USA Services Intergovernmental Newsletter

Protecting Personally Identifiable Information

Issue 19 • May 2007

http://www.gsa.gov/intergov

What is Being Done to Protect Your Personal Information

By Lisa Nelson
USA Services Intergovernmental Solutions
GSA Office of Citizen Services and Communications
U.S. General Services Administration

Identity theft is one of the fastest growing crimes in the country and concern by the public is growing rapidly with each new data breach exposed. This increase is directly attributable to advances made in the area of computer technology and data collection that allow information sharing across agencies, governmental boundaries and service providers. These advances have made it easy for public and private institutions to gather large amounts of information on citizens, including their names, addresses and Social Security Numbers (SSN). One indicator of the scope of the problem is the Privacy Rights Clearinghouse report of over 104 million security breaches since January 2005 involving personal information that could be used for identity theft.

In May 2006, the Department of Veterans Affairs (VA) jolted its constituents and the government with the revelation that the theft of a laptop from an employee's home made 26.5 million veterans' records vulnerable to identity theft. While it revealed to the general public the risk to their personally identifiable information held in government databases, it also prompted the VA to implement its Data Security – Assessment and Strengthening of Controls initiative. This is a multi-phased initiative to make the VA the "Gold Standard" in data security.

The VA incident raised the issue of allowing employees and contractors to carry data files away from secure government facilities in order to do work with them offsite. The incident also highlighted the inordinate delay between the discovery of the laptop theft and the announcement to the public. The White House Office of Management and Budget quickly issued policy directives requiring agencies to report within an hour even the suspicion of a data breach. This has helped raise the issue of data security to a top priority, moving agencies in the direction of strict accountability when it comes to the vulnerability of personally identifiable information.

The new reporting requirement revealed that the VA was not the only

Continued on next page...

The USA Services Intergovernmental Newsletter is produced twice a year by the USA Services Intergovernmental Solutions Division, GSA Office of Citizens Services and Communications; Lisa Nelson, Editor. Send comments and suggestions to: lisa.nelson@gsa.gov.

government department with concerns about securing personally identifiable information. The House Committee on Oversight and Government Reform issued a report on agency losses of personally identifiable information that detailed thousands of breaches of government computers since 2003. Meanwhile, Karen Evans, OMB Administrator of E-Government and IT, announced that more than 338 incidents of personal identity information loss between July and September 2006 had been reported to OMB. Most of the losses are not from attacks by outsiders, but are attributable to "people losing data," she said. Other Federal agencies that have reported data breaches include the Departments of Education, Agriculture, Commerce, Navy, Health and Human Services and State, as well as the IRS and Social Security Administration.

Even before the VA data breach, Executive Order 13402 had created a federal Identity Theft Task Force to formulate a comprehensive and fully coordinated plan to attack identity theft. The task force is focusing on ways to improve criminal prosecutions of identity theft, enhance protection of sensitive consumer information, provide guidance for consumers and the business community, and improve recovery and assistance for consumers.

The group issued specific recommendations in April of broad policy changes and small steps necessary to reduce the incidence of identity theft and the damage it does. These include:

- Reduce the unnecessary use of SSNs by federal agencies;
- Establish national standards requiring private entities to safeguard the personal data they compile and maintain and to notify consumers when a breach poses a risk of PII loss;
- Implement a sustained federal awareness campaign to educate consumers, businesses and government on methods to deter, detect and defend against identity theft; and
- Create a National Identity Theft Law Enforcement Center to investigate and prosecute identity thieves more effectively.

Data held by non-public institutions—such as credit bureaus, banks, mortgage companies, universities and corporations—are also at risk. A wake-up call came when consumer data broker ChoicePoint, Inc., acknowledged that the personal financial records of more than 163,000 consumers in its database had been compromised. As part of a settlement, ChoicePoint was required to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026.

This newsletter illustrates some of the many ways governments and other organizations are protecting personally identifiable information (PII) to provide better services to citizens. We begin with articles by the VA, ***Protecting PII: the VA Story***, and, ChoicePoint, ***Choicepoint Enhances Privacy and Information Security Framework***. These pieces highlight the progress they have made and the enterprise-wide strategies they are employing to reach a high level of excellence in data security. The National Association of Chief Information Officers (NASCIO) offers guidance to the states in ***Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy?***

What Governments Are Doing

In ***Protecting Personally Identifiable Information is a Hot Topic Worldwide***, five national policies for dealing with privacy and the protection and use of PII are discussed. ***Personal Information Protection in Japan*** describes that country's legislation for protecting personal information in the public and private sectors. ***The π of PII*** describes some of the innovative practices used in the State of California—the first to adopt comprehensive data security laws and the model for 33 other states.

What the U.S. Governments is Doing

The Federal Government's policy for ***Securing Government Systems and Protecting Privacy*** is excerpted from the Administration's 2008 budget documents. Agencies' unique approaches to different components of privacy/security policy are described in: ***Being Proactive about PII: A Case Study on Identity-Theft Risk Assessment at the IRS*** and ***The Evolution of Privacy Awareness Training at the VA***. In ***Moving Beyond FISMA Compliance,*** the Council for Excellence in Government looks at what agencies are doing as a result of FISMA and whether or not they are really improving security and mitigating risk to systems and information.

Ensuring Private Information Stays Private references the House Government Reform Committee Report on agency data breaches since January 1, 2003 and suggests the government do more to prevent e-mail, web and other infrastructure attacks (i.e. with VoIP). ***Protection of PII: The Role of Business Unit Management*** emphasizes the need to involve government managers in the development of security policy. The piece ***Ensuring Data Security and Protecting PII: The Federated Model*** looks at the advantages of a federated approach of secure data exchange. This approach is put into action in ***Leveraging a Federated Approach for Trusted Identity Management and Cross-Credentialing***, which describes the Department of Defense's "federated" approach to issuing credentials in which personal data remains in individual employer records and minimal information is shared.

Continued on next page...

Do We Need Additional Legislation?

Some experts argue that stemming the flow of personal information out of government and commercial entities will require new legislation. In ***Federal Data Privacy***, a security strategist suggests legislation to define what personal data and identity are and establish national benchmarks for all levels of government and the private sector. ***Privacy and Information Assurance: Deceptive Look-Alikes*** discusses the differences between privacy and information assurance and recommends broad legislation that extends the Code of Fair Information Practices consistently.

Processes, Procedures and Products

GAO Recommendations for ***Protecting Personal Information*** outlines key elements of an agency strategy for protecting personal information. Dovetailing with the GAO article, the Privacy Rights Clearinghouse suggests ways employers can implement responsible information-handling practices in ***Prevent Identity Theft with Responsible Information Handling Practices in the Workplace***.

The marketplace offers countless processes, procedures and products to address security issues. ***Can This Device Be Trusted? Using Trusted Computing to Build a Secure Environment*** suggests a security foundation that could help establish the trustworthiness of devices. The International Association of Privacy Professionals (IAPP) advocates professional certification in information privacy in ***The IAPP Offers Government Privacy Professionals A Specialized Privacy Credential***. Encryption segmentation to help secure PII within and between agencies is recommended in ***Protecting PII with on-the-Fly Encryption*** and the use of privacy scans are promoted in ***Implementing Privacy Best Practices Through Automated, Ongoing Privacy Scans***.

What are the Prospects for Privacy?

We will close the newsletter by looking at the prospects for privacy. IBM poses the question, ***Which Would You Rather Have: Privacy or Convenience?*** In the article ***How to Avoid Appearing in The Washington Post***, EDS looks at the three major activities that agencies must accomplish. In conclusion, the National Electronic Commerce Coordinating Council takes a frank look at the demise of personal privacy in ***Privacy (for You and Me) is Dead***. We hope you will find this newsletter useful and that it will help your organization further its goal of protecting personally identifiable information. ■

Lisa Nelson is Editor of the USA Services Intergovernmental Newsletter. For additional information, contact lisa.nelson@gsa.gov.

Protecting PII: the VA Story

By Robert Howard
Assistant Secretary for Information and Technology
U.S. Department of Veterans Affairs

As a result of the laptop and external hard drive theft in early May 2006, Secretary Jim Nicholson vowed to "make the Department of Veterans Affairs (VA) the *Gold Standard* in the area of information security, just as we (the VA) have done in the areas of electronic medical records." The May incident was a "wake-up call" to many people because of the relative ease with which the personal records of millions of veterans could be placed at risk. The Secretary quickly established the *Gold Standard* mandate and is determined to substantially reduce the risk of sensitive data loss in the future.

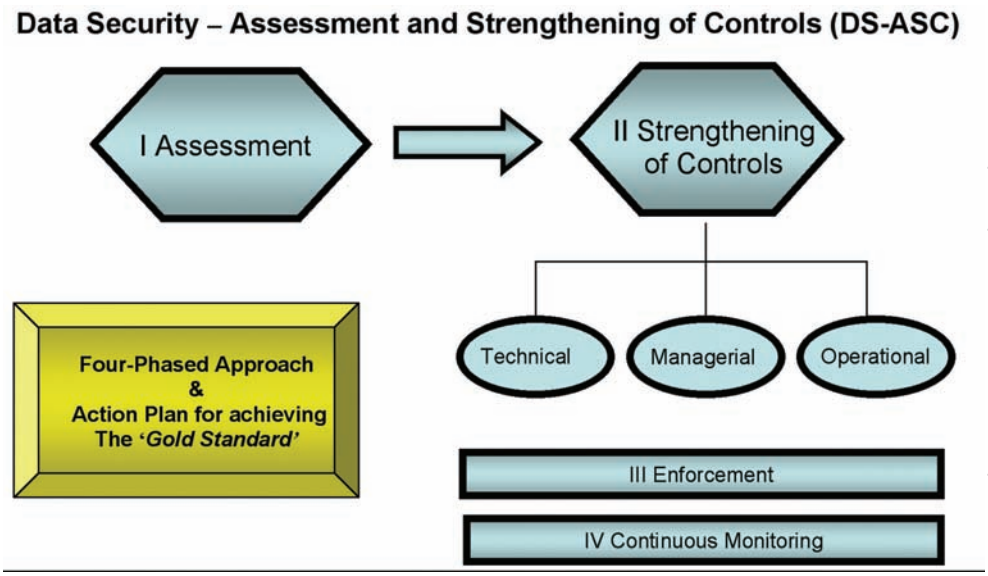
Fortunately, the FBI recovered the stolen equipment and after a thorough investigation determined with a high degree of confidence that the data contained on this equipment had not been accessed or compromised.

Responding to the Secretary's mandate, the Data Security – Assessment and Strengthening of Controls (DS-ASC) program was established. This is a multi-phased initiative to reduce the risk of a recurrence of incidents involving personal data and to remedy information security weaknesses. The first step was to carefully assess the state of data security throughout the department. As a result of this assessment, a number of actions were identified to strengthen data controls in three specific areas:

- In the *technical area*, such as encryption processes and tools;
- In the *management area*, such as a complete review of policies and directives; and
- In the *operational area*, such as procedures for monitoring access to and the extraction of sensitive information.

A top priority is to reach a high level of excellence in data security - in

Continued on next page...



Source: U.S. Department of Veterans Affairs

other words, to achieve the *Gold Standard*. VA recognizes that to achieve this objective, it will need to implement enterprise-wide strategies that (1) promote awareness among all employees and contractors and (2) effect a change in the culture and capability in all of VA's facilities from central office to remote locations.

The DS-ASC program is the action plan for achieving the Gold Standard in IT Security. Some of the key elements to protect PII and prevent security incidents are explained in further detail below. These are steps that any government agency can take to stem data loss and reduce the risk of security incidents – especially involving sensitive data. For more detailed information, refer to the *VA Strategic Plan, FY 2006 – 2011*, published in October 2006.

Some Key Elements of the VA Gold Standard for Data Security:

Promulgation of Policies and Procedures

Information security policy is an essential component of Information Security Governance – without the policy, governance has no method of enforcement. The VA Information Security Policy is derived from several sources, which include: appropriate legislation, such as the Federal Information Security Management Act (FISMA); applicable standards, such as National Institute for Standards and Technology (NIST); Federal Information Processing Standards (FIPS) and guidance; and internal VA requirements.

IT Strategic Planning

VA is integrating information security into the agency strategic planning processes by first establishing, then documenting, the information security strategies that directly support agency strategic planning and performance activities. The VA's Information Security Strategy will establish a comprehensive framework to enable the development, institutionalization, assessment and improvement of the agency's information security program.

Training and Education (For VA and Non-VA Personnel)

Security awareness and training is a critical component of the VA information security program. It is the vehicle for disseminating security information that employees, including managers, need to do their jobs. Establishing and maintaining a robust and relevant information security awareness and training program is the primary conduit for providing the workforce with the knowledge needed to protect the VA's vital information resources.

Securing of Devices

As more systems become portable within the VA computing environment, VA must instill in users an awareness of their responsibility for maintaining the security of those assets. The intent of IT asset management policies is to secure VA assets and mitigate risk.

Encryption of Data

All VA data subject to physical or virtual loss will be encrypted. Examples of situations that require encryption are: laptops, tapes, e-mail with sensitive information, enterprise data exchange, and other systems subject to physical loss.

Enhanced Data Security for VA's Sensitive Information

Federal mandates require the protection of many types of information through adherence to Federal Information Processing Standards promulgated by NIST. In accordance with FISMA, VA has begun implementing these standards as specified. When complete they will contribute towards enhanced protection for VA sensitive information.

Enhanced Protection for Shared Data in Interconnected Systems

Interconnecting information systems can expose the participating organization to risk; security failures could compromise the connected systems and their data. Federal policy requires that federal agencies establish interconnection security agreements. Specifically, *OMB Circular A-130, Appendix III*, requires that agencies obtain written management authority before

Continued on next page...

connecting their information systems to those of another agency based on a mutually acceptable level of risk.

Incident Management and Monitoring

FISMA specifically directs federal agencies to develop and implement procedures for detecting, reporting, and responding to security incidents. Enhanced incident management within the VA focuses on:

- Establishing a formal incident response capability;
- Creating an incident response policy and using it as the basis for incident response procedures;
- Identifying all groups within the VA that may need to participate in incident handling.

One of the Secretary's five priorities outlined in the VA Strategic Plan is to achieve the *Gold Standard* for data security and stewardship for veterans, their families, and VA employees. In order to achieve this standard, VA will continue to implement system-wide strategies that promote data security awareness among all employees and a change in the culture and capability in all of VA's facilities and remote locations. Additional strategies are likely to evolve as VA advances its data security efforts. For now, having a well-defined and detailed information security program is a significant step forward. We have already seen improvement in areas such as encryption and incident management, which demonstrates VA's strong commitment to and progress in achieving the highest standards of performance in data security. ■

Robert Howard is the Assistant Secretary for Information and technology. For additional information contact laura.nash@va.gov

ChoicePoint Enhances Privacy and Information Security Framework

By Tammy Meckley, CIPP
Assistant Chief Privacy Officer
ChoicePoint

ChoicePoint helps businesses, government agencies and nonprofit organizations make better decisions through information and technology solutions. Each year, ChoicePoint helps more than six million people get the jobs they seek and more than 100 million people get fairly priced home and auto insurance. Our products assist small businesses in obtaining affordable commercial insurance. Businesses grow revenue with our marketing services and cut costs through our authentication and anti-fraud tools. Government agencies use our data and technology to fulfill their missions in all parts of the world.

During the past two years, ChoicePoint has enhanced and transformed its information security and privacy programs into a comprehensive security and privacy framework ("the framework") designed to: identify, assess and control risks; enhance security; and protect consumers' personally identifiable information. The key components of the framework include: enterprise-wide employee and customer accountability; corporate security; information security; credentialing and re-credentialing of individuals having access to ChoicePoint information both internally and externally; policies, procedures and guidelines; audit and compliance; and outreach and education. All of these framework components work together and are equally important. This essay focuses on two areas: credentialing and re-credentialing, and audit and compliance.

To fully understand the extent to which credentialing fits within the framework, it is important to understand what is involved in the process. The term "credentialing" essentially refers to ChoicePoint's comprehensive front-end audit to help ensure customers who will have access to ChoicePoint information are who they say they are and will use the information for legitimate business and permissible purposes in accordance with the law and ChoicePoint policies. ChoicePoint enhanced its credentialing process by establishing a centralized corporate credentialing center to help ensure security and consistency.

As part of its enhanced credentialing procedures, new and existing customers are asked to undergo a certification or recertification audit that in many instances includes a site visit to their primary places of business to verify their legitimacy. Given that ChoicePoint has more than 100,000 customers, this undertaking involves a massive commitment on the part of the company's senior leadership and all associates.

In addition to credentialing customers, ChoicePoint recognizes the importance of knowing its own employees, independent contractors and vendors. It is just as important to know and to continue knowing your employees and contractors who will have internal access to

Continued on next page...

consumers' personally identifiable information as it is to know your customers.

ChoicePoint's U.S.-based employees and contractors are required to undergo a background check as part of the pre-employment process. Furthermore, U.S.-based employees and contractors are required to complete a re-credentialing background check every five years as a continuous condition of employment. ChoicePoint has also implemented an assessment and audit process for vendors that have access to or potentially will come into contact with consumers' personally identifiable information. This process assesses that the vendor(s) has implemented and is maintaining appropriate information security and privacy safeguards.

These credentialing and re-credentialing efforts are designed to mitigate risk and are part of an initial, very important and ongoing journey toward being an industry leader in protecting consumers' personally identifiable information. ChoicePoint carefully selects its customers and only provides certification to certain customers.

Audit and compliance is another critical part of the framework. This is the back end part of the process. There are two types of audits. Those driven by ChoicePoint customers', otherwise know as independent third-party audits and assessments, and those performed internally by ChoicePoint. ChoicePoint successfully completed more than 40 independent audits and assessments in 2005 and more than 50 in 2006, by customers including several large insurance companies and financial institutions. Internal ChoicePoint audits include random, event-driven or suspicious activity, third-party audits. This process examines ChoicePoint's customers' use of information to ensure that the basis for use falls within the confines of legally enumerated "permissible purposes." ChoicePoint even goes beyond looking at its customers by performing consumer sampling audits where ChoicePoint engages directly with the consumer to validate ChoicePoint's customers' assertion that a consumer granted consent before his or her information was accessed.

ChoicePoint's privacy and security framework and safeguards have proven to be effective in mitigating risk, enhancing security and protecting consumer privacy. While ChoicePoint's efforts have been recognized as leading practices in the industry, being good stewards of protecting consumer privacy and information is a continuing endeavor and one that ChoicePoint takes very seriously. ■

Tammy Meckley is Assistant Chief Privacy Officer at ChoicePoint. For additional information contact Tammy at tammy.meckley@choicepoint.com.

A Summary of NASCIO's "Keeping Citizen Trust: What Can a State CIO Do To Protect Privacy?"

By Mary Gay Whitmer
Senior Issues Coordinator
National Association of State CIOs (NASCIO)

The National Association of State CIOs (NASCIO) has published a research brief, "Keeping Citizen Trust: What Can a State CIO Do to Protect Privacy," which is summarized here. It provides state CIOs with a common frame of reference for the importance of citizens' information privacy and some initial ways for states to implement and manage privacy protections.

Privacy—A Defining Issue:

Privacy is a defining issue of the day for both the public and private sectors. Citizens are now aware of data breaches, identity theft and the risks that can result from personal information finding its way into ill-intended hands. Even state legislatures have taken notice of privacy's importance in recent years. From 2004 to the present, thirty-eight state legislatures have enacted data breach notification laws mandating, to varying extents, notification requirements for citizens whose personal information has been compromised by a security breach. In spite of legislative measures taken on this issue, data breaches have been frequent in the private, public and university sectors.

The Evolving Nature of the Privacy Discussion:

Privacy has always been an important issue that has even been recognized and protected by the U.S. Supreme Court. However, the nature of the privacy discussion is evolving and has become increasingly complex. It has not been that long since privacy protections were provided, at least to an extent, by public records being discretely tucked away within locked file cabinets of government agencies. Now, though, the privacy discussion is driven by an environment of increased information sharing across traditional agency and governmental boundaries and the ease with which information can be collected, compiled, manipulated, used and transmitted. Rapidly evolving technologies have and will only continue to facilitate this, while the legal framework for privacy, as well as the generally accepted business practices to guard against privacy compromises, have failed to keep pace. The rise of homeland security efforts at all levels of government has also played a significant role. Moreover, privacy has become an important facet of many of the high-priority issues of the day, including:

- Homeland security
- Emergency management
- Disaster recovery and business continuity after natural disasters, such as Hurricane Katrina or homeland security-related events
- Electronic health records
- Driver's license reform through REAL ID Act implementation
- IT consolidation and shared services initiatives.

In the context of this evolving privacy discussion, many states are still in the process of determining how best to address privacy across the state enterprise, and the state CIO's involvement varies greatly from state-to-state. Regardless of where responsibility for privacy may reside

in a given state, the one constant among all states is the need for the many privacy stakeholders to understand privacy's importance and how citizen privacy can be protected.

State Privacy at Present:

With states functioning in an environment of expanding information sharing efforts across traditional governmental boundaries, all too prevalent data breaches, and heightened levels of citizen distrust, the criticality of developing an organized way to address privacy issues across the state enterprise has also increased. To understand when and how state CIOs may encounter privacy issues, an important first step is to examine how privacy issues come into play within the current state environment.

The Decentralized Nature of State Government: Comprised of many agencies, branches, and quasi-governmental entities, states hold mounds of sensitive, personal information in disparate places across the enterprise. The same information relating to an individual,

Continued on next page...

such as a Social Security Number, may be collected, used and stored by multiple state agencies. With data stored in a distributed fashion across the state, protecting that data in all of the places in which it exists can be a monumental task. In addition, agency policies and business practices with respect to that information may vary greatly, increasing the risk that a privacy compromise could occur, even if most agencies have adequate privacy protections in place.

Greater Opportunities for Information Sharing: Within many contexts, such as justice and health care, there are expanding opportunities for information sharing across agencies, among levels of government and with the private sector. Many of these information sharing initiatives stem from the need to detect fraud, enforce tax and child support payments, prevent medical mistakes, and even avert terrorist attacks and other serious crimes.

A Complex Legal Framework: Adding more complexity is a legal framework that addresses privacy on a sector-specific basis. There are both state and federal laws that address the privacy of certain types of information—health information, financial information, and other types of sensitive, personal information. However, since privacy has been addressed in a somewhat organic fashion, there may be conflicting statutes across state agencies. Some agencies may collect personal information that other agencies are legally prohibited from collecting. The same may be true regarding the resale or secondary use of information. For example, one state agency may be able to share or sell

information, while another, such as a state motor vehicle department, may be restricted from sharing or reselling the information unless it is for certain, specified purposes. The secondary use or resale of citizen information is especially important in the government context, because citizens frequently must provide personal information in order to receive a government entitlement or service. However, citizens may be unaware that this information can be shared with other agencies or even resold to a private sector data reseller.

NASCIO's research brief details 32 avenues through which State CIOs may be able to provide for improved privacy protection. They focus around CIO efforts in the following areas:

- Governance
- Enterprise Architecture Efforts
- Policy
- Business Processes and Practices
- Laws and Regulations
- Security and Data Protection
- Communications and Awareness

This brief may be downloaded at: http://www.nascio.org/publications/researchBrief.cfm. ■

For more information contact Mary Gay Whitmer, Senior Issues Coordinator, at mwhitmer@amrms.com or (859) 514-9209.

Protecting Personally Identifiable Information Is a Hot Topic Worldwide

By Darlene Meskell
Director, USA Services Intergovernmental Solutions
GSA Office of Citizen Services and Communications
U.S. General Services Administration

Senior information technology officials from the U.S., Canada, Australia, the U.K. and New Zealand met by videoconference in November 2006 to share their experiences with protecting personally identifiable information (PII) held in government databases. Following are the highlights of the discussion.

The five national policies for dealing with privacy and the protection and use of PII were very similar in some ways, but each country took a slightly different approach to the issue. These approaches ranged from the U.S.' drive to protect PII even at great cost, to New Zealand's "avowed intent" that the Internet will soon be the dominant way to deal with the government, requiring the routine use of PII online.

New Zealand law has specific constraints around the use of government databases; the other four countries cited national Privacy laws dating to the 1970s and 1980s—before the Internet. Most countries also have specific policies regarding the collection and protection of PII. They reported that their citizens are of two minds about government collecting personal information. On the one hand, they don't want the government to maintain databases of their personal information; on the other hand, they want the convenience of being identified when they transact business with the government.

All five countries are dedicated to becoming increasingly citizen-centric and want to use PII to improve their service to citizens. Driven by its Transformational Government initiative, the U.K. is revising its approach to data-sharing across the public sector and has published an Information Sharing Vision Statement. A Ministerial Committee has been established to develop government strategy for sharing information across agencies to expand opportunities for the most disadvantaged, to protect against fraud, to provide better citizen services and to reduce the burden on business.

Australia also recognizes that implementation of its E-Government Strategy will depend on sharing personal information across agency boundaries. Sound ID management will be critical to implementing connected government while respecting privacy and complying with privacy legislation.

All five countries limit the reasons PII can be collected, restricting access to it and allowing individual citizens to control the "who/what/why" of how their information is used. All are developing codes, principles and guidelines to control PII use.

The U.K. Information Commissioner is developing guidelines for assessing proposals involving personal data and a framework Code of Practice that will help protect personal privacy.

The Australian Government E-Authentication Framework Privacy Principle provides that agencies will only collect personal information where necessary for the processes being undertaken and will conduct Privacy Impact Assessments. Australia's Privacy Act contains 11 Information Privacy Principles based on the OECD Privacy Guidelines:

- Personally identifiable information must only be collected for a lawful purpose;
- The information owner must be informed;
- Collection must not be unreasonably intrusive;
- Unauthorized use of information must be prevented;
- Collection and use of data must be disclosed in public records;
- Owners must have access to their own personally identifiable information;
- Information must be correct and up-to-date;
- Government must ensure the information is accurate before using it;
- Information may be used only for a relevant purpose with some legal or health exceptions; and
- Personally identifiable information must not be disclosed unless for a relevant reason.

Continued on next page...

The Privacy Act is being amended to better enable the sharing of personal information in emergencies. In addition, the Australian Privacy Commissioner regulates interagency data-matching.

Canada has adopted a governmentwide approach that requires "a broad consideration of all aspects of the issue to ensure proper protection of privacy and human rights." Specifically, it states:

- PII is collected only when it relates directly to an operating program or activity with legislative or regulatory authority;
- The use of PII in any government program or service must also consider legislative context, regulations, relevant policies and program requirements;
- Any secondary use of PII must be justified by explicit consent by the client, specific legal investigative purposes, or emergency preparedness or disaster situations.

Canada is considering a set of 11 Pan-Canadian identity principles that would apply to jurisdictions at national, provincial and local levels:

- Justify the use of ID;
- Identify with specific reason;
- Use appropriate methods;
- Enhance public trust;
- Use a risk-based approach;
- Be collectively responsible;
- Uphold the rights and values of Canadians;
- Ensure equity;
- Enable consistency, availability and interoperability;
- Maintain accuracy and integrity;
- Preserve proportionality.

Canada allows PII to be collected only when related directly to an operating program or activity with legislative or regulatory authority, It must also take into consideration legislative context, regulations, relevant policies and program requirements. Secondary use of PII must be further justified by explicit consent by the client, specific legal investigative purposes, or emergency preparedness or disaster situations.

The U.S. established an Identity Theft Task Force in May 2006, chaired by the Attorney General and the Federal Trade Commission Chair. Its purpose is to improve the ability to bring identity thieves to justice, to mitigate the risks of identity theft for individuals and companies and to assist identity-theft victims.

The task force issued a set of Interim Recommendations for protecting PII and asked for public comments before submitting to the President its final Identity Theft Plan for improving government handling of sensitive personal data. The final recommendations were issued in April 2007 and include:

- Reducing the unnecessary use of Social Security numbers by federal agencies;
- Establishing national standards that require private sector entities to safeguard the personal data they compile and maintain and to provide notice to consumers when a breach occurs that poses a significant risk of identity theft;
- Implementing a broad, sustained awareness campaign by federal agencies to educate consumers, the private sector and the public sector on methods to deter, detect and defend against identity theft; and
- Creating a National Identity Theft Law Enforcement Center to allow law enforcement agencies to coordinate their efforts and information more efficiently, and investigate and prosecute identity thieves more effectively.

New Zealand's All-of-government Authentication Programme includes the creation of policy, law, standards and shared services in relation to identity-proofing for people. Unlike the other countries, New Zealand policy is not driven by national security, illegal immigration or financial fraud concerns. Rather, it is based on a need for privacy, security, acceptability, user-centricity, proportionality, dis-aggregation of data. And there are specific legal constraints, e.g.:

- Data must be kept on the existing register so existing protections apply;
- Responses to a breach are modeled on existing processes;
- Data dissemination is controlled by the owner;
- No cross-agency data sharing;
- Audit records stay with the operating agency.

On other issues, there was general agreement that citizens in all five countries trust government more than the private sector to keep their personally identifiable information secure.

Participants in the videoconference included: Karen Evans, U.S. Administrator of E-Government and IT; Kenneth Cochrane and James Alexander, CIO and Deputy CIO, Canada; Ann Steward, CIO, Australia; Laurence Millar, CIO, New Zealand; and Andrew Stott, Deputy CIO, U.K. ■

Darlene Meskell is the Director, USA Services Intergovernmental Solutions, U.S. General Services Administration. For more information contact darlene.meskell@gsa.gov.

Personal Information Protection in Japan

By Yoko Miyazaki
Deputy Director
Administrative Management Bureau
Ministry of Internal Affairs and Communications,
Government of Japan

In 2003, the Japanese Government established legislation that set standards for the protection and use of personal information held by the public and private sectors. These standards became effective in April 2005.

Following enactment of the 1980 Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, Japan introduced legislation in the late 1980s on personal data protection targeting exclusively the central government. Enforcement in the private sector was through regulation by individual business acts and guidelines. Since then, remarkable changes have taken place in the business sector with the advent of E-Commerce, leading to the dramatic increase of cross-border flows of personal data. Similar changes are taking place in the public sector which launched E-Government projects to harness Information and Communication Technology (ICT) to serve citizens. In addition, introduction of the Resident Registry Network, enabling local governments to share and exchange residential information sparked a controversy over personal information protection enforcement in the Diet.

In light of the growing recognition of the necessity to enhance privacy protection, the government enacted personal protection legislation governing both the public and private sectors, as well as extensively revising the act regulating the central government.

System for Legislating Personal Information Protection

The system of legislation for personal information protection is made up of two parts: a basic law governing both the public and private sectors and a general law governing the public and private sectors in different acts. (Figure1)

Specifically, the Act on the Protection of Personal Information (referred to as the Personal Information Protection Act) sets forth the provisions that form the framework for both the public and private sectors (Chapters 1 to 3) and at the same time sets rules for the protection and use of personal information by businesses (Chapters 4 to 6).

The fundamental purpose of this act is to set a general rule for handling personal information between private parties, while leaving specific matters to businesses' voluntary actions. The matters unique to individual industries are included in guidelines set by relevant ministries (33 guidelines for 21 business sectors including finance, health and education have been published).

In the public sector, the two acts were established to govern the administrative organs and the incorporated administrative agencies[1] as a general law; the Act on the Protection of Personal

Continued on next page...

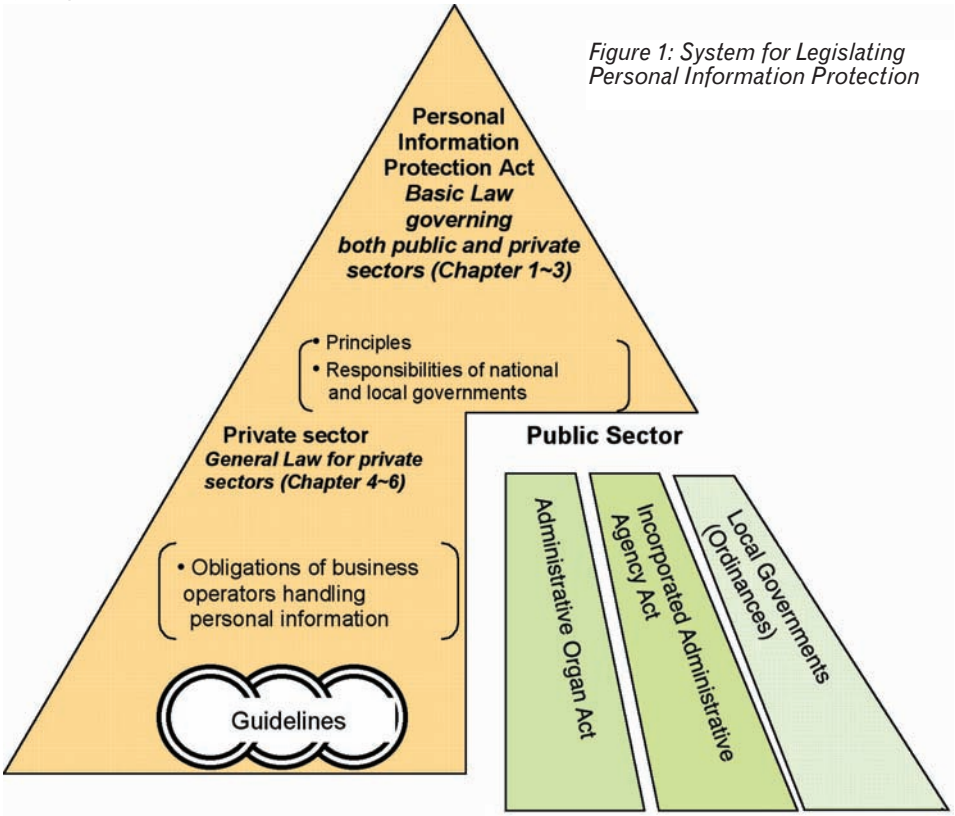


Figure 1: System for Legislating Personal Information Protection

Information Held by Administrative Organs (referred to as the Administrative Organ Act) and the Act on the Protection of Information Held by Incorporated Administrative Agencies (referred to as the Incorporated Administrative Agency Act).

While both acts have similar regulations following the OECD Privacy Guidelines, the obligations for the public entities are stricter than the ones imposed on the private sector. This reflects the view that the public sector should be regulated more stringently than the private sector as it exercises government authority in collecting personal information (Appendix).

As for regional level enforcement, all local governments have established their own ordinances for personal information protection, which is subject to the provisions of the basic law.[2]

Situation after Enactment of the Laws

One of the major challenges since the acts were put into force is information security breaches. The number of data breach cases businesses reported to the government in FY 2005 exceeded 1500, while the number of those reported by administrative organs was 320 and those by the incorporated administrative agencies was 855.

Another issue is "excessive reaction" to privacy protection. For example, cases have been reported where basic personal information has been withheld and local residents' association lists or class name lists at primary schools are incomplete because the individuals refuse to put their names forward.

In the wake of these circumstances, the government has striven to ensure that the purpose of the laws — protecting personal information while paying due consideration to the usefulness of such information — and their content are fully known by data owners as well as citizens.

In addition, as a result of the Diet discussion, the Cabinet Office is required to review the Personal Information Protection Act every three years and to take necessary action to keep it up to date.

Security Measures Set by the Government

The need to protect personal information maintained by the government was highlighted by the leakage of personal data through the file-sharing program, Winny.[3]

So-called "exposure viruses" targeted Winny and leaked information stored in computers onto the Internet. This resulted in a string of leaks of confidential information, including personal privacy data held by governments as well as businesses.

Along with the guidelines setting the common framework across ministries formulated by the National Information Security Center in the Cabinet Secretariat in December 2005, each ministry was called on to set the standards to properly safeguard its information assets. The measures against information leakage include a prohibition on the use of private personal computers at work, introduction of a monitoring system by asset management software, access log management servers and the use of encryption.

All ministries are strengthening security measures to protect their information assets including privacy data, which are checked and evaluated periodically by the Cabinet Secretariat.

Government Public Key Infrastructures

In addition to security measures, another essential effort toward fostering confidence in online transactions with the Government is E-Authentication. Government Public Key Infrastructure, in operation since April 2001, enables users to securely exchange information through the use of cryptographic key pairs that are obtained from Certification Authorities.

Continued on next page...

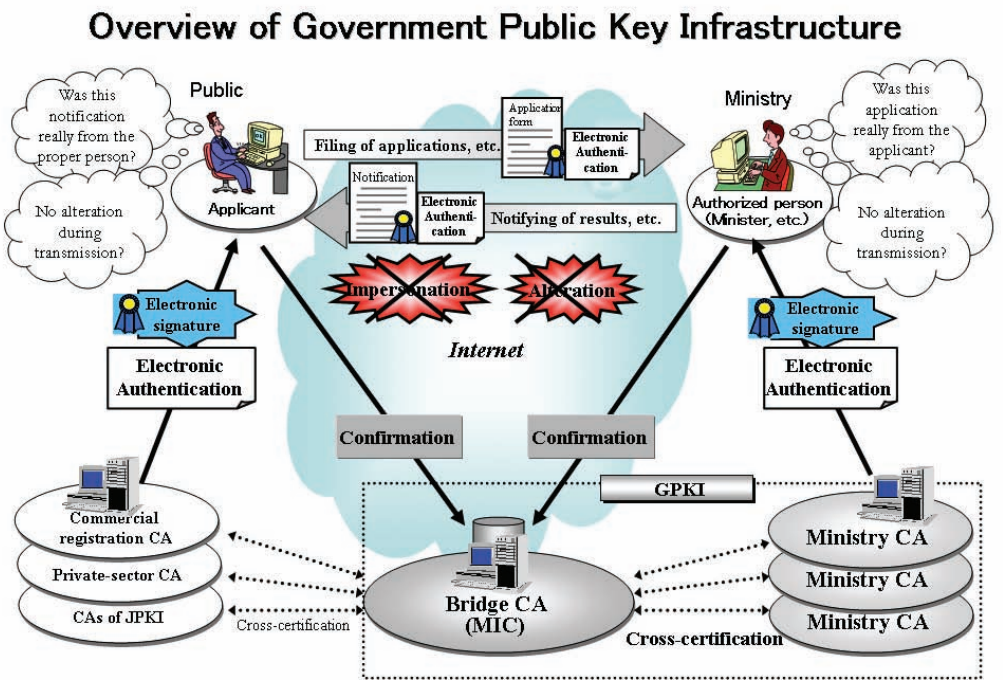


Figure 2

There are two types of Certification Authorities: Ministry CAs, issuing the electronic official seal, and the Bridge CA, mediating mutual certification between Ministry CAs and private CAs.[4] Applicants can apply to private (i) CAs, (ii) Commercial Registration CAs operated by the Ministry of Justice, and (iii) CAs operated by local governments as a part of the Basic Resident Registry Network. Under the Enterprise Architecture projects, 14 Ministry CAs will be merged into one CA by 2008. (Figure 2) ■

Yoko Miyakazi was a Deputy Director of the Administrative Management Bureau, Ministry of Internal Affairs and Communications for the Government of Japan. She is now in the Ministry of Foreign Affairs and can be reached at yoko.miyakazi@mofa.go.jp.

Appendix

OCED-Set 8 Principles and Corresponding Provisions of Japan's Personal Information Protection Legislation

OECD-Set 8 Principles	Obligations of Business Operators Handling Personal Information under Personal Information Protection Act	Obligations of Administrative Organs and Incorporated Administrative Agencies under Administrative Organ Act & Incorporated Administrative Agency Act
(1) Purpose Specification	Must specify purpose of use as much as possible.	Must not use information beyond the scope necessary for the conduct of affairs under jurisdiction, and must specify the purpose of use as far as possible.
(2) Use Limitation	Must not use information beyond the scope necessary for achieving the original purpose. Must not provide information to a third party without prior consent of the individual concerned.	Must not use information for purposes other than the one originally intended except by the authority of law and regulation.
(3) Collection Limitation	Must not collect information by deception or other wrongful means.	(As required under Article 73, paragraph 1 and Article 99 of the Constitution.)
(4) Data Quality	Must endeavor to keep information accurate and up to date.	Must endeavor to keep data true to past or present facts.
(5) Security Safeguards	Must take necessary measures for security control. Must exercise necessary supervision of business operators handling information.	Must take necessary measures for proper supervision.
(6) Openness	After obtaining information, must notify the individual concerned of the purpose of use or publicly announce the purpose. Must keep the purpose of use and other items accessible for the individual concerned.	Must compile a register of personal information files and make it public. The Minister of Internal Affairs and Communications should publicly release annual reports concerning the status of law enforcement.
(7) Individual Participation	Must disclose retained personal data when requested from the individual concerned. Must correct etc. when requested by the individual concerned. Must suspend use of information when requested by the individual concerned.	Any person may request disclosure of his or her own personal information retained by administrative organs. Any person may request correction of information. Any person may request suspension of use and provision of information.
(8) Accountability	Must endeavor to process complaints appropriately and promptly.	Specifies the obligations of the heads of administrative organs.

1. Incorporated administrative agencies are entities responsible for administrative affairs which are necessary for public interest but which the government does not need to undertake itself. As of April 2006, the act was applicable to 217 entities, including 87 incorporated national universities.
2. Local governments established so-called computer processing ordinances in the 1960s and 1970s. Full-fledged ordinances for the protection of personal information started to be established in 1984.
3. Winny, developed by a Japanese researcher, enables computer users worldwide to access each other's designated space of hard disks to search for music, movies, and files to download.
4. As of November 2005, 16 Ministry CAs and 18 private CAs were mediated by Bridge CA.

The π of PII

By Joanne McNabb, CIPP/G
Chief California Office of Privacy Protection
State of California

In the flood of data spills and breach notifications that have made headlines in recent years, one constant has been California's leadership role in privacy protection. It was a 2003 California law, since copied by at least 33 other states, which began requiring notification of individuals when their personal identifying information – or PII – is breached. That law has led to significant improvements in many organizations' practices for managing PII.

Not only are other states following California's lead, but the U.S. Congress also looks to California for privacy innovations, from breach notification and security freezes, to Social Security number restrictions, online privacy protection, and identity theft response.

One California privacy innovation that is just beginning to be imitated is the California Office of Privacy Protection (COPP), which was launched in 2001. COPP is not a regulator or enforcer of privacy laws. It is an education and advocacy office. COPP's small staff (8.5) assists thousands of people who call or e-mail each year. About 60 percent of the questions to COPP are about identity theft. Fortunately not all of these callers are victims, but some are people fearing that they may become victims, perhaps because they lost their wallets or received a breach notice.

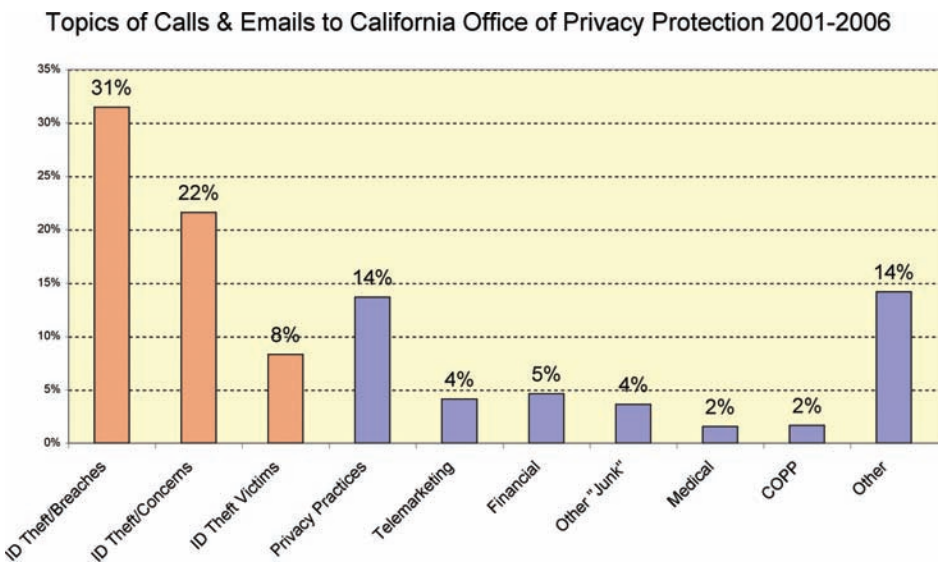
People also contact COPP to complain about the privacy practices of companies and agencies. We receive many outraged e-mails on the topic of online data brokers from people who are surprised to find their home addresses and telephone numbers, as well as other PII, posted on the Web sites of companies with which they have no relationship. And we are regularly asked if there isn't a law that bars a company from requiring a consumer's Social Security number as a condition of a sale. (There isn't.)

In order to educate consumers, businesses, and other organizations on privacy issues, COPP produces information sheets and conducts around 100 seminars, workshops and other presentations annually. We also work with law enforcement and just completed an "ID Theft Reference Manual for California Law Enforcement," issued on CD-ROM, which draws on the expertise of investigators and prosecutors on the state's regional High Tech Crime/Identity Theft Task Forces. We periodically issue best practice recommendations on topics including breach response, Social Security number confidentiality, and privacy policy statements. These materials are available on our Web site at www.privacy.ca.gov.

So Goes the Nation

California's history of enacting the strongest privacy protection laws in the nation has contributed to COPP's status in state privacy protection. Since 1999, more than 80 laws have been enacted to provide Californians with privacy protection and legal rights and resources to combat identity theft. Several of our identity theft and data protection laws were incorporated into the 2003 Fair and Accurate Credit Transaction Act (FACTA) amendments to the federal Fair Credit Reporting Act. Identity theft victim rights—such as access to records on fraudulent accounts and blocking of fraud-related items on credit reports, and data protection provisions, such as truncation of credit card numbers on receipts and

Continued on next page...



Practices refers to business practices, privacy laws. Other "Junk" is faxes, mail, spam. Other refers to general privacy concerns or non-privacy issues.

secure document destruction—were extended to all American consumers by these amendments.

The state's security freeze law of 2001 provides Californians with the strongest consumer protection against new account identity theft. Placing a security freeze on your credit files essentially prevents the opening of new credit accounts, while permitting you to temporarily lift the freeze when needed. As of the end of 2006, 24 other states have adopted this measure and some federal bills also contain it, along with a federal breach notification requirement.

Protecting Privacy in Government

California has adopted strong privacy protection policies for state agencies, as well. With an active breach response procedure for state agencies in place for several years, the state has been able to learn from experience and adjust policies to meet identified needs. One such adjustment was the adoption in 2005 of an encryption policy for portable computing devices (laptops, notebook computers, PDAs) and data storage media (compact disks and thumb drives).[1] While the policy does not set an encryption standard, most agencies use encryption software that complies with the standard set by the National Institute of Standards and Technology (AES/FIPS 197).

Another lesson learned from breaches is the role played by paper records containing PII. The paperless office has yet to materialize and agencies, like banks and other organizations, have experienced losses and thefts of paper records, as well as digital data. While the California law only requires notification in the case of breaches of "unencrypted *computerized* data" of specified types (name plus either Social Security number, driver's license number, or financial account number), the risk to individuals remains the same whether their data is on a computer, a CD, or piece of paper. Last year California issued a management memo that clarifies agency responsibilities for protecting personal information under the state's privacy laws and sets a policy requiring notification of breaches involving specified types of PII—*regardless of their medium*.[2] It also requires state agencies to provide annual privacy training to all employees and to contractors who handle personal or confidential information.

What's Next?

In recognition of the critical importance of protecting privacy through responsible management of PII, the Schwarzenegger Administration has proposed an innovative merger of two state programs, the Office of Privacy Protection and the State Information Security Office. The merger will strengthen the efforts of both offices, and will bring a consumer privacy perspective to state information security management.

If approved by the California Legislature this year, COPP will move from its location in the Department of Consumer Affairs to the cabinet-level State and Consumer Services Agency, where it will be joined by the State Information Security Office, currently located in the Department of Finance.

A new state office will emerge—the California Office of Information Security and Protection, providing services to consumers and policy direction to state government. Each component office will continue to play its current role, with COPP providing consumer education and advocacy on privacy issues. A slightly expanded State Information Security Office will provide more tools in identifying and managing risk and planning for business recovery. The Office also will take on monitoring of compliance with state information security directives.

This union of consumer privacy protection with government information management is the latest California innovation in privacy and could set the stage for new trends. ■

Joanne McNabb is Chief of the California Office of Privacy Protection, and co-chair of the International Association of Privacy Professionals' Government Working Group and a member of the Privacy Advisory Committee to the U.S. Department of Homeland Security. For additional information contact Melanie_Bedwell@dca.ca.gov.

1. BL 06-32, available at http://www.dof.ca.gov/FISA/BudgetLetters/BudgetLetters.asp.
2. MM 06-12, available at http://www.osp.dgs.ca.gov/On-Line+Publications/SAM+Management+Memos.htm.

Privacy and Security in the U.S. Budget for FY 2008

The following is an excerpt from Analytical Perspectives, Budget of the United States Government, Fiscal Year 2008*, one of the explanatory documents issued along with President Bush's 2008 budget request. This excerpt is from the section on information technology, entitled "Integrating Services with Information Technology."*

Securing Government Systems.—The federal government continues to improve information security performance, however, declines in a few agencies have resulted in a net decrease in overall performance in some areas. Additionally, aspects of IT security, such as securing data on removable media, remain under-addressed government-wide. Departments and agencies progress against their corrective actions plans will be measured in the President's Management Agenda Expanded Electronic Government Scorecard. On balance, the majority of agencies continue to improve or sustain high performance.

Government-wide incremental progress in resolving fundamental IT security weaknesses has been made in many aspects of information security, however, departments and agencies must continually assess the risks associated with technological developments and service offerings. Thus, each year brings new challenges and approaches and potentially new measures for performance. Additional information and detail concerning the federal government's IT security program and agency IT security performance can be found in OMB's Annual Report to Congress on IT Security.

Protecting Privacy. — In 2006, several agencies experienced high profile data security breaches involving personal information. Most notable of these was the Department of Veterans Affairs, but significant problems also exist at other departments and agencies. Virtually all of these incidents resulted from "internal" problems within agencies and not external attacks on agency systems.

To help address this issue, in May 2006, the President signed an Executive Order creating the Federal Identity Theft Task Force. Several of the Task Force's interim recommendations address the need to improve data security in the government, improve the agencies' ability to respond to data breaches, and reduce the risk to personally identifiable information.

In this context, OMB has issued four security and privacy policy and advisory memoranda. These memoranda re-emphasize agency responsibilities under law and policy regarding protection and safeguarding of sensitive personally identifiable information, including information accessed through removable media, and incident reporting. They are included in Table 9-2, "Management Guidance," and are available at: www.whitehouse.gov/OMB/memoranda.

To help safeguard personally identifiable information, agencies are required to report on several performance metrics related to information privacy. Additionally, this year agencies were also required to provide quantitative performance measures to assess the privacy of agencies' personally identifiable information. The FY 2006 agency FISMA reports reveal modest success in meeting several key privacy performance measures:

- Program Oversight. In 2006, the majority of agencies report having appropriate oversight over their privacy programs in place. All agencies report having a privacy official who participates in privacy compliance activities, however, 84 percent report coordinated oversight coordination with the Office of the Inspector General (OIG). Most agencies report privacy training for Federal employees and contractors, with 92 percent reporting general privacy training and 84 percent reporting job-specific privacy training.
- Privacy Impact Assessments. In 2006, 82 percent of applicable systems government-wide have publicly posted privacy impact assessments versus the goal of 90 percent.
- System of Records Notices (SORNs). In 2006, 82 percent of systems government-wide with personally identifiable information contained in a system of records covered by the Privacy Act have developed, published, and maintained current systems of records notices versus the goal of 90 percent. ■

Analytical Perspectives, Budget of the United States Government, Fiscal Year 2008 contains analyses that are designed to highlight specific subject areas or provide other significant presentations of budget data that place the budget in perspective. It can be found online at http://public.cq.com/public-content/overview_analytical.pdf.

Moving Beyond FISMA Compliance

By, Fred Thompson
Vice President, Leadership and Performance
The Council for Excellence in Government

More than 100 Federal leaders gathered in fall 2006 for two half-day sessions on *Beyond FISMA Compliance: Measuring Security and Mitigating Risk*. Hosted by the Council for Excellence in Government, these sessions brought together chief information officers, inspectors general and security research experts from both the public and private sectors for thought-provoking panel discussions about current and future challenges to information security and best practice approaches for mitigating risk.

FISMA refers to the Federal Information Security Management Act of 2002, which was enacted as Title III of the E-Government Act of 2002. The Act was meant to bolster computer and network security within the Federal government and affiliated parties (such as government contractors) by mandating a set of processes that must be followed for all information systems used or operated by or on behalf of a United States government agency. The Act clearly identifies system owners (not the IT staff) as having authority and responsibility to certify and accredit systems for operation in their agencies.

The discussions focused on whether agencies are simply complying with guidance in a rote fashion or whether the things that they are doing as a result of FISMA are really improving security and mitigating risk to systems and information. "Our goal is to help these leaders look at security from a broad perspective," says Pat McGinnis, CEO of the Council for Excellence in Government. "Protecting public information and the systems that provide access to it is a management job, and all agencies need to fulfill this responsibility while they are delivering results."

Three topics were identified as having particular impact on the security of Federal systems and deserving future investigation. They were:

- National Institute of Standards and Technology (NIST) priorities – e.g., should NIST move from issuing regulations to focus on certifying contractors to perform FISMA certification and accreditation work, evaluating tools, and creating a clearinghouse of best practices for security protection
- Revisions to the Federal Acquisition Regulation (FAR), and standard clauses to be used in contracts to ensure that contractors build adequate privacy/security elements into any system that they develop or provide to Federal customers
- Implications of outsourcing/centers of excellence on security/privacy

The NIST Role

Most of the participants felt that NIST should not change its focus from clarifying and expanding FISMA guidance. They felt that this policy and guideline work was more valuable to them than a change in focus toward certifying contractors or evaluating tools that could be used in securing systems. One participant used the example that "a car is not driven 100 miles an hour simply because it can go that fast." We should use all of the features that can be used safely and securely in performing the mission, but we shouldn't use new and untested features merely because they are available for use. Security needs to be considered a threshold safety issue: we don't do more with a system than we can do safely and securely.

Nearly half (48 percent) of the meeting registrants believe that clarification of existing FISMA guidance is the highest priority for NIST in terms of security/privacy. Many commented that future guidance could benefit greatly from broad interdisciplinary and interagency feedback and that NIST can ensure that future changes add the greatest value in terms of security by soliciting suggestions from a diverse group.

While many praised NIST's efforts, they also warned against an unquestioning compliance to guidance. There is no such thing as a universal checklist for security. For example, NIST guidance calls for lockout when a password fails three times—which is not always operationally possible. Imagine the disaster if the Federal Aviation Administration locked out air traffic controllers while planes were in flight! FAA designed and implemented compensating controls to secure its air traffic control systems. Subsequent panel discussion emphasized that it is incumbent on program and IT officials to use good judgment and deviate from the checklists when their actions improve agency results. Inspectors General at the meetings agreed that compensating controls were an appropriate response in a situation like the one that FAA faced, but they noted that these need to be documented and subject to audit testing if the agency made a conscious decision to deviate from the NIST guidance.

Contractor Responsibilities

Contractors play an important role in systems security. They may provide the hardware and software for running systems, they may engineer solutions, and they may even operate those systems. A key issue that rose was how to ensure contractor accountability for security for the entire lifecycle of the system. An informal on-line survey of registrants found that a majority (66 percent) did not believe

Continued on next page...

that Federal Acquisition Regulation (FAR) adequately covered security requirements. The discussion revealed that FAR on its own is not enough – security cannot be isolated in the acquisition shop. IT and program managers need to be involved in developing security requirements and outlining them clearly in requests for proposals. These need to be closely examined and evaluated by all sides — IT, program management, acquisition — in the proposal review process. Evaluating and scoring these plans sends the message that security is a core requirement. Agencies need to clearly communicate to contractors that security plans' approaches and certifications can make the difference between winning and losing a contract.

Outsourcing or Use of Centers of Excellence

Agency leaders remain accountable for system security when these systems are operated by others either through outsourcing or center-of-excellence shared service arrangements. They should ask for, review and approve security plan and C&A work done by these organizations and examine how this work integrates with their own efforts. To foster an agency-wide focus on delivering a secure system to the public, ownership and accountability for secure systems should be at the management and executive level at every agency and should not be delegated to the IT organization.

Speakers at the *"Beyond FISMA"* sessions included Alan Paller, Director of Research, SANS Institute; Ron Ross, Senior Computer Scientist and Information Security Researcher, NIST; and CIOs Lisa Schlosser of the Department of Housing and Urban Development and George Strawn of the National Science Foundation. ■

Fred Thompson is the Vice President, Leadership and Performance, at the Council for Excellence in Government. He can be reached at fthompson@excelgov.org.

Protection of PII: The Role of Business Unit Management

By, Patrick D. Howard, CISSP, CISM
Chief Information Security Officer
Department of Housing and Urban Development

The protection of personally identifiable information (PII) by Federal agencies has come under close scrutiny by the press and the American public over the past six months, and agencies of the Federal government are having to defend the practices that they employ to protect the private data relating to its customers, business partners, and employees. There have been several incidents in which personal information held by Federal agencies that pertains to millions of individuals has been lost or compromised. These incidents have pointed out significant gaps in security controls necessary to protect sensitive personal information, and the Office of Management and Budget (OMB) has directed agencies to take action to identify and eliminate weaknesses in necessary security controls to improve privacy protection. In particular, agencies have been directed to ensure that controls have been implemented to update policies on the protection of PII; to train users on securing PII; to encrypt, log, or control access to sensitive data; and, to report incidents involving PII within one hour.

In recent months, agencies have focused much attention on the implementation of physical and logical controls by agencies in response to government directives to mitigate risks to sensitive information. While this is prudent and necessary, in concert with the implementation effort, Chief Information Officers and Chief Information Security Officers need to consider the role of business management in the protection of PII.

To be effective, controls implemented to protect personal data need to first be based on an approved policy that has actual business needs at its foundation. This requires informed participation of business unit management in the development of the security policy. Second, the implementation and maintenance of security controls requires the active involvement of management to provide ongoing 360-degree protection. This is based on the Federal Information Security Management Act (FISMA) requirement for system owners to play the lead role in identifying, implementing, and maintaining information security controls.

In order for system owners, program officials, and other managers to play their proper roles in protecting personal information, they must be aware of their responsibility in that regard. CIOs can help these program officials by clarifying their responsibility for protecting PII and helping them understand that they are responsible for the security of personal information that they use. CIOs can also provide assistance to system owners in defining the business impact of a loss or compromise and helping business unit managers determine how the loss or compromise of customer, business partner or employee personal data will impact their operations.

To ensure that requirements are clearly and consistently provided, the CIO should ensure that policy requirements are clear, and then they should provide face-to-face briefings to individual business unit executives

Continued on next page...

and potentially managers, as well, on needs for protection of sensitive information. This briefing should include details on the following issues:

- Risks associated with loss or compromise of private data.
- The agency's policy on protecting personal data.
- Definition of personally identifiable information.
- Processes for identification of PII, including the assessment of all business processes, systems, and forms to determine how personal information is being used.
- Identification and implementation of controls for protecting PII.
- Breach notification requirements.

With the assistance of CIOs, program office officials can determine how PII is being used in their business processes and can decide if its use is actually warranted. Many times Social Security Numbers and other forms of PII are used to uniquely identify an individual when an alternative means of unique identification (i.e., a cross-reference number) could easily be used.

Business unit executives and managers can also play a large role by focusing attention on the need to protect personal data. With specific knowledge of their own business processes and personnel, they can highlight what information needs special protection, why such emphasis is necessary, and how increased security will be implemented. Formal communications from program executives to their employees, contractors, and business partners based on realistic business needs can be highly effective in assuring their willing involvement in protecting sensitive information.

Program officials can also assist the CIO in exercising his/her security responsibilities by ensuring that suspected security breaches are given priority for resolution within their areas of responsibility. In order to comply with the one hour notification requirement in the event of lost or compromised PII, users must be actively aware of and engaged in the notification process. They must first be able to identify an actual or suspected breach, and then they must also be aware of the reporting procedures. The CIO can establish reporting requirements and can provide awareness training on this topic, but business unit management can promote the effectiveness of the process by placing increased emphasis with their users on the importance of timely and accurate reporting.

The protection of sensitive information requires teamwork. While the CIO plays the lead role in the protection of personally identifiable information across the agency, business unit management has to provide undivided support to the CIO in this effort in order to protect sensitive agency data, to avoid the embarrassment that PII breaches have brought in the past, and to achieve OMB's stringent protection and notification requirements. Agency officials need to make a concerted effort to work together to find solutions, to update and implement policies for protecting PII, and to ensure employees, contractors, and business partners are fully engaged in the effort to protect PII as well as other sensitive data that the agency uses. ■

Patrick Howard is the Chief Information Security Officer at the Department of Housing and Urban Development. For additional information, contact Patrick at Patrick_D._Howard@hud.gov.

Ensuring Private Information Stays Private

By Margaret Leary
Senior Policy Analyst
Nortel Government Solutions

The loss of personally identifiable information (PII) by government agencies has escalated to new heights, attracting the attention of the U.S. Government Accountability Office (GAO) and Congressional leaders. A report prepared for the Government Reform Committee, "Agency Data Breaches Since January 1, 2003", detailed reports of the loss of PII among 19 Departments and agencies, concluding that the losses were government-wide with most agencies not tracking such incidents that occur. The majority of data losses cited in the report largely stemmed from misplaced physical devices containing the data, such as hard drives and laptops, and did not fully address the magnitude of loss that can result from the flow of data across networks. PII contained in electronic forms such as e-mail, Web sites, and digital voice are also vulnerable and must be protected by a unified security architecture.

E-mail Breaches

Only one report of an e-mail breach appears in the Committee's report. This breach occurred at the Department of Agriculture, in which personal information for 1,537 individuals was inadvertently sent within an e-mail to all of these individuals. Such cases are common in the corporate world and should be reflected to a greater extent than they are in the agency breach reports. One possible reason for the scarceness of examples is that e-mail breaches are not addressed in the organization's risk assessments.

An e-mail breach can result from "human error" (as with the Dept. of Agriculture's incident) or through the intentional transmission of personal data – generally for identity theft purposes. At minimum, all e-mail containing PII must be encrypted, whether transmitted over the local network or beyond the network's security boundary. E-mail security solutions exist that can provide automatic e-mail encryption, as well as content filtering, to ensure that PII is only distributed in compliance with privacy polices. As with SSL-secured Web sites, Web-based secure e-mail services should be provided to citizens for the transmission of sensitive information– even for those cases where this information is unsolicited and mistakenly sent by the citizen in an e-mail inquiry from the agency's site.

Web Content Breaches

The report highlighted several instances of PII loss as a result of personnel inadvertently posting sensitive information to agency Web servers. All content placed on Web sites should be closely moderated, with access provided only after a review of the data by a security specialist or privacy officer to ensure compliance with privacy regulations. Many technical solutions exist presently that allow the Web server to review content on the server, replacing any unauthorized content as soon as it is detected. Proxy servers that monitor access to the Internet from agency personnel may store PII as computer names or user names. URLs are also stored in Web server referral links that may contain sensitive personal data. Access controls to the Web server should be carefully managed to ensure that only trusted agents can access these logs, and the use of data from these logs should be clearly defined in the agency's Privacy Policies and integrated into machine readable privacy policies such that the user can opt out of accessing the site if the agency's policies are not consistent with the user's policies.

Future VoIP Privacy Considerations

Converging voice and data in a network gives an enterprise many advantages, allowing networks to streamline an organization's communications architecture, drive down operational costs, and extend services to remote locations over more cost-effective IP links. While the report did not address any VoIP breaches of PII, these advantages can come at a cost to confidentiality if a robust, secure infrastructure is not provided. Consider the case in which a patient's medical information must be discussed over the phone with other medical personnel. It is expected that these will be the next areas of attack for unauthorized access to an agency's privacy data. In weakly secured networks, attackers will be able to attack voice messages using the same mechanisms that successfully attack data networks. At the same time, strong security controls can negatively impact latency – something which voice messaging is more sensitive to than data transmissions.

As the need to secure agency PII information in transit grows, an end-to-end network security solution that enforces agency policies is required. At minimum, IP phones and endpoint devices (including PDAs) used to transmit PII must be authenticated prior to being used. Once authenticated, endpoints can be automatically assigned to a virtual local area network (VLAN) that can control device security policy. Encryption must be enabled on IP phones over which PII content will be transmitted. Media traffic can be encrypted using different protocols depending on the type of traffic, to include Secure RTP (SRTP), TLS (SSL) or IPSec.

Continued on next page...

A Unified Security Architecture to Protect Healthcare PII

As a regional healthcare provider, Care New England (CNE) leverages a diverse information infrastructure to better serve its patients. CNE has adopted a holistic approach to securing this infrastructure that relies in part on the Unified Security Architecture Framework from Nortel. The framework provides the systems and software to appropriately secure CNE networks using a layered approach. For example, CNE uses Nortel's Web-based virtual private network (VPN) systems to authenticate healthcare providers and make the secure transmission of PII simpler without in-depth information security training. The architecture framework, illustrated in the accompanying figure, addresses all aspects of protecting healthcare information on the network and reduces risk of unauthorized disclosure from the network's many access points.

Conclusion

The Government Reform Committee's report highlighted reported agency breaches of PII, generally through the loss of physical devices, concluding that agency data is still at risk. The minimal reporting of e-mail, Web and other infrastructure attacks (i.e. with VoIP) in the report demonstrates a need on the part of government agencies for additional training and monitoring to ensure that all avenues of PII leakage are secured and monitored. Solutions that encrypt and monitor all local and outbound network traffic are critical to keeping PII private during transmission. ■

Margaret Leary is a senior program analyst for Nortel Government Solutions. For additional information contact Margaret.Leary@nortelgov.com.

Leveraging a Federated Approach for Trusted Identity Management and Cross-Credentialing — A Federal Case Study

By Michael Mestrovich, Ph.D.
President and CEO of Unlimited New Dimensions, LLC
President of The Federation for Identity and Cross-Credentialing Systems (FiXs)

From data breaches to terrorist attacks, no one is more concerned about security and identity management than the U.S. government community. Following the recent Homeland Security Presidential Directive (HSPD-12) implementation in October 2006, agencies and contractors alike continue to work diligently to produce compliant identification cards for members of their organizations. While the concept behind HSPD-12 is sound, without an interoperable network and an improved biometric infrastructure at secure entry points, card verification and authentication systems cannot serve to significantly improve an organization's security posture.

Contractors are challenged to implement scalable systems that meet Federally mandated requirements, support physical and logical access applications, and integrate with their existing organizational personnel systems. What solutions exist for contractors of all sizes seeking an "HSPD-12 aligned" credentialing system? What ways are government agencies currently working with contractors to provide trusted, interoperable credentials for employees accessing U.S. government facilities and networks worldwide? The following case study takes a look at one agency that has evaluated, tested, and implemented a federated approach and—based on its success—is now leading the way for other agencies to follow suit.

Introduction

The following case study outlines the U.S. Department of Defense's approach to identity cross-credentialing, currently in implementation by the Defense Manpower Data Center

Continued on next page...

(DMDC) through a pilot program called the Defense Cross-Credentialing Identification System (DCCIS). The DMDC now has a set of products and services that are ready for deployment at military installations worldwide, with the objective of hosting a federated identity management infrastructure to support identity credentials for DoD and its contractors.

Deployment of a Federated Solution

While there are varying approaches to trusted cross-credentialing for agencies and their contractors, DMDC opted for a "federated" approach, where required data remains resident in individual employer records and only minimal information is shared for credential verification with federation member organizations.

The processes and technologies used in the Defense Cross-Credentialing Identification System (DCCIS) pilot project have been combined within the infrastructure products and services noted below. Implementation will begin in 2007 at selected U.S. overseas locations.

The Common Access Card (CAC) program provides the means for the Defense Department to authenticate its employees. Each employee is issued a CAC, which carries information on a barcode and integrated circuit chip. The card can be used for physical access to DoD facilities (via the Defense National Visitors Center [DNVC] System), as well as for logical access onto DoD networks. The card is Public Key Infrastructure-enabled for identity verification, privilege assignments, and systems management. The CAC also is issued to selected DoD contractors who work regularly on DoD facilities and who have a need for frequent access to DOD installations and networks.

The Defense Biometric Identity System (DBIDS) is a fully configurable security and privilege management system built to enhance DOD force protection and identity management. The system incorporates accurate identity verification and registration data required for frequent physical access, registration of personal property, and workstations that can access a centralized biometric and personnel identity database via DNVC and DCCIS. DBIDS improves the security posture of installations and streamlines personnel identity verification by eliminating much of the human decision-making required by earlier card validation systems.

The Defense National Visitors Center (DNVC) is a Web-based system that allows DoD organizations to authenticate credentials and credential holders using photograph and text data, accompanied by strong fingerprint data stored in enterprise databases. DNVC applies industry-standard encryption techniques and is designed to accommodate differences in DoD facility access system configurations. The DNVC system saves participating organizations the cost of maintaining independent identity management systems, and it complies with HSPD-12 and Federal Privacy Act standards for the secure transfer of information across open networks.

The Defense Cross-Credentialing Identification System (DCCIS) is a set of operating rules, interface specifications, and a supporting infrastructure that allows trusted credentials from DoD's industry and government partners to be authenticated at DoD sites and, correspondingly, for DoD employee credentials to be authenticated at participating industry sites. There is no issuance of a specified "DCCIS credential." The CAC is the recognized DoD credential for the DCCIS infrastructure, and an employee's company credential, which has been issued in accordance with DCCIS-like operating rules, is the recognized industry credential for the DCCIS infrastructure.

The Federation for Identity and Cross-Credentialing Systems (FiXs) is a not-for-profit coalition of commercial and other organizations whose objective is to support efforts to create and deploy an interoperable identity cross-credentialing network. FiXs has developed its own set of trust models, policies, and operating rules, which permit it to interoperate with the DCCIS construct. FiXs, working with DoD and other Federal government organizations, is in compliance with HSPD-12 and provides the interoperable network required by the Directive.

FiXs and its affiliation with the DCCIS program enables participating DoD and industry organizations to achieve strong and interoperable identity verification and authentication of participating contractor and other private sector personnel who present a company-issued trusted credential, in accordance with a set of common operating rules. Similarly, participating industry locations will recognize DoD-issued CAC and DBIDS credentials, which require no modification to operate with FiXs and DCCIS. These interoperable infrastructures permit DoD and its contractors to use a common trust model and strive to maintain pre-existing organizational physical security systems and human resources policies, significantly reducing contractor cost to issue trusted, HSPD-12 aligned credentials.

The keys to creating a successful interoperable environment for DCCIS and FiXs are 1) a strong, common, and interoperable identity management and protection policy and 2) a federated infrastructure. FiXs and DCCIS borrow many core concepts from proven best practices initially designed for the electronic payments industry. This federated approach currently meets the demands of a critical national security requirement for improved identity authentication and will support multiple credential types for DoD, other agencies, and industry participants in the future. DMDC and FiXs were recently recognized by the Federal IT community for excellence in collaboration through a public/private partnership. ■

Michael Mestrovich, Ph.D. is President and CEO of Unlimited New Dimensions, LLC, and President of the Federation for Identity and Cross-Credentialing Systems (FiXs). For more information contact mjm@undllc.com or visit www.fixs.org.

Evolution of Privacy Awareness training at the Department of Veterans Affairs

By Yvette Kelly
IT Specialist
VA Privacy Service
Department of Veterans Affairs

In light of rapidly changing threats to the Department of Veteran Affairs (VA) infrastructure and compliance requirements in privacy protection regulations, the VA set the goal of becoming a model Federal agency in the development and implementation of policies and procedures to protect the privacy of personally identifiable information (PII). The VA has found that the most effective means to achieve this goal is through a workforce well-trained in the areas of privacy, security and ethics.

In July 2002, the VA Privacy Program was established to preserve and protect the privacy of data maintained by VA in the course of performing official duties. The program also provides oversight and guidance on VA's implementation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Although the Veterans Health Administration (VHA) is the only covered entity within VA's three administrations under HIPAA guidelines, VA has determined that in order to achieve consistent privacy practices throughout the Department it was necessary to implement the HIPAA mandate for annual privacy training and continuous privacy awareness VA-wide.

The VA Privacy Program directs the full range of Department-wide privacy programs. It is comprised of four functional areas: Assurance, Policy, Outreach, and Training, Education & Awareness (TE&A). TE&A is the cornerstone of VA's Privacy Program. Its responsibilities include converting the various privacy-related policies into privacy awareness training materials for VA organizations and staff offices, targeting these staff with the appropriate level of training, developing and disseminating privacy awareness training materials nationwide, tracking training completion, and reporting end of year training statistics to the office of the Chief Information Officer (CIO).

Initially, the primary focus of TE&A was to establish an annual privacy awareness-training program and show progress toward the goal of having all VA employees, contractors, and volunteers trained by the HIPAA enforcement deadline of April 2003. To achieve this goal, in the fall of 2002, the Privacy Program developed a 30-45 minute Web-based, general privacy training module. This training gave a basic overview of both Federal and VA privacy policies and regulations, the consequences of breaching these polices, and provided information on how to dispose of, retain and secure PII in various mediums. The first iteration of this training module was deployed February 2003. Approximately 30,000 individuals completed this training by the end of FY04.

After the first iteration of the general privacy training, the VA Privacy Program held several employee focus groups at various VA facilities nationwide to gain feedback on the general privacy-training module. Most employees felt that the training increased their knowledge of privacy; however, there was a need to create future privacy training that was tailored to specific functions. In response to that need, the VA Privacy Program created three new Web-based specialized privacy training programs in 2004 for VA Privacy Officers, Senior Executives, and Program/Project Managers. These training programs emphasized specific aspects of privacy laws that must be followed by employees within these respective functions (e.g. the requirement for Program Managers to identify systems that need a privacy impact assessment (PIA) and/or a system of record notice (SORN)). Furthermore, these specialized training programs highlighted the greater level of privacy awareness and responsibility required to effectively and appropriately lead projects and teams.

In addition to the original Web based privacy awareness training suite, the training program has evolved to include privacy awareness training videos for employees who do not have access to computers (e.g. maintenance workers); informational brochures for employees and veterans; and additional training programs for VA privacy officers (e.g. Privacy Violation Tracking System (PVTS) Web-based training and regular meetings to review the latest privacy issues within VA). TE&A has also updated the entire training suite to reflect new privacy concerns in the Federal government and to present employees with a different look and feel.

The Privacy training program is recognized by many government agencies as an excellent resource. It has provided privacy training guidance and training materials to The United States Postal Service,

Continued on next page...

Department of Homeland Security, and Department of Justice to assist in the development of their privacy awareness training programs.

The VA Privacy program offers the following advice to other agencies that are considering, developing or updating their privacy training program:

- Ensure that within the training application you provide a link to all applicable laws and agency policies pertaining to privacy and security.
- Consider both general and specific privacy training for employees based on position, level of responsibility and access to sensitive information.
- Coordinate with senior management (e.g. Secretary, Asst. Secretaries, Chief Information Officer, etc) to ensure importance of privacy training is emphasized throughout the agency and completed in a timely manner.
- Provide specific requirements for how to protect sensitive information and offer suggestions to senior managers and other project leads on how to implement policies to safeguard data.
- Test the comprehension of course content by periodically placing graded quizzes throughout the training.
- Require all employees, contractors, students and volunteers to take privacy training.
- Update the 'look and feel' of the privacy training at least every two years and offer different modes of training such as Web-based, video, presentation, etc. ■

Yvette Kelly has worked at the Department of Veterans Affairs for 26 year and worked in the VA Privacy Service since its inception in July 2002. For additional information contact yvette.kelly@va.gov.

Being Proactive About PII: Identity-Theft Risk Assessment at the IRS

By Stephanie Phillippy, Andrew Hartridge, Hassan Afzal, Joni Swedlund
Deloitte Consulting LLP

Public sector organizations today face many difficult challenges managing and protecting personally identifiable information (PII). The explosion of the information age offers new ways to conduct business, drives E-Government initiatives, eases data exchanges, and enables outsourced operations. Recent media reports on data breaches and identity theft incidents have caused the public to more closely scrutinize information protection practices. Citizens demand faster, more convenient access to data, but expect their personal information and privacy to be protected. In response, lawmakers have introduced new requirements regarding the management of PII. The OMB has issued a series of memoranda, specifying a number of required actions to improve data protection, mandatory use of encryption, and timely incident reporting procedures. These new requirements, along with the creation of the President's Task Force on Identity Theft, and increased public scrutiny, has led agencies to focus more attention on how to adequately safeguard PII.

In order to efficiently manage this challenging technical and regulatory environment, a proactive approach is necessary. However, many organizations operate in reactive mode by attempting to retrofit privacy and security safeguards after an incident has occurred or in response to a new regulatory requirement. Operating in reactive mode puts a tremendous strain on resources and further erodes the ability of the organization to invest in strategic approaches to the problem. Without a proactive program in place, the government will find itself constantly trying to address the latest regulatory guidance or reacting to a specific incident (inside or outside an agency).

The Internal Revenue Service's proactive roadmap to reduce identity theft risk began in the fall of 2004. At that time, IRS leadership expressed concern about the impact identity theft may have on the IRS mission and their challenge in determining the size of the issue. The agency was concerned not only with data breaches, but also how identities stolen outside of the IRS's span of control could be used to disrupt its operations and impact taxpayers. Any burden on taxpayers was of particular concern, as it could potentially drive interactions with the agency away from the more efficient, strategically important, electronic channels to less efficient paper or in-person channels. From the outset, the IRS understood that the traditional system-oriented approach to looking at risk and safeguards was of only limited value in reducing the risks to PII. The IRS knew that technical security safeguards and FISMA compliance were not a 'silver bullet' approach to addressing this risk as the classification of systems was not always aligned with the amount and type of PII processed. It was, at best, a tangential approach and left a lot of risk unaddressed.

The IRS decided to take a process-oriented approach to document and review the vulnerabilities from end-to-end. A service-wide risk assessment was performed to properly document and prioritize risk reduction strategies. In a departure from using resources that focused only on information

Continued on next page...

technology, Deloitte Consulting LLP was asked to assist. As part of the identity theft risk assessment, a large sample of business processes were reviewed that process or store PII. The scope of these processes covered both internal processes that process employee PII and externally facing processes that process taxpayers' PII. The initial scope of all processes for this organization was prohibitively resource intensive, so a rapid prioritization methodology was needed. The business processes were evaluated and given a ranking based on specific criteria that, at a high-level, revealed the potential risk of identity theft. Criteria included the amount of PII involved, whether data was exchanged with third parties, and whether the process was manual or automatically executed. This enabled the IRS to rapidly identify those business processes that were at higher risk to be impacted by identity theft and required further review.

At this stage it was critical that support was received from the highest levels of leadership within IRS to ensure resource availability for the data gathering exercise. Once this support was received, detailed data gathering workshops were conducted for each of the processes. These workshops consisted of a series of half-day meetings to map out how the process functioned, how the PII was processed and how it was protected. Using information collected from these workshops and other supporting security-related documentation, a comprehensive risk analysis was performed to determine the probability and impact of each identity theft threat. Along with specific issues relating only to the process, several service-wide observations were noted as a result of this assessment in the areas of governance, incident response, training and awareness, user access, and information management. The IRS did not want to take a 'binary approach' to remediation efforts. There were never going to be unlimited resources for remediation and, indeed, some of the risks identified would probably need to be accepted, as remediation would, in effect, shut the process down. Therefore another prioritization process that focused on remediation efforts was performed.

After the completion of the risk assessment and prioritization of remediation efforts, the IRS embarked on a series of identity theft risk reduction initiatives. There were several pre-requisites identified to provide a strong platform on which to build the risk reduction program. Governance bodies were identified and systems to track incident metrics were implemented.

Centrally documenting potential identity theft threats in a large organization is a substantial task. Threat sources are as varied as a hacker exploiting a technical system, to a mailroom employee selling PII to an external party. However, identifying these threats by performing an independent risk assessment has helped the IRS implement appropriate control mechanisms to safeguard PII and reduce the impact of identity thieves using stolen identities to interact with the services processes. The IRS is now better prepared to respond to new data protection requirements when Congress or OMB imposes them. ■

Andrew Hartridge and Stephanie Phillippy are with Deloitte & Touche's Security and Privacy Services Practice. Hassan Afzal and Joni Swedlund are with Deloitte Consulting LLP. For additional information please contact Hassan via email at hafzal@deloitte.com or Joni at jswedlund@deloitte.com.

Protecting PII: The Federated Model

By Scott Schumacher, PhD
Chief Security Officer and Chief Scientist
Initiate Systems, Inc.

Privacy, security, and mitigating risk have always been at the forefront of Federal agency requirements. However, the recent data breaches involving the Veterans Administration, U.S. Department of Commerce, U.S. Department of Agriculture and other agencies have been quite a wake-up call.

Simply put, government and civilian agencies have been lax about where data reside. Last May, millions of veterans' records left a secure database and wound up on a contractor's laptop. Agency workers regularly pull data out of databases and float that often times private information around the Internet. This practice puts personally identifiable information (PII) at serious risk.

We have this problem because data sharing and exchange are an absolute necessity.

Unfortunately, downloading and transmitting data to another location, as well as storing those records where they were not originally meant to be stored—on a laptop or desktop outside of the organization, have caused many problems.

How do we enable data exchange without compromising security and putting PII at risk? The answer is: a federated data model.

Same Access, Less Risk

A federated data model gives agencies the ability to access and present data without actually moving the data from

Continued on next page...

its original location. Federated data technology creates an index of, and pointers to, data stored in multiple source systems. In other words, this technology lets agencies create a virtual arrow that says, "Data, this way"—without moving or compromising PII.

Without moving data from its original location, the owner of each source database decides exactly what data will be shared, both within and outside the organization. Access rules continue to be applied because the data has not moved.

The security arguments are overwhelming; a federated data model may have prevented the aforementioned breaches. Privacy and regulatory arguments are equally overwhelming. Again: the data do not move from the database, therefore the data can only be accessed if permission is allowed using existing policy, organizational, and database rules.

Real-World Uses

This type of data model is being used today, primarily in healthcare, where protecting PII is a high priority as well as a significant challenge. In the healthcare industry, patient records are critically private. The goal is to allow hospitals and other healthcare facilities to share patient information without compromising the PII within patient records.

There has been some discussion around solving this issue by developing a National Patient Identifier. This would be similar to a Social Security Number, but used specifically to identify individuals in the context of their medical histories.

Using a federated data model provides the same results at a fraction of the cost, confusion, and logistical difficulties.

U.S. Healthcare

One of the most advanced regional and national health information networks running today was created by Massachusetts SHARE (Simplifying Healthcare Among Regional Entities)—a collaborative initiative run by the Massachusetts Health Data Consortium.

In its work with Computer Sciences Corp. (as the recipient of an award to help create a national health information network demonstration project) and public-private collaborative Connecting for Health, MA-SHARE has created a three-state prototype health-information network linking about 20 million medical records associated with 500,000 patients across networks in Massachusetts, Indiana and California.

Canadian Healthcare

Canada's healthcare industry is also using federated data technology within its nationwide electronic health records (EHR) initiative. Canada plans to have half the country using an interoperable EHR system by 2010. Critical to this plan is Canada Health Infoway—an independent, not-for-profit organization making strategic investments in public sector EHR projects across the country.

The plan involves multiple Canadian jurisdictions (provincial, regional, and territorial) implementing a client/patient registry. The registry will link all identifiers and their associated data elements within and across all applications—regardless of their disparate or similar characteristics—to provide a complete patient care imprint at any point of service in the region, province or territory.

The Federated Approach

So, how does this technology work? Let's start by looking at more traditional ways of sharing data.

A Transactional Approach

With a transactional approach, data is shared through a transactional hub system. This type of system physically stores data from multiple locations in a centralized database and shares it with users throughout the enterprise. This type of data-sharing solution is certainly effective. It can also be costly and time consuming. And, it requires that original data leave the original database. It requires restructuring of data ownership. Any time data is restructured or moved, security becomes a factor and PII is at risk.

A Federated Approach

A federated approach incorporates aspects of centralization, but ultimately lets individual units retain local control. A federated system establishes a central "index" of where data can be found, rather than creating a database of the records themselves. Unlike a transactional hub approach, a federated solution does not require replication, migration, or modification of pre-existing data. Legacy systems that maintain agency information continue to function as originally intended—the model does not modify processes already running. Privacy, access control, and other agency policies are kept intact.

Final Thoughts

The alarm has gone off. Now is the time to wake up, recognize the PII security risks, and do something about it.

If your agency chooses to move to a federated model, rest assured there are proven products available today. Be sure to take a long, hard look at the product and the vendor to ensure there is a history of providing this type of data integration. There are, of course, no official mandates saying we must move to a federated approach. In fact, there are no regulations saying we need to do anything differently than we're doing today to help secure data and protect PII. It just makes good sense. ■

Scott Schumacher, Ph.D., is a government and commercial expert in complex data analysis. For additional information contact sschumacher@initiatesystems.com.

Recover Quickly from a Data Breach — Call GSA

By Robert Smudde
USA Services Federal Solutions
U.S. General Services Administration

When the Department of Veterans Affairs had to announce that privacy information for 26.5 million veterans was on a laptop stolen in May 2006, they naturally expected a lot of calls. So one of the first things VA did was to get a high-volume call center up and running on short notice using GSA's FirstContact contract, an indefinite delivery, indefinite quantity (IDIQ) contract vehicle with five pre-qualified vendors. VA contacted GSA on Friday; a contact center capable of answering 260,000 calls a day was taking calls from veterans and their families by Monday morning.

A month later, when Department of Agriculture officials learned they had had a data breach compromising the personal information of USDA employees, they came to GSA. GSA quickly updated information in its database of Frequently Asked Questions so those who answer toll-free calls at 1-800-FEDINFO GSA's National Contact Center could provide up-to-date answers to USDA employees' questions.

GSA is geared up to provide quick solutions to help agencies establish call-center services to meet the needs of an anxious public. These tools allowed the VA to issue a task order against an existing contract, and gave customized answers to allay the concerns of USDA employees. Both offer citizens a level of personal reassurance during a time of anxiety that would have been difficult to deliver a few years ago.

The GSA Office of Citizen Services and Communications, which manages these and other sources of citizen information, coordinates the information provided through other official U.S. government channels, including USA.gov, the government's Web portal. During the VA incident, for example, the information provided to callers was used to update USA.gov's FAQ database, and questions posed online at USA.gov were forwarded to the contact center to answer e-mails using the same information.

GSA's www.usaservices.gov website has information about a number of tools for agencies that need emergency communications support. These include the FirstContact contract vehicle, a toolkit for procuring emergency support, and contact information to get immediate assistance in an emergency. The GSA Federal Acquisition Service provides credit monitoring services via blanket purchasing agreements with three vendors.

Its broad experience providing privacy breach recovery in recent years leads GSA to recommend several steps for agencies to follow if they need to respond to emergency situations. These recommendations echo the lessons learned about federal data breaches released in an April report by the Government Accountability Office.

What to Do When a Data Breach Occurs

1. **Report the breach to the agency's security committee.** Each agency should have designated senior officials empowered to make decisions regarding the agency's response to security breaches.
2. **Report the breach to the U.S. Computer Emergency Readiness Team (US-CERT).** The Office of Management and Budget requires federal agencies to report "all incidents involving personally identifiable information in electronic or physical form" to US-CERT within one hour of becoming aware of the occurrence. All incidents whether suspected or confirmed must be reported.
3. **Report the breach to relevant law enforcement agencies.**
4. **Clarify the agency's ability to respond:**
   a. Exactly what information has been compromised?
   b. How many people are affected?
   c. Anticipate questions affected people and media will have and prepare answers to them.
   d. Determine whether the agency should provide free credit monitoring services to those affected.
   e. Do adequate communication channels exist to handle the expected number of inquiries?
5. **Work with the agency's Public Affairs office on messages for the public and the affected individuals:**
   a. Tell what the breach is and how it is going to be fixed.
   b. Explain where to get additional information, i.e., websites and phone numbers.
   c. Describe what to expect as a result of the breach and the agency's corrective action, i.e., will credit monitoring be provided?
   d. Provide reassurance that the situation is under control.
6. **Take inquiries and work with Public Affairs to coordinate information disseminated via all communication channels and all offices.** ■

Robert Smudde is the Manager of the USA Services E-Gov Program Office. For additional information, contact robert.smudde@gsa.gov.

Federal Data Privacy - Regulations and Solutions

By David Etue
Senior Security Strategist
Fidelis Security Systems

The past few years have seen a sharp increase in the leakage of personal data like credit card and social security numbers from institutions ranging from universities, to banks, to government agencies such as the Department of Veterans Affairs. According to a list maintained by the Privacy Rights Clearinghouse, a San Diego-based advocacy group, more than 190 such incidents have been reported since February 2005. The Federal Trade Commission (FTC) estimates the inadvertent or deliberate extrusion of critical data costs consumers and businesses $50 billion a year. Beyond these immediate costs, data leakage threatens the integrity and growth of E-Commerce. Even more ominously, it could harm national security.

From the assessments we have provided for our customers, we believe this is just the tip of the iceberg. Most people use the leaky faucet analogy to describe data leakage—but we have seen it is more akin to a fire hose and that protected information is flowing out of both government and commercial entities at alarming rates. The good news is that both legislation and technology solutions are available and evolving to start addressing the problem.

California SB1386 and the Payment Card Industry (PCI) Security Standard set the bar for standards for protecting personal identity information (abbreviated PII or referred to as nonpublic personal information or NPI). In addition, these regulations require notification to both the regulator and the person affected by the unauthorized disclosure. The disclosure component of the laws is very important as it has proven more effective than fines in getting an organization to address the problem. A public announcement is a terrible public relations event. The ensuing scrutiny from the public and regulators has been a great motivator in moving organizations into action to prevent data leakage.

Last year the Federal government also entered the picture in a more significant way. Prior to 2006, there were a number of laws passed to protect identity information including the Gramm-Leach-Bliley Act (GLBA) regulating NPI in financial services; the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and the Privacy Act of 1974 that regulated the use of personal information by Federal executive branch agencies. However, prior to 2006 little punitive action had been initiated and legislation lacked a focused direction. On the punitive side, in 2006 the FTC leveled the largest data privacy fine in its history. In addition, OMB Memorandum 06-16 provided detailed guidance to Federal agencies on the protection of "Sensitive Agency Information" focused on PII. The House Government Reform Committee requested a list of all breaches of personal information by Federal agencies. The list was published in a report made available to the public.

We believe this is only the beginning of both legislation and enforcement. It is likely the 110th Congress will enact legislation that will apply to both public and private entities to ensure that identity information isn't mishandled, stolen or peddled to the highest bidder. This legislation should be guided by the following principles:

1. Clear, Uniform and Comprehensive Application. By the end of 2005, 17 states had some type of data privacy law. Compliance with multiple and often conflicting legal frameworks increases costs and, more important, minimizes the clarity necessary to inspire trust among users. Federal legislation should be clear, uniform and comprehensive. It should authoritatively define "personal data" and "identity." It must establish national benchmarks that set a floor of protection, rather than a ceiling. Finally, privacy legislation should apply to private and public enterprises, including Federal, state and local governments.
2. Use of Current Best Practices. Working together, public and private organizations have developed best practices that can and should be utilized in the development of a national standard. These best practices include an expansive understanding of private data; disclosure of a breach even if security procedures are in place; disclosure of a breach when data is reasonably believed to have been compromised; delayed disclosure to meet the legitimate needs of law enforcement; and an annual risk assessment by organizations that meet a certain threshold, such as the quantity of identities held.
3. Vigorous Enforcement and Substantial Penalties. Appropriate government agencies must be fully empowered and possess necessary resources to enforce a data privacy law. In addition, penalties must be designed to encourage compliance that genuinely lessens the risk of private data loss. This translates into significant funding; substantial penalties for intentional violations; lesser penalties for unintentional violations; and penalties based on the number of identities

Continued on next page...

disclosed. It is also critical that the legislation reward the organizations that make significant efforts to comply.

Existing and new legislation will accelerate organizations' desires to deploy processes and technology to protect sensitive information. However, there is no need to wait and risk experiencing the negative public relations event and the significant financial costs associated with a data leak. Many technologies are available to address the problem today. Historically, information security solutions were focused on who was getting in and/or able to access information and not what was done with the information once in the users' control. However, solutions are now available to inspect the data leaving the network and report on data leaks. In addition, some of the more advanced technologies can prevent the leak from occurring! These solutions are often referred to as extrusion prevention, data leakage prevention or content monitoring and filtering. In addition, many vendors provide assessment services to help organizations understand the risk presented by data leakage and actually monitor identity information leaving the network during the assessment period.

Digitization of information has provided productivity enhancements in the delivery of services to taxpayers, employees and contractors. Yet at the same time, this digitization has also created risk of unauthorized disclosure leading to identity theft. It is expected that 2007 will bring new Federal privacy legislation. However, it is imperative that Federal agencies, government contractors, and the private sector not wait. Today is the time to implement processes and technology to protect personal identity information. ■

David Etue is senior security strategist at Fidelis Security Systems of Bethesda, Maryland. He can be contacted at david.etue@fidelissecurity.com. For more information on extrusion prevention visit http:||www.fidelissecurity.com|prevention|

Privacy and Information Assurance: Deceptive Look-Alikes

By, Charles Thompkins III, Esq.
Professor and Chairman
Systems Management Department
National Defense University

Making a mistake between "look-alikes" can be a source of fun, mild embarrassment, or *real* trouble (as anyone who has dated twins will attest). It is the same with the "look-alikes" of information management: assurance and information privacy. Though they may look alike to a casual observer, close attention to their differences can avoid embarrassment or worse. This discussion will differentiate the "look-alikes," present some principles governing privacy, and highlight some growing concerns about Federal privacy law.

Information assurance, privacy's headline-grabbing look-alike, attracted a great deal of attention during 2006. Security lapses and personal information losses multiplied as government, industry, and academia seemed to compete to be the Biggest Loser. The Federal government started with a huge competitive advantage because of the amount and variety of information it has. The Department of Veterans Affairs loss of up to 26.5 million veterans' records established an early lead. However, industry competed gamely. The Boeing Company, for example, lost a laptop in early November with information on 762 employees. This appears to have been a rehearsal for the company's subsequent loss of information on 382,000 former and present employees in December. Not to be left behind, Ohio University staked its claim to the title of the Biggest Loser when poor security led to the exposure of the personal information of 137,000 people last summer. Several other government and private organizations qualified for (dis)honorable mention.

Nearly all of these highly publicized incidents related to only one facet of information assurance: confidentiality. There are two or (according to some experts) three other facets: integrity, availability and non-reputability. Integrity addresses the concern that data be valid and that it is not altered without proper authorization. Availability is concerned with access to data when and under the conditions required for a transaction. Finally, non-reputability concerns itself with insuring that data changes or transactions are not deniable by their author. Because of public concern about identity theft and legal requirements to report loss of information in some cases, potential confidentiality breaches are well reported. Problems with information integrity, denial of service, and non-repudiation make headlines less frequently, though they may be equally troubling.

The insurance industry's introduction of products to protect against identity theft and corporate data loss liability is the surest indicator of rising concern about poor information assurance. If the past is any indication, there is good reason to believe that the marketplace, court system and rising public concern will provide incentives for information assurance.

There is less reason to be sanguine about the prospects for information privacy than for information assurance. Consumer willingness to surrender personal information for sales or

Continued on next page...

convenience incentives suggests little public concern about commercial acquisition and sharing of potentially revealing information, for example, reading interests, political beliefs, etc. Commercial acquisition and marketing of information about these and other items of personal information is a substantial industry that tends to resist regulation. Finally, after 9/11, Americans appear more willing to permit intelligence and law enforcement agencies to gather and analyze large amounts of personal information in the interest of greater security.

Perhaps for these reasons, information privacy doesn't make the front pages frequently. In addition, information assurance is an important contributor to information privacy, so while assurance is in the center of the stage, its "look-alike" privacy hangs demurely in the background. While assurance lends itself to a clear definition, privacy does not. Assurance focuses upon control of information by its custodian. Privacy focuses upon control of information by its subject.

As information system scope and interconnectivity have increased and data matching tools have become more sophisticated, increasing attention has been focused upon attempts to define information privacy principles and practices. In 1973, the U.S. Department of Health, Education and Welfare published a highly influential report advocating a Code of Fair Information Practices. It recommended that:

- There should be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for a person to find out what information about him or her is in a record and how it is used or to be used.
- There must be a way for a person to prevent information obtained for one purpose from being used for a different purpose without his or her consent.
- There must be a way for a person to correct or amend a record of identifiable information about him or her.

Any organization creating, maintaining, using or disseminating records containing personally identifiable information should be responsible to assure the reliability of data for its intended use and must take reasonable precautions to prevent its misuse.

Rather than provide blanket statutory protection consistent with these principles, Federal statutes and regulations have been enacted piecemeal to deal with specific, narrow threats as they've made the headlines. Perhaps the best example is the Video Privacy Protection Act of 1988 that restricts access to consumer videocassette rental and sales information. (The act was enacted in response to disclosure to the media of a list of movies rented by Judge Robert Bork, a controversial nominee under consideration for a seat on the Supreme Court.) More recent examples include the Health Insurance Portability and Accountability Act (HIPAA) which protects health-related information, while the Gramm-Leach-Bliley Act protects financial information, etc.. In addition, many states have adopted their own regulations. The result is a patchwork that increases the burden and economic cost of compliance with multiple regulatory and technical standards while leaving some personal information unprotected.

The "grand-daddy" of information privacy laws is the Federal Privacy Act. While the Privacy Act may have provided adequate safeguards 30 years ago, there is reason for increasing concern about its adequacy today. Passed in the immediate aftermath of the Watergate scandal, compilation of White House "enemies lists," and revelations of domestic spying by both intelligence and law enforcement agencies, the Privacy Act focused upon regulating acquisition and protection of personal information by the government and by contractors managing information for it.

The Privacy Act's narrow focus, poorly defined exceptions, and limited legal remedies make it inadequate to today's information technology environment. Since 1974, the government's abilities to aggregate, share and data mine personal information have grown dramatically. The Act's broad exceptions to permit sharing of information among Federal agencies for "routine use" and law enforcement purposes are of particular concern. In addition, the Privacy Act provides citizens and aliens lawfully admitted for permanent residence a right to notice of systems of record in which their personal information may be kept and a right to review and correct the information. However, the act doesn't require commercial data companies to provide citizens the same safeguards. Government is expanding its use of commercial information for investigatory and antiterrorism data mining and matching. Inadequate notice and safeguards place citizens at risk of bad government decisions, for example, improper inclusion on a "no fly" list or other unwanted scrutiny. The risk is compounded when citizens are denied information about the sources of information being used to make decisions and are unable either to correct the information or hold the commercial provider responsible for its quality.

It is time for Congress to pass broad privacy legislation extending the principles of the Code of Fair Information Practices consistently across both the public and private sectors. In the meantime, agency senior leaders and privacy officers should apply the Code's principles liberally, rather than using as their model the narrow legal strictures of the Privacy Act. ■

Charles Tompkins, a lawyer and former Defense Department program manager, teaches classes on acquisition, privacy and information assurance law at the National Defense University's Information Resources Management College.

GAO Recommendations for Protecting Personal Information

By Gregory C. Wilshusen
Director of Information Security Issues
Government Accountability Office

In May 2006, the Department of Veterans Affairs announced that computer equipment containing the personal information of approximately 26.5 million veterans and active duty service members was stolen from the home of a VA employee. Although this incident was remarkable in its scope, it is by no means unique. An October 2006 report issued by the then Committee on Government Reform concluded that data loss was a government-wide occurrence and that all Federal agencies that responded to its data request reported the loss of personally identifiable information.

The loss and disclosure of personal information can lead to identity theft and privacy concerns. Identity theft generally involves the fraudulent use of another person's identifying information—such as Social Security Number, date of birth, or mother's maiden name—to establish credit, run up debt, or take over existing financial accounts. According to identity theft experts, individuals whose identities have been stolen can spend months or years and thousands of dollars clearing their names. Some individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft. Beyond the serious issues surrounding identity theft, the unauthorized disclosure of personal information also represents a breach of individuals' privacy rights to have control over their own information and to be aware of who has access to this information. Accordingly, it is incumbent upon Federal agencies to prevent the disclosure of this information to unauthorized individuals.

So what can agencies do to help protect personal information? They can take the following actions.

Implement a robust information security program. A comprehensive security program is a prerequisite for the protection of personally identifiable information held by agencies. Such a program should provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Federal Information Security Management Act (FISMA) requires that agency security programs include the following elements:

- Periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- Risk-based policies and procedures that cost-effectively reduce risks to an acceptable level and ensure that security is addressed throughout the life cycle of each information system;
- Security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies through plans of action and milestones; and
- Procedures for detecting, reporting, and responding to security incidents.

Conduct privacy impact assessments. It is important that agencies identify the specific instances in which they collect and maintain personal information and proactively assess the means they intend to use to protect this information. This can be done most effectively through the development of privacy impact assessments (PIAs), which are required by the E-Government Act of 2002, when agencies use information technology to process personal information. PIAs are important because they serve as a tool for agencies to fully consider the privacy implications of planned systems and data collections before those systems and collections have been fully implemented, when it may be relatively easy to make critical adjustments. PIAs can identify areas of noncompliance with Federal privacy laws, evaluate risks arising from electronic collection and maintenance of information about individuals, and evaluate protections or alternative processes needed to mitigate the risks identified. Agencies that do not take all the steps required to protect the privacy

Continued on next page...

of personal information risk the improper exposure or alteration of such information.

Limit collection of personal information. One item to be analyzed as part of a PIA is the extent to which an agency needs to collect personal information in order to meet the requirements of a specific application. Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information—such as Social Security Numbers—may not be needed for many agency applications that have databases of other personal information. Limiting the collection of personal information is also one of the fair information practices, which are fundamental to the Privacy Act and to good privacy practice in general.

Limit data retention. Closely related to limiting data collection is limiting retention. Retaining personal data longer than needed by an agency or statutorily required adds to the risk that the data will be compromised. In discussing data retention, California's Office of Privacy Protection recently reported an example in which a university experienced a security breach that exposed 15-year-old data, including Social Security Numbers. The university subsequently reviewed its policies and decided to shorten the retention period for certain types of information.[1] As part of their PIAs, Federal agencies can make decisions up front about how long they plan to retain personal data, aiming to retain the data for as brief a period as necessary.

Limit access to personal information and train personnel accordingly. Only individuals with a need to access agency databases of personal information should have such access, and controls should be in place to monitor that access. Further, agencies can implement technological controls to prevent personal data from being readily transferred to unauthorized systems or media, such as laptop computers, discs, or other electronic storage devices. Security training, which is required for all Federal employees under FISMA, can include training on the risks of exposing personal data to potential identity theft, thus helping to reduce the likelihood of data being exposed inadvertently.

Use technological controls such as encryption. In certain instances, agencies may find it necessary to enable employees to have access to personal data on portable devices such as laptop computers. As discussed, this should be minimized. However, when absolutely necessary, the risk that such data could be exposed to unauthorized individuals can be reduced by using technological controls such as encryption, which significantly limits the ability of such individuals to gain access to the data. Although encrypting data adds to the operational burden on authorized individuals, who must enter pass codes or use other authentication means to convert the data into readable text, it can provide reasonable assurance that stolen or lost computer equipment will not result in personal data being compromised, as occurred in the recent incident at VA. A decision about whether to use encryption would logically be made as an element of the PIA process and an agency's broader information security program.

While these suggestions do not amount to a complete prescription for protecting personal data, they are key elements of an agency's strategy for reducing the risks that could lead to data loss and identity theft. ■

Greg Wilshusen is the Director of Information Security at the Government Accountability Office. For additional information please contact WilshusenG@gao.gov.

1 State of California Department of Consumer Affairs, Recommended Practices on Notice of Security Breach Involving Personal Information (April 2006), p. 6.

Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace

By Beth Givens
Director
Privacy Rights Clearinghouse

Most guides on preventing identity theft focus on steps consumers can take, such as shredding their trash and protecting their SSN. But realistically, while these steps reduce the risk of becoming a victim, there is little individuals can do to actually prevent identity theft.

True prevention resides in two arenas – the adoption of more effective application-screening procedures by the credit industry and the implementation of responsible information-handling practices by employers. This article focuses on the latter.

Experts in identity theft report that an increasing number of cases can be traced back to dishonest employees in the workplace who obtain the sensitive personal information of employees and customers and disclose it to identity thieves.

One of the keys to preventing identity theft, therefore, is to safeguard personal information within the workplace, whether it's a business, government agency, or nonprofit. Targets for identity thieves include SSNs, driver's license numbers, financial account numbers, PINs, passcodes, and dates of birth.

Workplace Information-Handling Practices

- **Adopt a comprehensive privacy policy** that includes responsible information-handling practices. Appoint an individual and/or department responsible for the privacy policy — someone who can be contacted by employees and customers with questions and complaints. (See Resources below, Checklist of Responsible-Information Handling Practices.)
- **Store sensitive personal data in secure computer systems. Encrypt!** And make sure your wireless network is protected with the proper security settings. Store physical documents in secure spaces such as locked file cabinets. Data should only be available to qualified persons.
- **Dispose of documents properly**, including shredding paper with a cross-cut shredder, "wiping" electronic files, destroying computer drives and CD-ROMs, and so on. Comply with California's document destruction law, Civil Code 1798.80-1798.84, and the Federal Fair Credit Reporting Act FACTA provision on document disposal, section 216. (See Resources.)
- **Build document destruction capabilities into the office infrastructure.** Place shredders around the office, near printers and fax machines, and near waste baskets. Use cross-cut (confetti) shredders rather than strip-shredders. Make sure dumpsters are locked and inaccessible to the public.
- **Conduct regular staff training**, including new employees, temporary employees, and contractors.
- **Conduct privacy "walk-throughs"** and make spot checks on proper information handling. Reward employees and departments for maintaining "best practices."
- **Put limits on data collection** to the minimum information needed. For example, is SSN really required? Is complete date of birth needed, or would year and month be sufficient?
- **Put limits on data display and disclosure of SSN.** Do not print full SSNs on paychecks, parking permits, staff badges, time sheets, training program rosters, lists of who got promoted, monthly account statements, customer reports, and so on. Do not print SSNs on mailed documents or require that they be transmitted via the Internet unless allowed by law. In compliance with California law, do not use SSN as customer number, employee ID number, health insurance ID card, and so on. (California Civil Code 1798.85-86 and 1786.6) (See Resources)
- **Restrict data access to staff** with legitimate need to know. Implement electronic audit trail procedures to monitor who is accessing what. Enforce strict penalties for illegitimate browsing and access.
- **Conduct employee background checks**, especially for individuals who have access to sensitive personal information. Screen cleaning services, temp services, and contractors.
- **Safeguard mobile devices** that contain sensitive personal data, such as laptops, Blackberries, PDAs, and mobile phones. These are a favorite target of thieves.
- **Notify customers and/or employees of computer security breaches** involving sensitive personal information. More than 30 states have adopted security breach notice laws. (See Resources.) Also

Continued on next page...

notify individuals when security breaches involve paper records, outside the scope of most laws.

- **Develop a crisis management plan** to be used if sensitive employee or customer data is lost, stolen, or acquired electronically. The plan should include instructions to prevent identity theft if SSNs and/or financial account numbers are obtained illegitimately.
- **Regularly audit compliance** with all information-handling practices and privacy policies.

In summary, everyone from the mail clerk to the CEO must make it their business to handle personal information responsibly in the workplace. Don't make the workplace a breeding ground for identity theft.

Resources

- Checklist of Responsible-Information Handling Practices, PRC Fact Sheet 12, www.privacyrights.org/fs/fs12-ih2.htm
- FACTA: the Fair and Accurate Credit Transactions Act, PRC Fact Sheet 6a, www.privacyrights.org/fs/fs6a-facta.htm#2g
- Business Identity Theft Risk Test, Identity Theft Resource Center, www.idtheftcenter.org/busrisktest.shtml
- Lists of security breach notice laws in U.S.: PIRG: www.pirg.org/consumer/credit/statelaws.htm. Consumers Union: www.consumersunion.org/campaigns/Breach_laws_May05.pdf
- Recommended Practices for Protecting the Confidentiality of Social Security Numbers, California Office of Privacy Protection, www.privacy.ca.gov/recommendations/ssnrecommendations.pdf
- Recommended Practices on Notification of Security Breach Involving Personal Information, California Office of Privacy Protection, www.privacy.ca.gov/recommendations/secbreach.pdf
- A California Business Practices Handbook, California Office of Privacy Protection, www.privacy.ca.gov/business/ca_business_privacy_hb.pdf.
- Guide for Small Businesses by Better Business Bureau, "Security & Privacy Made Simpler," www.bbb.org/securityandprivacy ■

Beth Givens is founder and director of the Privacy Rights Clearinghouse, established in 1992. She represents the interests of consumers in public policy proceedings at the state and Federal levels. For additional information contact bgivens@privacyrights.org.

Can This Device Be Trusted? Using Trusted Computing to Build a Secure Environment

By David Hoffman
Director of Security and Privacy Policy
and Claire Vishik
Manager of Trust/Security Standards Regulations
Intel

Introduction

Information crucial to individuals or enterprises is almost always available in digital formats from interconnected applications. Thus, security breaches have a devastating effect on organizations and affect millions of users around the world. Security for networks, computers, and data is the result of the dedicated work of thousands of technologists, but it is insufficient to ensure protection. Today's exclusionary models lose their efficiency as the mobility of networked devices and diversity of applications spanning thousands of systems accessed by millions of users make it impossible to account for all the elements in need of protection. Moreover, a combination of secure components doesn't equate to a secure complex system. Technologists are at a disadvantage in this fight to protect networks and information: the attacker needs to discover one vulnerability to compromise a system, while technologists have to eliminate all the weaknesses to guarantee security.

Client Personal Computers (PCs) Need Better Protection

The concept of a perimeter that separates protected (trusted) and public networks has changed with the growing mobility of devices and business collaboration. In theory, only authorized users and applications access protected systems and networks to perform authorized functions. In reality, the picture is not clear-cut. Most laptops, PDAs, and removable storage tools operate both inside and outside organizations, with the same devices performing internal and external activities. The older ways of creating a "trusted environment" no longer work.

The complexity of functions performed on PCs increases with their computing

Continued on next page...

power. Today, PCs are involved in key activities in an organization and have become repositories of highly confidential information collected and aggregated from multiple sources. With many attacks directed at networked clients, a breach into a PC is extremely damaging for an individual or a department. Yet PCs are lightly protected compared to servers and networks.

PCs in an organization are patched on a regular basis, use up-to-date anti-virus/anti-spyware tools and a hardened operating system, but they don't undergo a serious configuration analysis during normal operations, and a non-generic Trojan or unauthorized users may remain undetected for considerable periods of time or until consequences of the attack become apparent.

Trusted Computing

As the sophistication of attacks increases ahead of detection techniques, can we continue to trust our own computers and other devices and ensure that an entity "will behave in a particular manner for a specific purpose "? A series of open specifications developed by the Trusted Computing Group (TCG), an international organization with more than 140 members, is defining an environment that can be trusted by users or service providers and establishes a higher standard of safe computing, with the immediate impact on client machines. The core TCG specification is for Trusted Platform Module (TPM), a chip, typically attached to the motherboard of a PC, enabling important security features, such as secure non-volatile storage for encryption keys, integrity reports, and secrets. TCG is also working on Trusted Modules for other devices, e.g. mobile phones and PDAs, to achieve greater trust in multi-device mobile environments typical of modern computing providing stronger protection for information in all locations where it resides. Using a set of standard procedures that are extremely sensitive to changes, TPMs measure the integrity of a system, increasing the likelihood that unauthorized changes are detected. TPMs enable platform authentication providing assurance to users and administrators that only trustworthy devices participate in secure transactions. If authorized by the user, TPMs can also perform attestation, informing the trusted network about the security status of a platform. TPMs have been designed to "seal" data to a predefined platform status, closing access if measurements detect that it has been compromised and segregating different platform configurations.

Intel® Trusted Execution Technology

Intel® Trusted Execution Technology (TXT), formerly LaGrande Technology, extends capabilities of a TPM. Directed at business customers, Intel® TXT helps create a trusted computer – one that provides its users enough information to decide whether to trust the platform. In conjunction with Intel® Virtualization Technology (VT), Intel® TXT enables a secure partition where applications requiring greater confidentiality can be executed in isolation. Protected execution in isolated domains and memory protection ensuring that only a CPU in protected execution mode accesses protected memory pages enhances security of confidential data and applications. Local or remote verification ensures that the correct environment is executing as expected, and that confidential information is only visible and accessible to applications operating in a secure domain. The verification process uses Intel® TXT measurement capability to confirm the viability of the local configuration to the users (local verification) or to report, using the TPM, the security status to an external entity (remote verification). Future versions of Intel® TXT will include protected input and graphics, making sure that applications using protected execution cannot be breached through corrupted inputs or graphics.

Upholding Security, Protecting Privacy

TCG specifications have developed procedures and architecture necessary to mitigate potential privacy concerns in a trusted platform. TPM-equipped PCs require the owner's authorization to enable the TPM and for activities including TPMs. The TPM specification designs the key hierarchy so that the static identifiers are substituted with domain-oriented keys to limit the exposure of a trusted platform in standard protocols. TCG also endorsed Direct Anonymous Attestation (DAA) protocol to support complete anonymity while preserving the level of assurance.

At Intel, privacy, ease of use, and manageability are among the guiding principles of the design process. Intel® TXT supports the privacy safeguards already present in standard TPMs, adding opt-in for Intel® TXT and Intel® VT to uphold the user's choice in all the components of the platform.

Conclusions

Universal digitization of sensitive information makes it imperative to enhance protection of client PCs where such information is frequently stored. In today's dynamic environment which prizes mobility, efficient protection of personal information from increasingly sophisticated software attacks can be carried out only through a combination of multiple hardware and software technologies. Trusted Computing technologies focus on building a security foundation that helps establish trustworthiness of devices. An environment composed of trusted platforms will be extremely beneficial for preserving confidentiality and integrity of personal information. ■

David Hoffman is the Director of Security and Privacy Policy, Intel. Claire Vishik is the Manager of Trust|Security Standards Regulations. For additional information contact david.everard@intel.com.

The IAPP Offers Government Privacy Professionals a Specialized Credential

By Peter Kosmala
Assistant Director
International Association of Privacy Professionals

In July 2006, the International Association of Privacy Professionals (IAPP) passed the 2,600-member mark and became the largest professional organization serving the privacy industry today. Just six months later, the IAPP has grown to nearly 3,000 members worldwide.

The IAPP represents privacy professionals in business, government and higher education from 23 countries in North America, Europe, Asia and Latin America. These professionals work within a variety of industries from healthcare, financial services and retail, to technology and consumer goods in addition to state and Federal government agencies.

The growth of the IAPP is a testament to the services and programs the association offers. It also reflects the increasingly important role that privacy professionals play in governments, businesses and academic institutions around the world. In light of growing data security concerns and the desire for stronger customer trust and citizen service, corporations and government agencies alike are creating positions and programs that address information privacy effectively and proactively.

Founded in 2002 from what was previously known as the Association of Chief Privacy Officers, the IAPP since has grown to represent a broader spectrum of privacy professionals other than solely corporate executives – just as the privacy profession itself has expanded from a pure legal compliance function to a broader set of disciplines that now include information access, data security, privacy program management, international data flows, customer relations and employee awareness.

Much of the association's growth can be attributed to its introduction of the first major professional certification in information privacy. In October 2004, the IAPP launched the Certified Information Privacy Professional (CIPP), a foundation course in U.S. and E.U. private sector information privacy laws, technologies and practices. The program was established with founding grants from HP and Microsoft, and its five-part curriculum was developed with support from leading privacy executives at HP, Microsoft, Nationwide Insurance, Nordstrom, Wal-mart, Procter & Gamble, Corporate Privacy Group and Privacy and Information Management Services, P.C.

Recognizing the growing importance of privacy officers in government, the IAPP followed the successful launch of the CIPP with the first publicly available certification program in U.S. government privacy, the Certified Information Privacy Professional/Government (CIPP/G). This advanced credential debuted at the IAPP National Summit in Washington, D.C. in March 2005 with underwriting support provided by IBM.

To date, the IAPP has certified more than 1,000 people, including 250 who have earned the CIPP/G credential, which is awarded only to those individuals with the greatest body of knowledge. In October, the IAPP launched its newest credential, the Certified Information Privacy Professional/Canada, the first professional certification program designed by Canadian privacy officers for the dual purpose of establishing an educational standard for Canadian privacy professionals and furthering the privacy industry across the Canadian private sector.

Just like the CIPP/C program, which drew from Canadian privacy experts, the CIPP/G was developed in close coordination with privacy leaders from U.S. Federal and state governments, including Zoe Strickland, the former Chief Privacy Officer of the U.S. Postal Service; Stephania Putt, Privacy Office Director at the U.S. Department of Veterans Affairs; Eva Kleederman, Policy Analyst for the U.S. Office of Management and Budget; and Joanne McNabb, Chief of the Office of Privacy Protection at the California Department of Consumer Affairs. The program also benefited from the expertise of top government vendors and consultants including Harriet Pearson, VP Corporate Affairs and Chief Privacy Officer, IBM Corporation; Julie Smith McEwen, Principal Information Privacy and Security Engineer, MITRE Corporation; Dr. Stuart Shapiro, Lead Information Security Scientist, MITRE Corporation. Timothy Skinner and Jill Rhodes, both of SRA International, also were instrumental in the effort.

The IAPP continues to draw from the expertise of the talented ranks of privacy officers in government service. Just recently, two high-

Continued on next page...

visibility privacy officers joined the CIPP/G advisory board; Jane Horvath of the Department of Justice and Barb Symonds of the Internal Revenue Service.

The CIPP/G program requires understanding of the CIPP foundation course in addition to essential government privacy laws and policies such as the Privacy Act, the e-Government Act, FOIA, FISMA, the Data Quality Act, systems of records notices (SORN), and privacy impact assessments (PIAs). The program also assesses knowledge of Federal-standard practices for privacy management, policy enforcement, records management, and privacy auditing and compliance. The CIPP/G is an advanced course intended for privacy officers and employees of U.S. Federal and state governments who currently hold privacy or security related responsibilities, such as information access, records management, record retention and compliance.

The credential is also relevant to private sector professionals, such as vendors and consultants, who serve clients in the U.S. government on matters of information privacy and security.

The IAPP has certified government privacy professionals from a number of Federal agencies and Departments including Agriculture, Commerce, Homeland Security, Postal Service, Treasury, Veterans Affairs, and the Office of the Director of National Intelligence. Just two years after its launch, the IAPP already is offering an expanded training course to help examinees prepare the overhauled CIPP/G exam, which will double in size to a one-hour, 60-question exam, beginning in March 2007. ■

Peter Kosmala is the Assistant Director for the IAPP. For additional information contact peter@privacyassociation.org.

Protecting PII with On-the-Fly Encryption

By Brandon Hoff
Chief Security Office and Vice President of Product Technology
CipherOptics, Inc.

As information sharing continues to grow, the privacy of personal information is increasingly at risk. More frequent information sharing brings with it the very real possibility of security breaches and data loss, situations that compromise an agency's ability to achieve mission success. Between the threat of identity theft and the increase in inter-agency information transfer, we face a heightened need and demand for the protection of personally identifiable information (PII).

The challenge of securing this critical information is, however, a moving target.

Most agencies have a variety of technologies in place to help mitigate network security risks. Yet nearly 80 percent of security attacks now originate within the firewall, according to studies by CERT, the FBI and InterGov.

To truly secure PII, we must focus on securing the network and the information. Data protection defends against intrusions that get past traditional safeguards and guards the critical core of the agency's mission—its information. Control access, defend the infrastructure, and protect the data ... these are the three keys to ensuring your secure information remains secure.

Today's Solutions

Intruder Controls

A wide variety of security technologies in use today play a significant role in securing PII within networks. Firewalls, access control software, anti-virus offerings—all of these types of security measures are essential, offering a first line of defense against intruders.

That said, a single line of defense is not sufficient in protecting against all vulnerabilities. Remember, in any data-sharing situation data is physically moving, originating in one place and ending up in another. The goal is to get that data from point A to point B without compromise. Intruder controls work effectively to control network access and defend the infrastructure, but they don't work to protect the data.

PKI Encryption

The most common method of data protection in use today is encryption. The most common type of encryption uses PKI, or public key infrastructure.

PKI encryption uses a two-key approach. Every sender and receiver has their own private key and public key. The private key stays private; the public key becomes part of a list of public keys that other people can use for decryption. This key combination is used to identify network users (through digital signatures) and to encrypt the data such that only those with decryption keys can read it.

PKI encryption is very effective and widely accepted as an encryption technology. However, it has limitations—particularly when it comes to scalability.

Standard encryption focuses on a one-to-one relationship between encryption points. As the number of

Continued on next page...

installations increases, so does the cost and risk of key management. Additionally, one-to-one encryption cannot take advantage of load-balancing capabilities or voice-over-IP (VoIP) technologies as these rely on a multitasking model. Simply put, PKI encryption solutions may work counter to what's already in place.

Cryptographic segmentation is a network-wide encryption solution that successfully protects data without the drawbacks of ordinary encryption models. It provides that additional level of security necessary to protect PII—securing data at all times as it travels across the network.

The technology works by separating the policy management and key generation/distribution from the policy enforcement layer. It virtualizes the connection-oriented approach used in other encryption schema. In other words, cryptographic segmentation is akin to dynamic encryption.

The primary advantage of cryptographic segmentation is encryption over the wire—on the fly—at wire speed with little or no performance degradation. All data-in-motion is encrypted.

Cryptographic segmentation offers other advantages as well:

- Secure workgroup collaboration. With cryptographic segmentation, you can set up encryption-specific workgroups. Public key assignments are dynamic. You can assign different encryption policies for different groups within the same agency, or for multiple groups that span multiple agencies or multiple government entities.
- Non-intrusive architecture. Cryptographic segmentation is technology that fits on top of the network and security components already in place. It's router agnostic. It's also network-type agnostic, as some other encryption solutions work only within a mesh-network environment. You can implement this technology directly on top of what you've already got.
- Scalability. Cryptographic segmentation provides encryption at network scale. Because it separates the policy and key-management layers from the enforcement layer, the technology is not limited by the size of the implementation, the number of public or private keys, or the number of users.

A Deployable COTS Solution

The final advantage of a cryptographic segmentation solution: it's available today, as a commercial off-the-shelf (COTS) product. Cryptographic segmentation removes most of the cost and complexity associated with traditional encryption, allowing agencies to deploy a defense-in-depth strategy as a layer in the network. A wide variety of proactive Federal, state and local entities are already using cryptographic segmentation to help assure secure PII within and among agencies.

With cryptographic segmentation, protecting PII can be more than just a concept—it can be a reality. ■

Brandon Hoff is the Chief Security Officer and Vice President of Product Technology. For additional information contact Brandon.hoff@cipheroptics.com.

Implementing Privacy Best Practices Through Automated, Ongoing Privacy Scans

By Kurt Mueffelmann
President and CEO
HiSoftware

The Internet age has revolutionized how government agencies communicate, publish and find information. While this technology has created new opportunities for global communication and commerce, it has also created new challenges in risk management. With the rush to put information online, many agencies have fallen prey to the exponential growth of Web-based electronic information. The volume of information now available on agency Web sites, Intranets, government to business portals, and networks has increased dramatically, and is also provided by multiple content contributors in multiple forms and languages. This makes online risk management a critical component of any successful online technology strategy.

Protecting the privacy of online personal information is one of the most important challenges that government agencies face today. Through online technology, storing and accessing records and personal information within government agencies is easier than ever before. With these services, however, the potential for misuse of personal data has increased. With poor online privacy practices, government agencies can experience negative events. How do you know if your agency is at risk? If you

Continued on next page...

have a Web site that collects or stores personal information from employees or other online visitors, you are at risk.

Government agencies must identify and manage online privacy and risk issues to ensure regulatory compliance and to earn and retain trust among their employees and others whose personal information they store. An online privacy best practices program provides a model that gives government agencies confidence in the proper collection, usage and protection of personal data, while also allowing control over that personal data.

Failing to comply with regulatory requirements may result in negative media attention, large fines and penalties, and may create impact perceptions of "trustworthiness" of an agency, creating a negative effect on an agency's image. While more and more government agencies are recognizing the importance of an online privacy risk management strategy, many of those agencies get a sense of false security by scanning their Web sites for privacy issues once a year, or even worse, only when the site is first developed and implemented. As Web content is dynamic by nature, Web sites should be monitored continuously and automatically to assist in ensuring regulatory compliance 365 days a year.

The first step in a successful online privacy risk management strategy is to define exactly what methods your agency uses to protect the personal information of a visitor to the Web site. This is done through an online privacy policy. A privacy policy assists your visitors in understanding agency practices for capturing and distributing visitor information that may be required of site users to submit. Without a clearly documented privacy policy on your Web site, you may risk losing visitors wary of providing personal information, and you may also expose yourself to an unnecessary risk of litigation.

An online privacy risk management strategy should give an agency the ability to view policy implementation from a project management perspective, which will enable the allocation of resources appropriately across an agency and track site progress, as well as identify problem areas so action items can be assigned against them. A good privacy strategy should also provide the ability to integrate testing into any quality assurance and content delivery processes associated with existing Web development and deployment practices. And finally, a user should be able to keep a historical view of their testing over time, which provides a great way to measure the progress of a project and set goals for the future.

An adequate privacy compliance program should consist of the following steps:

- Obtain commitment and support from senior management;
- Delegate responsibility to a privacy official;
- Conduct inventory of current privacy practices;
- Develop privacy policies and procedures;
- Educate employees on privacy policies and procedures;
- Implement and monitor the privacy compliance program;
- Automatically and continuously monitor Web sites for privacy compliance.

Agencies must perform regular self-assessment audits to verify that their privacy policy is accurate, comprehensive, prominently displayed, correctly implemented, communicated and accessible. Government agencies should work with third-party testing programs that will provide oversight to the agency's privacy program. An effective privacy monitoring program should include detailed reporting capabilities that scan online properties continuously and automatically throughout the year, enabling organizations to better mitigate risk and more easily identify, assign and track privacy issues for remediation.

For agencies with large Web sites, ongoing scanning for privacy issues is essential because Web pages are updated constantly, sometimes by different business units or managed by other groups within an agency that may not have communication with each other. Large government agencies can have millions of Web pages, making manual compliance impossible. Many serious privacy breaches have occurred through poor Web site standards. A privacy breach is a disaster for any privacy manager.

If not controlled properly, Web sites can provide a major privacy weak point that can have dire consequences for a government agency. Continuous Web monitoring for privacy issues provides an excellent illustration of due diligence on the part of an agency. By implementing an automated and ongoing privacy scanning solution, agencies will be able to mitigate risk and ensure compliant Web properties, while also assuring their Web site visitors and employees that they are taking the proper measures to ensure all personal information is kept secure and private. ■

Kurt A. Mueffelmann is President and Chief Executive Officer of HiSoftware (www.hisoftware.com). He can be reached at kam@hisoftware.com.

How to Avoid Appearing in The Washington Post

By Greg Alexander
EDS
US Government Solutions Office of Information Security

It's a Data Loss. Again.

Department of Data Reports That Any Employee Lost Data

By I.M. Awriter

Washingtonian Posted Staff Writer
Tuesday, December 26, 2006

WASHINGTON — The Department of Data reported today that one of its employees mistakenly gave away critical department personnel data as a "gift". In the spirit of the holidays, the employee (name withheld pending further investigation) decided to give away two department laptops that had been tagged as excess equipment to a local charity as fund raising prizes. As it turns out, the laptops had been marked as excess, but not yet processed for disposal and still contained the data on all 5,555 Department of Data employees including their employee numbers, social security numbers, home addresses and home telephone numbers, as well as data on citizens. Mr. Ostrich, Department spokesman, stated that the laptops were not encrypted and that there were specific policies in place on how to dispose of excess Department property, as well as how to ensure that computing devices are properly sanitized before disposal. In addition to Department data, one of the laptops also contained personal data on citizens. However, the department is not able to determine exactly how much citizen data has potentially been exposed by this breach. Mr. Ostrich said that there is an ongoing investigation and that he'll provide an update as soon as more information is garnered. No information was released on when and if any of the individuals affected by this loss will be notified.

Obviously, the above "article" is not real but the data breaches that we have been reading about in the papers are. According to the Congressional Committee on Government Reform, all 19 Departments and agencies reported at least one loss of personally identifiable information (PII) since January 2003.[1] The report goes on to state that the vast majority of the data breaches dealt with the physical loss of equipment – not hackers breaking into systems online. These problems are not just associated with government agencies; they also involve contractors and commercial businesses. A senior auditor at a large accounting firm left the office and placed his computer bag in the back of his pickup truck. On his way home, his wife called and asked him to stop at a convenience store to pick up some milk. He was in and out of the store in less than five minutes. However, this was plenty of time for his laptop computer to disappear. His laptop was not encrypted, and it contained audit records going back five years – data that contained both PII and Personal Health Information (PHI). In another case involving a large systems integrator, a senior consultant was asked to check his computer bag (including his laptop) in main storage since there was no room in the overhead storages bin on his short flight home. Being a helpful individual, the traveler agreed, and though he arrived at his destination, his laptop did not. In this case, the laptop was encrypted so the potential damage was limited.

In each of the above situations, there were more than adequate policies and procedures in place to help protect the data, and in one case there was also technical protection (encryption). However, what was missing was an understanding on the part of the employee of what his role was in protecting critical PII and PHI. None of these individuals intended anything malicious – but what they didn't do was think about what they were doing and the risks they were assuming.

So, how do you ensure that the next article in The Washington Post is not about your agency?

There are three major activities that have to be accomplished:

1. Know what data elements you own. This means you have to understand what data elements your systems are collecting, where the data is stored, and who has access to it and what they can do with it (i.e., download it to their laptop, print it out, etc.) Most Departments and

Continued on next page...

agencies have viable policies in place that address how data is to be controlled. What is lacking is validation on why the data is being collected and ensuring that employees understand what their roles are under these policies. In the case of the Veterans Affairs incident, there was a clear policy in place that PII was not to be taken home.

2. Ensure that the data is properly classified. Ensure that PII, PHI and other sensitive data are properly classified so that appropriate technology controls can be put in place to enhance its protection in case of loss, such as strong authentication for access and encryption for data at rest.

3. The most important activity is to ensure that you have a robust and effective security awareness training program.

What the above examples all have in common is the lack of effective security training. These employees were trying to do a good job and in a number of cases were actually going beyond requirements by taking work home with them so they could continue to work. What they didn't understand was the potential risk to both the Department and the data that they were accepting. This is where effective training comes in. In any information system, the weakest link is people – because we are unpredictable. To help mitigate this, organizations put in place management policies, operational procedures and technological controls. However, these controls are only as good as the training that goes with them. Employees want to do a good job, and they also want to do the right thing. Again, effective security training allows them to do both and increases the protection of critical and sensitive data.

In order for a training program to be effective, it needs to consist of two key pieces: training should be focused on the individual roles that employees have in the organization; and training needs to be ongoing. If the policy states sensitive data is not to be removed from the office, then this needs to be communicated to the employees. This communication must be more than just a 30 minute annual awareness training session – it needs to be continually reinforced. It is critical that the key role that end users play in protecting data is properly communicated. End users must understand both their role as well as their responsibility in protecting data. This means that the organization must provide the appropriate resources necessary to develop and execute training and to ensure that all employees actively participate. Given the right training at the right time, employees will respond and do the right thing. Without robust and effective security training programs, we will continue to learn about frightening and disconcerting security compromises from the news media. ■

Greg Alexander leads the EDS US Government Solutions Office of Information Security. For additional information contact greg.alexander@eds.com.

1 Staff Report: Agency Data Breaches Since January 1, 2003, Committee on Government Reform, October 13, 2006

Which Would You Rather Have: Privacy or Convenience?

Dr. Mahnaz Dean and Bonnie Glick
IBM Global Business Service

Would you rather have privacy or convenience? Why can't we have both? Technology provides us with more capabilities in broader areas. New technologies have allowed us to connect our information needs to those who will provide them – retailers, healthcare providers, financial institutions, etc. Information connections and dependencies are growing to the point that, for most people, there is no way back.

Do we have to give up one in order to have the other? Every individual and enterprise has a specifically tailored answer, and those answers are based neither on absolute privacy nor on absolute convenience, but rather levels of one balanced against levels of the other.

Privacy

How does one know when her or his privacy has been violated? What is an individual's expectation of privacy at home? In the workplace? In his or her healthcare maintenance?

How much of our information and personal data are we willing to share as a tradeoff for convenience in our day to day lives?

These are the questions that policymakers must wrestle with today and in the future. These are not easy questions to answer, and it will take privacy experts and, no doubt, many debates before the public reaches a consensus. Furthermore, an important issue that privacy experts must wrestle with is how to keep up with the "bad guys," people who hack into credit card databases and steal personal identities. Methods which these individuals and groups use to manipulate technology toward their ends seem endless. The resources that government and private security companies have at their disposal to meet these threats are limited, whereas the resources available to those who subvert the system seem limitless. In order to combat those who try to violate privacy limits, government and private security company experts need to be able to react nimbly and rapidly as the threats continually evolve.

Convenience

Technology has streamlined our lives in so many different ways – grocery delivery, book purchases, bank or credit card transactions, insurance quote comparisons, etc. The list goes on. Do individuals realize that, with each transaction they complete, they are giving up some amount of their privacy? Because our lives have become so dependent on having technology at our fingertips, we frequently ignore the fact that there are potential privacy compromises with each of our transactions. Each time a credit card or paypal transaction is made, an individual's financial accounts traverse the worldwide web. Do enterprises realize that with each transaction they become responsible for an individual's private data and for keeping it secure? Enterprises are fast becoming aware that they must be accountable for keeping individuals' data secure. Not doing so costs them money in the form of fines and lost business. Government entities are aware of the costs to them associated with data breaches in the form of Congressional inquiries, GAO reports, and potential firings.

Convenience, therefore, is something that we can no longer take for granted. There is a real cost associated with data breaches, on both sides of the breach.

The Tradeoff: Convenience for Privacy

For those of us who regularly use the Internet for such transactions, it is almost impossible to think of the "olden days" when bank transactions involved waiting in long lines or sending transactions through the mail. We can't imagine a world without instant gratification, because this is the world we have become accustomed to.

This begs the further question of "how much privacy do we really need in our lives to ensure that our identities cannot be stolen and that the government (or banks or ex-spouses, etc.) are not prying unnecessarily into our lives."

We all know or have heard of people (maybe even ourselves) who carried their Social Security cards with them or whose Social Security Numbers appeared on their driver's license. No one was concerned about privacy then, so what has changed? The answer: Because we are more connected. This connection makes it easier to draw a complete picture of who we are much faster or more completely than before, and it can result in more convenience to the "bad guys" than to the "good guys."

Intrusions into our privacy occur under various names: data breach,

Continued on next page...

identity theft, invasion of privacy, etc. Are these the unintended consequences of our network dependence in this more-than-ever connected world? Can one stop this trend? Or it is too late? The total number of records containing sensitive personal information involved in security breaches between February 2005 and early January 2007 (including the latest breach on January 2, 2007) reached 100,453,858 as reported by Privacy Rights Clearinghouse (www.privacyrights.org)[1].

Could the same capabilities and tools that make us more vulnerable also be used to protect us? It is accepted that technology brings convenience to consumers, providers, policy makers, implementers, users and holders of information. By using the right technologies and by setting up and enforcing appropriate policies, we can modify or transform organizations to meet the requirements of our new environment to be able to ensure privacy.

Giving up the convenience that the 21st century provides in favor of stringent privacy guidelines is not going to happen. However, there can be a balance between privacy and convenience. While it is not a hard and fast solution that will apply to every instance, the bottom line is that privacy must find a way to be present in our lives without being ever-present. By this we mean that privacy experts must find ways to ensure that individual and enterprise accounts are secured without the public being aware of that fact. The entire process must be part of a seamless transaction set with security and privacy operating in the background.

Information Overload

When weighing privacy vs. convenience, the answer is not "one size fits all." The use of technology led by governance policies to ensure that private data is not compromised is the key to keeping our identities secure and our data uncompromised. Successful organizations understand the benefit of IT and use this knowledge to bring value to people who use it.[2] Organizations that have implemented successful IT security standards offer guidelines to us for best practices and the collected wisdom can apply to many different types of organizations.

We have all read articles about protecting our identities. For as many articles as have been written, there are at least that many different ways individuals interpret their needs for information security. The best general advice for individuals is to be aware that data breaches occur and that personal data is just that, personal. It is up to each individual to share only as much data as they are willing to risk having breached in the future. We can trust secure Websites, but even they may have vulnerabilities. We trade off a certain amount of privacy for convenience, and the acceptable tradeoff will differ from person to person.

For enterprise control, the best advice is to ensure that IT governance policies are in place for internal audits and controls. Because of increased scrutiny and regulations worldwide, enterprises must incorporate new thinking on the importance of controls. The challenge may be to get management, IT, and audit to "speak the same language," while still respecting enterprise culture. Standardized processes, along with defined and documented change management processes, are basic minimal organizational standards. This is sometimes easier said than done, but it is a model that has been proven successful.[3] For enterprises, the Federal government has taken some of the gray areas out of the planning process with passage of the Sarbanes-Oxley (SOX) legislation. The business process of IT, including securing data, can improve by using internal controls for ongoing SOX compliance and other IT governance-related projects.

Whether you are exploring IT security issues as an individual or as an enterprise, the good news is that you are not alone. There are countless programs, policies, and possibilities out there for everyone to use. The problem lies more in determining what is the right fit than in finding a one-size-fits-all solution.

It is possible to have privacy and convenience, but you must wade through the many options and tradeoffs that are out there.

On the other hand, isn't it better to have too many options than not enough? ■

Bonnie Glick is a Project Executive for IBM Global Business Services. Mahnaz Dean is President of MazMaz IT Consulting. For additional information contact blglick@us.ibm.com or Mahnaz_Dean@comcast.net.

1 e-Week, The Enterprise Newsweekly, Vol. 23, No 50, December 18-25, 2006 – "UCLA didn't study for security test", by Victor Loh

2 ISACA, CoBIT Overview, www.isaca.org,

3 CoBIT and IT Governance Case Study: Harley Davidson, www.isaca.org.

Privacy (for You and Me) Is Dead.

By Dan Combs
Board Member and Work Group Chair
National Electronic Commerce Coordinating Council

Privacy seems like a good thing. I would like to have some. But I do not believe I have any privacy (this may be a slight overstatement), and there is relatively little I can do about it right now. As I anticipate e-mailing this article, I know that there will be a trail of commercial and governmental systems that log and track the content of my communication and to whom I am sending it. There could also be a government agency or two that, if I were interesting enough, might want to look at this information. Today I will be tracked and tallied by my cell phone, my instant messages and by walking, driving or clicking through various toll plazas and other public zones with cameras or other means of trailing me through both the physical and virtual worlds.

Privacy has never enjoyed robust health in this country. The term itself was not included in our Constitution. That group of very capable wordsmiths did not see fit to include the word privacy. The Constitutional "concept" of privacy was "discovered" a century later by a dedicated explorer:

"More than a century ago Supreme Court Justice Louis Brandeis, perhaps best known for his ardent defense of the 'right to be let alone,'" (from which much of our privacy legislation bloomed), "also argued that '[i]f the broad light of day could be let in upon men's actions, it would purify them as the sun disinfects.' He proposed a 'companion piece' to his influential Harvard Law Review article, 'The Right to Privacy,' on 'The Duty of Publicity.'" Fred H. Cate and Richard J. Varn, The Public Record: Information Privacy and Access—A New Framework for Finding the Balance (1999)

Even in what might be considered the heyday of privacy, it was strongly counter-balanced by the societal requirement for publicity. Recently, personal privacy has fared much worse than in the best of times.

What Happened to My Privacy?

We made a lot of small choices that had big unintended (?) consequences.

Collecting and storing our information became cheap and easy. Up to and including the early stages of the computer age, there were strong physical limitations to the amount of information that could be collected. Creating and collecting information on individuals was relatively costly compared to potential benefits. Capturing, storing and retrieving information in the "paper world" is a resource expensive process. Even in the early days of computer use, storage was costly and thus a strong limiting factor. Creating and collecting has been largely automated, and storage has become massively cheaper, so we collect and store everything including lots of new information about us.

The Internet. It used to be that, to transfer information, a physical file or piece of paper would be moved or a phone call made or a person-to-person conversation held. These are all relatively costly for moving big amounts of information. During the same time that storage became almost infinitely cheaper, this Internet "thing" was built. The Internet did for sharing or moving information similar things to what cheap storage and automation did for collecting and keeping it. The Internet made moving information massively cheaper, so we move it.

Commoditization of Personal Information. One kernel of corn or a soybean has very little value. Shiploads have large values. Loading ships with corn or beans and sending them off without markets in which to sell shiploads is a risky operation. Markets developed to facilitate buying and selling. Our personal information has been commoditized. It is traded and shared like the commodity it has become. Data is bought and sold like shiploads of corn and beans across the virtual world. Virtual commodities, such as our personal information, do not necessarily perform the same as physical commodities. Corn or beans, once consumed, cannot readily be used again as corn or beans. Consumption of information may actually lead to an increased market appetite for the same information, as the initial consumption leads to further ways of consuming the same data.

Criminals, Other Governments and Terrorists (COGT). Our individual information has value on a variety of levels. All of these COGTs have rapidly adapted to new opportunities in the information age. The physical barriers to crimes have been rendered largely irrelevant in the virtual world. We have thrown open the virtual gates and rolled out a welcome mat to COGTs around the Earth. Information events, criminal, tactical and strategic, changed from retail to wholesale. At a point not so long ago, accessing personal information involved opening a file drawer and pulling out paper. Now that information is a few mouse-clicks away, and those may be automated.

Law Makers and Executives. One of the best ways to ensure the

Continued on next page...

ineffectiveness and non-compliance with law is to over-legislate. We have lots of laws that make doing bad things with our information illegal. Oddly this patchwork of law can treat the theft of personal information differently depending upon the computer port from which the information emerges. Whether a particular information crime happens through an Ethernet cable, a wireless connection or a radio frequency transmitter can make a difference. This patchwork, often contradictory, makes compliance difficult or impossible.

Me and You, Us. We became loose and then profligate with our most intimate details. If we are asked if we think privacy is important, most of us answer an emphatic, "Yes!" Most of us will then gladly give out our personal information for a can of pork and beans at the grocery store or 50 cents off the price of a Happy Meal.

As a whole, we have never been very protective of our personal information. Jerry Springer (and others) taught us to force our most intimate details on our neighbors, even very distant ones. Once the world has seen you naked, how concerned are you likely to be about your Social Security Number? (Remember when we printed it on our checks and used it as our driver's license number?)

There may come a backlash from "guests" on "Girls Gone Wild" or other show all/tell all personally intrusive venues, when they realize the consequences of sharing all. I can imagine a certain discomfort with the question, "Mom/Dad, why are there pictures of you naked on the Internet?" We may reach a point where the weight of the results of stolen personal information serves as a catalyst to change. As technology to which we are subjected or processes in which we participate intrudes further into our lives, there may be other reactions. A lot of other evidence indicates we are pretty adaptable and will just accept it. Like the frog in the pot of water, as long as the water doesn't get too hot too fast, we will sit in the same spot until we boil. In the meantime, I do like to save on my hamburgers and fries. ■

Dan Combs, is a member of the Board and Work Group Chair of the National Electronic Commerce Coordinating Council, Program Director of the MIT Real ID Forum, and member of the Harvard Policy Group among several other affiliations. He can be reached at Dan.combs@globalidentitysolutions.com.

U.S. General Services Administration
Office of Citizen Services and
Communications
Intergovernmental Solutions Division

Official Business
Penalty for Private Use, $300