Protecting Corporate Personally Identifiable Information

Because You and Your Business Depend On It

June 24, 2014

by

Jay Wack, President

TecSec, Inc

Nearly every business acquires, uses, and stores personally identifiable information (PII) about its employees, customers, and business partners. Organizations are expected to manage this private data appropriately and take every precaution to protect it from unauthorized access or theft. Misusing, losing or compromising this information can carry a significant financial cost, damage a business's reputation and in some cases result in criminal prosecution.

Given the various costs associated with a breach or exposure of PII, safeguarding PII is necessary for business. The good news is there are cost-effective ways available to secure data, using an integrated encryption and key management solution, solidly based on Standards.

There are laws and regulations governing the collection, storage and use of all manner of PII. These regulations pertain to any data that could potentially be used to identify, contact, locate, or impersonate a customer, employee, patient or any other individual that interacts with your organization. Some regulatory measures focus on specific market segments, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act for health care. HITECH and other regulations not only apply fines, but they require disclosure and notification of those affected. In some cases, companies have been required to pay for free credit monitoring reports for each record compromised.

There are other measures that have implications across a broad range of industries. The Payment Card Industry Data Security Standard (PCI DSS) applies where payment and debit card transactions are prevalent, including retail, insurance, banking, brokerage, education, hospitality, entertainment, government, health care and transportation businesses.

At least 46 U.S. States and territories have passed data breach legislation, significantly increasing businesses' exposure to civil actions by individuals and state administrative agencies over the issue of maintaining security of personal data. These laws mandate that a company which compromises the PII of anyone living in their state, including access by an unauthorized employee, must notify the affected individuals. There are severe monetary penalties involved, from $500 to $750,000 in some states, for not properly notifying those individuals whose PII data was compromised. Some states have now even built PCI DSS compliance into their data breach legislation. And others have passed legislation requiring businesses to proactively implement security measures to protect PII before a data breach occurs.

PII data is generally defined as any data that can potentially be used to uniquely identify, contact, or locate an individual. The broad definition includes first name, or initial, and last name in combination with any of the following categories of information (as long as that information is not otherwise publicly available): Social Security and National Insurance numbers, passport number, bank account number, PIN, employee identification number, driver's license number, date of birth, mother's maiden name, credit card or financial account information, results of a background or criminal history check, payroll and salary information, medical records, as well as digital or other electronic signature files.

The passage of the HITECH Act increased penalties for information security negligence and extended enforcement authority to state attorneys general. The passage of the associated guidance from the Department of Health and Human Services (HHS) signals the first time a federal regulation addresses data breaches, specifically breaches involving unencrypted Personal Health Information (PHI). The data security sections of the HITECH Act were developed to require organizations that handle PHI to meet baseline criteria for protection of data in motion,

in use, at rest, and when disposed. The HITECH Act reinforces HIPAA to encourage use of electronic patient records and to deliver more strict data protection regulations for more secure patient privacy and confidentiality.

Data security experts and technology analysts agree HITECH is significant because it provides clarity around the protection of PHI and puts an unprecedented emphasis on encryption. Encryption of PHI data at rest and in transit provides a safe harbor that protects organizations from the costs and hassles associated with data breach notifications, and fines that can reach $1.5 million.

Over the last several years, in order to meet the protection requirements of PII regulations, there has been an increasing recognition for the need to move protection from the perimeter to the data itself, protecting data at its source, whether at rest or in transit, is now a widely adopted best practice for organizations around the world. Why?

- Perimeter security does not secure PII throughout its entire lifecycle, leaving it vulnerable on mobile devices, in eCommerce transactions, and in applications.
- The frequency of data breaches is increasing and PII is among the most valuable data for cybercriminals.
- The consequences of a data breach are becoming much more significant in terms of cost, lost business, and brand trust.
- Data protection laws in at least 46 U.S. States specifically mandate protection of PII, as do laws in the United Kingdom and the European Union.
- Other government and industry mandates call for protection of data that falls under the definition of PII, including the PCI DSS, HIPAA, the HITECH Act and Sarbanes-Oxley.

Encryption and Key Management

As enterprises seek to protect PII from cybercriminals, internal theft or even accidental loss, encryption and the associated key management, have become increasingly important and proven weapons in the security arsenal for data at rest in databases, files, and applications, and for data in transit.

One constant in the laws is a safe harbor provision, which provides an exemption to disclosure requirements if the sensitive data was encrypted and the keys used for the encryption were not compromised. What this means is that even if the sensitive data was accessed, as long as it is rendered useless, there is no reason to disclose the breach. By not requiring notification of affected individuals following a security breach where sensitive personal information is encrypted, the laws are encouraging businesses to encrypt data, avoiding the cost and complexities.

Enterprises face a daunting security challenge. Not only must they build an impregnable fortress around their internal networks and applications, but at the same time, they must also contend with the complication of sending and receiving encrypted data, and encrypting data at rest within application files and databases that were not designed for the secure handling of data.

Encryption is a perfect companion to strong perimeter and firewall protection. Encryption is not new. Enterprises have been using cryptography for computer security purposes for several decades. When networks were private, data was rarely encrypted. Its primary purpose was to protect certain secret fields such as passwords from someone accessing them in an unauthorized manner, and for the most part the associated encryption keys and passwords were rarely changed.

Organizations today must rely on public networks to access and transmit information. Computing power is everywhere; on laptops, PDAs, tablets, and thumb-drives. Wireless connectivity is even more open and a larger opportunity for eavesdroppers and thieves. The amount of information that must be encrypted and decrypted at rest and in transit is increasing exponentially, leading to a corresponding encryption key management challenge.

In the past years of cryptographic usage, keys were fixed, and the keys would proliferate throughout the data encryption lifecycle, multiplying with re-keying and increasing in complexity over time. If not managed properly, a problem emerges…how to control and protect access to the large number of fixed keys to ensure that they don't get into the wrong hands, and assure that they are available when needed to unlock data, today and in the future. There is mounting demand for an effective, practical, risk-mitigating way to manage keys throughout their lifecycle so that good guys are facilitated and the bad guys are defeated.

To address this demand for a manageable approach to cryptographic keys one must look at the entire process, recognizing that there is no "one size fits all" approach. What is necessary is a cryptograph framework…an approach that provides a mechanism that addresses the move from the communication security (Comsec) to information security (Infosec), while at the same time allowing the various components of each particular subset of requirements to be adjusted in response to the risk and address the associated cost of the implementation.

Cryptography or encryption can be manifested as protected channels or protected content. Methodologies incorporated into the key management process can also expand the application

of either the protected channel or the protected content approach. There are advantages and disadvantages to which application of encryption is chosen – the protected channel with its encryption is treated as separate of content and is limited to a point-to-point capability – the protected channel offers security for encrypted data in transit; whereas, the protected content with its encryption expands the security model to include encrypted data in transit and encrypted data at rest – by having encryption directly impacting the data or content, the resultant encrypted security model is traveling with the data and not related to whatever channel is available. Content protection can exist within protected channel architecture approach. Encryption solutions exist that contain protected channels, but shifting the security parameter to marry with the content that exists within the protected channel offers another level of protection and threat deterrence.

Encryption for protecting content can be a static key model or a dynamic key model – fixed keys that may be found in symmetric and public key models can be viewed as static, and can have inherent scalability limitations – encryption models have evolved with a central server for executing fixed keying among entities that want to share data, and at an encryption event, keying associated with the encryption event includes the participation of a server. For a second content protection model, a dynamic key model uses the same encryption components found in symmetric and public key math, but can include a further step to create a working key for each encryption event which is generated at the time of the event. The result is that the keying components can be bound to the content which in itself may be manipulated as Objects.

Encryption technology necessary to accomplish the object level protection required exists, and has been peer reviewed and standardized, such that it can further define the framework for protecting content with data separation that uses encryption enforcement.

ATTRIBUTE BASED ACCESS CONTROL AND CONSTRUCTIVE KEY MANAGEMENT

Attribute Based Access Control is a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request. ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) concepts. ABAC enables precise access control, which allows for a higher number of discrete inputs into an access control decision, providing a bigger set of possible combinations of those variables to reflect a larger and more definitive set of possible rules to express policies.

The Constructive Key Management (CKM) system relies upon the assignment of subject attributes to subjects and object attributes to objects, and the development of policy that describes the access rules for each object. Each object within the system must be tagged or assigned specific object attributes that describe the object. For example, consider a document residing in a directory within a file management system. This document has a title, an author, a date of creation, and a date of last edit—all object attributes that are determined by the creator, author, or editor of the document. Additional object attributes may be assigned such as owning organization, intellectual property characteristics, export control classification, or security classification. Each time a new document is created or modified, these object attributes must be captured. These object attributes are often embedded within the document itself, but they may be captured in a separate table, incorporated by reference, or managed by a separate application.

Each subject that uses the system must be assigned specific subject attributes. Consider a user accessing a file management system. The user is established as a subject within the system by an administrator and characteristics about that user are captured as subject attributes. This subject has a name, a role, and an organization affiliation. Other subject attributes may include US Person status, nationality, and security clearance. These subject attributes are assigned and managed by an authority within the organization that can maintain the subject identity information for the file management system. As new users arrive, old users leave, and characteristics of subjects change, these subject attributes must be updated.

Every object within the system must have at least one policy that defines the access rules for the object. This policy is normally derived from documented or procedural rules that describe the business processes and allowable actions within the organization. For example, in a banking environment, a rule may state that only approved personnel shall be able to access a customer's account record. If a subject has a Personnel Type Attribute with a value of Secretarial Staff and they are trying to perform the operation *Read* upon a document with a Record Attribute of Customer Account Record, access will be denied and the operation will be disallowed.

The rules that bind subject and object attributes indirectly specify privileges (i.e., which subjects can perform which operations on which objects). Allowable operation rules can be implemented through many forms of computational language such as:

- A Boolean combination of attributes and conditions that satisfy the authorization for a specific operation, or
- Specified lists of attributes or similar methods of explicitly relating specific subjects to specific objects and the allowable set of operations.

Once object attributes, subject attributes, and policies are established, objects can be protected using CMK. Cryptographically enforced access control mechanisms guard access to the objects by limiting access for allowable operations by allowable subjects. The CKM run-time environment assembles the policy, subject attributes, and object attributes, then renders and enforces a decision based on the logic provided in the policy. CKM run-time is able to manage the workflow required to make and enforce the decision, including determining what policy to retrieve, which attributes to retrieve in what order, and where to retrieve attributes. The run-time environment then performs the computation necessary to render a decision.

The policies that can be implemented in a CKM model are limited only to the degree imposed by the computational language. This flexibility enables the greatest breadth of subjects to access the greatest breadth of objects without having to specify individual relationships between each subject and each object. For example, a subject is assigned a set of subject attributes upon employment (e.g., Nancy Smith is an Account Manager in the *Trust Department*.). An object is assigned its object attributes upon creation (e.g., a folder with *Trust Instructions* of *Client)*. The object owner creates an access control rule to govern the set of allowable operations (e.g., all *Account Managers* in the *Trust Department* can *View* the *Client Records).* Adding to the flexibility, attributes and their values are then available to be modified throughout the lifecycle of subjects, objects, and attributes.

Provisioning attributes to subjects and objects governed by a rule-set that specifies what operations can take place enables an unlimited number of subjects to perform operations on the object—all without prior knowledge of the specific subject by the object-owner or rule-maker. As new subjects join the organization, rules and objects do not need to be modified. As long as the subject is assigned the attributes necessary for access to the required objects (e.g., all Nurse Practitioners in the Cardiology Department are assigned those attributes), no modifications to existing rules or object attributes are required. This benefit is often referred to as accommodating the external user and is one of the primary benefits of employing CKM solutions.

Standardization is important, and the CKM key management model is comprised of processes which are based on NIST or x9 banking standards. These standards can identify the overall process as well as specifics found in an encryption framework, life cycle for the keys, keying protocols, and encryption algorithms

The encryption technology of Constructive Key Management (CKM) includes an administrative process that establishes and distributes various CKM keys to be used in a dynamic key management process called the Combiner – the result of the Combiner process is a dynamic working key that is directly linked to a data encryption event.

Further, the result of the CKM process provides active *data label awareness or attribute based awareness,* and *access control* to any digital object, enforced by cryptography. This CKM process provides self-protecting data objects that are data label aware; which in turn enables services to be based on that awareness. This technology approach makes transmission a matter of availability and storage a matter of convenience; supporting multiple levels of information on a common platform. The solution set addresses differential access to content, information sharing, and coalition force differential access control to information. Features of the CKM process include: creation of self-protecting data objects, fine grained objects that are data label aware, dynamic key constructed at time of need, and role based access to content over time.

For more information contact:

Jay Wack

TecSec, Inc
12950 Worldgate Drive
Herndon, Virginia 20170

571 299 4107 office
301 758 6344 cell