

Protecting Sensitive Data and Meeting Compliance Requirements

Michael Whitcomb

President
Loricca, Inc.

Vinny Sakore

Vice President, Business Development
Immersion, Ltd.

A company's data is its most valuable asset. Regardless of whether it is sensitive intellectual property on the newest product, financial records, or confidential customer health information, protecting and controlling data is the heart of every company's security and compliance program.

Protecting Sensitive Data and Meeting Compliance Requirements

On the night of September 1, 1798 the vault at Carpenter Hall was breached and the then massive amount of \$162,821 went missing. This first bank robbery, attributed as an “inside job”, in the United States ushered in an era of robberies that made criminals into celebrities. Jesse James, Bonnie and Clyde, and John Dillinger become legends.

Today’s bank robbers go by names like Anonymous, Soupnazi, Dark Dante, and are often in their twenties and thirties. “Inside jobs” still exist, but instead of physically breaching the security of a bank, criminals are hacking into and accessing electronic vaults. Instead of raiding the storeroom of a blacksmith and key-maker, they are raiding laptops, hard drives and “spear-phishing” to obtain usernames and passwords.

A company’s data is its most valuable asset. Regardless of whether it is sensitive intellectual property on the newest product, financial records, or confidential customer health information, protecting and controlling data is the heart of every company’s security and compliance program. Verizon’s 2011 Data Breach Investigations Report found major changes in how cyber criminals are trying to steal this data. According to the report the number of lost records dropped significantly but the number of breaches was the highest to date.

Verizon found outsiders were responsible for 92 percent of breaches, a significant change from earlier years. The number of attacks from insiders remained relatively constant, but is a smaller percentage of the overall problem due to a huge increase in smaller external attacks.

Verizon found outsiders were responsible for 92 percent of breaches, a significant change from earlier years. The number of attacks from insiders remained relatively constant, but is a smaller percentage of the overall problem due to a huge increase in smaller external attacks. This represents a major change in focus from previous years where insiders were considered the largest threat.

The study also found that 97 percent of the breaches were avoidable, with relatively simple and inexpensive corrective actions. Data breaches can and will happen to any business, regardless of size, industry or location. A company cannot eliminate data breaches, but they can greatly reduce their frequency and the amount of data involved.

This white paper examines the threats and corrective actions companies can employ to protect their sensitive data.

Data Breach Risks

Cyber criminals change the methods used to attack companies and steal data based on what is working. As companies improve their security and compliance programs, the criminals look for areas of weakness and change their tactics accordingly. An example of this is the onslaught of attacks by organized crime against the hospitality industry.

SpiderLabs Global Security report states the following:

“While a reduction of breaches within the hospitality industry was observed from the prior year, hospitality businesses should remain on high alert. At this time, it appears that the organized crime group responsible for the majority of hospitality breaches in 2009 expanded their target list. Instead of focusing exclusively on the hospitality industry, this group became active within the food and beverage and retail markets as well. Evidence suggests this single organized crime group was responsible for 36% of all data breaches investigated by SpiderLabs in 2010.”

To address these new tactics, organizations must adjust their security and compliance programs to address new trends while keeping a solid foundation in place.

The risks in 2011 have changed significantly from previous years in their source and frequency of attacks. Risks can be generally categorized into logical risks or physical risks, although criminals frequently use a combination of methods to conduct an attack. There has been a significant drop in the large scale breaches widely reported in previous years; now the focus is on smaller, more specific attacks. The attacks are also increasingly targeting small- and medium-sized businesses.

“While a reduction of breaches within the hospitality industry was observed from the prior year, hospitality businesses should remain on high alert. At this time, it appears that the organized crime group responsible for the majority of hospitality breaches in 2009 expanded their target list. Instead of focusing exclusively on the hospitality industry, this group became active within the food and beverage and retail markets as well. Evidence suggests this single organized crime group was responsible for 36% of all data breaches investigated by SpiderLabs in 2010.”

Physical attacks doubled as a percentage of all breaches in 2009; in 2010 they doubled again. Physical attacks include not only the obvious theft of physical documents or computer hardware, but also manipulation of computer devices to allow the transfer of electronic data. Recent attacks involved monitoring of the communication links for ATM terminals and modification of point-of-sale terminals. The risks of physical threats need to be recognized as a main vector that cyber criminals are using and included in the overall security program.

Social engineering, the practice of manipulating people, is frequently used in conjunction with other physical means to obtain the necessary access. “Spear-phishing” is a virtual trap set by cyber thieves that uses official-looking emails to lure you to fake websites and trick you into revealing your personal information. The most infamous Internet scam was one promising about a million U.S. dollars as fees to the recipient if he/she helped transfer funds of about 5 million USD. The email supposedly originated from Nigeria (or one of the African countries) and was sent by the wife/son/daughter of a slain military commander and hence it is sometimes also referred to as the Nigerian Letter Scam.

The most popular and successful data breach methods utilize some form of a logical attack. Logical attacks can be highly automated, repeatable and committed at lower risk for the criminal. In 2011, most of these attacks came from external sources. Logical attacks include malware and hacking which Verizon found to be responsible for almost 80 percent of the lost data in their study. The 2011 hack of Sony’s PlayStation network is a good example of a logical attack. Many believe the group Anonymous to have used a denial of service attack to take down the network. Other famous examples of logical attacks are Heartland and TJX. In the Heartland incident, the now infamous Albert Gonzalez used a SQL injection attack to install “back door” malware onto a server and then proceed to transfer credit card data to his own servers.

Weak and ineffectual passwords/credentials are another major focus for cyber criminals. Testing completed during security assessments has frequently found passwords to be easily broken and even left at the out-of-the-box default value.

Logical risks are best addressed by focusing on essential controls across the business. Establish strong security/compliance policies and ensure they are enforced. Insure employees are trained and reminded of the need for security through an awareness program. Further, proactive monitoring of logs and events for all systems containing sensitive data will identify potential hacking attempts early.

Data Discovery

Before an organization can protect its data it needs to identify and locate valuable or sensitive data. This can be a difficult and time-consuming process but is essential to focus the available budget where it will best address the business risk. The discovery process should include all forms where data might exist: 1) structured data; 2) unstructured data; and 3) physical documents. Also consider including production, test and development systems as well as their electronic backups. Structured data refers to data stored in organized file systems or databases and used by applications. These are generally identified by creating an inventory of applications and the associated data stores. Conduct interviews with the subject matter experts for the applications to identify specific database tables or file names which contain the sensitive data. Additionally, the type of data should be documented. The type of data frequently determines

Before an organization can protect its data it needs to identify and locate valuable or sensitive data. This can be a difficult and time-consuming process but is essential to focus the available budget where it will best address the business risk.

the compliance requirements and assists in evaluating the overall business risk a data breach of that application represents. Examples of types of data to be identified include credit card data, healthcare records, corporate financial data, and customer lists.

Unstructured data is the data stored in electronic form, but outside of the corporate applications. Examples are spreadsheets, word documents, or FTP files, but could be in any format the organization uses on a day to day

basis. Unstructured data represents a high risk of loss as organizations are less able to control access to these files. The files are extremely portable with a simple file copy process, and access to them is difficult to control or log. Electronic personal health information or credit card data in these types of files creates a significant compliance concern due to the inability to track individual access. This type of data can be located through the interview process of business personnel, but is generally more accurately located using software tools. There are numerous software tools which can assist with the discovery process. Which tool is best will depend on the environment and available budget. Data Loss Prevention (DLP) tools and file search tools can greatly simplify the process of identifying which systems, storage areas or processes involve sensitive data.

Physical documents represent a similar risk as the unstructured data in that they are difficult to track and easily transferred without an automated record. Numerous data breaches have been caused by improper disposal or outright theft of documents. The loss is frequently unknown until a customer reports a problem or the records show up in the news media. The best way to mitigate the risk physical documents represent is to minimize their use. Ensuring the applications support the business processes reduces the need for employees to print documents. A clean desk policy to require all sensitive documents be locked away will reduce the chances of unapproved access to the data they contain. Finally, implementing a shredding process for all documents will prevent any of these documents from being thrown in the garbage and lost. The risk of loss cannot be eliminated as long as physical documents are used for sensitive data.

Classification of Data

Once you have identified where your organization has sensitive data, an effort should be completed to evaluate the value of the data. This process identifies where the greatest impact to the business would be if a data breach were to occur. Knowing which systems and processes represent a higher risk allows remediation efforts and controls to be focused. Part of the effort to classify data should be to determine how long the organization is required to retain it to meet business or legal requirements. Data retained longer than necessary represents significant risk of loss which can be completely avoided.

Types of data to consider in this process and the compliance issues they represent are below:

- Credit card data (PCI)
- Electronic personal health information (HIPAA, HITECH)
- Corporate financial data (SOX)
- Customer information (GLBA, State Privacy Laws, competitive, reputation)
- Employee data (State Privacy Laws)
- Corporate proprietary information (competitive)
- U.S. Government data (FISMA)

The data classification of the system should be tracked for the life of the system and reviewed on an annual basis or when system changes are made which might impact the type of data it contains.

Data Destruction

Destruction of physical documents has already been covered – shred them. Numerous service companies can provide lockable bins and mobile shredders to destroy documents on-site.

The electronic records are slightly more difficult to properly destroy. The destruction method needs to be tailored to the lifecycle of the data. Data stored within active systems can be simply deleted as long as the integrity of the system is ensured. The specific data locations will be overwritten as new data is stored on the media.

Electronic files which are simply deleted continue to exist on the storage media until it is properly wiped. These files can be reconstructed by someone with proper access until the actual file locations on the drives are overwritten. Numerous data losses have been reported due to the loss of hard drives or portable media where the files had been deleted, but not properly destroyed.

Electronic files which are simply deleted continue to exist on the storage media until it is properly wiped. These files can be reconstructed by someone with proper access until the actual file locations on the drives are overwritten.

If the storage media is being decommissioned or will be repurposed, the data should be destroyed. This may involve physical destruction of the media (hard drive, tape, USB) or it may involve wiping the media to destroy the 1's and 0's and return it to a state where the data cannot be retrieved. Hard drives or other physical media from servers, workstations, copiers and other devices should not be simply discarded. Shredding is the recommended method for physically destroying hard drives used for sensitive data. This requires specially designed equipment which can be hard to locate.

Wiping storage media is best accomplished using any number of available software programs. These programs systematically overwrite each location on the media several times, rendering the sensitive data irretrievable. Under no circumstances should the media be removed from the organizations' control or premises prior to being properly destroyed.

Destruction Methodologies

Methodology	Description
Storage Device Destruction	The physical destruction of the storage media assures data destruction. However, the rendering of a drive unusable does not guarantee that media contained within the drive cannot be recovered. Partial physical destruction such as drilling the drive does not guarantee the media will be unrecoverable. To ensure that the internal media cannot be recovered, the physical destruction must obliterate the media. Examples are the shredding or burning of the drive.
Magnetic Destruction	Information stored on hard drives, floppy diskettes and removal media such as ZIP disks and CD-ROMs is stored on the magnetic media using electronic values. These electronic values can be scrambled using magnetic energy. This process is known as "degaussing." While this method highly guarantees that the data will be unrecoverable, it requires a high energy level, and the degaussing devices are cumbersome and expensive.
Systematic Overwriting	Systematic overwriting involves the writing and erasing of random data in the sections containing the deleted data. The overwriting must be completed a sufficient number of times to assure that undelete technologies will be unsuccessful. The industry recommended standard is twelve times. Several commercial products permit the overwrite to continue to as many as ninety-nine overwrites.

Data Storage

Proper storage of sensitive data can turn a major breach, with data loss, to an incident with no data loss. This risk reduction can be accomplished by establishing a sound plan for storing organizational data. A storage plan should be made considering the data classification, retention requirements and destruction methods in addition to the technical requirements. Be aware of the various laws and regulations affecting organizational compliance requirements for data retention.

The simplest way to avoid data loss is to use encryption. The method of encryption is important, with the 3DES and AES256 algorithms being among the strongest and most common encryption forms available. Numerous commercial and open source tools exist to manage the encryption and associated keys for protecting data.

Encryption of structured data can be accomplished through the relational database management software (RDBMS), but there are limitations on versions and complexity concerns. Using the RDBMS the entire database can be encrypted, but frequently it is a better option to encrypt only those tables which contain the sensitive data. This form of encryption provides the best protection against loss as the encryption key is required to access the data, making it more difficult for hackers or other unauthorized persons from being able to view the data.

Unstructured file systems can be protected by encrypting the hard drives or storage media. This method provides protection against loss, but generally not against unauthorized access. If an unauthorized person obtains access to the computer containing the media, it can frequently be accessed as long as the user has an active account or if the computer was left logged on.

All storage locations used for sensitive data should be encrypted, including system backups and production data. Great care is required in the management of the encryption keys as the data is inaccessible without the key.

The simplest way to avoid data loss is to use encryption. The method of encryption is important, with the 3DES and AES256 algorithms being among the strongest and most common encryption forms available.

About the Authors



Michael Whitcomb, PMP, CISM

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.

Loricca, Inc. | www.loricca.com | 813.600.3005



Vinny Sakore, CIPP/IT

Vinny is the Vice President of Business Development of **Immersion, Ltd.** He has 15 years of experience in Healthcare IT and Operations. At Immersion Ltd., Vinny is focusing on the continued growth of its data breach notification service and other business development activities for its parent company, NPC, Inc.

He is an active member of PLUS, the Professional Liability Underwriters Association and IAPP, the International Association of Privacy Professionals and HIMSS, the Healthcare Information & Management Systems Society. Vinny holds a CIPP/IT credential through IAPP and often gives presentations on data breach risks and best practices for data breach incident response.

Immersion, Ltd. | www.immersionltd.com | 866.377.8210