Enterprise Data Protection: A Security Strategy for Improving Business Processes and Reducing Data Losses

Derek Tumulak, vice president, product management, SafeNet, Inc.

With data breaches on the rise, financial institutions must constantly develop new strategies and security architectures to safeguard their assets. Failure to stay in front of data threats will inevitably result in further breaches, financial losses, and tarnished reputations.

For years, financial institutions focused on perimeter security to thwart the ever-increasing number of data threats. But now, with more than 50 percent of security breaches perpetrated internally, perimeter defenses are no longer sufficient for securing data.

Today, companies need to extend their data infrastructure across business units, partners, suppliers, customers, and a growing mobile workforce. The outsider is now an insider. Because of this, financial institutions must adopt an enterprise data protection strategy in order to effectively protect data from the core to the edge of the enterprise, an end-to-end encryption solution across databases, applications, networks, and endpoint devices. The result is secure data at all times—at rest, in motion, and in use.

Many financial institutions are looking towards consolidation and merging security infrastructures in an effort to cut costs, retain customers, and improve business

processes. Be careful. Data is extremely vulnerable during consolidations because it resides on multiple heterogenous systems that are often complex, incompatible, and difficult to secure; the slightest hiccup can be disastrous.

Classifying Sensitive Data

Data classification is an important element of achieving data privacy. When performing this task, take the following actions:

- Determine data confidentiality levels
- Identify and classify sensitive data.
- Determine where sensitive data is located
- Determine data access models

Define a Security Policy Around Identified Data

Once the data identification and classification process is complete, you are ready to develop a security policy, which turns enterprise expectations into tenable objectives. The essential points of a comprehensive security policy include the following:

- **Acceptable Threat Level**—Determine an acceptable level of threat, keeping in mind that the sooner in the data processing life cycle the data is encrypted, the more secure the overall environment.

- **Authentication and Authorisation Policies**—Develop an authentication and authorisation policy that leverages best practices and historical information to help determine which users, processes, and applications have access to sensitive information.

- **Compliance Measures**—Identify the legislative measures that apply to your organisation, and, once an acceptable threat model is agreed upon, translate those legislative requirements into technical requirements.

Determine a Mode of Data Privacy Implementation

Implementing a data privacy solution can be done at multiple points within the enterprise. Choosing the point of implementation dictates the work ahead and significantly affects the overall security model.

- **Network-level encryption** guarantees the most secure deployment of a data privacy solution, ensuring that the data is secured at every point within the enterprise. Enterprises routinely interact with customers, partners, and other entities over the Internet, and secure the transport of those communications with well-defined and mature technologies, such as SSL and IPsec. Yet, once these secure communication points are terminated, typically at the network perimeter, secure transports are seldom used within the enterprise. Consequently, information that has been transmitted is in the clear and left unprotected. One solution is to selectively parse data after the secure communication is terminated and encrypt sensitive data elements at the SSL/Web layer. Doing so allows enterprises to

choose, at a very granular level, sensitive data and secure it throughout the enterprise.

- **Application-level encryption** allows enterprises to selectively encrypt granular data within application logic. This solution provides a strong security framework and will leverage standard application cryptographic APIs. This type of solution is well-suited for data elements (e.g., credit cards, e-mail addresses, critical health records, etc.) that are processed, authorised, and manipulated at the application tier. Application-level encryption protects data against database and storage attacks, and theft of storage media.

- **Database-level encryption** secures data as it is written to and read from a database. This type of deployment is typically done at the column level within a database table and, if coupled with database security and access controls, can prevent theft of critical data. Database-level encryption eliminates all application changes required in the application-level model, and also addresses a growing trend towards embedding business logic within a DBMS through the use of stored procedures and triggers. Careful consideration has to be given to the performance impact of implementing a database encryption solution. First, enterprises must adopt an approach to encrypting only sensitive fields. Second, this level of encryption must leverage hardware to increase the level of security and to offload the cryptographic process in order to minimise any performance impact.

- **Storage-level encryption** enables enterprises to encrypt data at the storage

sub-system, either at the file level (NAS/DAS) or at the block level SAN. This type of encryption is well-suited for encrypting files, directories, storage blocks, and tape media. In today's large storage environments, storage-level encryption addresses a requirement to secure data without using LUN masking or soning.

Essential Building Blocks of Data Privacy

When considering a data privacy solution, there are clear choices regarding the modes of implementation. All of these options vary in terms of security model, yet each provides a level of protection aligned with the potential requirements of an enterprise.

- **Secure Key Management**—At the heart of any data privacy solution are the secret cryptographic keys used for encrypting and decrypting sensitive data. The data privacy solution must include the ability to securely generate and manage keys. This can be achieved by centralising and automating key management tasks on a single platform, leading to both operational efficiency and reduced cost.

- **Cryptographic Operations**—Enterprises should fully understand the capabilities of cryptographic operations, including when to use certain algorithms to secure data, and hashing functions and keyed hashes for data elements, such as passwords and digital signatures, to ensure non-repudiation.

- **Authentication and Authorisation**—Authentication allows the enterprise to restrict which users are allowed to access data in the clear. Coupled with an

authorisation component, this can provide a strong layer of security with granular access controls.

- **Logging, Auditing, and Management**—When encrypting data, one has to consider the fact that data, keys, and logs will be accessed, encrypted, managed, and generated on multiple devices and in multiple locations. When contemplating an enterprise-wide solution, it is essential to consider one with a centralised interface to view information as attacks occur, and that ensures compliance with logging and auditing requirements.

- **Backup and Recovery**—Backing up all cryptographic keys and configuration information is essential so all information can be restored from a secure device after an unplanned outage. As the enterprise considers key rotation as part of a proper security strategy, they must also design a mechanism with which to associate cryptographic keys to periods of time during which the keys were used.

- **Hardware**—Today's complex and performance-sensitive environments require the use of specialised cryptographic chipsets built around handling high volume cryptographic operations. Doing so will help keep application, database, and storage systems at optimal performance levels.

Leveraging Existing Technology Standards

In addition to reducing IT expenses, it is important to leverage existing technology

standards that will help ensure security, performance, scalability, interoperability, and supportability of the overall solution. Furthermore, by leveraging existing technology where appropriate, enterprises can more quickly and effectively deploy a complete data privacy solution.

- **Leverage Secure Transport Standards**—Existing standards, such as SSL and IPsec, are widely used for securing data transport over IP networks, and are easily leveraged for deploying a data privacy solution.

- **Authentication, Authorisation, and Auditing Technologies**—Leverage all of the AAA services within an organisation to augment a data privacy solution. This includes users and processes that have access to different resources, as well as an audit trail that can provide detailed logs for each access event.

- **Specialised Hardware**—Dedicated hardware platforms can perform cryptographic operations at a much faster rate than a software-based solution running on standard hardware. Some hardware solutions even provide an additional level of security by never allowing private keys to leave the device and performing all cryptographic operations internally.

- **Cryptographic Algorithms**—Use of standard and proven cryptographic algorithms, such as AES and RSA, are critical to ensuring a high level of security and managing risk associated with evolving to future data privacy solutions.

- **Software Interfaces**—Use of standard software interfaces is important for managing the risk of future enhancements to data privacy solutions.

An effective data privacy solution must follow the data from the core, where key data repositories exist, to the edge, where the data is used. When selecting a data privacy solution—especially in times of transition or consolidation—you should know the fundamental elements of the solution, be sure to leverage standards-based technologies, and insist that proper planning and cooperation occur. Doing so will ensure an effective security solution that reduces the complexity, management, and maintenance costs of the organisation's IT infrastructure, as well as provide a foundation for addressing future data protection needs, business processes, and regulatory compliance mandates.