

Personally Identifiable Information (PII)

A White Paper on Information Security

Version 1.6, Revised August 2008

Michael Metzler, Ph.D., CISSP, CGEIT, CISM
Master Security Architect
SAVVIS Federal Systems

Paul Harker, CISSP, CISM, PMP
Master Security Architect
SAVVIS Communications

ABSTRACT

With more public exposure of data security breaches than ever before, attention is focused on personal information held by organizations that may be at risk for identity theft. Diligence in prevention of data loss is necessary for legal reasons, to meet security standards or regulatory requirements, and to mitigate damage to an organization's reputation. This paper provides examples of what Personally Identifiable Information is, and helps the reader understand how to determine what types of data require protection based on laws or regulations in the United States.

TABLE OF CONTENTS

3	Introduction	9	Publicly Available Data
4	Impact of PII Breaches	9	Summary
5	State Laws on Privacy and Notification	10	How SAVVIS Can Help
6	Moderately Sensitive PII Data	12	About the Authors
7	Highly Sensitive PII Data	12	About SAVVIS

“Each organization must work with legal counsel to interpret these laws and define its own list of PII data types that are to be treated as sensitive data.”

Introduction


Unauthorized access to Personally Identifiable Information (PII) on computer systems, storage media, or in physical paper form introduces the potential for fraud, identity theft and other risks every day to organizations and companies that need this data for business purposes. As sensitive information is stored, processed and shared in electronic, verbal and paper form, safeguards are required to address data classification, handling, storage and disposal.

In May 2006, a U.S. Veterans Affairs Department laptop that contained 26.5 million personal records including names, Social Security Numbers and dates of birth for the military veterans and some spouses was stolen from a private residence. This is the type of information used in identity theft, and the event concerned both lawmakers and citizens. “It was an unprecedented loss of personal information... Personal information can include your financial data, your medical data, and, basically, your virtual identity. All valuable data could easily lead to identity theft and no one seems safe.”¹

Reacting to the increase of sensitive information breaches, a growing number of federal and state regulations, as well as the Payment Card Industry (PCI), now mandate that businesses, private organizations and government agencies that handle personal information on individuals (such as employees or customers) implement security best

practices to protect the data. Failure to protect this data – or at least to apply reasonable measures to mitigate a potential breach – places the organization at risk of adverse publicity, harm to the reputation of the company, loss of consumer trust, potential litigation and fines, and ultimately may force the company or organization into bankruptcy or closure.

Personal information, defined differently in many state laws on privacy and notification, does not include any publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. Each organization must work with legal counsel to interpret these laws and define its own



In March 2007, TJX Companies (T.J.Maxx, Marshalls and other retail stores) admitted that 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.² TJX now faces lawsuits from consumers, financial institutions, the credit card industry, and many U.S. States' attorney generals. In October 2007, complaints filed on this case by banks amended the number of credit and debit cards stolen to 100 million.³

list of PII data types that are to be treated as sensitive data. The primary purpose of this paper is to provide example lists of two types of PII data with different levels of sensitivity.

PCI standards define sensitive information as data whose unauthorized disclosure may be used in fraudulent transactions. It includes credit cardholder data, the credit card account

¹ Wilbanks, L. (2007, July/August). The Impact of Personally Identifiable Information. IT Professional, 9 (4), 62-64.

² Vijayan, J. (2007, March 29). TJX data breach: At 45.6M card numbers, it's the biggest ever. Computerworld, Retrieved Sept 5, 2007 from: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9014782>.

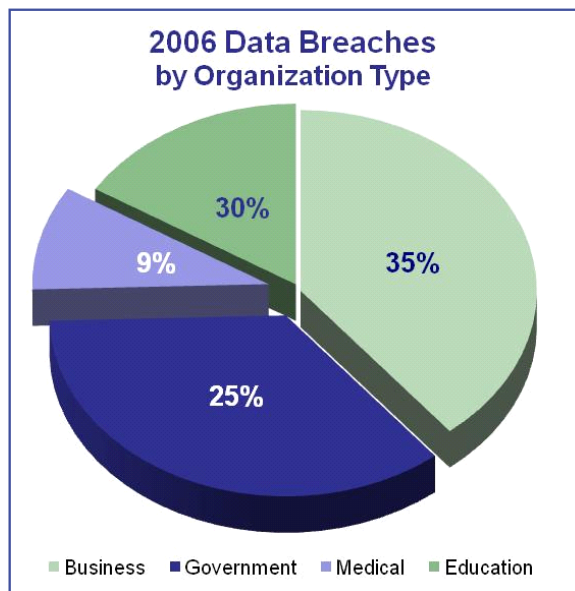
³ Adler, P. (2007, Nov 5). Consequences of a Large Security Breach: A TJX Companies Inc. Timeline [Electronic version]. Retrieved Nov 14, 2007 from: <http://infocounsel.files.wordpress.com/>

number, magnetic stripe data, Card Verification Value or Code (CVV or CVC) used for card-not-present transactions, and the card expiration date. Cardholder data also includes all personally identifiable data about the cardholder and all data gathered by the merchant/agent, including addresses, telephone numbers, and other contact information of the consumer.

SAVVIS does not in any way guarantee and makes no representation or warranty that any of its services comply with any applicable data security law or satisfy any particular control standard. SAVVIS does not purport to provide any customer or potential customer with legal or regulatory or compliance advice and nothing herein shall be interpreted as such advice. SAVVIS does not assume any liability for any good faith classification of any information, potential risk or control. There are inherent limitations in any such classifications as well as any assessments and audits and SAVVIS does not guarantee that any such classification, assessment or audit is adequate or appropriate. Full responsibility for all regulatory compliance remains the sole and exclusive responsibility of the customer and not SAVVIS.

Impact of PII Breaches

Data breaches or loss of PII have impacted people and businesses from all sectors and walks of life. Each year, a growing amount of data loss is occurring the United States and worldwide. The impact of identity theft and loss of PII databases is multifold. It impacts



Source: Privacy Rights Clearinghouse.³

the economy, as thieves use PII to steal from financial institutions, retail stores and individuals. It impacts large organizations and corporations (some have been forced out of business) as they lose their reputation, and suffer litigation and fines. But, most of all, it greatly impacts the owner of the identity.

One such example is Michelle Brown, who testified of her suffering before the U.S. Senate in July 2000. Ms. Brown's identity was stolen from her original rental application, acquired from her landlord's property management office. The thief created a "shadow identity" that still haunts Ms. Brown today, as the thief destroyed her credit, waged a multi-year crime spree (in and

out of jail), made many purchases on credit under her name, was arrested on drug and other felony charges, all of which resulted in a felony criminal record and debt against Ms. Brown, all committed by someone else.

Ms. Brown testified, "My world had become a living nightmare. I personally was affected extremely: I was significantly distracted at a job that I had just started three weeks prior to the day of discovery, I suffered from a nearly non-existent appetite, very little sleep, and was consumed with the ferocious chore of restoring my name and attempting to quell any future abuse. I lost identification with the person I really was inside and shut myself out of social functions because of the negativity this caused on my life..." To this day, she is no

⁴ Rosenberg, B. (2007, February 1). Chronology of Data Breaches 2006: Analysis [Electronic version]. Privacy Rights Clearinghouse. Retrieved Sept 6, 2007 from: <http://www.privacyrights.org/ar/DataBreaches2006-Analysis.htm>

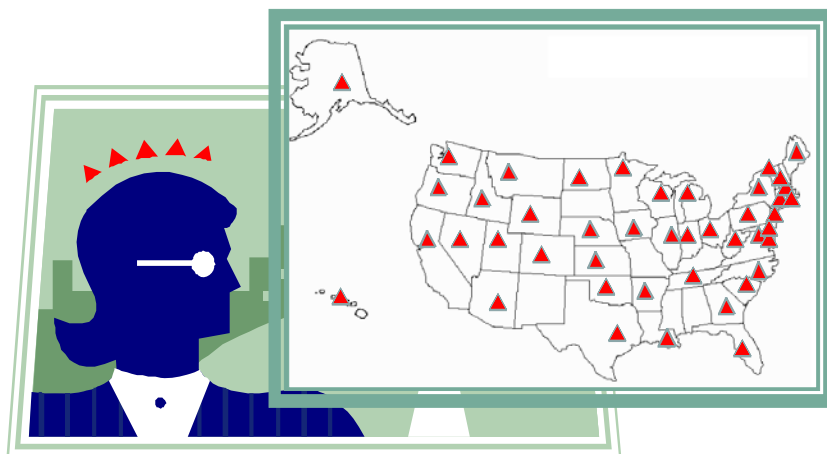
longer able to travel internationally, for fear of being detained upon re-entry to the U.S., or arrested and jailed overseas.⁵

The increase in complaints to the Federal Trade Commission, frequent reports of multimillion record breaches, and devastation caused by the identity theft has resulted in new privacy laws and breach notification legislation, which began in the state of California.

State Laws on Privacy and Notification

Each organization that holds or processes PII must consult with legal counsel, and together evaluate the data to be designated as PII based on:

- Existing laws in 44 U.S. states, the District of Columbia and Puerto Rico have individual data privacy or notification of breach rules regarding PII.



The states that have passed legislation or have laws in effect as of August 20, 2008 include: Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming, as well as the District of Columbia and

Puerto Rico⁶ Other states are considering legislation. These laws do not all agree with each other, causing confusion, and apply when conducting business in the applicable state, or in many cases if data from citizens of the state where the law is in effect was in the database that was breached (no matter where the organization or business is based).

- Pending federal legislation that might replace state laws or provide minimum standards for state laws regarding data privacy and notification of data breach.
- Open Records Acts or Laws in the state where the organization is based or doing business that require data be disclosed by government agencies (if the organization considered is a local, county, state or federal government organization).
- State of California Civil Code § 1798.80, § 1798.81, § 1798.82, which relate to computer security breach notification and data privacy. California has the most extensive law that is considered by legal and security professionals as a reasonable standard. No matter what state

⁵ Brown, M. (2000, July 12). Written Testimony of Michelle Brown, before U.S. Senate Committee Hearing on the Judiciary Subcommittee on Technology, Terrorism and Government Information [Electronic version]. Privacy Rights Clearinghouse. Retrieved Sept 6, 2007 from: <http://www.privacyrights.org/cases/victim8.htm>

⁶ Greenberg, P. (2008, June 20). State Security Breach Notification Laws [Electronic version]. National Conference of State Legislatures. Retrieved Aug 20, 2008 from: <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>

the organization or company is based in, legal counsel may well consider California data privacy and security breach notification law in addition to local laws.

The data listed as PII in this paper is based on these potential considerations. The contents of this paper are not to be interpreted as legal opinion, but rather as a guide to help security professionals to work with legal counsel in arriving at an appropriate list for the given organization.

Moderately Sensitive PII Data

All PII data may be determined by an organization and legal counsel to be treated as “highly sensitive” as described in the next section. However, if an organization’s legal counsel has determined that a portion of PII requires less protection, a benefit may be realized in the cost of security by protecting data such as “Name, Address, and Phone Number” as less than “highly sensitive.”

Examples of this type of PII are those data elements that government agencies may need to disclose under the “Open Records” laws or “Freedom of Information” acts, which generally include:

- Name (first and last name or first initial and last name).
- Home Address.
- Telephone Numbers.
- Date of Birth.
- E-mail Addresses.

This PII data must not be treated lightly, and is normally protected with measures for storage, transmission and destruction at the same level as any “Internal Use Only” or Proprietary Data at private or public corporations. Caution must be used with electronic, physical or verbal use of this data.

Using and Storing in a Secure Manner

When storing this type of “Moderately Sensitive PII” on computers, the electronic data should at a minimum be secured on a password-protected server or host, with other information security measures that include server hardening, firewalls, intrusion detection, and file integrity monitoring.

Hard Copy (paper) that contains this level of PII should not be left in plain sight where a passerby can observe the data, memorize it, photograph it, duplicate it on a photocopier, or write it down.

Laptops or Removable Media such as CDROMs, USB Flash Memory Drives, Magnetic Tapes, and Removable Disk Drives that contain this type of PII data must be controlled and the custody of this media must be managed at all times. It is a common best practice to encrypt PII data when stored on Laptops or Removable Media.

Transfer or Transmission from Point A to Point B

When transferring this type of “Moderately Sensitive PII” by electronic means, such as in an e-mail message, electronic file transfer or via removable media (CDROM, Magnetic Tapes such as those used for system backups, USB Flash-Memory Drive, etc.), it is a recommended practice to consider encryption of the data in transit to inhibit interception by unauthorized parties. One of the most common vulnerabilities for PII data is during transit, including when it exists on a Laptop, Mobile, or Notebook computer.

When shipping or carrying Hard Copy documents or reports that contain “Moderately Sensitive PII,” seal the material in an inner opaque envelope and mark the envelope and documents with the appropriate sensitivity level such as “Internal Use Only” or “Proprietary Data,” or for government agencies, “Official Use Only.” These labels should not be on the outer envelope used for shipping. Use a bonded courier that provides tracking of the

package. Only use facsimile (FAX) when you can confirm that the fax machine is in a secure area and under supervision. Do not leave printed output on the printer.

When communicating the “Moderately Sensitive PII” to other individuals verbally, verify the identity of other person and confirm that they have a need to know the information.

When the Data is No Longer Needed

When it is time to destroy the “Moderately Sensitive PII” data that has been stored on electronic media, acceptable physical destruction methods may include: incineration, melting, pulverizing or shredding of the media. Disk drives reused or offered as surplus must be overwritten a minimum of three (3) times, using special algorithms or software to obscure the deleted data and make it difficult to recover.

When it is time to destroy the “Moderately Sensitive PII” data that is contained on Hard Copy: The preferred method is cross-cut shredding either by using a shredder in the office, or by outsourcing high volume shredding to a bonded agent. The material should be locked up until shredding occurs.

Highly Sensitive PII Data

Personally Identifiable Data (PII) that government agencies do not normally expect to be forced to disclose under the “Open Records” laws or “Freedom of Information” acts generally includes:

- Social Security Number (SSN) or individual Tax Identification Number.
- Bank or Checking Account Number.
- Credit Card Number (by itself) or the combination of Credit Card number and Expiration Date - but NEVER store the magnetic stripe data or Card Verification Value (a.k.a the “security code”), as storage of those CVV numbers and track data is prohibited by PCI standards.
- Debit Card Number (but never store the PIN).
- A person’s previous names used, such as aliases, maiden names, previous married names, or Mother’s Maiden Name.
- Physical characteristics or description of person (i.e., eye color, hair color, height, weight), and biometric data of an individual (including fingerprints).
- Digital or Electronic copies of a Personal Handwritten Signature.
- Passport Number.
- Drivers License Number or State ID card Number.
- Insurance Policy Number.
- Protected Health Information, as covered by Health Insurance Portability and Accountability Act (HIPAA) that includes any information about health status, provision of health care, or payment for health care that can be linked to an individual.
- Any other “confidential” financial information associated with individuals, private organizations, or businesses.

Whether at a publicly-held company, private company, or government agency, this PII data must be protected with measures for storage, transmission and destruction the same as any highly sensitive data – with more strict security than described earlier for “Moderately Sensitive PII”. Elevated caution must be used with electronic, physical or verbal use of this data. It should always be marked as “Limited Distribution – DO NOT DUPLICATE OR DISTRIBUTE.”

Using and Storing Highly Sensitive PII

When storing “Highly Sensitive PII” on computers, **the electronic data containing PII must be encrypted** when “at rest” or when stored in a database using strong encryption technology, and secured on a password-protected server or host (using strong passwords), with other standard information security measures that include server hardening, firewalls, intrusion detection, and file integrity monitoring.

Hard Copy (paper) that contains this level of PII must be stored in a vault (secure safe) or **under lock and key when not in use**. When not locked up, it must be under direct supervision at all times. A limited number of people with need-to-know should have keys or access to the locked room or cabinets that store files with these documents containing “Highly Sensitive PII.” A locked desk drawer is not secure enough to store this type of data. **Strong metal cabinets, safes, or secure rooms must be used. Additional controls such as video surveillance and tracking of access to the storage area or cabinet is encouraged.** Actual articles that represent the PII (a Social Security Card, Credit Cards, Driver’s License, Birth Certificate, etc.) must also be secured at the highest level. Records with procurement-cards (credit cards used for small purchases such as office supplies) must be kept secure – these are credit card numbers!

One of the most serious articles or items that contains PII and must be protected is a check. Personal bank checks not only contain all the information an identity thief needs, but the check itself may be stolen, then duplicated or “washed,” to remove the pen ink and commit check fraud.

Laptops or Removable Media such as CDROMs, USB Flash Memory Drives, Magnetic Tapes, Removable Disk Drives that contain this type of PII data must be controlled and the custody of this media must be managed at all times. **The “Highly Sensitive PII” stored on removable media and laptops must be encrypted when “at rest” or when stored in a database using strong encryption technology.** When not being transported or used, these items should be secured in the same manner as Hard Copy above.

Transfer or Transmission from Point A to Point B

When transferring this type of “Highly Sensitive PII” by electronic means, such as in an e-mail message, electronic file transfer or via removable media (CDROM, Magnetic Tapes such as those used for system backups, USB Flash Memory Drive, etc.), **encryption of the data in transit is required to inhibit interception by unauthorized parties.** Possible methods include the use of an IPsec VPN tunnel or encrypted e-mail using strong encryption such as PGP.



Acceptable Methods to Protect PII Data While it is Transmitted Over a Network:

- Use an IPsec VPN with strong encryption.
- Web page security may use Secure Socket Layer (SSL) with 128bit encryption.
- Encrypt e-mail with PII using a tool such as PGP (for message and/or attachment).
- Encrypt data on removable media or laptops/mobile computers.
- Use WPA for WiFi (WEP not acceptable to protect PII).

encryption of the data in transit is required to inhibit interception by unauthorized parties. Possible methods include the use of an IPsec VPN tunnel or encrypted e-mail using strong encryption such as PGP.

One of the most common vulnerabilities for PII data is during transit, including when it exists on a Laptop, Mobile, or Notebook computer. Secure Socket Layer (SSL) may also be used to secure the transmission (this is the most common method for e-commerce web sites today).

When shipping or carrying Hard Copy documents or reports that contain “Highly Sensitive PII,” seal the material in an inner opaque envelope, and mark the envelope and documents with the appropriate sensitivity level such as “Limited Distribution” or “Sensitive Data,” and always label with DO NOT DUPLICATE OR DISTRIBUTE.” These labels should not be on the outer envelope used for shipping. Use a bonded courier that provides tracking of the package. Only use facsimile (FAX) when you can confirm that the fax machine is in a secure area and under supervision. **Never leave printed PII output on the printer – it must be secured immediately.**

Highly Sensitive PII might possibly never be communicated to other individuals verbally, but if it must be, verify the identity of other person and confirm that they have a need to know the information. Provide security awareness training to all employees, and explain how social engineering works – when someone might call by telephone to obtain bits of information, usually masquerading as someone they are not. Many times PII is lost to these types of attacks.

When the Highly Sensitive PII is No Longer Needed

When it is time to destroy the “Highly Sensitive PII” data that has been stored on electronic media, acceptable physical destruction methods may include: incineration, melting, pulverizing or shredding of the media. Disk drives reused or offered as surplus must be overwritten a minimum of **six (6) times**, using special algorithms or software to obscure the deleted data and make it extremely difficult to recover.

When it is time to destroy the “Highly Sensitive PII” data that is contained on Hard Copy: The preferred method is cross-cut shredding either by a using a shredder in the office, or by outsourcing high volume shredding to a bonded agent. The material should be locked up until shredding occurs, and should be certified (signed for) by the bonded agent upon destruction.

Publicly Available Data

Personal information, as defined in most state laws on data privacy and notification, does not include any publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media. Examples of widely distributed media include:

- Newspaper, Internet News, Radio, and Television News Reports.
- Classified Advertisements, marketing materials available to the public.
- Periodicals and Publications (printed or online).
- Official Public Web Sites where data is published by the owner of the data.
- Published Telephone Company Residential and Business Directories.

Telephone directories must be “published” by the telephone company providing service to the customer in order to be “widely distributed media” – as many “internal” directories may contain phone numbers for individuals who have requested their data be “unlisted” or “unpublished” by the telephone company in its directory or listings. For this reason, organizations should be careful with home telephone numbers for employees or customers. This “unlisted” or “unpublished” directory information is also protected based on selected state laws, including State of California Civil Codes § 1798.80, § 1798.81, and § 1798.82., and should not be confused with published telephone directories.

Summary

While this paper is not intended to be a complete guide to protecting PII, an overview has been provided to help understand what PII is, and why it is important to mitigate and reduce the associated risk. The drivers for protecting PII are clear and becoming increasingly urgent. These include legal compliance, industry standards, shareholder and customer confidence and protecting the reputation of the organization. Failure to properly protect PII in the digital age has already had disastrous consequences for consumers and the organizations that have been compromised by loss of media, laptop containing PII or security breach of information systems that use and store PII.

Organizations are faced with a tremendous amount of PII that they have a duty to protect. This paper has offered some examples of the different types of PII and practical advice on how to treat it. Each organization must confer with legal counsel to determine which data elements require protection.

Standards such as PCI/DSS provide specific data security practices that must be met by anyone processing or accepting credit cards for payment. It is imperative that an organization make a thorough study of the data used in computing applications or daily operations, and understand:

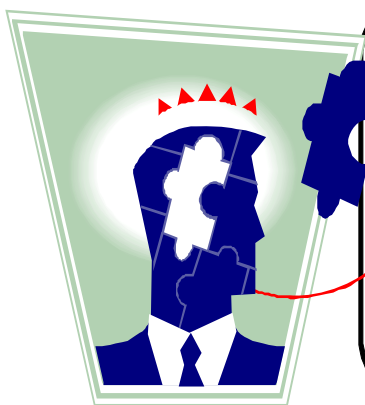
- Where is PII stored?
- How is PII protected?
- Who has access to PII?
- What is the path that PII is flowing through (e-mail, between applications, etc.)?

Once this is documented, appropriate data classification and handling policies and procedures should be developed to provide clear guidance on how the data should be secured and handled. The necessary protections to achieve the data handling guidelines can then be implemented across the organization. Success in protecting PII at any organization requires support from upper-level management, as well as participation from the various departments and business units.

While protecting PII is vital, much more must be considered in creating a security program. Integral components of a successful security plan, including security standards, policy, awareness training and implementation of controls, can be further explored in the SAVVIS White Paper: "Promoting Security Policy Longevity." Be prepared. Get ready before a breach occurs, reduce the risk or probability of an event, and plan for what must be done when it happens.

How SAVVIS Can Help

Based on over 10 years of experience with clients seeking to outsource select portions of their IT infrastructure, SAVVIS has achieved a balance between people, process, and technology. No Information Systems Security Architecture solution is achieved by using the best in just one area – a best-practice security solution requires a proper balance



Outsourcing to SAVVIS:

- Provides peace of mind in knowing that each part of the SAVVIS solution implements industry best practice.
- Includes access to our team of world-class security architects and consultants who provide the technical and program management experience to help bring concept to reality.
- Benefits from our mission to deliver the industry's best value in managed security services

between each security discipline. Developing a security program can place a demand on personnel resources, and SAVVIS has a team of experienced security architects who may advise a client on policy development and maintenance, or provide services to establish new policy for an existing or planned environment.

SAVVIS is able to contribute to the success of any organization in meeting the goals presented in this paper. A brief examination of some of the tasks necessary to

promote security policy longevity can yield concern over resources required to complete the effort required to become compliant with security standards and build a security policy document set.

SAVVIS' Security Professional Services is a specialized business that focuses on providing an end-to-end security solution to our customers. SAVVIS has developed an extensive range of consulting services that can help our customers to address the ever-changing and increasing security threats to their applications, systems and network. Security Services cover every aspect of the security cycle, from assessment and design to implementation and management, and include the following services:

- Security Assessment Services
- Security Architecture Review
- Security Code Review
- Security Policy Development
- Security Architecture Development and Implementation
- Cyber Incident Response Planning
- Business Continuity and Disaster Recovery Planning
- Security Compliance Consulting Services
- Security Awareness Workshops

Building a Security Program to Protect PII

The secret ingredient for success of protecting PII stressed in this paper is for the team of contributors to work together and view security as a business enabler. SAVVIS provides security consulting services to coordinate efforts from the team of contributors into recommendations and action plans for reducing security risk, developing security policy documents or standards, and facilitates the editing and review of the security policy toward approval and implementation.

The SAVVIS security program strategy is to only develop policy or security standards which include requirements that the organization is able to enforce. SAVVIS analyzes the

current security posture and provides recommendations for adjustments to meet specific security goals, such as the implementation of PCI DSS or ISO/IEC27001/27002 security standards (formerly ISO17799).

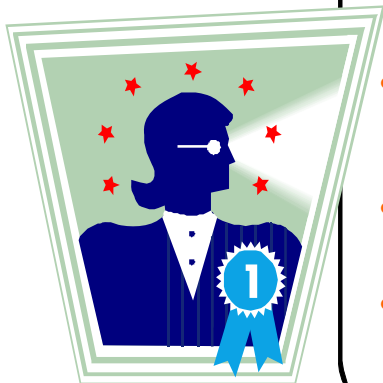
SAVVIS consultants are experienced in adjusting security policy to support the organization's culture, mission and business focus. This results in the creation of a security policy that will be practiced by all users, staff, and management of the organization.

When necessary, SAVVIS is able to engage contributors with specializations in

individual technical fields to produce a suite of security documents required for security best practices. Examples of these areas include individuals with extensive experience drafting hardening standards for server and desktop platforms, network devices, and security devices; security patch management; network security standards; incident response plans; business continuity and disaster recovery plans; and proposing solutions for security measures such as centralized logging, intrusion detection, and file integrity, as well as other areas required to protect PII as discussed in this paper.

SAVVIS is an industry leader in Security Utility services:

- Flexible and scalable managed security offerings that don't require hardware or software to be installed or managed at the customer's premises.
- Centralized management by SAVVIS, which allows for timely technology refreshes, as IT threats change and security solutions evolve over time.
- Customer monitoring provided via SAVVIS' Web portal. This permits users to monitor activity in their environment directly and conveniently.
- Extraordinary customer value, since SAVVIS' Security Utility services are typically less expensive than dedicated infrastructure solutions and allow for simpler capacity planning.



Payment Card Industry Security Services

All merchants and payment processing firms with internal systems that store, process, or transmit cardholder data must comply with the PCI DSS. For some, self-assessment and quarterly network scans could be the only formal requirements. For high-volume merchants and service providers, compliance must be demonstrated by means of an

annual assessment that is conducted by a certified third-party assessor. SAVVIS and Coalfire Systems have teamed to provide an end-to-end program for PCI. Geared to all merchant and service provider levels, the program is designed to provide a comprehensive solution for both PCI assessment and compliance services.

SAVVIS' Security Legacy

SAVVIS' legacy of delivering security services dates back to 1987, with the formation of our ARCA Common Criteria Testing Lab (CCTL). With such a rich legacy, customers can be assured that the SAVVIS Security Services team practices security-industry-standard tenets of confidentiality, integrity, and availability. Our fully managed security devices are kept current with the latest patches and upgrades. In addition, we only allow individuals with security responsibility to access information about the way we deliver security services to their organizations, and all communications with the devices that SAVVIS manages is either encrypted or restricted to our private networks. Lastly, our Security Technical Assistance Center (STAC) infrastructure and processes are fully redundant, to provide service reliability round-the-clock.

In summary, SAVVIS provides the professional services that transform an existing organization with security challenges into a secure organization prepared for security threats and enabled to provide services and products in a secure fashion.

About the Authors

Dr. Michael T. Metzler has over 25 years of work experience in Computer Science, Computer Networking and Security. He has delivered consulting service internationally that includes expertise and experience in security policy, security planning, network design and troubleshooting. Dr. Metzler has designed global networks for many of the Fortune 500 and provided network security services for many major corporations, as well as for the United States and foreign government agencies. He has been a Certified Information Systems Security Professional (CISSP) since 1998, and also is a Certified Information Security Manager (CISM) and is Certified in the Governance of Enterprise Information Technology (CGEIT).

Mr. Paul Harker is a respected professional with distinguished 12-year career analyzing, designing, implementing and managing Information Systems Security infrastructures for large global businesses and government institutions across multi-platform environments. He has developed consulting methodologies that focus on compliance with security industry standards such as the former Visa CISP, MasterCard SDP, ISO/IEC27001/27002 (formerly ISO17799) and the current Payment Card Industry (PCI) Data Security Standards. He has an MBA from the University of Washington, and is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and is a certified Project Management Professional (PMP).

About SAVVIS

SAVVIS, Inc. (NASDAQ: SVVS) is a global leader in IT infrastructure services for business applications. With an IT services platform spanning North America, Europe, and Asia, *SAVVIS leads the industry in delivering secure, reliable, and scalable hosting, network, and application services.* These solutions enable customers to focus on their core business while SAVVIS ensures the quality of their IT systems and operations. SAVVIS' strategic approach combines virtualization technology, a global network and 24 data centers, and automated management and provisioning systems. For more information about SAVVIS, visit www.savvis.net.



BUILT TO RESPOND™

Corporate Headquarters

SAVVIS Inc.
1 SAVVIS Parkway
St. Louis, MO 63017
800-SAVVIS-1
www.savvis.net

SAVVIS Federal Systems

2355 Dulles Corner Blvd.
Suite 300
Herndon, VA 20171
703-667-6000
www.savvis.net/federal

ASIA

SAVVIS
50 Raffles Place
Singapore Land Tower
#13-01/04 Singapore,
Singapore 048623
65 6768 8000
www.savvis.net

EMEA

SAVVIS UK Limited
Eskdale Road
Winnersh Triangle
Workingham
Berkshire RG41 5TS
United Kingdom
+44 (0)118 322 6000
www.savvis.co.uk