic procedures involved with operating a card or identity issuance system can be performed using a hardware security module.

Securing Online Transactions

An incredible amount of commerce has moved to online retail sites which are also susceptible to fraudulent transactions. In an effort to increase security and curtail fraudulent transactions, a security protocol called 3-D Secure has been adopted by the major credit card brands. Customers are required to enter a value tied to the use of the credit card at the time of the transaction. This value acts like a PIN in debit card transactions as an additional authentication step.

A hardware security module must be used both to generate this value for the card issuers and to validate the transactions. Like PIN issuance, however, 3-D Secure requires a dedicated hardware security module.

PIN Issuance and Printing

In instances where customers need to obtain their debit card PIN but cannot appear at a bank branch in person, their PIN can be securely printed and mailed to their location. PIN printing allows debit card issuers to print PINs directly and securely from a hardware security module. Solutions involving PIN printing should be compliant with PCI PIN Transaction Security requirements, and as these regulations mandate, the PIN printing function must be carried out on a dedicated, single-purpose HSM.

Prepaid Card Issuance

Employees spend an increasing amount of time at work, and some enterprises are large enough to rival the size and complexity of small towns. For the convenience of these groups as well as the benefit of the organization, closed-loop prepaid cards provide an ideal, mutually beneficial solution. Prepaid cards can be loaded with funds for use in the cafeteria, vending machines, or other monetary exchanges, and periodically reloaded with funds for repeated use.

Database Encryption

Some enterprises require storage of vast repositories of data. Healthcare organizations must store millions of patient records, universities store academic research and student records, and retail organizations must store the transaction records of customers to be able to conduct customer returns or void transactions. Storing records in clear repositories makes them high-value targets for criminals. In some industries, individual records hold a street value in the hundreds of dollars. Negligence falls on the other end of the spectrum. Sometimes the hardware these databases are stored on can be inadvertently lost or can be disposed of improperly, exposing sensitive information to anyone who could casually gain access to them.

For these reasons, it is important to encrypt data while it is at rest. Some databases support encryption using a standards-based library such as PKCS#11 that is linked with an HSM so that data entering the database for storage may be encrypted and only decrypted when access is needed.

EMV Card Issuance and Transaction Processing

Payment card fraud is an increasingly troubling issue for acquirers, issuers and merchants. In 2012, losses of $11.27 billion were reported, a 14.6 percent increase from 2011. For issuers, counterfeit cards presented at the point of interaction are the main source of losses; for merchant and acquirers, losses occur as a result of fraudulent card-not-present transactions.[8]

EMV card technology has proven effective at deterring fraud and increasing security. EMV stands for Europay, MasterCard, and Visa and is a global standard for chip-based debit and credit card transactions. EMV cards, also known as smart cards, are embedded with a microprocessing chip. Smart cards guard against the use of counterfeit cards which are produced inexpensively by criminals who either "skim" card numbers from Point of Sale terminals or purchase large quantities of valid card numbers on the Internet. EMV reduces fraudulent transactions because even if the account data is stolen, it cannot be used to create a duplicate card due to the secure nature of the embedded smart card chip.

An HSM can be used in the issuance of EMV smart cards as well as the processing of EMV transactions. It is essential for a compliant hardware security solution be integrated into smart card-based payment systems to protect the encryption keys needed to validate transactions. EMV cards support Public Key Infrastructure, a two-key encryption system that has been used for many years to provide critical security services for online banking, secure VPN connections, and more.

Validation occurs when EMV cards, used in online mode, and a transaction processor communicate with an HSM to authenticate the cardholder prior to transaction approval.

Conclusion: Putting It All Together

It's important for system administrators to pursue a holistic approach when developing a plan for their cryptographic infrastructure. Investment in an HSM is not a decision to be taken lightly; a best-in-class HSM will be a significant purchase, however if industry experts are consulted during the decision process, an organization can significantly improve the return on their investment.

An industry expert, one with training certifications such as CTGA (Certified TR-39 Auditor), as well as hands-on experience, will be able to see your organization through the same lens an auditor would. A trusted advisor can bring significant experience of how other organizations in the same industry have implemented solutions, and how your cryptographic solution can be specifically tailored to your unique infrastructure.

The very same expert will be able to provide invaluable advice in developing versatile core cryptographic infrastructure that achieves additional business goals beyond simply fulfilling regulatory compliance mandates. A hardware security module is effective in reducing the risk of a breach, but cannot succeed without the proper management of information and people. An old industry axiom states that, "security is a combination of information, people, and technology." All three facets must be properly managed in order to create a secure environment.

Have you considered what other functions your hardware security module can fulfill? Are you using other services to sign your documents or are you considering other encryption methods for your databases? A hardware security module can easily integrate into your current infrastructure and considerably increase the security of your IT ecosystem.

About Futurex

For over 30 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions. More than 15,000 organizations worldwide have trusted Futurex's Enterprise Security Platform to provide innovative, first-to-market solutions for the secure encryption, storage, and transmission of sensitive data.

http://www.futurex.com

Sources

1. McCallister, Erika; Grance, Timothy; and Scarfone, Karen A.."NIST Guide to Protecting the Confidentiality of Personally Identifiable Information." NIST SP - 800-122. 6 Apr. 2010.
2. "2013 Data Breach Investigations Report." Verizon Enterprise Security. May 2013.
3. "24% of Data Breaches Target Retailers." Computerworld Hong Kong. 3 May 2013.
4. "Dataloss Database Statistics." Open Security Foundation. May 2013.
5. Armerding, Taylor. "Line blurs between insider, outsider attacks." Network World. 25 Oct. 2012.
6. "2013 Data Protection and Breach Readiness Guide." Online Trust Alliance (OTA). 15 Mar. 2013.
7. "2011 Cost of a Data Breach Survey." Ponemon Institute. Mar. 2012.
8. "Global Card Fraud Losses Reach $11.27 Billion." The Nilson Report. 15 Aug. 2013.

Global Headquarters 864 Old Boerne Road, Bulverde, Texas 78163 USA
TF 800.251.5112 P +1 830.980.9782 F +1 830.438.8782 info@futurex.com
WWW.FUTUREX.COM