



## A Management Perspective of Encryption Today

### **AITP – Research and Strategy Advisory Group**

Christine, Leja, CCP, Chair

Richard C. Barnier

Charles L. Brown, CCP

Paul F. Dittmann

Robert J. Heimann

J.T. Westermeier, JD, CCP

***Encryption is seen as a deterrent for Personal Identity Information (PII) and corporate theft. Most state laws provide corporations and institutions a “safe haven” from public disclosure if encryption has been used. This white paper presents a brief look at the state of encryption and presents “best practices” that are emerging. The Association of Information Technology Professionals (AITP) Research and Strategy Advisory Group (RASAG) recommends that “best practices” evolve as one significant approach to thwart those with malicious intent and to protect PII with a quality approach to improving encryption and security processes.***

Copyright 2007, Association of Information Technology Professionals. Permission to copy for personal non-commercial use granted. When the paper is referenced or quoted, direct the reader to [www.aitp.org](http://www.aitp.org).

Special thanks to the following editors: Karen Haynes from DLA Piper US LLP, and Mike Hinton and Teresa Valleroy from Southwestern Illinois College

## **A Management Perspective of Encryption Today**

### **Executive Summary**

Encryption is being sited as a significant player in protecting Personal Identity Information (PII). Thirty-eight states have passed breach disclosure bills since 2001 relating to identity theft but the number of published incidents over the last few years continues to grow. Identity theft is reportedly the fastest growing crime (Footnote 1). Some states note that if encryption has been used there is no requirement for the organization to notify the individuals respecting the breach and possible compromise of their PII.

Encryption products are prevalent in the market place with many references on what types of data should be encrypted. How are these products evaluated to determine which ones to use? What encryption features are important? And, given that there is no universal encryption standard, what encryption algorithms are more secure?

Given our mobile society and the plethora of portable devices, how is data protected as it moves from a secured network server to a laptop, USB drive, or smartphone? As more and more business is transacted over the Internet, how do businesses share information in a secure way when there are no universal encryption standards? How will mobile workers keep data protected?

The states and Information Technology (IT) industry are responding to secure data yet keep it available for transactions while hackers are moving more swiftly to break any security in place. Since encryption algorithms are only good until broken, how are new algorithms selected and tested? What determines algorithm strength with respect to hacking? And, are encryption algorithms the only answer to protecting personal and organizationally sensitive data? What about the human side of the equation?

Encryption began its industry growth in the 1990s. Only recently have encryption and security processes taken a fore-front of thought in the IT systems and services life cycle. This white paper has collected best practices learned from vendor interviews and IT management processes to formulate a living outline of best practices. At this time, there is little literature focused on security and encryption processes that are embedded in the work environment. Encryption products abound, but, it is the IT industry that has begun to look deeply into its IT management processes to establish sound security and encryption processes that permeate the whole business process. Implementing best practices and following a continual quality improvement process will better data security in all its “data states” and press vendors to produce products and services that keep our data safe.

Best practices are evolving and given a quality improvement process, the “good hats” will win over the “bad hats”. The challenge is known and accepted. As organizations press vendors for forward-thinking products and services, the Internet industry will remain vibrant and growing with a channel of communication and a continual improvement in quality processes that leaves the “bad hats” outdated and the “good hats” in charge.

## **A Management Perspective of Encryption Today**

Security has become an integral part of Information Technology (IT) services and encryption is swiftly becoming part of the security solution. Although encryption has existed since the days of messengers delivering from one person to another in code, its entry as part of Information Technology is relatively new. Personally identifiable information and laws in thirty-eight states are swiftly moving encryption to a mainstream service within IT.

IT managers are rapidly moving beyond the question of “Why is encryption important?” to “How is encryption effectively implemented?” Large corporations have pioneered using encryption and as encryption moves to a mainstream solution, best practices are emerging. So, how has encryption evolved? How is it being used and what best practices are emerging?

### **System Intrusion**

One of the first novels on security intrusion, The Cuckoo’s Egg by Clifford Stoll, brought public awareness to a new and growing threat - IT system intrusion. From the birth of mainframes to minicomputers to today’s world of mobile access to information, data is under constant threat of being inadvertently exposed and maliciously taken for criminal use or other misuse.

With the growth of the Internet, islands of computing with compartmentalized data were connected for the purpose of sharing information electronically. Corporations moved to secure their campus networks by securing the perimeter of their network. As corporate information sharing moved from a “supplier to business” model to a “customer centric” model with the advent of the web, data suddenly was moved from the protected corporate networks to the exposed “consumer to business” network, outside the perimeter. As data traversed the Internet, the types of data that moved changed from product information, to order information, to financial transactions, to consumer or “my” data!

### **Data Exposure**

Today, our personal data is globally available and entirely dependent on the security measures of the holders of our data. Consumers cannot control their personal data yet bear the consequences of any security breaches that expose their data to the public and place information in the wrong hands. Our lives are no longer private. Our information is everywhere and being utilized for all types of services – some of which we may want as a consumer and some that we may not want.

As the data moves from corporate servers through the Internet to my computer, cell phone, PDA, ... , anyone can intercept and view my information. So, as my data proliferates around the world in real time, how can I protect “my personal data”? One answer may be the use of cryptography!

If data is encrypted, the consumer has a higher level of confidence that their private life can remain private. If their data is inadvertently exposed, it will look like gibberish to the viewer. Malicious intent takes a deeper criminal nature since the criminal can’t just swipe the data and use it but, must now spend time to make sense of what they took. That extra time could be just enough to nab criminals before they complete their criminal intents to use stolen personal data to their advantage.

## A Management Perspective of Encryption Today

Let's take a deeper look at securing data, at delivery systems and the use of encryption to protect "my personal data". What role should encryption have in security? What are the views and actions of industry, states, and the federal government? What innovations may help improve encryption?

### Securing the Perimeter

Today, routers provide a secure perimeter to systems for known breaches. Both software and hardware routers are programmed to allow or block entry or exit. Routers shore up protection and greatly improve the ability to grant access to the network and its systems and to prevent access to the known intruder. But how is the unknown intruder detected?

One solution, the virtual private network (VPN), builds a unique path from the initiating location to the destination. The user must be identified and authenticated. There are two types of encryption: transport and tunneling. The transport encryption sets up a secure, encrypted link across the Internet wires and encrypts the data you are sending. The data is protected but not the headers and trailers around the data. Tunneling adds encryption of the headers and trailers. There are a number of tunneling protocols that may be used. Creating VPNs has become easier for technicians but the increasing number of unique connections between two points for business partnerships also increases costs. When business partnerships change, the telecommunication lines upon which VPN encryption has been established also change. The cost of making connection changes and paying penalties for premature changes in telecommunication lines increases the cost of doing business.

The growth of the Internet with its spider-like paths that traverse the world, offer a much lower cost of transporting data and the freedom to easily transact business with whomever one desires. But keeping data secure has escalated as the openness and the number of attacks increases. What has been designed as an electronic world of information sharing for honest, trustworthy merchants has become a huge opportunity for malicious treasure seekers.

### Data at Risk

As awareness grows concerning the value of data, from corporate secrets to financial transactions to personal information, protection for data from the start of its journey to its destination has elevated to a major concern. Even data at rest is a target. The mobility of data with laptops and PDAs provide easy theft opportunities. The table (Footnote 2) below shows some significant 2006 security breaches:

<b>Victim of Security Breach</b>	<b>Number of Consumer Records Affected</b>
Ameritrade	226,000
AOL	600,000
Boston Globe & Worcester Telegram & Gazette	240,000
Department of Veterans Affairs	26,500,000
First Trust Bank	100,000
GMAC	200,000
Kent State University	100,000
LexisNexis	300,000
Metropolitan State College	93,000

## A Management Perspective of Encryption Today

Miami Office of the U.S. Dept. of Transportation	133,000
San Jose Medical Group	185,000
TJX Companies	45,600,000
University of California, Berkeley	98,400
University of California, Los Angeles	800,000

Published data breaches continue in 2007. While, thirty-eight states require disclosure when personally identifiable information has been exposed, there is pressure on the federal government from businesses to provide a united approach to identity management for interstate data transport.

### **Securing the Data**

Algorithms have emerged that would establish a hand-shake exchange to identify two parties that desired to pass data. Once the identification hand-shake is complete, the connection is trusted and the data makes its journey. No one anticipated what has come to be called “packet sniffing” or “man in the middle” techniques to gather data without awareness. Packet sniffing allows copying the data as it passes by and then utilizing the obtained data for nefarious purposes. “Man in the middle” intercepts packets by first becoming what is thought to be the trusted destination, copying data, and then passing the data to the actual destination desired. Typically, neither the sender nor the receiver is ever aware of the attack. As techniques become more sophisticated, protection becomes more difficult.

The movement and storage of data are proliferating. The speed and convenience of transactions entice consumers and business to utilize the Internet to conduct business as sophisticated models emerge to provide predictive information for consumers. How can data be secured while in transit and stored for later analysis and business transactions?

In discussions on securing the data, the topic of focus is encryption. Cryptography deals with encryption and decryption but encryption becomes the topic of discussion. Why? It is the encryption algorithms that are attacked by hackers seeking to break the code. So, the stronger the encryption, the longer it will take for hackers to decrypt.

### **Sources for Encryption**

Data has two states – static (at rest or stored) and dynamic (in transit). So, it follows that there are two sources for encryption – stored data and data in transit. Data may be stored in files or databases and on many other devices – computer (personal or server), USB drives, PDAs, iPods, CDs, DVDs, tapes, etc. Dynamic data may be in the form of a transaction (small bursts of data in transport) or numerous data records such as file downloads/uploads.

Network encryption protects data while in transit. Data encryption cannot only protect data in transit but also stored data. There are two kinds of data encryption: file and media. File encryption will protect stored data. Media encryption focuses on where data resides such as hard drive, USB drives, CDs, DVDs, iPods, etc.

File encryption protects a file while stored in a given folder. If a user saves the file to an unencrypted folder, the file data is no longer encrypted. Thus, it is easy to lose the encryption.

## A Management Perspective of Encryption Today

There are vendors like Microsoft who encrypt the entire file system but password-hacking utilities can circumvent this security. A vulnerability that remains with encrypting the file system is the ease of offline access. Any person with physical access to turn on the computer can access and view the data if it is unencrypted.

Media encryption such as full disk encryption protects the operating system, the master boot record and even unused disk space. This encryption occurs prior to the operating system loading giving both local and network protection. Current recommendations from vendors like GuardianEdge suggest two-tiered encryption using both file and media encryption. File encryption provides secondary compartmentalized security.

As business becomes “increasingly mobile,” the risks of unwanted intrusion and unintended loss of corporate knowledge and customer/employee information also increase. Businesses must treat the new mobile devices – Laptops, PDA’s, smartphones, and other custom wireless-enabled devices with the same level of security and oversight as any device connected to the normal “wired” environment.

**Wireless Handheld Devices** pose a variety of usage, access and security problems for today’s organizations. Uncontrolled wireless access to corporate data assets is obviously not a good idea. Therefore, deciding what should be the “allowed” methods of connecting a corporate-issued wireless device to corporate data is the first step in “locking down” access to only those who should have it. While the local coffee house and other businesses are providing wireless access points for customers, it is questionable (or should be questioned) whether or not an organization should allow even e-mail access from these types of networks. Organizations have various options in managing their own wireless assets, but over the “open air” encrypted traffic offers a “bottom line” solution to protect information in the wireless environment.

Encrypted traffic has become the lowest common denominator in safeguarding wired and wireless data shared among state, local and federal law enforcement and criminal justice agencies. The guidelines set by the US Department of Justice (USDOJ) might also be used by other industries. These guidelines define “untrusted” and “trusted” networks in a manner that clearly outlines the issue and the solution. An “untrusted” network (wired or wireless) is one where traffic from all types of agencies runs over the network. On the other hand, a “trusted” network is one where only defined law and justice agencies share the network. This is analogous to a public network versus privately-owned corporate network. The USDOJ directive, since virtually everything goes to or through an “untrusted” network, is that network message traffic will be encrypted using 3DES (Footnote 3).

**Laptops and data devices** have proven to be a “lush” target for loss, as exemplified by the Veterans Administration (VA) laptop incident. “In the second-largest data breach on record -- and the biggest Social Security numbers breach ever -- the Department of Veterans Affairs (VA) disclosed Monday (5/23/06) approximately 26.5 million veterans are at risk of identity theft.” (Footnote 4). In this incident, the data loss occurred when a VA employee lost a laptop containing the entire VA patient database. While this instance was a loss of confidential “customer” and medical data, it could as well have been corporate intellectual property. Best

## **A Management Perspective of Encryption Today**

practices were not in place to evaluate the need to take the data “off site” or to have a policy that would prevent it.

While this initial incident relates to laptop loss/theft, the danger is by no means constrained to this single incident. The risk issue, it is important to note, also extends to USB storage peripherals.

**The Server Farm**, regardless of how data is collected, distributed or shared within the organization, remains the “richest” target for snooping and theft. While organizations continue to proactively work on technology security, manual intervention is often more difficult to predict, control or thwart. The downside is loss of data from employee laptop loss/theft (e.g. the Veterans Administration) and backup tapes, noted below:

### **Bank of America Loses a Million Customer Records**

“A “small” number of backup tapes with records detailing the financial information of government employees were lost in shipment to a backup center, Bank of America said on Friday.” (Footnote 5)

The tapes contained information on the customers and accounts of the U.S. government's SmartPay charge card program, which has more than 2.1 million members and annual transactions totaling more than \$21 billion, according to the General Services Administration. Reports have pegged the number of cards affected at 1.2 million.

### **Encryption Standards**

With the growth of information exchange, standards become important. Communication must be simple to execute for the common user but strongly secured behind the scenes whether the data is at rest or in transit. Many algorithms did not stand the test of time. Let's first look at encryption of data while at rest.

DES (Data Encryption Standard) emerged as the strong algorithm and was adopted by the federal government in 1977. DES was a block cipher that transforms a 64-bit data block by using a 56 bit secret key. In 1999, using a specially built computer, the algorithm was broken in less than 24 hours. The computer went through the 72 quadrillion different combinations to break the code! The good news was that Triple DES was already under development. The encryption key became 112 bit. The hardware and software were minimally impacted so the strengthened 3DES quickly became the new standard.

PGP (Pretty Good Privacy) is another standard gaining popularity. This standard starts with a 128 bit key. It divides the key into sub-keys and with the use of switching and cutting, the algorithm is three times faster when encrypting than 3DES. Even though it is not known to have been broken, it has not yet become a common standard like 3DES. Yet, PGP is a standard that involves no outside parties. People create their own keys and establish trust among themselves.

RSA (authors Rivest, Shamir and Adleman) is the only asymmetrical algorithm in widespread use since 1978. It is used for private/public key generation and encryption using prime numbers

## **A Management Perspective of Encryption Today**

in the creation of the key. Given the length of time to encrypt, the algorithm is typically combined with a symmetrical algorithm such as DES for more practical use.

Neither PGP nor RSA addresses employee violations. To differentiate personal versus company documents will need a different type of algorithm. Vendors are emerging to address this market (Appendix B – Encryption Products).

AES (Advanced Encryption Standard) was the first algorithm that was created through organized competition. The government has adopted AES and industry is beginning to deploy it as well. The movement for AES comes not only from the government interest but from the fact that a standards organization called the National Institute of Standards and Technology (NIST) conducted the first contest ever to find the successor for 3DES. Fifteen algorithms emerged in 1999 for further consideration. In 2000, AES or Rijndael (named after Vincent Rijmen and Joan Daemen) was declared the winner.

For data that is in transit, there are two standards, S-HTTP and SSL, that may be used independently or together. The first standard was the evolution of secure HTTP or S-HTTP. S-HTTP evolved after 1995 to allow secure web transactions. HTTP could not service encrypted data. S-HTTP allowed encrypted data for web transactions but does not in fact encrypt the data. Encryption algorithms were applied but the lack of an encryption standard made S-HTTP difficult to use in a global network. Along came SSL.

Secure Socket Layer (SSL) provides a secure connection between the browser and the web server. All data that travels within this connection is encrypted using a 128 bit key (if the web browser is a current version and the client operating system is XP or Vista). S-HTTP and SSL can be used together. The user is aware that a secure connection is in place when they see “https” as part of the URL and when the lock icon appears in their browser.

### **Encryption Held Secret**

From early times, messages were encrypted to keep content between the sender and the receiver. The first significant use of cryptography came in World War II. The Germans were using an encoding machine called Enigma to distribute messages. The U.S., Britain and other nations spent several years before breaking the German code. Once the code was broken a turn in the war occurred. Since WWII, governments have had tight control on cryptography. The government of the United States banned businesses from exporting strong encryption algorithms outside the country.

In September 1999, the Clinton administration proposed new encryption export legislation. On January 12, 2000, the U.S. Department of Commerce Bureau of Export Administration (BXA) announced more open encryption export regulations. U.S. businesses could now export any licensed encryption product. The BXA would still do a one-time product review. U.S. businesses could now compete with European firms who had been selling stronger encryption solutions. In addition, Internet and telecommunications service providers could use any licensed encryption product from abroad or in the U.S. including public key infrastructure (PKI) services.

## **A Management Perspective of Encryption Today**

Websites emerged to protect the right of encryption use outside the government. A popular non-profit website is The Center for Democracy and Technology, [www.cdt.org](http://www.cdt.org), whose mission is:

Our mission is to conceptualize, develop, and implement public policies to preserve and enhance free expression, privacy, open access, and other democratic values in the new and increasingly integrated communications medium.

After 9/11, there was a desire for anti-encryption mandates. Fortunately, the mandates were dropped from the Financial Anti-Terrorism Act of 2001. Today, business and governments continue their research for improving cryptography. The government is very quiet about its pursuits and watches the business algorithms with care.

### **The Black Hats**

What started as fun or the gathering of bragging rights has grown into a criminal industry. Hacking started as a way to see if someone left their code open, or just to see what could be seen. Many of us remember the movie, War Games, where a teenager spends his time looking for places over the Internet to gain access. Then, the ethical decision emerges and he changes his school grades. Next, never meaning to and thinking that he was just “playing a game”, he inadvertently enters the Department of Defense War Games, where the game is real!

Today, the black-hat hackers have crossed the ethics line and are consciously looking for vulnerabilities on websites and, more importantly, on application systems and databases where big profits are made from the stolen information. Obtaining personal information, credit card numbers and other financial sources, gives black-hat hackers increasing profits the longer they can stay within a system undetected.

### **The White Hats**

The law is so busy trying to stop crime that their cases are limited to known big catches. As time permits, they provide awareness but time is their enemy as statistics show the increasing number of publicized intrusions. Some of the data theft is as easy as “lifting” a laptop. The more penetrating intrusions involve penetrating applications and databases. The “good guys” are on the defensive, trying to predict where the next attack will be, trying to contain intrusions, and trying to inform the community at large on how to protect themselves.

### **IT Professionals**

Early security for business has come from a network perimeter approach. Network professionals looked to protect business data by building a mote around application systems. While network professionals sought to protect networked systems, other IT professionals were merrily going along their professional lives leaving protection to the network staff.

Only in the last few years is the IT industry building security into each of its activities. Application programmers have the responsibility to build in security, database administrators have the obligation to protect data in their databases, and, yes, end-users have the responsibility to protect the data they access. It is a tough sell. The perception is that everything is much more complicated and takes more time. Slowly, awareness builds that if each IT professional includes security with their area of expertise, the black-hat hackers will have to deal with a layered defense system that will not be easy to penetrate.

## **A Management Perspective of Encryption Today**

Besides security products and processes that can be implemented to protect data, there is the “homegrown” IT defense. Whether product, service or “homegrown” solution(s) are in place, here are a few guidelines for all IT professionals to incorporate:

1. If your area fails, do you have a real-time approach to debug and fix the problem?
2. Do you prepare and use a disaster recovery process that is deployed for all technical problems not just a disaster so that your team experience matures?
3. What is in our IT environment that can be used to defend ourselves today and is it being used?
4. Is IT informed on current security research and what can immediately be applied?
5. Does IT work as a team across its many areas to solve everyday problems including security?

### **Everyone Hats**

Everyone who uses a computing device has a responsibility for security. If we are all watching, it is much harder for a black hat to slip past. Do we know what to watch for, what to stop, and whom to inform if we notice something unusual or suspicious? Are we, the end-user, willing to be a diligence good citizen?

### **Encryption Legislation and Industry Policies**

In the 1990s, the government began to focus on encryption legislation. Federal legislation included both government and industry use and looked to the states to implement and enforce the privacy and security regulations. The federal government encouraged encryption based on key issues such as criminal justice, public health, employee background, financial transactions and credit checks.

Security and privacy issues have become a “winning” target for legislators. Both federal and state bodies are enacting security and privacy legislation aimed at protecting an individual’s data, but also at causing notification to the individuals and, in some instances, penalties against the data source owner when a breach occurs. Some examples of this legislation include:

- Senate (109) Bill 1789: To prevent and mitigate identity theft; to ensure privacy; and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.
- Federal security policies typically require the states to implement and enforce the privacy and security regulations, which in turn are implemented and managed at the county and city level.

Encryption legislation has crossed government and industry lines:

- S.1726: A bill to promote electronic commerce by facilitating the use of strong encryption, and for other purposes.
- 1997 S.909: Secure Public Networks Act.
- 1999 HR.695: The Security and Freedom through Encryption (SAFE) Act.
- HR.1259: Computer Security Enhancement Act of 2001.

## A Management Perspective of Encryption Today

Encryption issues have led to the development of many white paper offerings that can assist government and private organizations in developing best practice processes:

- Criminal Justice – CJIS Security
- Public Health – The Health Insurance Portability and Accountability Act (HIPAA)
- Employee Background
- Financial Transactions (white paper)
- Credit Checks
- NIST Computer Resource Center <http://csrc.nist.gov/>

Using public criminal justice as an example, the Criminal Justice Information Systems (CJIS) Security Policy Version 3.2, US Department of Justice, Federal Bureau of Investigation, August 2003, provides very concrete direction for criminal justice and law enforcement data management. Since there is really “nothing new under the sun,” many of these directives and initiatives are being applied across federally-regulated industries. While these guidelines may be viewed as “overkill” in the private sector, if an organization chooses to adopt them, not only are the general security and privacy issues addressed, but there may also be positive impact on other areas, such as industrial espionage.

The FBI security policies for law enforcement and criminal justice organizations were stated in 2002, with a specific directive that “all local, state and federal” agencies must comply by 9/30/05. The security policies were all-encompassing. The technology-specific subjects covered by the security policy/directive included wired and wireless networks, and went so far as to define requirements for networks shared with the public, with other non-justice government agencies and private networks used among justice agencies.

**Wired Networks** – The FBI security policy defined “public networks” as any network not owned and operated by a criminal justice agency, which includes all public carriers, where the carrier’s switching equipment handles commercial and “other government agency” traffic. Overall, the implication is that there are few, if any truly dedicated networks. The implementation issues of the public, or non-secure, network for criminal justice agencies lead to the adoption of private key encryption, as described in the Federal Information Processing Standards (FIPS) Data Encryption Standard (DES) and by ANIS X3.92 and ANSI X3.106 standards. The policy also recognized the FIPS Standard 196, Advanced Encryption Standard (AES) and recommended its use over the DES standard.

**Wireless Networks** – The FBI Security policy for law enforcement and criminal justice organizations requires at least 128 bit encryption of all wireless data transactions. However, the 802.11 Wireless Equivalency Privacy Algorithm is not acceptable. Encryption algorithms must be approved by the National Institute of Standards and Technology (NIST) Computer System Laboratory and must meet the Federal Information Processing Standards (FIPS) 140-1 for “Security Requirements for Cryptographic Modules.”

**Internet and Other Networking** – In addition to the network traffic encryption recommendations for primary networking, the security standard also discussed IP Security (IPSEC) for VPN connectivity; the RSA encryption for Secure Socket Layer (SSL) connections;

## **A Management Perspective of Encryption Today**

and secure dial-up protocols using secure firewall ports. Access via these methods is highly controlled and requires, in addition to traffic encryption, advanced authentication tools (digital signatures, certificates, biometrics, etc.).

Many companies began to use encryption following such legislation as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), etc. Data became encrypted and protected. But, there were a myriad of algorithms. Accompanied by rapid changes in technology and the lack of industry encryption standards, how do you move data from one encryption standard to another? The problem became similar to the move of data from 5 ¼ inch disks to 3.5 disks to CDs to DVDs, etc. Given the different encryption standards and technologies, the data had to be touched again, i.e., unencrypted, moved and re-encrypted on new technology platforms. New vulnerabilities emerged during the transition from one product to another.

One story tells of a large corporation transitioning from one media and standard to another and moving the data from their computer room to a secure, off-site storage facility. All was planned. The data was decrypted in its current location with the older algorithm. The data was stored on media that could be transported to the off-site storage facility with the new encryption standards. In transit, the data was lost and never made it to the off-site storage facility to be encrypted with a new algorithm. Ten years later, the data has not been found. Great numbers of employee data have been lost.

Industry began to rethink encryption and decryption. Maybe encryption should be minimized within the corporate network for ease and speed of use and only encrypt the data when it is leaving the corporate network. But, what do you do about internal hackers?

Companies began to issue Acceptable Use Policies. CedarCrestone recently updated their Acceptable Use Policy and have graciously permitted us to use excerpts from their policy on encryption (See Appendix C). Employers and employees are struggling with compliance given the versatility of many devices. How do you manage employees who are not allowed to attach mp3 devices to prevent downloading of corporate data, yet attach their mp3 players to recharge them so that they can listen to music on the way home from work? How do you prevent downloading of trade secrets to USB drives when USB mice are used? Email traffic contains both corporate and personal messages. Even when corporate policies prohibit using email for personal use, how does a corporation protect itself from employees who login to their email service and download corporate email or attachments?

### **Keys and Certificates**

A fundamental component of cryptography is the use of keys. To keep information private between sender and receiver, a key (code) is used to translate the information to look like gibberish. Only the receiver who has the same key can translate the information into its original form. With the amount of information that is stored, accessed and moved, individual keys between sender and receiver would greatly limit the speed with which information can be shared. To expedite the process and remove the responsibility of cryptography from each sender and receiver, a centralized process emerged.

## A Management Perspective of Encryption Today

The Public Key Infrastructure (PKI) system provides digital IDs and provides a mechanism to utilize a “single sign on” feature. An authenticated user can access data and traverse networks and systems based on their identification and approved access. The benefit of PKI is that it goes deeper than just a login and password that can easily be obtained. PKI offers an extra level of trust by using encryption and a digital certificate that is obtained from a Certificate Authority (CA) such as VeriSign, RSA, etc. An organization registers with a CA and is given digital certificates (public and private keys) to use. Computers have an installed client and key that is used to encrypt and decrypt data. Note that each CA has its own PKI system and there is no guarantee of compatibility between systems.

Digital Certificates are used to identify a person or business via the CA. Upon validation, encryption or decryption takes place. Depending on the type of Digital Certificate, the process will work for email or files. Digital Certificates are files stored on your computer that contain the public keys. The installed client is the software that uses the Digital Certificates to encrypt or decrypt data. For eCommerce transactions, the web browser uses the installed client. Companies and institutions typically have Virtual Private Networks (VPN) in addition to Digital Certificates. Digital Certificates authenticate the registered user and does the encryption/decryption while VPN establishes a secure and encrypted connection. Companies and institutions may also use Digital Certificates for firewalls, routers and servers to help identify them, their roles and compliance to security policies.

PKI in the workplace is usually used to:

1. Identify system users
2. Describe access permissions
3. Encrypt email and other data

Common problems with PKI are:

1. Not an universal system
2. Not all applications can handle PKI
3. Digital Certificates can be forged
4. People can't tell if the digital certificates are forged
5. Difficult to tell what person the digital certificate belongs to
6. When a digital certificate is no longer valid, not all key servers are updated with the new information
7. If you lose your keys, you cannot access the data
8. Setting up PKI is neither easy nor simple

Secure Socket Layer (SSL) is part of PKI. It was created to fix or mitigate problems of interception and impersonation (like MITM – Man In The Middle attacks). Before an encrypted session with a web server begins, the following activities take place with SSL:

1. Your computer requests a secure connection with the web server
2. The web server sends a digital certificate to your computer
3. Your web browser checks your digital certificates and decides if the received digital certificate is trustworthy
4. If trustworthy, your web server sends a one-time session key and sends it to the web server to use to encrypt the web server's public key

## A Management Perspective of Encryption Today

### 5. Communications begin and “https” appears in the web browser

As hacking techniques improve, encryption techniques continue to improve. Currently, XML (eXtensible Markup Language) adds another layer of security. XML creates tags on a web page that define the type of encryption to be used. SSML (Security Sheet Markup Language) is a list of security policies and rules that XML tags use. Between tags on a web page, a designated SSML security policy is used allowing different keys to be used between different sets of tags. Thus, if one encryption key is broken, only the information between the two tags is accessible.

Wireless networks come with no built in security. So, this new ubiquitous WiFi environment is totally open for all to share and... steal your information. There is software available to encrypt transactions called Wired Equivalent Privacy (WEP) but there is more than enough freeware and shareware out there to break WEP. Individual users should change the default SSID that comes from the vendor and turn off the broadcasting feature. Companies have added VPN to secure their wireless networks.

WiFi Protected Access (WPA and WPA2) have emerged to provide some protection for the WiFi open environment. WPA provided an interim solution while WPA2 gives a full security solution. WPA works with an IEEE 802.1X authentication server and distributes different keys to each user. Data is encrypted using a 128-bit key and a 48-bit initialization vector. WPA dynamically changes keys which defeats the WEP key recovery vulnerability. The WPA algorithm called the Michael algorithm increases the size of the keys and vectors, reduces the number of packets sent with the related keys, and adds a secure message verification system. WPA works with older network cards and increase security over WEP. WPA2 has enhanced the Michael algorithm and uses the new AES-based algorithm giving considerably more security. WPA2 certifications are mandatory for all new devices wishing to be WiFi certified. Since 2005, many vendors are providing WPA2 devices.

### **Best Practices**

By the 1990s, as security and acceptable use policies developed, government and industry began to differ as to existing government regulations. Gradually two different sets of standards were evolving. Government held to its strong encryption standard while industry adjusted for employee use. Companies today are still struggling with what are best practices that meet legal requirements, protect personal and corporate data, and yet meet employee needs to do business effectively. Academic institutions have a great balancing act between open and secure depending on the information sought.

Besides accessibility standards, security has not been embedded within the IT life cycle process. Rather, in reaction to breaches, security solutions and standards have responded from a defensive perspective. For some reason, there is a reluctance or maybe just plain oversight from “the heat of the battle” to include security from the very inception of an IT product or service. Gradually, security is being recognized as an integral component designed into an IT product or service from inception. As research and development includes security in its process, security will become stronger and more robust. (See Appendix A - IT System Services Lifecycle.)

## A Management Perspective of Encryption Today

Encryption as a component of security offers the ability to keep data more secure no matter what media is used for data storage and data transport. Standard-neutral security professionals advocate a layered use of encryption. In its simplest form, here is a list of key components:

1. Encrypt sensitive personal and institutional data – at rest, as a transaction and while in transit
2. Provide acceptable use policies for employees, partners, vendors and customers
3. Proactively manage security and audit security practices regularly
4. Embed security throughout the IT system and services lifecycle
5. Train and educate anyone who may touch, see, or have access to the data or any device on which it is stored or transported.

From a data protection defense, Intel uses the following security layers (Taken from *Premier IT*, Winter 2007, “A Layered Approach to Security” by Malcolm Harkins and Jeff Moriarty):

1. Governance and personnel
2. Physical
3. Network
4. Platform
5. Application
6. Storage
7. File and Data

With policies in place and educated users, one can look at the technology layers. Locations where data is stored or sensitive data is accessed need appropriate physical access security. The remaining layers from Intel’s list are technology layers all viewed from a physical perspective. Technology solutions are tested periodically to affirm expected levels of security and perform the continual improvement process to maintain appropriate security levels.

Yet there are other data protection defenses besides the physical components and their physical locations. Software development and IT processes require data protection defenses. Integral to software development should be roles and permissions of who has access to what. Data must be identified that is personal or corporate and needs protection. From the start of a development life cycle through implementation, security should be addressed. In addition, the production and maintenance roles should have defined security processes. Access control should be tied to job descriptions and the roles of individuals to keep security processes applicable and current.

Mobile data, data that leaves the physical security of server rooms, needs protection. Mobile data includes both transactions and files of data. Today, devices such as USB drives can easily pull protected data that needs protection. Encryption, when done right, keeps data encrypted as it passes to mobile devices keeping the required defenses in place.

There are so many components to securing data that starting a process may seem overwhelming. Large corporations have begun an encryption process by looking at the highest risk first – mobile devices. When mobile devices are secure, desktops come next. State laws like California’s SB1386 guide encryption decisions. If encryption of data is proved, then there is no need to

## **A Management Perspective of Encryption Today**

disclose a breach because the data is unreadable. Once the highest risk has been addressed, a look at managing encryption and incorporating processes is addressed.

There is also the practice of deploying security in sizeable pieces. Perhaps a whole revamping of business processes and technology is too large a project at one time. Instead, establish security goals and apply them as you proceed with projects, services, technology and physical space. Over time, security is achieved and continual improvement becomes the pattern.

There are many misconceptions about encryption that have slowed its deployment. There are the typical comments about complexity, difficulty to use, performance issues, and key theft. And there are the comments about limited applicability such as encryption is available for the laptop but not PDAs and about operating systems coming with encryption tools. Given concerns and comments, how far does one go to secure data? Answering the question depends on the nature of the business, the sensitivity of the data, the types of security, and encryption needed. The goal is to define the scope and security requirements your data needs and implement the appropriate security and encryption services for the organization. Layering security and encryption where appropriate makes the hacker's goal near impossible!

### **Trends for Encryption**

In the early 1990s, cryptographers helped to open the encryption from a government only role to a U.S. business industry as seen in European markets. Data Encryption Standards (DES) could be developed by industry and Americans at large instead of just government. Some educational research institutions are beginning to study cryptography. Purdue University is a well-respected university for research on cryptography. The Center for education and Research in Information Assurance and Security (CERIAS) has white papers, reports, studies, techniques, products and vendors.

Many algorithms have emerged and have been immediately applied to solutions before thorough testing is done. Rigorous testing of these algorithms is suspect since many of them are broken in a relatively short time. Take the example of Microsoft Word. Earlier versions of Word took four days before a hacker had penetrated the algorithm to protect data. For Word 2003, less than 5 minutes was needed to crack the algorithm. How do you prepare and protect against the speed at which penetration of new algorithms is occurring? Perhaps the National Institute of Standards and Technologies (NIST), a non-regulatory federal agency, will provide that help. The NIST mission includes "advancing measurement science, standards and technology". (From the NIST website, [www.nist.gov](http://www.nist.gov).)

There is no standard for encryption and there are a number of vendor products (See Appendix B – Encryption Products). Selecting encryption standards and vendor products is an exercise in itself. NIST has recently issued a draft of the "Guidelines on Active Content and Mobile Code" by Wayne A. Jansen, Theodore Winograd and Karen Scarfone that has an emphasis on "active content". (Active content is defined as PDF documents, web pages, office suite files, email, and other interpretable data.) The guidelines encourage organizations to understand what their active content is and develop the appropriate policies regarding active content. Based on risk assessments and the benefits of the active content, appropriate security should be configured, integrated and maintained.

## A Management Perspective of Encryption Today

Encouraged in the NIST “Guidelines on Active Content and Mobile Code” is the use of digital signatures that uniquely identify the author. When applied to code with the use of SSL and PKI, the recipient has a better guarantee that the information received is from the identified sender. The document provides an outstanding checklist to use prior to handling active content documents (See Appendix D – Checklist from “Guidelines on Active Content and Mobile Code”).

Vendors are deeply invested in cryptography to secure their products. Having the opportunity to talk with a vendor and get an inside view of encryption algorithms and their future, is very difficult. Algorithms, after all, take years to develop and only minutes to crack. Andy Morris from Clearswift (who sells email encrypted software) is standard-neutral with respect to encryption. As he said, “Encryption is not foolproof.” But, he advises, layering encryption does raise the level of defense.

A key management issue is securing encryption keys. Sean Convery, Chief Technology Officer of Identity Engines says, "At the CIO level, cryptography is a black-box process. Unencrypted bits go in, encrypted bits go out. However, it is at this point that the real work begins: the choices you make around key management and operational process define the security of the overall system." So, as complexity of encryption increases and layers of encryption are used, there needs to be a central location where organizations manage the keys.

The pace toward encryption is increasing rapidly. Thirty-eight states have enacted bills on identity theft. Organizations must make public any data exposure of Personally Identifiable Information (PII). However, if organizations have encrypted the data, there is no need to make the data exposure public. With this safe haven, organizations are quickly moving to an encryption environment creating a new target, the central location where the “keys of the kingdom” are kept.

Ram Krishnan of GuardianEdge notes that as organizations become aware of the need to secure the central key management process, vendors are being pressed to provide an independent solution so that all layered encryption processes from a variety of vendors can be managed with one tool rather than a collection of vendor key processes that is very labor intensive. Policies and vendor solutions will need to grow quickly to respond to a new need for security, the central key management process for all deployed encryption solutions.

### **Implementing Encryption**

There are basically two approaches to implementing encryption today. There is the “big bang” project approach where encryption is infused throughout the organization at one time or there is the one step at a time approach where the biggest security weaknesses are addressed first, creating an iterative process of quality improvement for encryption. Most organizations are following the quality improvement process receiving the benefit of a regular review of encryption from both product and process perspectives.

The state of encryption and the building of encryption best practices is evolving. Using the overarching life cycle process of software development applying it to encryption (Appendix A –

## **A Management Perspective of Encryption Today**

IT System Services Lifecycle) is a good beginning. In software development projects and introduction of IT Services, it is the use of a lifecycle approach that makes the difference. Setting the mission and vision, establishing the scope and requirements, and following a rigorous process brings an encryption solution that is workable at a designated time for an organization.

The IT industry is in the midst of an encryption journey. How we prepare, how we deploy, how we monitor, and how we improve will minimize risk and keep our organizations serving their customers effectively.

## A Management Perspective of Encryption Today

### Footnotes

- (1) Koerner, Brian, “Your Guide to Identity Theft”, Identity Theft Statistics, [idtheft.about.com](http://idtheft.about.com)
- (2) “Managing Enterprise Risk With Full Disk Encryption”, GuardianEdge, March 2006 and “Worst Data Breaches Ever”, *eWeek*, [www.eweek.com](http://www.eweek.com), slideshow, August 17, 2007.
- (3) Criminal Justice Information Systems Division (CJIS) Security Policy, US Dept of Justice, FBI, Version 3.2, June 2003, pp 13-16.
- (4) “Data Theft at the VA”, CSO Magazine, Online Column, May 23, 2006.
- (5) “Bank of America Loses a Million Customer Records”, C/Net News, February 25, 2005.

# A Management Perspective of Encryption Today

## Bibliography

- “Bank of America Loses a Million Customer Records”, C/Net News, February 25, 2005
- Cobb, Chey, Cryptography for Dummies, Wiley Publishing, Inc., 2004
- “Common Data Encryption Misconceptions”, Utimaco, 2007
- “Controlling the Rising Risk of Removable Storage Devices in the Enterprise”, GuardianEdge, 2007
- “Data Theft at the VA”, CSO Magazine, Online Column, May 23, 2006
- Firstbrook, Peter and Hallawell, Arabella, Gartner, “Magic Quadrant for E-Mail Security Boundary”, Gartner, September 25, 2006, ID#G00142431
- Harkin, Malcolm and Moriarty, Jeff, “A Layered Approach to Security”, Premier IT, Winter 2007
- “How to Offer the Strongest SSL Encryption”, VeriSign
- “Implementation Issues for Cryptography”, NIST, [www.itl.nist.gov/lab/bulletins/archives](http://www.itl.nist.gov/lab/bulletins/archives), August 2007
- “Implementing Encryption: Challenges and Strategies”, Info-Tech Research Group, [www.infotech.com](http://www.infotech.com)
- Jansen, Wayne A., Winograd, Theodore, and Scarfone, Karen, “Guidelines on Active Content and Mobile Code (DRAFT)”, NIST (National Institute of Standards and Technology), August 2007
- Koerner, Brian, “Your Guide to Identity Theft”, Identity Theft Statistics, [idtheft.about.com](http://idtheft.about.com)
- “Managing Enterprise Risk With Full Disk Encryption”, GuardianEdge, March 2006
- Manjack, Martin, “Social Engineering, Your Employees to Information Security”, SANS Institute, June 1, 2006
- “Maximizing Site Visitor Trust Using Extended Validation SSL”, VeriSign
- Mogull, Rich, “Top Five Steps to Prevent Data Loss and Information Leaks”, Gartner, July 12, 2006, ID#G00141829
- “Privacy Guidelines for Developing Software Products and Services”, Microsoft, Version 2.2, May 11, 2007

## **A Management Perspective of Encryption Today**

RSA, Security Division of EMC, [www.rsa.com](http://www.rsa.com)

“State of Security; US Survey – 2007”, Websense, August 2007

US Dept of Justice, FBI, Criminal Justice Information Systems Division (CJIS) Security Policy, Version 3.2, June 2003

“U.S. Information Security Consulting and Implementation Service 2005-2009 Forecast”, IDC, June 2005, IDC#33583

“Worst Data Breaches Ever”, *eWeek*, [www.eweek.com](http://www.eweek.com), slideshow, August 17, 2007

“10 Essential Steps to Email Security, A Clearswift Best-Practice Guide”, Clearswift

## **Appendices**

## **A Management Perspective of Encryption Today**

### **Appendix A – IT System Services Lifecycle**

Considerations for including security throughout the IT System Services lifecycle:

1. When developing an application system, start with the data
  - a. Identify the data that needs to be secured
    - i. Personal data
    - ii. Business data that distinguishes the company or institution
    - iii. Financial data
    - iv. Network transport data that identifies traffic flow and network handshaking
    - v. Transaction data
    - vi. Movement of data
    - vii. Backup and recovery of data
    - viii. Identity management systems
    - ix. Authentication systems
  - b. Confine application systems to the core purpose
    - i. What data is really needed to fulfill the purpose of the application system
    - ii. Avoid system “add ons”
    - iii. Who really needs access to what data in the application system
    - iv. Define the appropriate access control between data, roles and job descriptions
    - v. When and from where is access to the data available
    - vi. What data may leave a secured database
    - vii. Who may change what data
    - viii. When may data be changed
    - ix. For how long should data be accessible for use
2. Physical network environment
  - a. Internal and external user appliances (desktops, laptops, PDAs, smartphones, etc.)
  - b. Servers (web, application, files, etc.)
  - c. Databases
  - d. Network components (firewall, open ports, network transport (wired and wireless), SANs, etc.)
  - e. Backup storage (on and off site)
3. Transportation of data
  - a. What type of data movement is expected in an application system
    - i. Transaction data – one transaction at a time
    - ii. Download of volume data
    - iii. Upload of volume data
  - b. Open environment (Internet, cellular, etc.)
    - i. General data – Need any precautions?
    - ii. Secure data
      1. Authentication mechanism
      2. Identity management
      3. Services available
      4. Access control

## A Management Perspective of Encryption Today

5. Encryption
6. Time limit of availability when authenticated
7. Activity logs
- c. Secure environment (private network)
  - i. Authentication system
  - ii. Identity management
  - iii. Services available
  - iv. Encryption
  - v. Usage time limit
  - vi. Activity logs
4. Secure data protection
  - a. Ring of protection in front of data
  - b. Encryption
  - c. Freeze activity when security breach detected
  - d. Self-destruction of aged data when separated from data source
  - e. Self-destruction of breached data when separated from data source
  - f. Encrypt data backups
  - g. Encrypt disaster recovery files
5. Securing existing application systems
  - a. Review managerial, operational and technical processes and data
  - b. Identify and document existing business requirements for security
  - c. Analyze existing security systems and determine adequacy and effectiveness
  - d. Perform a gap analysis of security practices against industry standards
  - e. Document mitigation recommendations of identified risks and threats including justification analysis
6. Security process cycle (iterative cycle)
  - a. Assess
  - b. Plan
  - c. Design
  - d. Implement
  - e. Run
7. Proactive policies and procedures
  - a. Enterprise encryption policy
  - b. Enterprise-wide procedures for sensitive data
  - c. Enforcement plan
  - d. Getting started
    - i. Be proactive – don't wait for a security breach to get started
    - ii. Be comprehensive
    - iii. Be iterative
  - e. Use an automated encryption plan
    - i. Paper plan sits on the shelf
    - ii. Active automated plan is in constant use showing users the plan is enforced
  - f. Key areas of ISO 17799:2005 – Code of practice for information security management
    - i. Human resources security

## **A Management Perspective of Encryption Today**

- ii. Physical and environmental security
  - iii. Communications and operations management
  - iv. Information systems acquisition, development and maintenance
  - v. System access control
  - vi. Information security incident management
  - vii. Business continuity management
  - viii. Compliance
  - ix. Asset management
  - x. Security policy
  - xi. Organizational information security
  - g. Annual independent security audit
8. Security Awareness
- a. Periodically inform employees and customers of healthy security safety practices
  - b. Include security in product and service communications
  - c. Keep employees and customers informed on new security processes in response to new hacking techniques
  - d. Make sure employees understand internal security controls
  - e. Provide employees with a set of values to use for security decisions
  - f. Identify and share with employees risk behaviors and attitudes
9. Preventing Data Loss and Information Leaks
- a. Proactive content monitoring and filtering
  - b. Encrypt all mobile devices (laptops, USB drives, PDAs, etc)
  - c. Encrypt backup tapes and mass storage devices
  - d. Secure workstations
  - e. Restrict home computers
  - f. Encrypt data at the source and databases
  - g. Utilize database activity monitoring
10. Disaster Recovery
- a. Ensure disaster recovery practices maintain security policies and procedures
  - b. Establish process to maintain data security when it is moved from the normal production environment to the disaster recovery environment
11. Auditing
- a. Annual audits of IT should include a review of security policies and procedures for establishing and maintaining data security
  - b. Changes in programming, hardware and services warrant a close look when sensitive data is involved
  - c. Changes in organizational structures and individual employees that access secure data need to be reviewed
  - d. Elimination of application systems, hardware and services warrant a review of the disposal of secure data
  - e. Normal use of secure data by approved employees need periodic review

## A Management Perspective of Encryption Today

### Appendix B – Encryption Products

Some useful encryptions products today:

1. PGP – Pretty Good Privacy
2. GAIM – encrypts online chatter
3. madeSafe Vault – online privacy and encryption vault
4. Password Safe – free software to store all those thousands of passwords, encrypted, in one little place
5. Kerberos – free authentication system
6. OpenSSL and Apache SSL – security for e-commerce
7. SafeHouse – drive encryption programs
8. WebCrypt – encrypts websites
9. Privacy master – encryption private information and set level of security of files and documents
10. Advanced Encryption Package – creates self-extracting encrypted files
11. Email encryption leaders per Gardner research (\*)
  - a. IronPort Systems
  - b. MessageLabs
  - c. Microsoft
  - d. Postini
  - e. Symantec
  - f. Secure Computing
12. GuardianEdge – Removable storage encryption and data protection platform
13. Some vendor products that differentiate personal and organization documents and integrate encryption solutions
  - a. Network & Endpoint Security by Centennial Software
  - b. Vontu 7 – Integrated, enterprise data loss prevention for data at rest, data in motion and data at the endpoint
  - c. Websense Content Protection Suite – Internet and external data loss

NOTE: The above list is a sampling of existing products today. No recommendation or completeness of offerings is implied.

(\*) “Magic Quadrant for E-Mail Security Boundary”, by Peter Firstbrook and Arabella Hallawell, Gartner, September 25, 2006, Source: Research, Note Number: G00142431

## **A Management Perspective of Encryption Today**

### **Appendix C – CedarCrestone Acceptable Use Policy**

#### **Encryption Excerpts**

(Permission granted to use  
From Walter Terrell and John Busby of CedarCrestone on August 7, 2007)

## **ENCRYPTION**

It is against the corporate security policy to store secret or confidential data, following the information classification guidelines presented in the CedarCrestone Information Security Policy, on any personally owned laptop or desktop. All reasonable effort should be made to not store critical information on workstations or similarly singular devices (USB drives, PDA's, smartphones, portable harddrives, etc). All information should reside on servers managed by CedarCrestone Information Technology staff, or in the case of client information, on the client's server(s) so designated for that purpose.

If there are circumstances under which secret or confidential data must be stored or transported outside of CedarCrestone secured information systems all data must be secured using CedarCrestone approved strong encryption ciphers to obfuscate the data in the unlikely event the data storage device (laptop, harddrive, PDA, USB drive, etc.) were to be inadvertently lost or stolen. The use of all encryption ciphers should be secured with a password which complies with all password policies as specified in the CedarCrestone Information Security Policy.

Any exemptions to the encryption policy must be approved by management. All possible alternative means will be used to provide additional security layers when data is not, or cannot, be encrypted due to technical or business reasons.

## A Management Perspective of Encryption Today

### Appendix D – Checklist from NIST “Guidelines on Active Content and Mobile Code”

(NIST Guidelines on Active Content and Mobile Code (Draft),  
Wayne A. Jansen, Theodore Winograd and Karen Scarfone),  
August 31, 2007: Draft Special Publication 800-28 Revision 2  
[www.nist.gov](http://www.nist.gov)

Before handling active content documents, consider the following checklist from the “Guidelines on Active and Mobile Code” summary:

- Develop the enterprise security policy regarding active content.
- Identify and assess the risk to critical information resources from active content.
- Audit systems on a regular basis to ensure the security policy is implemented correctly and remains effective.
- Identify critical information resources and maintain regular backups.
- Become knowledgeable of the security settings of desktop applications and turn off unneeded functionality.
- Keep systems current with the latest software upgrades and patches that address security vulnerabilities in desktop applications, such as Web browsers, readers, and email, and other critical software.
- Obtain all software through approved distribution channels.
- Evaluate and install anti-malware software, firewalls, active content filters, and dynamic behavior monitors according to enterprise security requirements. Keep these products upgraded to the latest version.
- Read the fine print before agreeing to download application software and plug-ins.
- Institutionalize how needed plug-ins and other software code are obtained from software manufactures, evaluated, and distributed throughout the organization.
- Do not peruse active content or run downloaded software from untrusted sources, Enable ActiveX code only from trusted Web sites that require its use.
- Create and distribute active content documents only after carefully considering the risk and benefits.
- Consider using an isolated system and safe browser settings when visiting untrusted Web sites.
- Limit the applications installed on a system, deleting any that are not used or no longer needed.

## **A Management Perspective of Encryption Today**

- Disable JavaScript and any other active content processing capabilities within email desktop applications that are capable of handling HTML or other markup language encoded messages.
- Do not open active content documents or execute any email attachments without first verifying them with the sender. Be especially wary of attachments to electronic chain mails forwarded from or through friends.
- Keep informed of latest security advisories from the United States Computer Emergency Readiness Team (US-CET) and the Computer Emergency Response Team (CERT) Coordination Center, and subscribe to security mailing lists.
- Periodically cross-check products against published lists of known vulnerabilities, such as the National Vulnerability Database (NVD), that provide pointers to solution resources and patch information.
- Regularly audit systems and networks, quickly remedying any deficits noted.
- Know who to contact and what steps to take when discovering evidence of an intrusion.

## **A Management Perspective of Encryption Today**

### **Appendix E – Vendor Contributors**

#### **Special Thanks to:**

John Busby, Managing Principle, Higher Education, CedarCrestone

Sean Convery, Chief Technology Officer, Identity Engines, Inc.

Andy Morris, Director of Marketing, CLEARSWIFT

Ram G. Krishnan, SVP of Products & Marketing, GuardianEdge

Walter Terrell, Senior Consultant, Project Manager, CedarCrestone

# **A Management Perspective of Encryption Today**

## **Appendix F – AITP Research and Strategy Advisory Group**

### **Purpose and Function**

#### **Mission**

Research trends and directions in the IT industry, state the findings and conclusions drawn from the research, recommend AITP strategy positions, and reevaluate existing AITP strategy positions based on new findings.

#### **Vision**

The Research and Strategy IT Advisory Group will perform an independent analysis of IT industry direction, giving AITP an overarching view of our profession. AITP will use the findings to create strategic and tactical goals and objectives to provide its members with current IT information unbiased by company or institutional directions. The AITP organization will use the recommendations to realign its organization and its member offerings and special interest groups with the direction of the IT industry.

#### **Advisory Group and AITP Commitment**

Annually, the advisory group will perform a research analysis of the IT industry and will reevaluate the strategic direction of AITP and its alignment with the industry. The advisory group will publish its findings and recommendations to be used by the AITP Board of Directors. The Board will evaluate the findings and recommendations of the advisory group in relation to its current strategic direction and will take actions it deems appropriate.

#### **Value**

For the industry: An independent assessment of the IT industry not influenced by company strategies -- written by IT professionals for IT professionals.

#### **Members**

Commitment by an advisory group member is for a minimum of three years. After three years of service, the advisory group membership may reconfirm a member for an additional three years.

#### **COMMITTEE CHAIRPERSON**

##### **Christine Leja, CCP**

Chris Leja has been a member of AITP since 1981 and currently serves as the AITP Region 5 Past President. Ms. Leja's involvement in AITP has earned her the Life Award for service. Chris has served in many of the chapter positions including Chapter President and has been active at the region level and served on the Association Board of Directors. She currently serves as chair for the AITP Research and Strategy Advisory Group (RASAG).

Ms. Leja, Chief Information Officer at Southwestern Illinois College, has held prior IT leadership roles in other academic institutions and industry including directing and teaching in the Masters of Management Information Sciences program. During her active role as Vice-

## **A Management Perspective of Encryption Today**

President and Partner of Le Com Enterprises, Inc., Ms. Leja has brought to market several software products for the home and commercial marketplace.

In addition to her AITP involvement, Chris is active as Treasurer of the Illinois Council of Community College Administrators - Technology Commission and has given a number of presentations and written several articles concerning Information Technology.

### **COMMITTEE MEMBERS**

#### **Richard C. Barnier**

Rich Barnier is Chairman of the Barnier Group. He has over 25 years with companies like IBM, Digital Equipment, Simpson Electronics, ECOS Electronics, CA and Phoenix Acquisitions Properties where he has held management positions in, Executive Management, Project Management, Trusted Strategic Advisor, CIO and President. Rich currently is on the National Board of Directors of the Association of Information Technology (AITP), Chairs the CEO/CIO focus group, Facilitates the CIO; CTO; governance; security SIG groups and is on the Senior Advisory Technology Board of Directors for the Executives Club of Chicago ([www.executivesclub.org](http://www.executivesclub.org)) and a member of the Society of Information Management (SIM). His contributions to the industry include the publication of numerous professional articles and frequent speaking engagements at professional organizations.

#### **Charles L. (Chuck) Brown, CCP**

Chuck joined AITP – San Diego in 1980 and is currently past-president of the San Diego Chapter. He has held every position at the chapter level; held secretary and director positions at the Region level; and served on national committees for membership, chapter operations, and RASAG. He is co-chair of the International Computer Science and Technology Conference, joint effort of National University and AITP – San Diego. He founded the AITP – SD Business Security SIG, with the FBI and InfraGard, in 2005. He participates in a variety of other local forums – AIIM, ACP & PMI.

Chuck has 40 years of information systems and management experience in applications development, project management and IT management. His applications development and management experience span mainframe, mid-range and desktop computing platforms in the IBM, DEC, UNIX, Novell and Windows environments for technology consulting, education, managed care, pharmaceuticals, public health public utilities and local government.

Chuck is currently the Manager of Integrated Justice Applications for the San Diego County Sheriff's Department, which has a staff of 4,000 and serves over three million people, covering 4,200 square miles. He is responsible for coordinating not only Sheriff's information systems used by other state, local and federal agencies, but also for coordinating the Sheriff's participation in regional law enforcement and criminal justice technology programs. He is currently managing regional projects for deployment of records management, mug shot, fingerprint, and criminal intelligence systems shared by all local law enforcement agencies, as well as representing the Sheriff in a project to retire the County's 35 year old integrated justice case management system.

## **A Management Perspective of Encryption Today**

### **Paul F. Dittmann**

Paul Dittmann has been an AITP member since 1998 and in the past had been a member of DPMA. He is in his 4<sup>th</sup> year as President of the Chicago (Windy City) Chapter and has also served as Chapter Executive Vice President and Chair of the CRM Special Interest Group.

Paul Dittmann currently is a Director with Pathfinder Associates LLC. Pathfinder specializes in User Experience Design and development of web applications, desktop applications and complex web sites. Mr. Dittmann began his career as a CPA with Touche Ross & Co and has served as a finance and risk manager for a manufacturer, the CFO and COO of two technology consulting firms and as Principal and Managing Director in the technology practice of a Chicago-based CPA firm that was acquired by American Express. He has also taught Accounting and Economics at both the undergraduate and graduate levels.

### **Robert J. Heimann**

Bob Heimann joined AITP – Northeastern Wisconsin Chapter in 1980 and has held many Board positions including Chapter President in 1989 and was voted Outstanding Chapter Member of the Year in 1992 and 2004. He was Co-Chairman of the 1989 Region 5 Conference and has assisted in other Region 5 Conferences and Leadership Workshops. Through most of his years in AITP, he has been especially focused on membership. He currently serves on the Chapter Membership Promotion and Retention Committees, the Association Professional Membership Retention Committee and the Association Research and Strategy Advisory Group (RASAG). He is also very active in the Boy Scouts Exploring for Life Program having led a student Technology Career Post for the past 16 years.

Bob has 33 years of information systems and management experience in software development, project management, strategic planning and IT management. Bob began his Information Technology career in the construction business in 1973 as a software developer, ran IT for a plumbing wholesale company and has copyrighted and marketed software on a national basis. In 1997 he was instrumental in establishing some of the first Internet based Project Websites for construction. During his career, Bob has worked closely with internal and external customers to improve productivity through the use of leading information technology systems, including optical imaging, e-business systems, pervasive computing and IP communications.

### **J.T. (Jay) Westermeier, JD, CCP**

J.T. “Jay” Westermeier has been a member of AITP since 1976 and is the past president of the District of Columbia Chapter of AITP. He is a partner in the DLA Piper US LLP law firm, one of the world’s largest law firms. Jay is the only lawyer to ever receive the Distinguished Information Sciences Award, AITP’s highest award. He received the DISA award in 1987 and is a lifetime member of AITP.

Jay is the past president of the International Technology Law Association (formerly known as the Computer Law Association), the world’s largest legal association representing information technology legal professionals with members in more than 60 countries. He is a Life Fellow of

## **A Management Perspective of Encryption Today**

the American Bar Foundation and 2001 Burton Award recipient. He serves on a number of legal journal editorial boards, contributes to a number of legal treatises, has published more than 170 articles and is a frequent speaker both in the U.S. and internationally. He was appointed by the Governor of Virginia and confirmed by the Virginia Assembly to serve a four-year term on Virginia's Council of Information Management. He is listed in Best Lawyers in America (2003-2008), Virginia Super Lawyers (2006-2007), Washington, D.C. Super Lawyers (2007) and Virginia's Legal Elite (2006). He is also listed in Euromoney's "Guide to the World's Leading Technology, Media and Telecommunications Lawyers", Euromoney's "Guide to the World's Leading Information Technology Lawyers," Mondaq's "Listing of the World's Leading Internet and E-Commerce Lawyers", and Law Business Research Limited's "An International Who's Who of e-Commerce Lawyers (2d Edition)"; "Who's Who Legal – The International Who's Who of Business Lawyers" (2002; 2008) and the International Who's Who of Internet and e-Commerce Lawyers (2008). He co-chairs the Virginia Information Technology Legal Institute.

He is admitted to practice law in Virginia, Maryland and the District of Columbia. He obtained a BS from the United States Military Academy, his JD from American University, and his MBA and LLM from George Washington University. He is a retired Colonel in the U.S. Army Reserves.